Силабус освітнього компонента
Програма навчальної дисципліни

Математичні моделі управління IT-проєктами

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
Спеціальна (фахова) підготовка, Обов'язкова

Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
2

Мова викладання
Українська

Викладачі, розробники

АКСЬОНОВА Ірина Вікторівна

Iryna.Aksonova@khpi.edu.ua
Кандидат економічних наук, 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 IT-проєктами» 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. 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)

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

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 управління IT-проєктами. Основні концепції управління проєктами. Визначення цілей, обмежень і критеріїв успішності IT-проєктів.	2
Тема 2. Математичні моделі управління проєктами. Типи математичних моделей: стохастичні, детерміновані. Основи теорії графів у плануванні проєктів.	2
Тема 3. Моделі планування часу та ресурсів. Метод критичного шляху (CPM). Метод оцінки та перегляду програм (PERT). Оптимізація ресурсів.	2
Тема 4. Оцінка ризиків та невизначеностей в IT-проєктах. Прогнозування ризиків з використанням імовірнісних моделей. Моделювання сценаріїв розвитку подій.	2
Тема 5. Лінійне програмування в управлінні IT-проєктами. Основи лінійного програмування. Задачі розподілу ресурсів.	2
Тема 6. Моделювання вартості проєкту. Методи оцінки вартості та аналізу витрат. Вплив часових затримок на вартість проєкту.	2
Тема 7. Теорія ігор у плануванні проєктів. Стратегії управління проєктами в умовах конкурентного середовища. Теорія ігор для моделювання взаємодії між командами.	2
Тема 8. Використання програмних засобів для моделювання управління проєктами. Інструменти для управління IT-проєктами (Microsoft Project, Primavera, Jira).	2

Використання симуляцій для оцінки ризиків.	
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Моделювання критичного шляху за допомогою Microsoft Project Студенти навчаються створювати діаграми Ґанта, визначати критичний шлях проєкту та оцінювати вплив окремих завдань на строки виконання.	8	0,2
Тема 2. Оцінка невизначеностей у плануванні за допомогою PERT Вивчається метод PERT для кількісної оцінки невизначеностей у тривалості завдань та прогнозування строків завершення проєкту.	6	0,1
Тема 3. Лінійне програмування для оптимізації витрат і ресурсів Розглядаються методи лінійного програмування для оптимального розподілу ресурсів і мінімізації витрат у рамках обмежень проєкту.	6	0,1
Тема 4. Аналіз ризиків у проєктах з використанням програмного забезпечення Навчання ідентифікації, оцінки та моделювання ризиків за допомогою спеціалізованого ПЗ для підтримки управлінських рішень.	6	0,1
Тема 5. Використання інструментів симуляції для аналізу ризиків та варіантів розподілу ресурсів Студенти проводять симуляції різних сценаріїв проєкту, оцінюють ризики та варіанти ефективного розподілу ресурсів для мінімізації негативного впливу на строки та бюджет.	6	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}6$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Особливості академічного письма англійською мовою. Аналіз структурних та мовних особливостей академічного тексту. Практичне опрацювання правил оформлення есе, звітів, анотацій і наукових статей англійською мовою.	0,2
Тема 2. Академічна комунікація: презентації, дискусії та публічні виступи. Вивчення принципів ефективної усної академічної комунікації. Формування навичок створення та представлення презентацій, участі в наукових обговореннях і дебатах англійською мовою.	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 проєктами Розглядаються базові поняття математичного моделювання, оптимізації та прийняття рішень у системах управління IT-проєктами.	8
Тема 2. Сітьові моделі та методи управління проєктами (CPM, PERT) Вивчаються принципи побудови та аналізу сітьових графіків, методи визначення критичного шляху та розрахунку резервів часу.	8
Тема 3. Теорія черг у плануванні проєктів Ознайомлення з моделями теорії масового обслуговування для оцінки затримок, черг та навантаження ресурсів у IT-проєктах.	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 проєктному середовищі.	7
Тема 6. Імітаційне моделювання у проєктному менеджменті Розглядаються принципи побудови симуляційних моделей, що дозволяють прогнозувати наслідки управлінських рішень.	7
Тема 7. Стохастичні процеси в управлінні IT-проєктами Вивчення моделей випадкових подій та процесів, що впливають на строки, ресурси і результати проєктів.	7
Тема 8. Економіко-математичне моделювання витрат проєкту Ознайомлення з методами побудови моделей витрат, прогнозування бюджетних потреб та оцінювання економічної ефективності.	7
Тема 9. Методи багатокритеріальної оптимізації Розглядаються підходи до прийняття рішень за кількома критеріями, зокрема баланс між вартістю, строками та якістю виконання проєкту.	7
Тема 10. Використання програмних засобів для математичного моделювання проєктів Досліджуються можливості сучасних інструментів (Excel Solver, MATLAB, Python, ProjectLibre тощо) для аналізу, оптимізації та візуалізації моделей управління IT-проєктами.	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

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

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Kerzner, Harold. Project Management: A Systems Approach to Planning, Scheduling, and Controlling. Wiley, 2017. URL: https://books.google.com.ua/books/about/Project_Management.html?id=xlASDgAAQBAJ&redir_esc=y
2. Meredith, Jack R., and Samuel J. Mantel. Project Management: A Managerial Approach. Wiley, 2018. URL: https://books.google.com.ua/books/about/Project_Management.html?id=xGRtQetWjNsC&redir_esc=y
3. Verzuh, Eric. The Fast Forward MBA in Project Management. Wiley, 2015. URL: https://books.google.com.ua/books/about/The_Fast_Forward_MBA_in_Project_Manageme.html?id=AgCJjwEACAAJ&redir_esc=y

Додаткова література

4. Cleland, David I., and Lewis R. Ireland. Project Management: Strategic Design and Implementation. McGraw-Hill, 2006. URL: https://books.google.com.ua/books/about/Project_Management.html?id=8t24QQE3lzAC&redir_esc=y
5. Lock, Dennis. Project Management. Gower Publishing, 2020. URL: https://books.google.com.ua/books/about/Project_Management.html?id=mipKLwEACAAJ&redir_esc=y
6. Pinto, Jeffrey K. Project Management: Achieving Competitive Advantage. Pearson, 2018. URL: https://books.google.com.ua/books/about/Project_Management.html?id=ffcEtAEACAAJ&redir_esc=y

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	0,2		

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:

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

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