Силабус освітнього компонента
Програма навчальної дисципліни

Інтелектуальна власність систем безпеки

Шифр та назва спеціальності
125 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Освітня програма
Кібербезпека

Кафедра
Кібербезпеки (328)

Рівень освіти
Бакалаврі

Тип дисципліни
Профільна, Вибіркова

Семестр
3

Мова викладання
Українська

Викладачі, розробники

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

Автор більше 30 публікацій: з них 3 монографії у співавторстві 1 посібник з грифом. Провідний лектор з дисциплін: «Інтелектуальна власність систем безпеки», «Правове регулювання кібербезпеки».
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Інтелектуальна власність систем безпеки" є вибірковою навчальною дисципліною. Вивчення дисципліни спрямовано на набуття студентами універсальних професійних компетентностей з використання об’єктів інтелектуальної власності в діяльності підприємства.

Мета та цілі дисципліни

Освоєння необхідних знань системи інтелектуальної та промислової власності у винахідницькій та патентно-ліцензійної діяльності, методологічних основ створення об’єктів промислової власності та інженерної психології, захисту патентних прав, міжнародного співробітництва у сфері інтелектуальної власності, авторського права і суміжних прав, а також системи патентної інформації; вміння використовувати на практиці нормативно-правові акти при забезпеченні правової охорони науково-технічних досягнень і творчої продукції, провести патентно-інформаційні дослідження в певній галузі техніки, знайти аналоги і оформити заявку на об’єкт промислової власності.

Формат занять

Лекції, лабораторні роботи, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

КЗ–2. Знання та розуміння предметної області та розуміння професії.
КЗ–5. Здатність до пошуку, оброблення та аналізу інформації.
КЗ 8. Здатність ухвалювати рішення та діяти, дотримуючись принципу неприпустимості корупції та будь яких інших проявів недоброчесності.
КФ 2. Здатність до використання інформаційно-комунікаційних технологій, сучасних методів і моделей інформаційної безпеки та/або кібербезпеки.
КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.
КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.
КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.
КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Результати навчання

РН–1. Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації;
РН–2. організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність;
РН–3. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.
РН–4. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН–5. Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.
РН–6. Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.
РН–7. Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.
РН–8. Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.
РН–9. Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.
РН–10. Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.
РН–11. Виконувати аналіз зв'язків між інформаційними процесами на віддалених обчислювальних системах.
РН–12. Розробляти моделі загроз та порушника.
РН–13. Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.
РН–14. Вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.
РН–15. Використовувати сучасне програмно-апаратне забезпечення інформаційно-комунікаційних технологій.
РН–16. Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.
РН–17. Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних

інформаційних ресурсів з відображенням взаємозв'язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.
РН–18. Використовувати програмні та програмно-апаратні комплекси захисту інформаційних ресурсів.
РН–19. Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.
РН–20. Забезпечувати функціонування спеціального програмного забезпечення, щодо захисту інформації від руйнуючих програмних впливів, руйнуючих кодів в інформаційно-телекомунікаційних системах.
РН–21. Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН–22. Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН–23. Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.
РН–24. Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).
РН–25. Забезпечувати введення підзвітності системи управління доступом до електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.
РН–26. Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.
РН–27. Вирішувати задачі захисту потоків даних в інформаційних, інформаційно-телекомунікаційних (автоматизованих) системах.
РН–28. Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.
РН–29. Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.
РН–30. Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.
РН–31. Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.
РН–32. Вирішувати задачі управління процесами відновлення штатного функціонування інформаційно-телекомунікаційних систем з використанням процедур резервування згідно встановленої політики безпеки.
РН–33. Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.
РН–34. Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.
РН–35. Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.
РН–36. Виявляти небезпечні сигнали технічних засобів.
РН–37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.

РН–38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
РН–39. Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
РН–40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
РН–41. Забезпечувати неперервність процесу ведення журналів реєстрації подій та інцидентів на основі автоматизованих процедур.
РН–42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.
РН–43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.
РН–44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.
РН–45. Застосовувати ріні класи політик інформаційної безпеки та/ або кібербезпеки, що базуються на ризик-орієнтованому контролі доступу до інформаційних активів.
РН–46. Здійснювати аналіз та мінімізацію ризиків обробки інформації в інформаційно-телекомунікаційних системах.
РН–47. Вирішувати задачі захисту інформації, що обробляється в інформаційно-телекомунікаційних системах з використанням сучасних методів та засобів криптографічного захисту інформації.
РН–48. Виконувати впровадження та підтримку систем виявлення вторгнень та використовувати компоненти криптографічного захисту для забезпечення необхідного рівня захищеності інформації в інформаційно-телекомунікаційних системах.
РН–49. Забезпечувати належне функціонування системи моніторингу інформаційних ресурсів і процесів в інформаційно-телекомунікаційних системах.
РН–50. Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
РН–51. Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.
РН–52. Використовувати інструментарій для моніторингу процесів в інформаційно-телекомунікаційних системах.
РН–53. Вирішувати задачі аналізу програмного коду на наявність можливих загроз.
РН–54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 32 год., практичні роботи – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Правознавство.

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

Теми лекційних занять

Тема 1. Поняття інтелектуальної власності та система її правової охорони.
Завдання навчальної дисципліни. Структура та зміст дисципліни, її зв'язок з іншими дисциплінами. Поняття інтелектуальної діяльності та її результату. Функції цивільного права щодо охорони та використання результатів інтелектуальної діяльності та прирівняних до них засобів індивідуалізації. Відображення в загальних нормах цивільного права особливостей інтелектуальної діяльності та її результатів. Спеціальні інститути цивільного права, що опосередковують інтелектуальну діяльність та її результати. Взаємозв'язок спеціальних інститутів цивільного права, що опосередковують інтелектуальну діяльність та її результати.
Тема 2. Юридична природа права інтелектуальної власності.
Поняття інтелектуальної власності, співвідношення права інтелектуальної власності та права власності. Юридична природа інтелектуальної власності. Правова охорона інтелектуальної власності. Об'єкти права інтелектуальної власності. Суб'єкти права інтелектуальної власності. Інтелектуальна власність і зобов'язальне право. Поняття володіння та користування.
Тема 3. Основні інститути права інтелектуальної власності.
Загальні положення. Авторське право та суміжні права. Патенти та споріднені поняття. Засоби індивідуалізації товарів і послуг. Нетрадиційні результати інтелектуальної діяльності.
Тема 4. Поняття й ознаки об'єкта авторського права.
Поняття об'єкта авторського права. Ознаки об'єкта авторського права. Цінність твору. Правове значення окремих елементів твору. Твори, що є об'єктами авторського права. Твори, які не є об'єктами авторського права.
Тема 5. Суб'єкти авторського права. Права авторів.
Первинні та похідні суб'єкти авторського права. Суб'єкти авторських прав за законом і договором. Вітчизняні й іноземні громадяни як суб'єкти авторських прав. Автори твору. Виникнення авторських прав у творця твору. Перекладачі як суб'єкти авторського права. Співавторство. Інші суб'єкти авторського права. Права авторів. Особисті немайнові права авторів. Майнові права авторів. Строк дії авторського права.
Тема 6. Передання майнових авторських прав.
Розпорядження майновими авторськими правами. Авторський договір. Суміжні права. Права виконавця. Колективне управління авторським правом і суміжними правами. Механізм створення, функції й обов'язки організацій колективного управління правами.
Тема 7. Захист авторських і суміжних прав.
Порушення авторських та суміжних прав. Юрисдикційна форма захисту авторських і суміжних прав. Способи цивільно-правового захисту авторських і суміжних прав. Адміністративна та кримінальна відповідальність за порушення авторських і суміжних прав.
Тема 8. Загальні поняття про право та його системи. Поняття, предмет і принципи патентного права.
Загальні поняття про право та його систему. Предмет та принципи патентного права.
Тема 9. Система джерел патентного права та його зв'язок з цивільним, адміністративним, господарським і кримінальним правом.
Система джерел патентного права. Багатосторонні міжнародні договори у сфері промислової власності, учасницею яких є Україна. Двосторонні міжнародні договори України про співробітництво у сфері охорони промислової власності. Перелік нормативних актів України у сфері охорони прав інтелектуальної власності. Патентне право і його зв'язок з цивільним, адміністративним, господарським і кримінальним правом.
Тема 10. Об'єкти патентного права.
Об'єкти винаходу (корисної моделі). Поняття і ознаки винаходу (корисної моделі). Новизна, поняття рівня техніки, пріоритет і порядок його встановлення, пільга по новизні, винахідницький рівень, промислова придатність. Основні вимоги до об'єктів патентного права.
Тема 11. Суб'єкти патентного права.
Автори винаходів, корисних моделей, промислових зразків. Права та обов'язки патентовласників. Службові винаходи. Права та обов'язки спадкоємців. Мета, структура і задачі патентного відомства в Україні. Представники у справах інтелектуальної власності (патентні повірені).
Тема 12. Охорона прав на об'єкти промислової власності. Способи захисту прав.

Патент як форма охорони об’єктів промислової власності. Зміст патентних прав. Способи захисту патентних прав на винахід (корисну модель, промисловий зразок).
Тема 13. Міжнародна система охорони об’єктів промислової власності.
Основні завдання та принципи Всесвітньої організації інтелектуальної власності. Договори, що забезпечують охорону промислової власності. Паризька конвенція з охорони промислової власності. Основні принципи. Вашингтонський договір про інтелектуальну власність стосовно інтегральних мікросхем. Договір про закони щодо товарних знаків. Угоди, які полегшують отримання охорони промислової власності в кількох державах та стверджують міжнародні класифікації.
Тема 14. Оформлення патентних прав в іноземних державах.
Оформлення патентних прав в Україні. Оформлення патентних прав в іноземних державах. Патентування винаходів відповідно до вимог різних патентних конвенцій. Патентування винаходів відповідно до вимог договору про патентну кооперацію (PCT). Патентування винаходів відповідно до вимог європейської патентної конвенції (ЄПК). Патентування винаходів відповідно до вимог євразійської патентної конвенції (ЕАПК).

Теми практичних занять

Тема 1. Правила складання і подання заявки на винахід та заявки на корисну модель.
Тема 2. Реквізити поточних рахунків закладу експертизи – ДП «Укрпатент», на які сплачуються збори за дії пов’язані з охороною прав на об’єкти інтелектуальної власності.
Тема 3. Здійснення пошуку нормативно-правових актів, що підтверджують права інтелектуальної власності. Програма для ЕОМ - особливий об'єкт авторського права.
Тема 4. Здійснення пошуку нормативно-правових актів, що підтверджують права інтелектуальної власності. Введення програм в господарський обіг.
Тема 5. Засоби індивідуалізації.

Теми лабораторних робіт

Лабораторні роботи в рамках дисципліни не передбачені.

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. Сайт Світової організації інтелектуальної власності (WIPO)
https://www.wipo.int/portal/en/index.html
2. Державне підприємство «Інститут інтелектуальної власності» // [Електронний ресурс]. Режим доступу: https://ukrpatent.org/uk
3. Попова Л.М. Інтелектуальна власність : підручник / Л.М. Попова., А.В. Хромов, І.В. Шуба: Харків, «Федорко», 2021, с. 262.
https://fpk.in.ua/images/biblioteka/3bac_pravo/Book_2021_Popova_Intelektualna_vlasnist.pdf
4. Про авторське право і суміжні права: Закон України редакція від 15 квітня 2023 р. № 2811-IX.

https://zakon.rada.gov.ua/laws/show/2811-20#n855
5. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
6. 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.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
7. 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.
https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Додаткова література

8. Про внесення змін до деяких законодавчих актів України щодо посилення захисту прав інтелектуальної власності: Закон України редакція від 20 березня 2023 р. № 2974-IX.
https://zakon.rada.gov.ua/laws/show/2974-20#Text
9. Про охорону прав на винаходи і корисні моделі: Закон України редакція від 31 грудня 2023 р. № 3687-XII.
https://zakon.rada.gov.ua/laws/show/3687-12#Text

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:
•практичні роботи: 40% семестрової оцінки;
•самостійна робота: 10% семестрової оцінки;
•контрольна робота: 10% 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 Сергій ЄВСЕЄВ