Силабус освітнього компонента
Програма навчальної дисципліни

Агентне моделювання

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
Професійна підготовка, Вибіркова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
3

Мова викладання
Українська

Викладачі, розробники

АКСЬОНОВА Ірина Вікторівна

Iryna.Aksonova@khpi.edu.ua
Кандидат економічних наук, старший дослідник зі спеціальності F5, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 150, з них свідоцтв на авторський твір - більше 15, розділів у монографіях - 10, статей, що реферуються у науково метричних базах Scopus та WoS - 9. Лектор з дисциплін: "Штучний інтелект і бізнес-аналітика", "Теорія інформації і кодування", "Технологія управління безпекою бізнес-процесів, "Агентне моделювання" та інших у студентів бакалавріата та магістратури.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна програма дисципліни “Агентне моделювання” розглядає теоретичні основи та застосування агентних технологій. Висвітлено сучасні підходи до подання й обробки знань, на яких базуються інтелектуальні програмні агенти. Наведено моделі та технології створення програмних агентів і мультиагентних систем, їх застосування для пошуку інформації та підтримки електронного бізнесу та забезпечення необхідного рівня захищеності ресурсів. Програма орієнтована на науковців і спеціалістів, які займаються дослідженнями та розробками в галузі кібербезпеки, інтелектуальних інформаційних систем, бізнес- застосунків інформаційної економіки.

Мета та цілі дисципліни

Метою вивчення дисципліни – це створення теоретичної основи для розробки та використання інтелектуальних агентно-орієнтованих систем. Наведені у роботі приклади застосування програмних агентів та мультиагентних систем мають показати ефективність агентного підходу та підкреслити сферу його застосуванню.

Формат занять

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

Компетентності

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.
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.

Результати навчання

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.
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.
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 роботи – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Основи програмування, Технології програмування, Алгоритми та структури даних. Основи математичного моделювання систем безпеки, Основи кібербезпеки.

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. Вступ до агентного моделювання. Основи агентного підходу до моделювання складних систем. Огляд основних концепцій: агенти, середовище, правила взаємодії. Приклади використання в кібербезпеці. Основи агентного підходу в моделюванні складних систем. Порівняння агентного моделювання з іншими методами (системна динаміка, дискретно-подійне моделювання).	2
Тема 2. Типи агентів та їх поведінка. Поняття агентів, їхні характеристики та поведінка. Взаємодія агентів між собою та з середовищем. Типи агентів (реактивні, когнітивні, навчальні). Моделі прийняття рішень агентами. Взаємодія агентів у розподілених системах кібербезпеки.	2
Тема 3. Моделювання поведінки агентів. Основи агентного моделювання. Процедура розробки агентної моделі. Створення моделей кібератак за допомогою агентного підходу. Аналіз атак соціальної інженерії, DDoS, зловмисного ПЗ. Приклади агентного моделювання. Побудова симуляційних середовищ для виявлення загроз. Реалізація агентів за допомогою машинного навчання та евристичних алгоритмів. Використання правил поведінки та адаптивних стратегій. Методи прийняття рішень агентами. Традиційні підходи моделювання поведінки агентів.	2
Тема 4. Інтелектуальні програмні агенти та їх архітектури. Основні властивості програмних агентів. Архітектури агентів. Мультиагентні системи. Мови комунікації агентів. Агентно-орієнтоване програмування. Методології розробки мультиагентних систем. Засоби інтелектуалізації поведінки програмних агентів.	2
Тема 5. Застосування агентних технологій. Інформаційна економіка як сфера застосування агентних технологій. Програмні агенти е-комерції. Програмні агенти логістики. Програмні агенти електронних ринків. Програмні агенти дистанційної освіти. Програмні агенти електронного урядування. Програмні агенти систем кібербезпеки. Програмні агенти електронної медицини.	2
Тема 6. Еволюційні технології та генетичні алгоритми в агентному моделюванні Концептуальні засади еволюційної теорії. Основні положення теорії генетичних алгоритмів. Моделі генетичних алгоритмів. Мурашині алгоритми та генетичне програмування.	2
Тема 7. Імітаційне моделювання та теорія ігор в агентному моделюванні. Теорія ігор у контексті агентного моделювання. Ключові аспекти використання теорії ігор в АМ. Методи теорії ігор в АМ. Імітаційне моделювання та його методи в АМ.	2
Тема 8. Системна динаміка в агентному моделюванні: поєднання макро- і мікрорівнів Методологія системної динаміки в контексті АМ. приклади використання гібридного підходу в кібербезпеці. Поєднання макро та мікрорівнів у складних системах. Функціональний та інформаційний опис системи.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Установка програмного забезпечення для розробки та тестування додатків. Ознайомлення з інструментами та середовищами розробки, необхідними для створення агентних систем. Перевірка коректності роботи програмного середовища. Встановлення та активація Anylogic. Створення популяції агентів.	6	0,1
Тема 2. Розробка програми моделювання агента. Створення базового програмного модуля агента, визначення його поведінки, ролей і станів. Реалізація взаємодії агентів через обмін повідомленнями. Тестування моделей на простих прикладах середовища моделювання.	6	0,1
Тема 3. Візуалізація результатів моделювання в Anylogic. Реалізація візуалізації результатів моделювання в AnyLogic шляхом визначення функцій для обчислення кількості агентів на певний момент часу. Додавання графічних елементів, які дозволять відстежувати динаміку змін в процесі моделювання, що дасть змогу аналізувати еволюцію кількості різних агекентів.	6	0,1
Тема 4. Порівняння поведінки моделі при різних умовах. Дослідження поведінки агентної моделі за різних початкових умов на підставі зміни значень вхідних параметрів, виконання серії запусків моделі та аналізу отриманих результатів. Використання вбудованих засобів AnyLogic, зокрема експерименту порівняння прогонів, який дозволяє систематизовано зіставляти результати моделювання за різних умов.	6	0,1
Тема 5. Побудова та використання ігрової агентної моделі «Відбиття атак у кіберпросторі» Ознайомлення з базовими положеннями теорії ігор та особливостями її застосування у сфері кібербезпеки. Розробка узагальненої ігрової моделі, що відображає взаємодію сторін у кіберпросторі, зокрема сценарії протистояння між атаками та захисними діями, із можливістю варіювання стратегій. Проведення аналізу результатів моделювання з метою оцінювання ефективності різних підходів до протидії кіберзагрозам.	8	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}5$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Системи, засновані на знаннях. Теоретичні основи інтелектуальних програмних агентів. Контрольна робота спрямована на закріплення знань про принципи побудови інтелектуальних систем і програмних агентів. Розглядаються основні поняття систем, заснованих на знаннях, методи подання знань, агентні системи та особливості їх функціонування. Особлива увага приділяється теоретичним основам програмних агентів: їх властивостям, архітектурам, мовам комунікації, а також методологіям розробки мультиагентних систем. Студенти повинні продемонструвати розуміння принципів інтелектуальної поведінки агентів та підходів до створення гнучких агентних архітектур.	0,25

Тема 2. Застосування агентних технологій у сучасних інформаційних системах. У роботі розглядаються практичні аспекти застосування агентних технологій у різних галузях діяльності. Аналізуються інформаційно-пошукові агенти, принципи їх роботи та роль у сучасних Інтернет-технологіях. Досліджуються приклади застосування агентних технологій в економіці, логістиці, електронній комерції, освіті, урядуванні, медицині та кібербезпеці. Метою є формування у студентів системного уявлення про можливості та переваги використання агентних підходів для формування бази даних, автоматизації процесів пошуку, аналізу та обробки інформації щодо кіберризиків та розробці стратегії кіберзахисту.	0,25
Загалом	$\sum_{i=1}^{m} b_i$=0,5

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1 Історія розвитку агентних технологій. Розглядаються етапи становлення агентного підходу — від ранніх експертних систем до сучасних мультиагентних платформ. Аналізуються ключові наукові школи та концепції, що вплинули на розвиток агентних систем.	8
Тема 2. Класифікація агентів і типи агентних систем. Вивчаються різновиди агентів: реактивні, когнітивні, адаптивні, навчальні. Описуються критерії класифікації агентних систем і сфери їх застосування.	8
Тема 3. Архітектури агентів: реактивні, розумні та гібридні моделі. Пояснюються відмінності між різними архітектурами агентів, принципи їх проєктування, а також способи реалізації поведінки на основі правил, логіки або навчання.	7
Тема 4. Комунікація між агентами. Мови та протоколи взаємодії. Розглядаються основи обміну повідомленнями між агентами, мови типу ACL (Agent Communication Language) та протоколи взаємодії (FIPA, KQML тощо).	7
Тема 5. Онтології в агентних системах. Вивчаються принципи побудови онтологій для формального опису знань у мультиагентних системах, роль онтологічного моделювання для взаєморозуміння агентів.	7
Тема 6. Координація, планування та переговори між агентами. Аналізуються методи узгодження дій агентів, алгоритми колективного планування, розподілу ресурсів і ведення переговорів між агентами в умовах конфлікту інтересів.	7
Тема 7. Агентні системи в Інтернеті речей (IoT). Розглядається застосування агентних технологій у смарт-середовищах, зокрема в інтернеті речей, для автономного управління пристроями та оптимізації процесів.	7
Тема 8. Агентні технології в системах кібербезпеки. Досліджуються підходи до використання агентів для виявлення вторгнень, моніторингу трафіку, аналізу загроз і реагування на інциденти безпеки.	7
Тема 9. Мультиагентне моделювання соціальних та економічних процесів.	7

Описується застосування агентного моделювання для аналізу поведінки людей, ринкових процесів, розповсюдження інформації, конфліктів і співпраці.	
Тема 10. Перспективи розвитку агентного моделювання та штучного інтелекту. Розглядаються сучасні тренди в інтеграції агентних технологій зі штучним інтелектом, машинним навчанням та хмарними обчисленнями.	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. Онлайн- курс «Спеціалізація Building AI Agents and Agentic Workflows» https://www.coursera.org/specializations/building-ai-agents-and-agentic-workflows
.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Плескач В.Л. , Рогушина Ю.В. Агентні технології: Монографія. – К.: Київ. нац. торг.–екон. ун–т, 2005. – 344 с.. – Режим доступу: https://core.ac.uk/download/pdf/38468943.pdf.
2. Безпекова синергетика: кібернетичний та інформаційний аспекти: монографія / І. Г. Грабар, Р. В. Грищук, К. В. Молодецька; за заг. ред. д.т.н., проф. Р. В. Грищука. – Житомир : ЖНАЕУ, 2019. – 280 с. – Режим доступу: http://ir.polissiauniver.edu.ua/bitstream/123456789/9581/1/Bezpekova_synerhetyka_2019.pdf.
3. Зінов'єва О. Г., Шаров С. В., Паламарчук І. Імітаційне моделювання та моделювання систем: навчальний посібник. Запоріжжя : ФОП Однорог Т.В., 2025. 203 с. – Режим доступу: http://www.tsatu.edu.ua/kn/wp-content/uploads/sites/16/posibnik_imms_print1.pdf.
4. Атаки на системи штучного інтелекту [Електронний ресурс] : навч.-практ. посібник / Євсеєв С. П., Шматко О. В., Ахієзер О. Б. [та ін.]. – Електрон. текст. дані. – Харків – Львів : "Новий Світ – 2000", 2025. – 108 с. – Режим доступу: https://repository.kpi.kharkov.ua/handle/KhPI-Press/93086.
5. Методи та системи штучного інтелекту: навч. посіб. / укл. Д.В. Лубко, С.В. Шаров. – Мелітополь: ФОП Однорог Т.В., 2019. – 264 с. – Режим доступу: https://elar.tsatu.edu.ua/server/api/core/bitstreams/c4c8e4d0-609d-4618-aad7-0c6d4b48d2c0/content.
6. Nicoletti L., Padovano A., Vartuli F. P., Vetrano M. HUMAN BEHAVIOR MODELING: A STATE OF THE ART // Proceedings of the International Defense and Homeland Security Simulation Workshop 2016/ Режим доступу: https://www.msc-les.org/proceedings/dhss/2016/DHSS2016_67.pdf.
7. Мілов О. В., Костяк М. Ю., Мілевський С. В., Погасій с. С. ЗАСОБИ МОДЕЛЮВАННЯ ПОВЕДІНКИ АГЕНТІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ // Системи управління, навігації та зв'язку, 2019, випуск 6(58). – Режим доступу: DOI: https://doi.org/10.26906/SUNZ.2019.6.063.

8. Grigoryev I. AnyLogic in three days: modelling and simulation textbook [Елект-ронний ресурс]: підручник. – AnyLogic, 2021. – Режим доступу: https://www.anylogic.com/resources/books/free-simulation-book-and-modeling-tutorials/.

Додаткова література

1. Штучний інтелект. Нейромережева обробка інформації : архітектури, навчання, застосування : навчальний посібник у 2-х ч. : Ч. 1 / О. Г. Руденко, О. О. Безсонов, С. П. Євсеєв, О. Б. Ахієзер, Ю. І. Зайцев ; за заг. ред. С. П. Євсеєва. – Харків : НТУ «ХПІ», – Львів : «Новий Світ-2000», 2025. – 426 с. – Режим доступу: https://repository.kpi.kharkov.ua/handle/KhPI-Press/93103.
2. Штучний інтелект. Нейромережева обробка інформації : архітектури, навчання, застосування [Електронний ресурс] : навч. посібник у 2-х ч. : Ч. 2. / О. Г. Руденко, О. О. Безсонов, С. П. Євсеєв [та ін.] ; Нац. техн. ун-т "Харків. політехн. ін-т". – Електрон. текст. дані. – Харків – Львів : "Новий Світ-2000", 2025. – 376 с. – Режим доступу: https://repository.kpi.kharkov.ua/handle/KhPI-Press/93105.
3. Milov, O., Hrebeniuk, A., Nalyvaiko, A., Nyemkova, E., Opirskyy, I., Pasko, I., Rzayev, K., Salii, A., Synytsina, U., & Soloviova, O. Development of the space-time structure of the methodology for modeling the behavior of antagonistic agents of the security system // Eastern-European Journal of Enterprise Technologies, 2020, *6*(2 (108), 30–52. – Режим доступу: https://doi.org/10.15587/1729-4061.2020.218660.
4. Томашевський В. М. Моделювання систем. – Київ: Видавнича група BHV, 2005. – 352 с. – Режим доступу: https://pdf.lib.vntu.edu.ua/books/2016/Tomashev_2005_352.pdf.
5. Імітаційне моделювання систем та процесів: Електронне навчальне видання. Конспект лекцій / В. Б. Неруш, В. В. Курдеча. – К.: НН ІТС НТУУ «КПІ», 2012. – 115 с. – Режим доступу: https://ela.kpi.ua/server/api/core/bitstreams/3fe27852-776f-4130-bc62-c9c2be44ed6e/content.
6. Остапенко , А., & Залевська , Д. ІМІТАЦІЙНЕ МОДЕЛЮВАННЯ ЕКОНОМІЧНИХ ЗАДАЧ В СЕРЕДОВИЩІ ANYLOGIC // Grail of Science, (35), 2024, 185–188. https://doi.org/10.36074/grail-of-science.19.01.2024.033

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
0,5	0,5		

Сума коефіцієнтів повинна складати одиницю: $k_1 + k_2 + k_3 + k_4 = 1$. Підбір вагових коефіцієнтів підсумкової оцінки здійснює розробник курсу.
Розрахунок підсумкової оцінки проводиться за формулою:

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

де: П – середньозважена середня оцінка за поточний контроль
І – оцінка за виконання індивідуального завдання
$К$ – середньозважена оцінка за контрольні роботи
Пк – оцінка за підсумковий контроль

$$П = \frac{П_1 \cdot a_1 + П_2 \cdot a_2 + \ldots + П_n \cdot a_n}{\sum_{i=1}^{n} a_i}$$

де: a_i - ваговий коефіцієнт за кожне практичне (семінарське) або лабораторне заняття.

$$K = \frac{K_1 \cdot b_1 + K_2 \cdot b_2 + \ldots + K_m \cdot b_m}{\sum_{i=1}^{m} b_i}$$

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