Силабус освітнього компонента
Програма навчальної дисципліни

Основи управління в проєктах галузі кібербезпеки та захисту інформації

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

ГАВРИЛОВА Алла Андріївна

alla.havrylova@khpi.edu.ua
PhD, доцент кафедри кібербезпеки НТУ «ХПІ».

Кількість наукових публікацій: понад 50, з них патентів на корисну модель 2, 5 монографії, з яких 3 – у рецензованому виданні, що входить до бази даних Scopus, 1 – в іноземному науковому виданні, 2 – у фаховому виданні України; 14 статей, з них 7 наукових статей – у наукових фахових виданнях України, 4 наукові статті – у рецензованих виданнях, що входять до бази даних Scopus, 3 статті – в іноземних наукових виданнях. Лектор з дисциплін: «Презентація та обробка знань», «Основи управління в проєктах галузікібербезпеки та захисту інформації», «Безпека та анонімність роботи в Інтернет» у студентів магістратури

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

У межах даної дисципліни здобувачі вищої освіти досліджують процеси управління ІТ-проєктами з врахуванням використання процесів кібербезпеки та захисту інформації. Крім того, студенти практично розробляють план ІТ-проєкту з використанням визначених обмежень та проведення аналізу отриманих результатів.

Мета та цілі дисципліни

Формування системного базового уявлення, первинних знань, вміння і навичок студентів з управління проєктами в галузі кібербезпеки та захисту інформації.

Формат занять

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

Компетентності

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.
КЗ-2. Здатність проводити дослідження на відповідному рівні.
КЗ-3. Здатність до абстрактного мислення, аналізу та синтезу.
КЗ-4. Здатність оцінювати та забезпечувати якість виконуваних робіт.
КЗ-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).
КФ2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування, а також інтегрувати, аналізувати і використовувати кращі світові практики, стандарти у професійній діяльності в сфері інформаційної безпеки та/або кібербезпеки.
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.

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 – 32 год., лабораторні заняття – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Аналіз шкідливих програм, Технології управління безпекою бізнес-процесів, Безпека та анонімність роботи в Інтернеті.

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. Управління ризиками інформаційної безпеки. 1. Основні етапи циклу управління ризиками інформаційної безпеки 2. Ключові концепції управління ризиками інформаційної безпеки 3. Моніторинг та перегляд управління ризиками інформаційної безпеки	2
Тема 2. Дотримання нормативних вимог (Комплаєнс) у кібербезпеці. 1. Нормативна база комплаєнсу 2. Взаємозв'язок із управлінням ризиками в комплаєнсі 3. Процес забезпечення комплаєнсу 4. Роль комплаєнсу у бізнесі	2
Тема 3. Захист конфіденційності, цілісності та доступності (C-I-A). 1. Конфіденційність. 2. Цілісність 3. Доступність	2
Тема 4. Розвиток стартапа. 1. Ролі в проєктах 2. Проєктний менеджмент 3. Підходи до управління проєктами 4. Основні функції на проєкті для менеджеру	2
Тема 5. Управління продуктом. 1. Кейси з практики 2. Система управління в проєкті	2
Тема 6. Побудова нормальної системи управління. 1. Вартість проєктного офісу 2. Тенденції в проєктному менеджменті 3. Штучний інтелект в управління IT-проєктами	2
Тема 7. Context. Гібридний метод організації проєктів та рабочих процесів. 1. Консолідація контекста	2

2. Локальне планування 3. Систематизація змін 4. Процеси на рельсах 5. Context-driven аналітика та рішення	
Тема 8. Проведення оцінки проєктного управління. 1. Оцінка результативності таи ефективності 2. Оцінка перешкод 3. Оцінка зрілості процесів 4. Оцінка керованості 5. Оцінка зрілості автоматизації 6. Оцінка зрілості звітності 7. Оцінка зрілості нарад 8. Оцінка зрілості органів управління 9. Оцінка проєктного офісу 10. Оцінка компетенцій персоналу 11. Оцінка контроля якості процесів 12. Оцінка поведінкових змін	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти *a*
Тема 1. Розробка Статуту проєкту ІБ та визначення обсягу (Scope). 1. Загальна інформація про проєкт 2. Обґрунтування проєкту 3. Цілі проєкту 4. Обсяг проєкту 5. Критичні стейкхолдер 6. Обмеження та Припущення	6	1
Тема 2. Ідентифікація та якісна оцінка ризиків 1. Ідентифікація активів 2. Матриця якісної оцінки ризиків 3. Реєстр ризиків	5	1
Тема 3. Планування реагування на ризики та вибір контролів. 1. Оновлений реєстр ризиків із планом обробки 2. Аналіз залишкового ризику	5	1
Тема 4. Розробка WBS та оцінка ресурсів (Час/Бюджет). 1. Структура декомпозиції робіт (WBS). 2. Графік та оцінка ресурсів (Діаграма Ганта).	5	1
Тема 5. Розробка плану комунікацій та управління змінами. 1. План комунікацій для політики безпеки. 2. Шаблон запиту на зміну. 3. Обґрунтування впливу на конфіденційність, цілісність, доступність та загальний ризик.	5	2
Тема 6. Аудит відповідності (Комплаєнс). 1. Вибрані заходи контролю. 2. Чек-лист аудиту робочих станцій. 3. Звіт про невідповідності та рекомендації.	6	2

4. Висновок аудиту		
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 8$

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Додатки для планування та управління проєктами. 1. Flowlu. 2. Monday.com 3. Kissflow. 4. Wrike 5. Proofhub 6. Jira 7. TeamGantt 8. Asana 9. ClickUp 10. Trello 11. nTask 12. Goodday 13. Notion	12
Тема 2. Розрахунок вартості проєкту 1. Декомпозиція проєкту за методом ієрархічної структури робіт 2. Ліквідація абстрактного 3. Опис проєкту із здорового глузду та досвіду 4. Формування кошторису проєкту	12
Тема 3. IT-проєкти без технічних завдань 1. Інтеграція з платіжною системою 2. Вибір технологій для зберігання даних 3. Стратегічне планування без технічного розуміння	12
Тема 4. Оцінка строків IT-проєктів 1. Рівень деталізвції технічного завдання. 2. Проблеми масштабування 3. Потенційні ризики та невраховані деталі 4. Методи оцінки проєкта 5. Досвід минулих проєктів	12
Тема 5. Технічна грамотність менеджера та штучний інтелект 1. Як штучний інтелект допомагає IT-менеджеру? 2. Де штучному інтелекту не варто довіряти? 3. Кейси, де технічні знання рятують 4. Постійні зміни вимог під час розробки 5. Технічний борг 6. Невідповідність між бізнес-очікуваннями та результатом	12
Тема 6. Які ролі є в проєктах? Що коїться на практиці? 1. Продюсер 2. Геймдизайнер 3. Нарратив-дизайнер 4. Арт-директор	12

5. UI/UX-дизайнери 6. Фронтенд та серверні розробники	
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. Гвоздь М. Я., Злидник Ю. О. AGILE – нова методологія менеджменту: теоретичні аспекти. Електронний журнал «Інфраструктура ринку», 2018. № 25. С 230-234. URL: https://er.nau.edu.ua/bitstream/NAU/61366/1/%d0%a3%d0%bf%d1%80%d0%b0%d0%b2%d0%bb%d1%96%d0%bd%d0%bd%d1%8f%20%d0%86%d0%a2-%d0%bf%d1%80%d0%be%d1%94%d0%ba%d1%82%d0%b0%d0%bc%d0%b8_%d0%a4%d0%b5%d0%bd%d0%b4%d1%8c%d0%be%20%d0%9e.%20%d0%9c..pdf
2. Демиденко М. А. Управління проектами інформатизації за методологією SCRUM : навч. посіб., 2016. – Дніпро. : Нац. гірн. ун-т. – 80 с. URL: https://ir.nmu.org.ua/jspui/bitstream/123456789/151152/1/scrum%20Demydenko%20Mykhailo.pdf
3. Довгань Л. Є., Мохонько Г. А., Малик І. П. Управління проектами: навч. посіб. до вивчення дисципліни для магістрів галузі знань 07 «Управління та адміністрування» спеціальності 073 «Менеджмент», 2017. – Київ : КПІ ім. Ігоря Сікорського. – 420 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/cf735d19-339f-44c8-8b5a-42f40468edf4/content
4. Мартін Р. Чистий Agile: назад до основ / пер. з англ. В. Луненко, 2021. Харків : Вид-во «Ранок». 224 с.
5. Моделі та засоби управління IT-проєктами: навч. посіб. / уклад.: В. О. Кузьміних, О. В. Коваль, Р. А. Тараненко, 2023. Київ: КПІ ім. Ігоря Сікорського. 222 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/057779d8-d88f-4cef-b2d5-67086a013516/content
6. Моделювання бізнес-процесів та управління IT-проектами : навч. посібн. / Є. М. Крижановський, А. Р. Ящолт, С. О. Жуков, О. М. Козачко, 2018. Вінниця: ВНТУ. 91 с. URL: https://ecopy.posibnyky.vntu.edu.ua/txt/2018/Kryzanovsk_yascholt_modelyuvanna_np_p024.pdf
7. Перит І. О. Перспективи впровадження Kanban в управління бізнесом вітчизняних суб'єктів господарювання. Бізнес Інформ, 2019. № 8. С. 218-228. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=binf_2019_8_31

Додаткова література

1. Управління IT-проєктами: Загальні питання теорії управління IT-проєктами (конспект лекцій) Навчальний посібник [Електронний ресурс]: навч. посіб. для студ. спеціальності 122 «Комп'ютерні науки» / уклад.: Л. М. Добровська, О. С. Коваленко, О. А. Аверьянова; КПІ ім. Ігоря Сікорського. – Електронні текстові дані (1 файл: 3,67 Мбайт), 2022. – Київ: КПІ ім. Ігоря Сікорського. 284 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/1feb7c50-e0ef-4967-9611-997f2bb6d215/content

2. Бізнес-планування та управління проектами : навчальний посібник. / П. Г. Ільчук, Р. В. Фещкр, А. І. Якимів та ін. ; за ред. П. Г. Ільчука. Львів : Новий Світ-2000, 2023. 240 с. URL: https://ns2000.com.ua/wp-content/uploads/2019/11/Bizne-planuvannia-ta-upravlinnia-proektamy.pdf
3. Блага Н. В. Управління проєктами : навчальний посібник. Львів : ЛДУВС, 2021. 152 с. URL: http://dspace.lvduvs.edu.ua/handle/1234567890/3870
4. Дворжак В. В., Томка Ю. Я. Управління ITпроектами. Частина 1: Бізнес-аналіз та ініціація проекту. Чернівці : Технодрук, 2022. 521 с. URI: https://archer.chnu.edu.ua/xmlui/handle/123456789/6756
5. Катренко А. В. Управління IT-проектами. Книга 1. Стандарти, моделі та методи управління проектами : підручник. Львів : Новий Світ- 2000. 2017. 550 с. URL: https://pdf.lib.vntu.edu.ua/books/2018/Katrenko_Upravlin_IT_2011_550.pdf
6. Когут І. В., Ільчук П. Г., Якимів А. І. Управління командою проекту : навчальний посібник. Львів : Новий Світ-2000, 2023. 154 с.URL: https://opac.kntu.kr.ua/cgi-bin/koha/opac-ISBDdetail.pl?biblionumber=53
7. Конінг П. Інструментарій agile-лідера : учимося успішно розвиватися за допомогою самокерованих команд / пер. з англ. В. Луненко. Харків : Видавн. дім "Фабула", 2023. 224 с. URL: https://odaba.edu.ua/upload/files/Materiali_konferentsii_UP__2023.pdf
8. Корчак Н. М., Обушна Н. І. Управління проєктами в публічній сфері : навчальний посібник. Київ : Каравела, 2022. 272 с. URL: https://caravela.com.ua/index.php?route=product/product&product_id=328
9. Микитюк П. П., Брич В. Я., Микитюк Ю. І., Труш І. М. Управління проектами : навчальний посібник. Тернопіль : ЗУНУ, 2021. 416 с. URL: http://dspace.wunu.edu.ua/handle/316497/45133
10. Основи управління IT проектами : навчальний посібник. / уклад.: В. О. Кузьміних, Р. А. Тараненко. Київ : КПІ ім. Ігоря Сікорського, 2019. 75 с. URL: https://ela.kpi.ua/server/api/core/bitstreams/7c313e5c-5477 -4be2-9806-d32e9eace0c3/content
11. Петренко Н. О., Кустріч Л. О., Гоменюк М. О. Управління проектами : навчальний посібник. Київ : ЦУЛ, 2021. 244 с. URL: http://elib.chdtu.edu.ua/e-books/4216
12. Словник термінів з управління проєктами PMI. Версія 3.3. Newtown : Project Management Institute, 2022. 25 с. URL: https://pmiukraine.org/lexicon.
13. Строкань О. В., Мірошниченко М. Ю. Управління IT-проєктами : лабораторний практикум. Мелітополь: Видавничо-поліграфічний центр «Люкс», 2020. 135 с. URL: http://elar.tsatu.edu.ua/bitstream/123456789/14494/1/6.pdf
14. Хіґні, Джозеф Основи управління проектами [Електронний ресурс] / Джозеф Хіґні ; пер. з англ. Я. Машико. – 5-те вид. – Харків : Фабула, 2020. – 272 с. – режим доступу: http://elib.chdtu.edu.ua/e-books/4229

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять, тощо у відповідності до силабусу і є інтегральною оцінкою результатів усіх вид навчальної діяльності здобувача вищої освіти. Підсумкова оцінка повинна відображати всі оцінки за складовими навчального процесу з урахуванням їх вагових показників k:

Поточний контроль (практичні, семінарські, лабораторні заняття), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,6	0,4		

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

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

де: П – середньозважена середня оцінка за поточний контроль

І – оцінка за виконання індивідуального завдання
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