



Силабус освітнього компонента

Програма навчальної дисципліни



Авторське право у цифровому суспільстві

Шифр та назва спеціальності

125 – Кібербезпека та захист інформації

Інститут

ННІ Комп'ютерних наук та інформаційних технологій

Освітня програма

Освітньо-наукова програма Кібербезпека

Кафедра

Кібербезпеки

Рівень освіти

Магістр

Тип дисципліни

Наукова підготовка, Обов'язкова

Семестр

1

Мова викладання

Українська

Викладачі, розробники



ХВОСТЕНКО Владислав Сергійович

vladyslav.khvostenko@khpі.edu.ua

Кандидат економічних наук, доцент кафедри кібербезпеки 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 «Авторське право у цифровому суспільстві» є вибірковою навчальною дисципліною правового спрямування. Зміст дисципліни охоплює питання сутності поняття авторського права, його об'єктів і суб'єктів, набуття та необхідності, значення, методів та форм його охорони і захисту, майнових і немайнових прав автора, їх особливостей у цифровому суспільстві. Оволодіння знаннями із зазначених питань дає можливість майбутнім фахівцям орієнтуватись у проблемах інтелектуальної власності в частині авторського права, що особливо актуально в умовах сучасних процесів загострення конкуренції у ринковому середовищі та його цифровизації.

Мета та цілі дисципліни

Освоєння необхідних знань авторського права, методологічних основ створення та розпорядження авторськими правами, захисту та охорони авторських прав, міжнародного співробітництва у сфері авторського права і суміжних прав, вміння використовувати на практиці нормативно-правові акти при що регулюють авторське право у тому числі в цифровому середовищі.

Формат занять

Лекції, практичні заняття, індивідуальне завдання, самостійна робота, консультації. Підсумковий контроль – залік.

Компетентності

- КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
КЗ-2. Здатність проводити дослідження на відповідному рівні.
КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
КФ4. Здатність аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації, формувати стратегію і політики інформаційної безпеки з урахуванням вітчизняних і міжнародних стандартів та вимог.
КФ5. Здатність до дослідження, системного аналізу та забезпечення безперервності бізнес/операційних процесів з метою визначення вразливостей інформаційних систем та ресурсів, аналізу ризиків та визначення оцінки їх впливу у відповідності до встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ6. Здатність аналізувати, контролювати та забезпечувати систему управління доступом до інформаційних ресурсів згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
КФ9. Здатність аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів в галузі інформаційної безпеки та/або кібербезпеки організації в цілому.
КФ10. Здатність провадити науково-педагогічну діяльність, планувати навчання, контролювати і супроводжувати роботу з персоналом, а також приймати ефективні рішення з питань інформаційної безпеки та/або кібербезпеки.

Результати навчання

- РН1. Вільно спілкуватись державною та іноземною мовами, усно і письмово для представлення і обговорення результатів досліджень та інновацій, забезпечення бізнес/операційних процесів та питань професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
РН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
РН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
РН5. Критично осмислювати проблеми інформаційної безпеки та/або кібербезпеки, у тому числі на міжгалузевому та міждисциплінарному рівні, зокрема на основі розуміння нових результатів інженерних і фізико-математичних наук, а також розвитку технологій створення та використання спеціалізованого програмного забезпечення.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
РН7. Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв'язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки.
РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

- РН9. Аналізувати, розробляти і супроводжувати систему управління інформаційною безпекою та/або кібербезпекою організації на базі стратегії і політики інформаційної безпеки.
- РН10. Забезпечувати безперервність бізнес/операційних процесів, а також виявляти уразливості інформаційних систем та ресурсів, аналізувати та оцінювати ризики для інформаційної безпеки та/або кібербезпеки організації.
- РН11. Аналізувати, контролювати та забезпечувати ефективне функціонування системи управління доступом до інформаційних ресурсів відповідно до встановлених стратегії і політики інформаційної безпеки та/або кібербезпеки організації.
- РН12. Досліджувати, розробляти та впроваджувати методи і заходи протидії кіберінцидентам, здійснювати процедури управління, контролю та розслідування, а також надавати рекомендації щодо попередження та аналізу кіберінцидентів в цілому.
- РН13. Досліджувати, розробляти, впроваджувати та використовувати методи та засоби криптографічного та технічного захисту інформації бізнес/операційних процесів, а також аналізувати і надавати оцінку ефективності їх використання в інформаційних системах, на об'єктах інформаційної діяльності та критичної інфраструктури.
- РН14. Аналізувати, розробляти і супроводжувати систему аудиту та моніторингу ефективності функціонування інформаційних систем і технологій, бізнес/операційних процесів у сфері інформаційної та/або кібербезпеки в цілому.
- РН15. Зрозуміло і недвозначно доносити власні висновки з проблем інформаційної безпеки та/або кібербезпеки, а також знання та пояснення, що їх обґрунтовують до персоналу, партнерів та інших осіб.
- РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень.
- РН17. Мати навички автономного і самостійного навчання у сфері інформаційної безпеки та/або кібербезпеки і дотичних галузей знань, аналізувати власні освітні потреби та об'єктивно оцінювати результати навчання.
- РН18. Планувати навчання, а також супроводжувати та контролювати роботу з персоналом у напрямку інформаційної безпеки та/або кібербезпеки.
- РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності.
- РН20. Ставити та вирішувати складні інженерно-прикладні та наукові задачі інформаційної безпеки та/або кібербезпеки з урахуванням вимог вітчизняних та світових стандартів та кращих практик.
- РН21. Використовувати методи натурного, фізичного і комп'ютерного моделювання для дослідження процесів, які стосуються інформаційної безпеки та/або кібербезпеки.
- РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки.
- РН23. Обґрунтовувати вибір програмного забезпечення, устаткування та інструментів, інженерних технологій і процесів, а також обмежень щодо них в галузі інформаційної безпеки та/або кібербезпеки на основі сучасних знань у суміжних галузях, наукової, технічної та довідкової літератури та іншої доступної інформації.
- РН24. Планувати та виконувати наукові та прикладні дослідження у сфері інформаційної безпеки та/або кібербезпеки із застосуванням сучасних технологій, експериментальних і теоретичних методів і моделей теорії прийняття рішень, системного аналізу, оптимізації процесів, математичної статистики.
- РН25. Оцінювати ефективність та практичну цінність результатів наукових і практичних досліджень та інновацій.

Обсяг дисципліни

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

Передумови вивчення дисципліни (пререквізити)

Для успішного проходження курсу необхідно мати знання та практичні навички з дисципліни «Інтелектуальна власність».

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. Сутність та поняття авторського права.

Поняття та предмет авторського права. Структура авторського права. Принципи авторського права. Історія виникнення та розвитку авторського права у світі. Джерела авторського права. Закон України “Про авторське право і суміжні права” - його зміст і значення. Правовідносини у сфері авторського права.

Тема 2. Об’єкти та суб’єкти авторського права.

Загальна характеристика об’єктів авторського права. Основні види об’єктів авторського права. Суб’єкти авторського права. Фізичні особи як суб’єкти авторського права. Співавтори як суб’єкти авторського права. Колективне авторство як продуктивна форма створення ОПІВ. Юридичний аспект колективного авторства. Особливості охоронних документів та процедури їх одержання.

Тема 3. Договори розпорядження авторським правом.

Поняття та види авторського договору. Відмежування авторського договору від інших видів договорів. Порядок укладання авторського договору. Зміст авторського договору. Відповідальність за невиконання авторського договору. Зміна та припинення авторського договору.

Тема 4. Міжнародне та національне законодавство про охорону авторського права у цифровому середовищі.

Міжнародно-правова охорона авторських і суміжних прав у цифровому середовищі. Авторсько-правова охорона на твори в ІТ-сфері в Україні. Особливості розповсюдження та використання об’єктів авторського і суміжних прав у цифровому середовищі.

Тема 5. Технічні засоби захисту авторських прав.

Технічні засоби захисту авторських і суміжних прав. Порушення авторських прав у цифровій сфері.

Тема 6. Ліцензії: поняття, види, правова природа.

Вільні публічні ліцензії. Ліцензії creative commons: поняття, види, правова природа.

Тема 7. Авторське право в ІТ.

Авторсько-правова охорона на твори в ІТ-сфері в Україні. Особливості розповсюдження та використання об’єктів авторського і суміжних прав у цифровому середовищі.

Тема 8. Захист авторських прав в Інтернеті.

Проблеми із захистом інтелектуальної власності на web-сайтах. Ситуація з крадіжками та плагіатом в мережі Інтернет як віддзеркалення загальної правової ситуації в суспільстві. Порушник права інтелектуальної власності в мережі Інтернет. Правові аспекти вміщення твору на вітрині Інтернету.

Теми практичних занять

Тема 1. Дослідження юридичної природи авторського права.

Тема 2. Складання заявки на авторське право.

Тема 3. Розробка договору відчуження авторського права.

Тема 4. Розробка договору співавторства.

Тема 5. Розробка ліцензії на цифрові твори.

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. Вахонєва Т. М. Авторське право і суміжні права в Україні : Навчальний посібник. – Київ : ВД «Дакор», 2019. – 2-ге вид., перероб. і доп. – 576 с.
<https://kmaecm.edu.ua/wp-content/uploads/2021/06/vahonyeva-t-m.-2019-avtorske-pravo-i-sumizhni-prava-v-ukrayini.pdf>
2. Право інтелектуальної власності : підручник / за заг. ред. С.Б. Булеци, О.І. Чепис. Ужгород: РІК-У, 2019. 488 с.
https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/23778/1/%d0%9f%d0%86%d0%92_2019.pdf
3. Державне підприємство «Інститут інтелектуальної власності» // [Електронний ресурс]. – Режим доступу: <https://ukrpatent.org/uk>
4. 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
5. Про авторське право і суміжні права: Закон України від 15 квітня 2023 р. № 2811-IX.
<https://zakon.rada.gov.ua/laws/show/2811-20#n855>
6. 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>
7. 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.
<https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju>
8. 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

9. Про внесення змін до деяких законодавчих актів України щодо посилення захисту прав інтелектуальної власності: Закон України від 20 березня 2023 р. № 2974-IX.
<https://zakon.rada.gov.ua/laws/show/2974-20#Text>
10. Про внесення змін до деяких законів щодо створення національного органу інтелектуальної власності: Закон України від 16.06.2020 № 703-IX.
URL: <https://zakon.rada.gov.ua/laws/show/703-20#Text> (дата звернення: 20.12.2020)
11. Про охорону прав на винаходи і корисні моделі: Закон України від 31 грудня 2023 р. № 3687-XII.

<https://zakon.rada.gov.ua/laws/show/3687-12#Text>

12. Конституція України : Закон України від 28. 06. 1996 р.

URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>

13. Цивільний кодекс України: Кодекс України від 16.01.2003 №435-IV.

URL: <https://ips.ligazakon.net/document/T030435>

14. Цивільний процесуальний кодекс України: Кодекс України від 18.03.2004 № 1618-IV.

URL: <https://zakon.rada.gov.ua/laws/show/1618-15#Text>

15. Господарський процесуальний кодекс України: Кодекс України від 06.11.1991. №1798-XII.

URL: <https://zakon.rada.gov.ua/laws/show/179812#Text>

16. Бернська конвенція про охорону літературних і художніх творів від 24.07.1971 р. Bernska konventsiaa pro okhoronu literaturnykh i khudozhnikh tvoriv vid 24.07.1971 r.

URL: https://zakon.rada.gov.ua/laws/show/995_051#Text

17. Конвенція про захист прав людини і основоположних свобод (з протоколами) (Європейська конвенція з прав людини).

URL: https://zakon.rada.gov.ua/laws/show/995_004#Text

18. Деякі питання Національного органу інтелектуальної власності

<https://zakon.rada.gov.ua/laws/show/943-2022-%D1%80#Text> (дата звернення: 12.12.2022).

19. Про державну таємницю: Закон України від 21 січня 1994 року.

URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>

20. Про науково-технічну інформацію: Закон України від 25.06.1993 р. URL:

<https://zakon.rada.gov.ua/laws/main/3322-12#Text>

21. Про охорону прав на знаки для товарів і послуг: Закон України від 15.12.1993 № 3689-XII.

URL: <https://zakon.rada.gov.ua/laws/main/368912#Text>

22. Кадетова О. В. Угода про асоціацію України з Європейським Союзом в системі джерел права інтелектуальної власності: монографія. Київ: Юрінком Інтер, 2019. 344 с.

https://yuricom.com/wp-content/uploads/2019/03/Kadetova_zmist.pdf

Система оцінювання

Критерії оцінювання успішності студента та розподіл балів

Бали нараховуються за наступним співвідношенням:

- практичні роботи: 30% семестрової оцінки;
- самостійна робота: 10% семестрової оцінки;
- індивідуальне завдання: 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

Дата погодження, підпис
28.08.2024 р.



Завідувач кафедри
Сергій ЄВСЕЄВ

Дата погодження, підпис
31.08.2024 р.



Гарант ОП
Станіслав МІЛЕВСЬКИЙ