Силабус освітнього компонента
Програма навчальної дисципліни

Авторське право у цифровому суспільстві

Шифр та назва спеціальності
F5 – Кібербезпека та захист інформації

Інститут
ННІ комп`ютерних наук та інформаційних технологій

Спеціалізація

Кафедра
Кібербезпеки (328)

Освітня програма
Кібербезпека

Тип дисципліни
Наукова підготовка, Обов'язкова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
1

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

Навчальна дисципліна «Авторське право у цифровому суспільстві» є вибірковим освітнім компонентом правового спрямування, орієнтованим на підготовку фахівців у сфері кібербезпеки та інформаційних технологій. Курс охоплює базові положення авторського права — його сутність, об’єкти й суб’єкти, майнові та немайнові права, механізми набуття й охорони — та поглиблено розглядає їх реалізацію в умовах цифровізації.

Особливий акцент зроблено на проблематиці інформаційної безпеки та кіберпростору: міжнародно-правові та національні норми щодо цифрового контенту, ліцензійні режими у сфері IT, технічні засоби захисту авторських прав (DRM, цифрові водяні знаки, blockchain), особливості охорони програмного забезпечення і баз даних, виклики, пов'язані з використанням штучного інтелекту, а також механізми захисту прав у мережі Інтернет і на цифрових платформах.
Оволодіння матеріалом дисципліни дає можливість здобувачам орієнтуватися у правових та кібербезпекових аспектах захисту інтелектуальної власності, виявляти і документувати цифрові порушення, застосовувати сучасні техніко-правові інструменти у професійній діяльності.

Мета та цілі дисципліни

Метою навчальної дисципліни «Авторське право у цифровому суспільстві» є формування у здобувачів знань і вмінь щодо правового регулювання авторських прав у цифровому середовищі та їх захисту із застосуванням інструментів кібербезпеки.
Основними завданнями вивчення дисципліни є:
- отримання знань щодо міжнародного і національного законодавства у сфері авторського права та його застосування у цифровому просторі;
- оволодіння методами виявлення, документування та попередження порушень авторських прав у мережі Інтернет;
- формування навичок використання технічних засобів захисту авторських прав (DRM, цифрові водяні знаки, blockchain, алгоритми цифрової криміналістики);
- засвоєння практики складання та аналізу авторських договорів і ліцензійних угод у сфері IT та кібербезпеки;
- розвиток компетентностей у сфері цифрової криміналістики, зокрема проведення первинних досліджень випадків порушення авторських прав у кіберсередовищі.
Предметом дисципліни є правові та техніко-організаційні механізми охорони і захисту авторських прав у цифровому суспільстві, а також методи цифрової криміналістики, що застосовуються у сфері кібербезпеки.

Формат занять

Лекції, лабораторні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований 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. Провадити 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 напряму 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., 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, системи законодавства та правозастосування;
«Інтелектуальна власність» – знання про правовий режим об'єктів інтелектуальної власності та навички аналізу правових відносин у цифровому середовищі;
«Основи кібербезпеки» (базовий курс) – початкові уявлення про інформаційні загрози, засоби їх виявлення і запобігання;
«Основи наукових досліджень» - поглиблення у студентів знань щодо специфіки наукових досліджень, вивчення термінології та методології сучасної науки, застосування отриманих знань на практиці в освітньому та дослідницькому процесах.

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. Авторське право та кібербезпека: базові поняття і виклики. Еволюція авторського права у цифрову епоху. Порушення прав у мережевому середовищі як фактор кіберзагроз. Цифрова ідентифікація автора, цифровий слід, доказова база.	2
Тема 2. Об'єкти та суб'єкти авторського права у сфері IT та кібербезпеки. Програмне забезпечення, бази даних, цифрові сервіси як об'єкти охорони. Співавторство, юридичний статус цифрових платформ та провайдерів.	2
Тема 3. Договори та ліцензії у сфері цифрових технологій. Авторські договори в IT-проєктах. Ліцензії GPL, MIT, Creative Commons. Ризики нелегального використання open source та пропрієтарного ПЗ.	2
Тема 4. Міжнародне та національне законодавство про охорону авторського права у цифровому середовищі. Бернська конвенція, TRIPS, WIPO Internet Treaties, DSM Directive, DMCA, українське законодавство.	2
Тема 5. Технічні засоби захисту авторських прав. DRM, цифрові підписи, водяні знаки, blockchain. Алгоритми виявлення плагіату й копіювання. Content ID, hash-based detection.	2
Тема 6. Колективне управління авторськими правами в цифровому середовищі. Організації колективного управління (ОКУ), виклики для цифрових платформ, блокчейн-рішення для роялті.	2
Тема 7. Авторське право і штучний інтелект. Генеративний контент і проблема доведення авторства. Використання датасетів. Правові колізії творів, створених ШІ, і підходи ВОІВ та ЄС.	2
Тема 8. Захист авторських прав в Інтернеті. Notice-and-takedown, safe harbour, DMCA. Відповідальність провайдерів і платформ (YouTube, TikTok, Telegram). Кіберінциденти, пов'язані з порушенням прав.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Аналіз судових кейсів у сфері авторського права у цифровому середовищі . Судова практика України, ЄС та США. Склад правопорушення. Суб'єкти та об'єкти правовідносин. Доказова база у цифровом середовищі.	4	1
Тема 2. Об'єкти та суб'єкти авторського права у сфері IT та кібербезпеки .	4	1

Програмне забезпечення. Бази даних. Цифровий контент. Правовласники, користувачі, провайдери, цифрові платформи.		
Тема 3. Ліцензії та авторські договори у сфері цифрових технологій . GPL, MIT, Creative Commons. Авторські договори в IT-проєктах. Open source і пропрієтарне програмне забезпечення. Ризики правового використання.	4	1
Тема 4. Механізм notice-and-takedown у захисті авторських прав. DMCA. Директива ЄС 2019/790. Українське законодавство. Політики цифрових платформ. Елементи notice-повідомлення.	4	1
Тема 5. Технічні засоби захисту авторських прав . DRM. Цифрові підписи. Водяні знаки. Blockchain-рішення. Алгоритми виявлення копіювання та плагіату. Content ID.	4	1
Тема 6. Авторське право і штучний інтелект. AI-generated контент. Правовий статус результатів роботи ШІ. Використання датасетів. Ризики та колізії.	4	1
Тема 7. Захист авторських прав на цифрових платформах . Політики YouTube, TikTok, Instagram. Скарги про порушення. Відповідальність провайдерів і платформ.	4	1
Тема 8. Методи цифрової криміналістики у сфері авторського права. Інструменти цифрової криміналістики. Виявлення плагіату. Перевірка оригінальності творів. Цифрове досьє. Доказова сила цифрових матеріалів.	4	1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Ліцензії та договори у цифровому середовищі. Авторські договори, невиключні та виключні ліцензії. Open source (GPL, MIT). Creative Commons. Ризики та правові наслідки використання ПЗ.	0,5
Тема 2. Судова практика у сфері авторського права у цифровому суспільстві. Справи України, ЄС, США. Аналіз фабули, правової кваліфікації, доказової бази. Рішення Суду ЄС (Digital Rights Ireland, Schrems II). Українська практика у сфері онлайн-піратства.	0,5
Тема 3. Авторське право і штучний інтелект. AI-generated контент. Проблема правосуб'єктності. Використання датасетів. Міжнародні підходи до регулювання (WIPO, ЄС). Колізії та перспективи правового врегулювання.	1

Загалом	$\sum_{i=1}^{m} b_i=2$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Національне законодавство у сфері авторського права України. Закон України «Про авторське право і суміжні права». Цивільний кодекс України (книга IV «Право інтелектуальної власності»). Кримінальний кодекс України (ст. 176).	8
Тема 2. Міжнародні договори у сфері авторського права. Бернська конвенція про охорону літературних і художніх творів. Договір ВОІВ про авторське право (WCT). Договір ВОІВ про виконання і фонограми (WPPT). Угода TRIPS.	8
Тема 3. Європейське регулювання авторського права. Директива 2001/29/ЕС (InfoSoc Directive). Директива 2019/790/EU (DSM Directive). Регламент Digital Services Act. Практика Суду ЄС (справи Digital Rights Ireland, Schrems II).	7
Тема 4. Правові механізми захисту авторських прав у цифровому середовищі. Механізм notice-and-takedown. Safe harbor. Політики онлайн-платформ (YouTube, Facebook, TikTok). Судова практика в Україні та США.	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. Авторське право і штучний інтелект. AI-generated контент. Правовий статус творів, створених ШІ. Використання датасетів. Підходи ЄС, США та ВОІВ.	7
Тема 7. Авторське право і захист персональних даних у цифровому середовищі. Закон України «Про захист персональних даних». GDPR. Використання персональних даних у творах та цифрових сервісах. Баланс між правом на приватність і правом автора.	7
Тема 8. Кіберзлочини, пов'язані з порушенням авторських прав. 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. Інформаційна безпека у сфері колективного управління правами. Організації колективного управління (ОКУ) та цифрові реєстри. Захист баз даних авторів і творів. Використання blockchain і smart contracts у системах роялті. Ризики кіберзагроз для ОКУ.	7

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. Khvostenko, 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:

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

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».

Шкала оцінювання

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C

Підсумкова оцінка виставляється відповідно до розрахованої О з округленням до найближчого цілого числа в більшу сторону.

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** Станіслав МІЛЕВСЬКИЙ