



Силабус освітнього компонента
Програма навчальної дисципліни



Математичні моделі управління ІТ-проектами

Шифр та назва спеціальності

F5 – Кібербезпека та захист інформації

Спеціалізація

Освітня програма

Кібербезпека

Рівень освіти

Другий (магістерський)

Семестр

2

Інститут

ННІ комп'ютерних наук та інформаційних технологій

Кафедра

Кібербезпеки (328)

Тип дисципліни

Спеціальна (фахова) підготовка, Обов'язкова

Форма навчання

Денна

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](#)



МІЛЕВСЬКИЙ Станіслав Валерійович

stanislav.milevskyi@khpi.edu.ua

Доктор технічних наук, доцент, професор кафедри кібербезпеки НТУ «ХПІ».

Автор понад 100 наукових та навчально-методичних праць. Гарант освітньо-наукової програми «Кібербезпека» другого (магістерського) рівня вищої освіти. Провідний лектор з дисциплін: «Основи математичного моделювання систем безпеки», «Основи машинного навчання для кібербезпеки», «Англійська мова в академічних застосунках», «Моделювання кіберфізичних дій», «Математичні моделі управління ІТ-проектами» у студентів бакалавріата та магістратури,

«Моделювання механізмів кібербезпеки», «Математичні методи, моделі та інформаційні технології у наукових дослідженнях» у аспірантів .

[Детальніше про викладача на сайті кафедри](#)

Загальна інформація

Анотація

Навчальна програма дисципліни "Математичні моделі управління IT-проєктами" охоплює методи та підходи до управління проєктами в інформаційних технологіях з використанням математичних моделей. Студенти вивчать базові принципи планування, контролю, оцінки ризиків та ресурсів у IT-проєктах, а також застосування сучасних математичних інструментів для моделювання процесів управління проєктами. Лабораторні заняття дозволять закріпити теоретичні знання на практиці за допомогою програмних засобів управління проєктами та аналітичних моделей.

Мета та цілі дисципліни

Метою дисципліни є надання студентам знань та навичок щодо використання математичних моделей для ефективного управління IT-проєктами, планування ресурсів та оцінки ризиків.

Формат занять

Практичні заняття, самостійна робота, консультації. Підсумковий контроль – диференційований залік.

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.

КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.

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.

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.

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., лабораторні заняття – 32 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Вища математика, Технології управління безпекою бізнес-процесів, Інноваційне підприємництво та управління стартап-проектами.

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

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Особливості IT-проектів та принципи управління ними. Головні елементи проекту в IT. Процеси проектування та поточна операційна діяльність. Класифікація типів проектів. Компоненти проекту. Основні концепції управління проектами. Типи структур в управлінні проектами. Життєвий цикл проекту. Визначення цілей, обмежень і критеріїв успішності IT-проектів. Стандарти в управлінні проектами.	2
Тема 2. Методології та математичні моделі управління проектами. Віхи в історії управління проектами. Класифікація методологій управління проектами. Принципи підбору методології, яка найкраще відповідає характеру проекту та його специфікаціям. Основні етапи розвитку негнучкої методології управління проектами. Визначення та основні характеристики гнучкої методології управління проектами. Типи математичних моделей: стохастичні, детерміновані. Основи теорії графів у плануванні IT-проектів.	2
Тема 3. Моделі планування часу та ресурсів. Сітьові (мережеві), структурні та графічні моделі проекту. Метод критичного шляху (CPM). Метод оцінки та перегляду програм (PERT). Календарне планування та діаграма Ганта. Оптимізація ресурсів.	2
Тема 4. Моделювання та управління проектними ризиками. Загальні поняття управління ризиками. Сутність ризиків та їх види. Різниця понять «ризик» та «невизначеність». Планування управління ризиками. Огляд процесів управління ризиком проекту. Методи аналізу ризиків проекту. Прогнозування ризиків з використанням імовірнісних моделей. Моделювання сценаріїв розвитку подій.	2
Тема 5. Лінійне програмування в управлінні IT-проектами. Основи лінійного програмування. Задачі розподілу ресурсів.	2
Тема 6. Моделювання вартості проекту. Методи оцінки вартості та аналізу витрат. Вплив часових затримок на вартість проекту.	2
Тема 7. Теорія ігор у плануванні проектів.	2

Стратегії управління проектами в умовах конкурентного середовища. Теорія ігор для моделювання взаємодії між командами.

Тема 8. Використання програмних засобів для моделювання управління проектами.	2
Програмні продукти для управління проектами (Microsoft Project, Jira, Miro, Trello, Primavera, Asana), особливості їх застосування. Інструменти для документування та комунікації в проектах. Використання симуляцій для оцінки ризиків.	
Загальна кількість годин	16

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти α
Тема 1. Стратегічний аналіз та планування ІТ-проєкту. Формування системних знань з теорії стратегічного управління та набуття практичних навичок стратегічного планування і стратегічного аналізу ІТ-проєктів з використанням методів SWOT-та PEST- аналізу.	4	0,1
Тема 2. Методології управління ІТ-проєктами. Знайомство з методологіями управління ІТ-проєктами та вивчення їх особливостей.	4	0,1
Тема 3. Структурне планування проєкту. Отримання навичок складання мережових графіків, розрахунку раннього і пізнього часу початку робіт, знаходження критичного шляху.	4	0,1
Тема 4. Мережеве моделювання проєктної діяльності. Засвоєння принципів календарного планування проєктів мережевими методами.	4	0,1
Тема 5. Використання методів оцінювання ризиків та інструментів симуляції для аналізу ризиків та варіантів розподілу ресурсів. Порівняння можливих варіантів впровадження системи захисту від кіберзагроз на підставі визначення «точки беззбитковості» для кожного з варіантів. Оцінка ризиків та вибір найвигіднішого сценарію за допомогою дерева рішень, яке враховує ймовірності подій та фінансові наслідки. Застосування методу Монте-Карло для оцінки ризиків у сфері ІТ та кібербезпеки.	4	0,1
Тема 6. Лінійне програмування для оптимізації витрат і ресурсів. Розв'язання задачі лінійного програмування із застосуванням надбудов засобами табличного процесора MS Excel.	4	0,1
Тема 7. Управління вартістю ІТ-проєкта. Формування системних знань та набуття практичних навичок з питань управління вартістю ІТ-проєктів шляхом оцінювання вартості операцій та розробки плану управління вартістю ІТ проєкту.	4	0,1
Тема 8. Стратегічне управління в ІТ-проєктах: аналіз рішень за допомогою теорії ігор.	4	0,1

Ознайомлення із базовими концепціями теорії ігор та набуття навичок застосовувати математичні моделі для аналізу стратегічних рішень в управлінні ІТ-проектами, що сприятиме кращому розумінню логіки прийняття рішень у реальних умовах планування та виконання ІТ-проектів.

Загальна кількість годин	32	$\sum_{i=1}^n a_i = 0,8$
---------------------------------	-----------	--------------------------

Контрольні роботи

Теми контрольних робіт

Вагові
коефіцієнти b

Тема 1. Теоретичні та прикладні аспекти управління ІТ-проектами. Питання охоплюють матеріал за темами 1-4.	0,2
Тема 2. Методи оптимізації та моделювання в управлінні ІТ-проектами. Питання охоплюють матеріал за темами 5-8.	0,2
Загалом	$\sum_{i=1}^m b_i = 0,4$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення

Кількість годин

Тема 1. Математичні основи управління проектами Розглядаються базові поняття математичного моделювання, оптимізації та прийняття рішень у системах управління ІТ-проектами.	8
Тема 2. Сітьові моделі та методи управління проектами (CPM, PERT) Вивчаються принципи побудови та аналізу сітьових графіків, методи визначення критичного шляху та розрахунку резервів часу.	8
Тема 3. Теорія черг у плануванні проектів Ознайомлення з моделями теорії масового обслуговування для оцінки затримок, черг та навантаження ресурсів у ІТ-проектах.	7
Тема 4. Оптимізаційні методи розподілу ресурсів Розглядаються математичні моделі та алгоритми оптимального призначення ресурсів при обмежених часових і фінансових параметрах.	7
Тема 5. Моделі прийняття рішень в умовах невизначеності Вивчаються методи прийняття рішень із використанням ймовірнісних та нечітких моделей, аналіз ризиків і стратегій у проектному середовищі.	7
Тема 6. Імітаційне моделювання у проектному менеджменті Розглядаються принципи побудови симуляційних моделей, що дозволяють прогнозувати наслідки управлінських рішень.	7
Тема 7. Стохастичні процеси в управлінні ІТ-проектами Вивчення моделей випадкових подій та процесів, що впливають на строки, ресурси і результати проектів.	7
Тема 8. Економіко-математичне моделювання витрат проекту Ознайомлення з методами побудови моделей витрат, прогнозування бюджетних потреб та оцінювання економічної ефективності.	7

Тема 9. Методи багатокритеріальної оптимізації

7

Розглядаються підходи до прийняття рішень за кількома критеріями, зокрема баланс між вартістю, строками та якістю виконання проекту.

Тема 10. Використання програмних засобів для математичного моделювання проектів

7

Досліджуються можливості сучасних інструментів (Excel Solver, MATLAB, Python, ProjectLibre тощо) для аналізу, оптимізації та візуалізації моделей управління IT-проектами.

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

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

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Кузьмич В.О., Коваль О.В., Тараненко Р.А. Моделі та засоби управління IT-проектами. // Навч. посіб. для студ. спеціальностей 121 «Інженерія програмного забезпечення». Київ : КПІ ім. Ігоря Сікорського, 2023. 222с. – Режим доступу: https://ela.kpi.ua/bitstream/123456789/57303/1/Modeli_ta_zasoby_upravlinnia_IT-proiektamy.pdf.
2. Практикум із управління IT-проектами: Методичні вказівки та завдання до лабораторних робіт / Укл. Філіпчук О.І., Кириченко О. Л., Кириченко О.О., Малик І.В. Чернівці: Чернів. нац. ун-т ім. Ю. Федьковича, 2023. 130 с. – Режим доступу: https://archer.chnu.edu.ua/bitstream/handle/123456789/10212/%D0%A3%D0%BF%D1%80%D0%B0%D0%B2%D0%BB_%D0%86%D0%A2_%D0%BF%D1%80_%D0%BF%D1%80%D0%B0%D0%BA%D1%82%D0%B8%D0%BA%D1%83%D0%BC.pdf?sequence=1&isAllowed=y.
3. Моделювання бізнес-процесів та управління IT-проектами : електронний навчальний посібник комбінованого (локального та мережного) використання / Є. М. Крижановський, А. Р. Ящолт, С. О. Жуков. – Вінниця : ВНТУ, 2022. – 129 с. – Режим доступу: https://pdf.lib.vntu.edu.ua/books/2023/Kryzhanov_2022_129.pdf.
4. Строкань О. В., Мірошніченко М. Ю. Управління IT-проектами: лабораторний практикум. Мелітополь: Видавничо-поліграфічний центр «Люкс», 2020. 135с. – Режим доступу: http://www.tsatu.edu.ua/kn/wp-content/uploads/sites/16/uitp_praktykum_10.01.2021_hotovo.pdf.

Додаткова література

1. Управління IT-проектами в Microsoft Project: Комп'ютерний практикум: навч. посіб. / Л.М. Добровська, О.В. Аверьянова; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2020 – 152 с. – Режим доступу: <https://ela.kpi.ua/server/api/core/bitstreams/1546697f-b66b-41e3-bfb1-7ceebd1fd7d7/content>.
2. Управління IT-проектами: Загальні питання теорії управління IT-проектами: навч. посіб. / уклад.: Л. М. Добровська, О. С. Коваленко, О. А. Аверьянова; КПІ ім. Ігоря Сікорського. – Київ: КПІ ім. Ігоря Сікорського, 2022 – 284 с. – Режим доступу: <https://ela.kpi.ua/server/api/core/bitstreams/1feb7c50-e0ef-4967-9611-997f2bb6d215/content>.

3. Основи управління IT проектами [Електронний ресурс]: навч. посіб. для студ. спеціальності 122 «Комп'ютерні науки»/ КПП ім. Ігоря Сікорського; уклад.: В. О. Кузьмініх, Р. А. Тараненко. Електронні текстові дані. Київ : КПП ім. Ігоря Сікорського, 2019. 75 с. – Режим доступу: <https://ela.kpi.ua/server/api/core/bitstreams/7c313e5c-5477-4be2-9806-d32e9eace0c3/content>.
4. Чумаченко І. В. Методологія управління проектами та програмами / І. В. Чумаченко, Н. В. Косенко; Харків. нац. ун-т міськ. госп-ва ім. О. М. Бекетова. Харків : ХНУМГ ім. О. М. Бекетова, 2020. 140 с. – Режим доступу: <https://eprints.kname.edu.ua/55384/1/2019%20%D0%BF%D0%B5%D1%87.%20139%D0%9B.pdf>.
5. A Guide to the Project Management Body of Knowledge (PMBOK® Guide). Seventh Edition : Project Management Institute, 2021. 250 p. – Режим доступу: <https://tegnum.edu.pe/wp-content/uploads/2023/09/Project-Management-Institute-A-Guide-to-the-Project-Management-Body-of-Knowledge-PMBOK-R-Guide-PMBOK%C2%AE%EF%B8%8F-Guide-Project-Management-Institute-2021.pdf>.
6. Cicala G. The Project Managers Guide to Microsoft Project 2019. Apress, 2020. 681 p. – Режим доступу: <https://download.e-bookshelf.de/download/0013/4405/55/L-G-0013440555-0041915315.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
0,8	0,2		

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:

$$O = \Pi \cdot k_1 + K \cdot k_2 + I \cdot k_3 + \text{Пк} \cdot k_4$$

де: Π – середньозважена середня оцінка за поточний контроль
 I – оцінка за виконання індивідуального завдання
 K – середньозважена оцінка за контрольні роботи
 Пк – оцінка за підсумковий контроль

$$\Pi = \frac{\Pi_1 \cdot a_1 + \Pi_2 \cdot a_2 + \dots + \Pi_n \cdot a_n}{\sum_{i=1}^n a_i}$$

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

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

де: b_i - ваговий коефіцієнт за кожну контрольну роботу.

Шкала оцінювання

Поточні оцінки за кожну складову (Π , K , I , ...) виставляються за 100-бальною шкалою згідно з [положенням «Про критерії та систему оцінювання знань та вмінь і про рейтинг здобувачів вищої освіти» НТУ «ХПІ»](#).

Сума балів	Національна оцінка	ECTS
90–100	Відмінно	A
82–89	Добре	B
75–81	Добре	C
64–74	Задовільно	D

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

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