Силабус освітнього компонента
Програма навчальної дисципліни

Інтелектуальна власність систем безпеки

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
3

Мова викладання
Українська

Викладачі, розробники

ХВОСТЕНКО Владислав Сергійович
vladyslav.khvostenko@khpi.edu.ua
Кандидат економічних наук, доцент кафедри кібербезпека НТУ «ХПІ».

Автор понад 170 наукових і навчально-методичних праць (за даними Google Scholar, h-індекс – 12), у тому числі 3 монографій та навчального посібника з грифом.
Має у своєму доробку 10 патентів та 10 авторських свідоцтв.
Провідний лектор з дисциплін: «Інтелектуальна власність систем безпеки», «Правове регулювання кібербезпеки», «Авторське право у цифровому суспільстві».
Сфера наукових інтересів охоплює питання інтелектуальної власності, правового регулювання кіберпростору, інформаційної безпеки, криптографічних методів захисту, цифрові активи.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Дисципліна «Інтелектуальна власність систем безпеки» спрямована на формування у студентів знань про правову природу інтелектуальної власності, її місце та роль у розвитку сучасних технологій і систем безпеки. Курс охоплює основні інститути авторського права, патентного права, права на торговельні марки, промислові зразки, комерційну таємницю, а також суміжні права. Особлива увага приділяється міжнародним договорам та угодам у сфері інтелектуальної

власності (Бернська, Паризька конвенції, TRIPS, PCT, EPC), а також питанням гармонізації національного законодавства з європейськими стандартами.
У програмі курсу передбачено розгляд механізмів правової охорони об'єктів інтелектуальної власності у сфері інформаційних технологій і систем безпеки, включно з питаннями укладання договорів, передання прав, захисту від порушень, судового й адміністративного врегулювання спорів. Практична складова дисципліни включає аналіз судових рішень, кейсів порушення прав у цифровому середовищі, використання сучасних технічних інструментів моніторингу та захисту прав.
Вивчення курсу дозволяє здобувачам розуміти принципи функціонування системи інтелектуальної власності, орієнтуватися у національних і міжнародних правових актах, застосовувати знання для захисту прав у сфері інформаційної безпеки та кіберпросторі.

Мета та цілі дисципліни

Метою навчальної дисципліни є формування у студентів систему знань про правові засади охорони та захисту об'єктів інтелектуальної власності, а також виробити практичні навички їх застосування у сфері інформаційних технологій та систем безпеки, з урахуванням сучасних викликів цифрового суспільства та кіберпростору.
Основними завданнями вивчення дисципліни є:
Ознайомлення з основними категоріями, принципами та інститутами права інтелектуальної власності.
Розкриття правових механізмів охорони авторського права, патентного права, прав на знаки для товарів і послуг, промислові зразки, комерційну таємницю.
Формування розуміння міжнародних стандартів у сфері інтелектуальної власності (Бернська, Паризька конвенції, TRIPS, WIPO, DSM Directive, Digital Services Act).
Висвітлення особливостей захисту прав інтелектуальної власності в умовах цифровізації, глобалізації та розвитку систем кібербезпеки.
Розвиток здатності застосовувати набуті знання при аналізі практичних кейсів, судових рішень та реальних ситуацій порушення прав.
Сприяння формуванню практичних навичок підготовки правових документів (ліцензійних угод, договорів про передачу прав, скарг про порушення в Інтернеті).

Формат занять

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

Компетентності

ЗК1. Здатність реалізувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
ЗК6. Здатність до пошуку, оброблення та аналізу інформації з різних джерел.
ЗК7. Здатність використовувати інформаційні та комунікаційні технології та формувати систему інформаційно-аналітичного забезпечення підтримки прийняття управлінських рішень щодо системи управління інформаційною безпекою.
СК4. Здатність прогнозувати реалізації управлінських рішень щодо захисту інформації.
СК10. Здатність забезпечувати неперервність бізнесу згідно з встановленою політикою інформаційної безпеки.

Результати навчання

РН1. Вміти реалізовувати свої права і обов'язки як члена суспільства, усвідомлювати цінності громадянського суспільства (вільного демократичного) та необхідність його сталого (безпечного) розвитку, верховенства права, прав і свобод людини і громадянина в Україні.
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.

РН6. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної безпеки
РН7. Вміти розробляти комплекс організаційних заходів щодо формування системи управління інформаційною безпекою.
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.
РН14. Вміти вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів та користувачів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
РН17. Вміти розв'язувати задачі управління інфораційною 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.
РН19. Вміти впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформації в інформаційно-мунікаційних системах.
РН20. Вміти аналізувати та проводити оцінку ефективності та рівня захищеності інформаційних ресурсів в інформаційно-комунікаційних системах згідно встановленої політики інформаційної безпеки.
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 заняття – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Для успішного проходження курсу необхідно мати знання та практичні навички з дисципліни Правознавство – розуміння основних принципів права, структури та функціонування правової системи, базових положень цивільного і господарського права.
Інтелектуальна власність – знання правового режиму об'єктів авторського права, патентного права, торговельних марок, промислових зразків, комерційної таємниці.
Основи кібербезпеки – початкові уявлення про інформаційні загрози, принципи побудови систем захисту інформації, інструменти забезпечення конфіденційності, цілісності та доступності даних.
Інформаційні технології – базові знання щодо роботи комп'ютерних систем, мереж, програмного забезпечення та цифрових платформ як середовища існування об'єктів інтелектуальної власності.

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. використання онлайн-ресурсів (WIPO, GDPR portal, реєстри судових рішень.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин

Тема 1. Інтелектуальна власність у системах безпеки Правова природа інтелектуальної власності. Об'єкти і суб'єкти ІВ у сфері безпеки. Роль інтелектуальної власності в інформаційній та національній безпеці.	2
Тема 2. Авторське право у цифрових системах безпеки. Охорона програмного забезпечення, баз даних, цифрових платформ. Виклики онлайн-піратства й нелегального використання контенту в інформаційних системах.	2
Тема 3. Передача і захист авторських та суміжних прав у сфері кібербезпеки. Ліцензії, договори та колективне управління правами у сфері ІТ. Судова та адміністративна практика захисту прав в Інтернеті. Використання цифрових доказів.	2
Тема 4. Патентне право і технології безпеки Охорона винаходів, корисних моделей і промислових зразків у сфері безпеки та ІТ. Патентні стратегії для захисту технологій кіберзахисту.	2
Тема 5. Торговельні марки та комерційна таємниця у системах безпеки Засоби індивідуалізації (бренди, доменні імена) в ІТ та кібербезпеці. Захист комерційної таємниці, інформації з обмеженим доступом і ноу-хау у цифрових середовищах.	2
Тема 6. . Міжнародно-правові стандарти у сфері ІВ та безпеки Бернська та Паризька конвенції, TRIPS, WIPO Internet Treaties. Європейські регламенти (DSM Directive, Digital Services Act, GDPR) як частина системи кібербезпеки.	2
Тема 7 Цифрові інструменти захисту прав інтелектуальної власності. DRM, цифрові підписи, водяні знаки, blockchain-рішення, системи виявлення плагіату. Використання forensic-інструментів у доказуванні порушень прав ІВ.	2
Тема 8. Інтелектуальна власність і сучасні виклики безпеки. Штучний інтелект та авторське право. Кіберзлочини, пов'язані з порушенням ІВ. Ризики для критичної інфраструктури. Тенденції інтеграції права ІВ і систем кіберзахисту.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти *a*
Тема 1. Аналіз інформаційних правовідносин у кіберпросторі. Визначення суб'єктів і об'єктів інформаційних правовідносин. Аналіз законодавчих норм (Закон України «Про інформацію», GDPR, DMCA). Розбір судових кейсів (Google Spain, Viacom v. YouTube).	4	1
Тема 2. Пошук об'єктів інтелектуальної власності у відкритих базах даних. Робота з національними та міжнародними реєстрами (Укрпатент, WIPO, EUIPO, USPTO). Перевірка торговельних марок, патентів, авторських прав. Формування пошукового звіту.	4	1
Тема 3. Складання заявки на об'єкт авторського права у сфері безпеки.	4	1

Підготовка заяви на реєстрацію програмного забезпечення чи бази даних. Формулювання опису об'єкта. Заповнення типової форми заявки.		
Тема 4. Пошук аналогів та визначення новизни об'єкта ІВ. Аналіз баз даних WIPO, Espacenet, Google Patents. Порівняння знайдених рішень із заявленим об'єктом. Визначення рівня техніки та критеріїв новизни.	4	1
Тема 5. Складання заявки на патент (корисна модель / винахід) у сфері ІТ-безпеки. Опис винаходу (сфера застосування, рівень техніки, відмінні ознаки). Формулювання формули корисної моделі. Використання прикладів з практики.	4	1
Тема 6. Ліцензійні договори та open source ліцензії. Порівняльний аналіз MIT, GPL, Creative Commons. Розробка проєкту ліцензійного договору для програмного продукту з кіберзахисту.	4	1
Тема 7. Реєстрація авторського права на програмне забезпечення чи базу даних. Ознайомлення з процедурою подання заявки в Україні. Формування опису твору, прикладу вихідного коду чи структури бази. Підготовка комплекту документів (заява, додатки, копії матеріалів).	4	1
Тема 8. Складання заявки на промисловий зразок. Аналіз охороноздатності інтерфейсу мобільного чи веб-застосунку як промислового зразка. Підготовка матеріалів заявки: графічні зображення інтерфейсу, опис, перелік класів за Локарнською класифікацією. Формування пакету документів для подання в Укрпатент.	4	1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Правовий режим програмного забезпечення для безпеки. Авторське право на системи шифрування, програмні комплекси захисту. Ліцензування і правові ризики використання уразливого або піратського ПЗ.	0,5
Тема 2. Патентування інновацій у сфері безпеки. Винаходи і корисні моделі в галузі криптографії, біометричних систем, засобів захисту даних. Критерії охороноздатності. Пошук аналогів у міжнародних базах (Espacenet, WIPO). Приклади патентних спорів у сфері ІТ-безпеки.	0,5
Тема 3. Промислові зразки та торговельні марки у цифровому середовищі. Правова охорона дизайну інтерфейсів, візуальних елементів застосунків і програм. Реєстрація торговельних марок у сфері кіберзахисту (назви, логотипи, доменні імена). Судова практика щодо кіберсквотингу та неправомірного використання брендів.	1
Загалом	$\sum_{i=1}^{m} b_i = 2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Міжнародні договори у сфері ІВ (Бернська, Паризька конвенції, TRIPS) та їх значення для безпекових технологій. Основні міжнародні угоди у сфері охорони ІВ. Їх значення для розробки та захисту технологій у сфері безпеки. Вплив на національне законодавство України.	8
Тема 2. Особливості правової охорони програмного забезпечення систем захисту інформації. Програмне забезпечення як об'єкт авторського права. Особливості охорони програм у сфері кібербезпеки. Практика захисту прав розробників.	8
Тема 3. Бази даних як об'єкт авторського права та їх роль у системах кіберзахисту. Поняття бази даних у праві. Критерії охороноздатності. Використання баз даних у системах безпеки та практичні приклади їх правової охорони.	7
Тема 4. Правове регулювання криптографічних технологій і патентування алгоритмів. Поняття криптографічних технологій. Міжнародні та національні підходи до їх регулювання. Дискусії щодо патентування алгоритмів.	7
Тема 5. Технічні засоби захисту авторських прав. DRM (Digital Rights Management). Цифрові підписи. Водяні знаки. Blockchain-технології у сфері авторського права.	7
Тема 6. Правові аспекти використання штучного інтелекту в системах безпеки. Використання ШІ для виявлення загроз. Правовий статус алгоритмів і рішень, створених ШІ. Відповідальність за шкоду від використання таких систем.	7
Тема 7. Право на інформацію та його обмеження: співвідношення з національною безпекою. Правовий статус комерційної таємниці та ноу-хау. Приклади їх використання у сфері IT-безпеки. Судова практика щодо порушення цих прав.	7
Тема 8. Комерційна таємниця і ноу-хау у сфері IT-безпеки: практичні кейси. Кримінально-правова кваліфікація. Незаконне відтворення та розповсюдження творів. Онлайн-піратство. Використання шкідливого ПЗ для обходу DRM. Статистика кіберзлочинів у сфері інтелектуальної власності.	7
Тема 9. Авторське право і кібербезпека цифрових платформ. Відповідальність провайдерів та платформ за порушення авторських прав. Регламенти ЄС (DSA, DMA). Політики YouTube, TikTok, Meta. Технології виявлення нелегального контенту.	7
Тема 10. Виклики захисту прав ІВ у блокчейн-технологіях та smart contracts. Короткий зміст: Особливості блокчейну як децентралізованої системи. Проблеми охорони авторських прав і патентів у середовищі blockchain.	7

Юридичні аспекти смарт-контрактів.	
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

1. WIPO Academy – Copyright and Related Rights (DL-201)
https://www.wipo.int/academy/en/courses/distance-learning
2 Coursera – Copyright for Educators and Librarians (University of Michigan)
https://www.coursera.org/learn/copyright-for-education
3 edX – Intellectual Property Law and Policy: Part 1 (University of Pennsylvania)
https://www.edx.org/course/intellectual-property-law-and-policy-part-1
4 FutureLearn – General Data Protection Regulation (GDPR) Training
https://www.futurelearn.com/courses/general-data-protection-regulation
5 Prometheus – Захист персональних даних в Україні
https://prometheus.org.ua
6 WIPO Academy – Advanced Course on Copyright in the Digital Environment (DL-511)
https://www.wipo.int/academy/en/courses/distance-learning
7 Udemy – Copyright, Trademark and Intellectual Property Law
https://www.udemy.com/course/copyright-trademark-and-intellectual-property-law

Література, навчальні матеріали та інформаційні ресурси

Основна література

1 Про авторське право і суміжні права: Закон України від 15 квітня 2023 р. № 2811-IX.
URL: https://zakon.rada.gov.ua/laws/show/2811-20#n855
2 Цивільний кодекс України: Кодекс України від 16.01.2003 №435-IV.
URL: https://ips.ligazakon.net/document/T030435
3 Бернська конвенція про охорону літературних і художніх творів від 24.07.1971 р. Bernska konventsiia pro okhoronu literaturnykh i khudozhnikh tvoriv vid 24.07.1971 r.
URL: https://zakon.rada.gov.ua/laws/show/995_051#Text
4 WIPO Copyright Treaty (WCT), WIPO Performances and Phonograms Treaty (WPPT).
5 Directive (EU) 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSoc Directive).
6 Directive (EU) 2019/790 on copyright and related rights in the Digital Single Market (DSM Directive).
7 Gervais, D. The TRIPS Agreement: Drafting History and Analysis. – London: Sweet & Maxwell, 2020.
8 Hugenholtz, P. B. Copyright in the Digital Age. – Amsterdam: IViR, 2018.
9 Сопільник Л. В. Право інтелектуальної власності: авторське право і суміжні права : навч. посіб. – Львів : ЛьвДУВС, 2021.
10 Войціховський А. Цифрові права в Україні: авторське право у мережі. – Київ : Юстініан, 2020.

Додаткова література

8. Андрощук Г., Хвостенко В. Цифрові інструменти визначення відомості об'єкту інтелектуальної власності (на прикладі персонажу і твору) // Інформація і право. – 2024. – № 3 (50). – С. 54–64. http://il.ippi.org.ua/article/view/311635

9. Воліков В., Хвостенко В. Визначення відомості твору з застосуванням цифрових інструментів маркетингу // Вплив інновацій на розвиток судової експертизи: від традиційних методів до цифрової трансформації : матеріали міжнар. наук.-практ. конф. – Львів : ЛНДІСЕ, 2024. – С. 30–35. https://ndekc.lviv.ua/pdf/19062024.pdf
10. Липко О., Хвостенко В. Порушення прав інтелектуальної власності при здійсненні інтернет-реклами // Інтелектуальна власність в Україні. – 2017. – № 12. – С. 58-64. https://intelvlas.com.ua/last?page=2
11. hvostenko, V. S., Kipa, M. A., & Aleksieienko, I. I. (2019). ФІНАНСОВО-КОМЕРЦІЙНИЙ АСПЕКТ ПРОЦЕСУ ПЕРЕДАЧІ ТЕХНОЛОГІЙ. Financial and Credit Activity Problems of Theory and Practice, 1(28), 430–440. https://doi.org/10.18371/fcaptp.v1i28.163934
12. Волков В.В., Хвостенко В.С. Практика застосування штучного інтелекту при проведенні експертизи торговельних марок // Збірник наукових праць НМетАУ. – 2025. – С. 298-305. https://nmetau.edu.ua/file/2025_zbirnik_naukovih_prats_konf_udunt_red._ibv_ostatochna_versiya.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:

$$О = П \cdot k_1 + К \cdot k_2 + І \cdot k_3 + Пк \cdot k_4$$

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** Роман КОРОЛЬОВ