Силабус освітнього компонента
Програма навчальної дисципліни

Основи наукових досліджень

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

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: Математичні основи криптології, Комп`ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

Детальніше про викладача на сайті кафедри

АХІЄЗЕР Олена Борисівна
Olena.Akhiiezer@khpi.edu.ua
К.т.н., доцентка, професорка НТУ "ХПІ", завідувачка кафедри Комп'ютерної математики і аналізу даних

Автор та співавтор понад 200 наукових та навчально-методичних праць. Курси: «Математичний аналіз», «Диференційні рівняння та комплексний аналіз», «Функціональний аналіз», «Вища математика».
Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна «Основи наукових досліджень» належить до нормативних, спрямована на поглиблення у студентів знань щодо специфіки наукових досліджень, вивчення термінології та методології сучасної науки, застосування отриманих знань на практиці в освітньому та дослідницькому процесах. Дисципліна орієнтує на вибір методів та інструментарію наукових досліджень, дотримання принципів академічної доброчесності.

Мета та цілі дисципліни

Ознайомлення з теоретичними засадами науково-дослідної діяльності, надання методичних рекомендацій щодо виконання конкретних видів наукових, навчально-дослідних та студентських робіт.

Формат занять

Лекції, практичні заняття, самостійна робота, консультації. Підсумковий контроль – іспит.

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).
КФ1. Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки.
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.
КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.
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.
КФ7. Здатність 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.
КФ8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, 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.
КФ11. Здатність здійснювати наукові та/або прикладні дослідження у галузі інформаційної безпеки та/або кібербезпеки із застосуванням сучасних експериментальних і теоретичних методів моделювання процесів, формувати науково-технічну звітність.

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 150 год. (5 кредитів ECTS): лекції – 32 год., практичні роботи – 32 год., самостійна робота – 86 год.

Передумови вивчення дисципліни (пререквізити)

Англійська мова в академічних застосунках.

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. Основні визначення та поняття. Що таке наукові дослідження: мета, методи та значення. Типи наукових досліджень: теоретичні та експериментальні підходи. Етапи проведення наукового дослідження.	4
Тема 2. Класифікація та основні етапи науково-дослідних робіт. Класифікація науково-дослідних робіт. Основні етапи. Додаткові аспекти досліджень.	4
Тема 3. Наукове дослідження та методика його виконання. Рівні наукового дослідження. Основні методи емпіричного дослідження. Обробка результатів експерименту. Метод індукції. Основні методи теоретичного пізнання. Структура і функції наукової теорії.	4
Тема 4. Вибір теми та планування наукових досліджень. Основні поняття. Обгрунтування актуальності теми. Новизна ідеї. Планування наукових досліджень. Вивчення та аналіз літературних джерел за темою досліджень. Структура наукової статті. Структура змісту магістерської роботи.	5
Тема 5. Вивчення та аналіз літературних джерел за темою досліджень. Як правильно робити огляд літератури: аналіз джерел. Використання наукових баз даних та бібліографічних менеджерів. Стилі цитування (APA, MLA, Chicago) та уникнення плагіату.	5
Тема 6. Методологія наукового дослідження. Якісні та кількісні методи дослідження: переваги та недоліки. Спостереження, експеримент, анкетування та інші методи збору даних. Вибір методів та інструментів для дослідження.	5
Тема 7. Організація наукового дослідження. Підготовка та виконання наукових досліджень. Результат наукової діяльності. Види, структура, етапи виконання наукового дослідження. Загальні поради до організації наукової діяльності магістранта. Визначення основних складових магістерської дисертації. Формулювання назви дисертації . Визначення об'єкта та предмета дослідження. Визначення мети та завдань дослідження. Визначення методології, методів та методики наукового дослідження. Результат наукової діяльності. види наукових видань для публікації результатів наукових досліджень. УДК – універсальна десяткова класифікація. Вимоги до усного викладу, презентації. Методика підготовки доповіді на науковій конференції.	5
Загальна кількість годин	**32**

Практичні заняття

Теми практичних/семінарських занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Еволюція науки. Теоретичні принципи та методологія науки.	4	0,1

Поняття та історичні етапи розвитку науки. Основні наукові парадигми (класична, некласична, постнекласична). Теоретичні принципи наукового пізнання. Основні підходи та методи в науці. Роль методології в сучасних дослідженнях.		
Тема 2. Аналіз наукової публікації. Види наукових публікацій (стаття, монографія, тези). Структура наукової статті. Методи критичного аналізу публікацій. Пошук та оцінювання джерел у наукометричних базах (Scopus, WoS). Практика аналізу актуальних наукових статей.	4	0,1
Тема 3. Організація виконання розробки автоматизованої інформаційної системи. Постановка завдання і визначення вимог. Етапи розробки АІС (аналіз, проєктування, реалізація, тестування, впровадження). Методи організації науково-дослідних робіт. Використання сучасних інструментів та методологій (Agile, Scrum, Waterfall). Документування результатів дослідження і розробки.	4	0,1
Тема 4. Методологія наукових досліджень. Загальнонаукові методи (аналіз, синтез, індукція, дедукція). Емпіричні та теоретичні методи дослідження. Моделювання як метод наукового пізнання. Використання статистичних методів у наукових дослідженнях. Міждисциплінарні підходи в науці.	4	0,1
Тема 5. Підготовка наукової публікації. Вимоги до структури наукової статті. Оформлення цитувань і бібліографії (APA, IEEE, ДСТУ). Використання наукометричних інструментів для вибору журналу. Практика рецензування та відповіді на зауваження рецензента. Етика публікаційної діяльності.	4	0,1
Тема 6. Підготовка дисертаційної роботи. Структура дисертаційної роботи. Формування наукової проблеми та гіпотези. Огляд літературних джерел і аналіз сучасних досліджень. Виклад власних результатів і наукової новизни. Підготовка до захисту (доповідь, презентація, апробація результатів).	3	0,1
Тема 7. Робота з кубітами. Емуляція вимірювань. Основи квантових обчислень: стан кубіта, суперпозиція. Математичний опис операцій над кубітами (матриці Паулі, Адамара). Емуляція квантових вимірювань на класичному комп'ютері. Побудова простих квантових алгоритмів (Deutsch, Grover). Аналіз потенційних загроз класичним криптосистемам з боку квантових обчислень.	3	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}7$

Контрольні роботи

Теми контрольних робіт	Вагові

	коефіцієнти b
Тема 1. Еволюція науки та методологія наукових досліджень. Історичні етапи розвитку науки та зміна наукових парадигм. Основні методологічні принципи сучасних наукових досліджень. Порівняльний аналіз класичної, некласичної та постнекласичної науки. Використання загальнонаукових методів у дослідженнях.	0,1
Тема 2. Практичні аспекти підготовки наукових праць. Аналіз структури наукової статті та вимог до її оформлення. Організація виконання наукового дослідження або розробки інформаційної системи. Методика підготовки наукової публікації та дисертаційної роботи. Проблеми академічної доброчесності та етики публікаційної діяльності.	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Філософські основи науки: роль філософії у формуванні наукових методів. Взаємозв'язок філософії та науки. Основні філософські напрями та їх вплив на наукові підходи. Проблема істини у науці. Наука як система знань і як соціальний інститут.	11
Тема 2. Наукова парадигма та наукові революції (за Т. Куном). Поняття «наукова парадигма». Нормальна наука та кризові ситуації. Наукові революції та зміна парадигм. Приклади змін наукових парадигм у різних галузях.	11
Тема 3. Класифікація методів наукових досліджень: емпіричні, теоретичні та загальнонаукові. Емпіричні методи (спостереження, експеримент, вимірювання). Теоретичні методи (моделювання, аналіз, синтез, індукція, дедукція). Загальнонаукові методи (системний, кібернетичний, історичний). Інтердисциплінарні методи дослідження.	11
Тема 4. Організація та планування наукового експерименту. Основні етапи експерименту. Постановка мети та завдань. Вибір об'єкта і предмета дослідження. Планування, проведення та аналіз результатів експерименту.	11
Тема 5. Методи збору та обробки наукової інформації. Джерела наукової інформації. Методи збору первинних даних. Методи статистичної обробки даних. Використання програмних засобів для аналізу даних.	11
Тема 6. Бібліометрія та наукометричні показники: індекс Хірша, імпакт-фактор. Основні поняття бібліометрії. Індекс цитування та індекс Хірша. Імпакт-фактор наукових журналів. Переваги та недоліки наукометричних показників.	11
Тема 7. Академічна доброчесність і запобігання плагіату у наукових дослідженнях.	10

Поняття академічної доброчесності. Види академічних порушень. Методи перевірки на плагіат. Етичні норми у науковій діяльності.	
Тема 8. Сучасні інформаційні ресурси для наукових досліджень: Scopus, Web of Science, Google Scholar, ResearchGate. Міжнародні наукометричні бази даних. Пошук і аналіз наукових публікацій. Використання електронних бібліотек та репозитаріїв. Формування наукового профілю дослідника.	10
Загальна кількість годин	**86**

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. За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Мазур О.В. Основи наукових досліджень : навч. посіб. Для студ. вищих навч. заклад. філол. спец. /О. В. Мазур, О.В. Подвойська, С. В. Радецька. – Вінниця : Нова Книга, 2013. – 120с. https://www.google.com.ua/books/edition/_/jl3XCQAAQBAJ?hl=ru&gbpv=1&pg=PP1&dq=inauthor:%22%D0%9C%D0%B0%D0%B7%D1%83%D1%80+%D0%9E.+%D0%92.+%D1%82%D0%B0+%D1%96%D0%BD.%22
2. Данильян О. Г. Методологія наукових досліджень : підручник / О. Г. Данильян, О. П. Дзьобань. – Харків : Право, 2019. – 368 с.
https://library.nlu.edu.ua/POLN_TEXT/SENMK/OMND.pdf
3. Методологія та організація наукових досліджень : навч. посіб. / І. С. Добронравова, О. В. Руденко, Л. І. Сидоренко та ін. ; за ред. І. С. Добронравової (ч. 1), О. В. Руденко (ч. 2). – К. : ВПЦ "Київський університет", 2018. – 607 с.
http://www.philsci.univ.kiev.ua/biblio/Methodol.pdf
4. 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
5. 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
6. 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

7. "Research Design: Qualitative, Quantitative, and Mixed Methods Approaches", John W. Creswell (2017)
https://www.ucg.ac.me/skladiste/blog_609332/objava_105202/fajlovi/Creswell.pdf.
8. "How to Write a Lot: A Practical Guide to Productive Academic Writing", Paul J. Silvia (2018)

https://books.google.com.ua/books/about/How_to_Write_a_Lot.html?id=xiCbEAAAQBAJ&redir_esc=y
9. "Social Research Methods", Alan Bryman (2021) https://www.academia.edu/45262372/Social_Research_Methods
10. Про затвердження Вимог до оформлення дисертації : Наказ Міністерства освіти і науки України від 12.01.2017р. № 40 https://zakon.rada.gov.ua/laws/show/z0155-17#Text

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
0,4	0,2		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».

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** Станіслав МІЛЕВСЬКИЙ