Силабус освітнього компонента
Програма навчальної дисципліни

СУЧАСНІ ТЕХНОЛОГІЇ БЕЗПЕЧНОГО ПРОГРАМУВАННЯ

Шифр та назва спеціальності
F7 – Комп'ютерна інженерія

Інститут
ННІ Комп'ютерних наук та інформаційних технологій

Спеціалізація
–

Кафедра
Комп’ютерна інженерія та програмування (326)

Освітня програма
Сучасне програмування, мобільні пристрої та комп'ютерні ігри

Тип дисципліни
Обов'язкова,

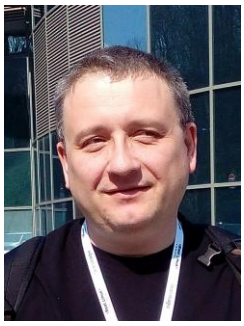
Рівень освіти
Другий (магістерський)

Форма навчання
Денна

Семестр
1

Мова викладання
Українська

Викладачі, розробники



Савченко Володимир Миколайович

кандидат технічних наук, доцент, доцент кафедри комп’ютерної інженерії та програмування НТУ «ХПІ» Має понад 100 публікацій.
Викладає курси: «Комп'ютерні мережі», «Сучасні технології безпечного програмування».
Авторські профілі: Scopus, ORCID, Web of Science.
Детальніше про викладача на сайті кафедри https://web.kpi.kharkov.ua/cep/2022/09/19/savchenko-volodymyr-mykolajovych/

Мнушка Оксана Василівна

Oksana.Mnushka@khpi.edu.ua
Магістр комп'ютерних наук, старша викладачка кафедри комп'ютерної інженерії та програмування НТУ «ХПІ». Має понад 100 публікацій.
Викладає курси «Програмування», «Розробка та застосування баз даних» та «Ризик-орієнтований аналіз в ІТ» англійською мовою.
Авторські профілі: Scopus, ORCID, Web of Science
Детальніше про викладача на сайті кафедри https://web.kpi.kharkov.ua/cep/2022/10/03/mnushka-oksana-vasylivna/

Загальна інформація

Анотація

Дисципліна спрямована на формування у студентів цілісного розуміння питань якості та ефективності програмного коду, а також забезпечення безпеки на всіх етапах життєвого циклу програмного забезпечення — від проєктування й реалізації до впровадження та супроводу. З

огляду на те, що програмні системи є ключовим елементом сучасної комп'ютерної інженерії, особлива увага приділяється актуальним практикам і проактивним заходам у сфері безпечного програмування.

Мета та цілі дисципліни

Мета навчальної дисципліни «Сучасні технології безпечного програмування» полягає у формуванні у студентів знань про сучасні методики та технології створення надійного програмного забезпечення. Курс передбачає засвоєння базових принципів дизасемблювання та реверс-інжинірингу, що дають змогу аналізувати рівень захисту програмних продуктів, код яких недоступний для вивчення. У процесі опанування дисципліни студенти набувають практичних навичок програмування з акцентом на безпечні методики розробки, що закріплюється виконанням серії практичних і лабораторних робіт.

Формат занять

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

Компетентності

ЗК6. Здатність виявляти, ставити та вирішувати проблеми.
СК2. Здатність розробляти алгоритмічне та програмне забезпечення, компоненти комп'ютерних систем та мереж, Інтернет додатків, кіберфізичних систем з використанням сучасних методів і мов програмування, а також засобів і систем автоматизації проектування.
СК3. Здатність проектувати комп'ютерні системи та мережі з урахуванням цілей, обмежень, технічних, економічних та правових аспектів.
СК10. Здатність ідентифікувати, класифікувати та описувати роботу програмно-технічних засобів, комп'ютерних систем, мереж та їхніх компонентів

Результати навчання

РН2. Знаходити необхідні дані, аналізувати та оцінювати їх.
РН4. Застосовувати спеціалізовані концептуальні знання, що включають сучасні наукові здобутки у сфері комп'ютерної інженерії, необхідні для професійної діяльності, оригінального мислення та проведення досліджень, критичного осмислення проблем інформаційних технологій та на межі галузей знань
РН10. Здійснювати пошук інформації в різних джерелах для розв'язання задач комп'ютерної інженерії, аналізувати та оцінювати цю інформацію.

Обсяг дисципліни

Денна форма навчання. Загальний обсяг дисципліни 150 (5 кредитів ECTS): лекції – 32 год., лабораторні роботи – 16 год., практичні роботи - 16 годин, самостійна робота – 86 год.
Заочна форма навчання. Загальний обсяг дисципліни 150 (5 кредитів ECTS): лекції – 4 год., лабораторні роботи – 4 год., практичні заняття - 4 год., самостійна робота – 138 год.

Передумови вивчення дисципліни (пререквізити)

Для успішного засвоєння навчальної дисципліни студенти повинні володіти базовими знаннями з програмування мовами C/C++, Assembler, Java та Python, а також мати уявлення про методи зворотної розробки, налагодження програмного забезпечення та основи веброзробки.

Особливості дисципліни, методи та технології навчання

У процесі вивчення курсу застосовуються проблемно-орієнтоване навчання, аналіз кейсів та командна робота. Для формування практичних компетентностей використовуються технології віртуалізації та інструменти зворотного інжинірингу, що забезпечують вивчення методів атак і захисту, оцінювання ризиків та контролю якості програмного забезпечення. Навчальний процес супроводжується використанням мультимедійних і хмарних сервісів Microsoft Office 365.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Вступ до безпечного програмування Вступ до курсу, огляд основних понять та завдань. Розгляд кіберзлочинності та кіберзлочинників, комп'ютерної безпеки та технічної безпеки. Обговорення впливу генеративного штучного інтелекту на технології безпечного програмування.	2
Тема 2. Огляд методів безпечного програмування Розгляд методів безпечного програмування, включаючи перевірку вхідних даних, фільтрацію вихідних даних, використання криптографії та автентифікації. Обговорення принципів захисту даних, стандартів та рекомендацій у галузі безпечного програмування (OWASP, CERT тощо). Правові та етичні аспекти безпечного програмування.	2
Тема 3. Пошкодження пам'яті та переповнення Детальний аналіз пошкодження пам'яті, проблем переповнення стека та купи. Огляд методів статичного та динамічного аналізу, які використовуються для виявлення та запобігання цих проблем.	2
Тема 4. Ін'єкції коду Дослідження різних видів ін'єкцій коду, включаючи ін'єкції команд операційної системи та SQL-ін'єкції. Обговорення безпеки скриптових мов програмування та командних оболонок.	2
Тема 5. Проблема конкурентності (перегонів) Огляд проблем конкурентності, що виникають при роботі з ресурсами. Розгляд методів запобігання перегонам, які можуть призвести до серйозних вразливостей у програмному забезпеченні.	2
Тема 6. Шкідливе програмне забезпечення та соціальна інженерія Аналіз шкідливого, рекламного та шпигунського програмного забезпечення, їх використання для експлуатації уразливостей. Методи програмування стійкості проти шкідливого коду. Основи соціальної інженерії та її вплив на кібербезпеку.	2
Тема 7. Методи безпечного програмування залежно від мови програмування Огляд специфічних методів безпечного програмування для різних мов програмування, таких як C, C++, Java, Python, JavaScript.	2
Тема 8. Віртуалізація, хмарні застосунки та безпечне програмування Огляд платформ низькорівневого програмування, віртуальних машин та їхніх засобів забезпечення безпеки. Обговорення ізоляції процесів, можливостей та дозволів як методів захисту. Обговорення типової архітектури хмарних застосунків. Обговорення проблем приватності даних на хмарних сервісах.	2
Тема 9. Загальні питання безпеки вебзастосунків Розгляд платформ вебпрограмування та методів забезпечення їх безпеки. Обговорення протоколу HTTP, форм, загроз на стороні клієнта та сервера та способів їх уникнення.	2
Тема 10. Безпека вебзастосунків - cookies, сесії та атаки Детальне вивчення питань безпеки, пов'язаних з cookies та сесіями, перенаправленнями, атаками CSRF та XXE.	2

Тема 11. Безпека програмного забезпечення мобільних пристроїв Огляд платформ мобільних операційних систем та типової архітектури мобільного застосунка. Методи безпечного програмування для ОС Android та iOS.	2
Тема 12. Життєвий цикл безпечної розробки програмного забезпечення (SSDLC) Огляд методів безпечного розгортання, огляду коду та статичного аналізу. Обговорення підтримки безпеки розгорнутих систем програмного забезпечення, включаючи проникнення та виправлення, а також перелік та класифікацію вразливостей (CVE та CWE).	2
Тема 13. Програмування безпеки на високому рівні Розгляд методів забезпечення безпеки на високому рівні та в корпоративних системах. Включає хешування та криптографію за допомогою криптографічних бібліотек, автентифікацію через GSSAPI та використання цифрового підпису.	2
Тема 14. Аналіз програмного забезпечення без доступу до вихідного коду програми Аналіз методів зворотної розробки, пакування, декомпіляції та аналізу мережевого трафіку. Огляд спроб підміни вебсервера та методів виявлення таких спроб.	2
Тема 15. Методи захисту програмного забезпечення та комп'ютерних ігор Розгляд методів захисту програмного забезпечення, таких як підписування коду, обфускація, водяні знаки, та захист від модифікацій. Обговорення криптографічних гарантій цілісності та походження, підвищення зусиль для зворотної розробки та методів виявлення змін та припинення роботи. Захист програмного забезпечення комп'ютерних ігор, методи безпечного програмування для мережних комп'ютерних ігор.	2
Тема 16. Захист програмного забезпечення на основі HMAC та електронного цифрового підпису Огляд використання HMAC для забезпечення цілісності та автентичності даних. Обговорення основ електронного цифрового підпису та його ролі у забезпеченні автентичності та невідкличності повідомлень.	2
Загальна кількість годин	**32**

Практичні заняття

Теми практичних/семінарських занять	Кількість годин	Вагові коефіцієнти а
Тема 1. Дослідження загроз безпеці вебзастосунків на основі аналізу OWASP Top 10 Знайомство зі стандартами, методологіями та інструментами оцінювання, запобігання та виявлення загроз безпеки для Web-орієнтованих застосунків. Проведення аналітичного огляду даних OWASP.	2	–
Тема 2. Дослідження онлайнових баз даних поширених вразливостей і ризиків (CVE) Дослідження обраних онлайнових баз даних вразливостей для вивчення вразливостей програмного забезпечення та створення аналітичного звіту на основі отриманої інформації.	2	–
Тема 3. Фішинг та бази даних фішингових URL	2	–

Збір, аналіз та візуалізація даних про фішингові та безпечні вебсайти з метою виявлення типових характеристик та тенденцій, які можуть допомогти в автоматичному виявленні фішингових атак. Робота також спрямована на розробку методології для виявлення потенційно шкідливих вебсайтів та подальшого вдосконалення механізмів кібербезпеки		
Тема 4. Виявлення шкідливого програмного забезпечення за допомогою YARA Набуття практичного досвіду виявлення та аналізу шкідливого програмного забезпечення за допомогою YARA – інструменту з відкритим вихідним кодом, призначеного для виявлення та класифікації зразків шкідливого програмного забезпечення.	2	–
Тема 5. Основи гешування Основи гешування, його концепції, застосування, типові проблеми гешування на прикладі некриптографічного гешування	2	–
Тема 6. Одностороннє гешування у криптографії Знайомство із методами одностороннього гешування в криптографії, основи використання гешування бібліотеки OpenSSL.	2	–
Тема 7. Використання кодів для захисту цілісності даних. Кодування інформації, кодування у сучасних комп'ютерних системах, використання кодів для захисту цілісності даних.	2	–
Тема 8. Методи забезпечення цілісності та автентичності даних Теоретичне знайомство з принципами роботи HMAC та ЕЦП. Огляд засобів та інструментів, що дозволяють реалізувати HMAC та ЕЦП. Ознайомлення зі стандартами та рекомендаціями щодо використання HMAC та ЕЦП	2	–
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i$=0

Лабораторні заняття

Теми лабораторних робіт	Кількість годин	Вагові коефіцієнти a
Тема 1. Дизасемблювання та налагодження за допомогою Radare2 Статичний і динамічний аналіз бінарних виконуваних файлів у ОС GNU/Linux за допомогою пакету утиліт Radare2	2	4
Тема 2. Аналіз формату виконуваних файлів ELF (ОС GNU/Linux) Вивчення та дослідження бінарного виконуваного файлу в ОС GNU/Linux з точки зору питань безпеки коду, що виконується.	2	4
Тема 3. Стек, управління буферами та рядки Вивчення та дослідження програмного стеку, методів управління буферами, С-рядків та пов'язаних із ними вразливостей програмного коду.	2	4
Тема 4. Експлойти. Механізми захисту від експлойтів. Зворотно-орієнтоване програмування Вивчення механізму реалізації експлойтів та методів й механізмів боротьби із ними	2	4

Тема 5. Обфускація коду, методи захисту коду від зміни Знайомство із методами обфускації та деобфускації коду, дослідження обфускації коду з точки зору зворотної розробки. Знайомство із методами захисту коду від зміни	2	2
Тема 6. Симетричне шифрування. Бібліотека OpenSSL Вивчення методів симетричного шифрування, знайомство із стандартними бібліотеками. Реалізація методів симетричного шифрування.	2	2
Тема 7. Криптографічні методи із відкритим ключем. Бібліотека OpenSSL Вивчення криптографічних методів із відкритим ключем, знайомство із стандартними бібліотеками асиметричного шифрування.	2	2
Тема 8. Реалізація методів забезпечення цілісності та автентичності даних. Реалізація алгоритмів HMAC та ЕЦП в ручному режимі або за допомогою обраної бібліотеки/засобу. Тестування та аналіз реалізованих алгоритмів на коректність та безпеку.	2	2
Загальна кількість годин	**16**	$\sum_{i=1}^{n} a_i = 24$

Контрольні роботи

Комплексний тест з сучасних технологій безпечного програмування	Вагові коефіцієнти b
Тема. Сучасні технології безпечного програмування у комп'ютерній інженерії. Тест охоплює основні теми, що вивчаються у курсі, проводиться засобами Офіс 365 (тестування у Microsoft Forms)	1
Загальна кількість годин	$\sum_{i=1}^{n} b_i = 1$

Самостійна робота

Студентам рекомендуються додаткові матеріали (відео, статті, підручники) для самостійного вивчення та аналізу, підготовки до лекційних, практичних та лабораторних занять.

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1. Вступ до безпечного програмування Опрацювання термінології та основних понять у сфері безпечного програмування.	4
Тема 2. Огляд методів безпечного програмування Вивчення стандартів OWASP, CERT та ознайомлення з етичними аспектами безпеки.	4
Тема 3. Пошкодження пам'яті та переповнення Аналіз прикладів вразливостей пам’яті та способів їхнього виявлення.	4
Тема 4. Ін'єкції коду Дослідження прикладів SQL-ін’єкцій та ін’єкцій ОС із подальшим описом механізмів захисту..	8

Тема 5. Проблема конкурентності (перегонів) Вивчення прикладів атак, пов'язаних із перегонами, та методів синхронізації ресурсів.	8
Тема 6. Шкідливе програмне забезпечення та соціальна інженерія Огляд класифікацій шкідливого ПЗ та методів соціальної інженерії.	4
Тема 7. Методи безпечного програмування залежно від мови програмування Порівняння практик безпечного програмування в C, C++, Java, Python та JavaScript.	4
Тема 8. Віртуалізація, хмарні застосунки та безпечне програмування Вивчення принципів безпеки у віртуальних машинах та хмарних сервісах.	4
Тема 9. Загальні питання безпеки вебзастосунків Ознайомлення з основними загрозами протоколу HTTP та методами їхнього запобігання	4
Тема 10. Безпека вебзастосунків - cookies, сесії та атаки Дослідження атак CSRF, XXE та методів захисту cookies і сесій.	4
Тема 11. Безпека програмного забезпечення мобільних пристроїв Аналіз особливостей безпечної розробки для Android та iOS.	4
Тема 12. Життєвий цикл безпечної розробки програмного забезпечення (SSDLC) Вивчення процесів коду-рев'ю, статичного аналізу та роботи з базами CVE/CWE.	6
Тема 13. Програмування безпеки на високому рівні Самостійна робота: ознайомлення з використанням криптографічних бібліотек, GSSAPI та цифрових підписів.	4
Тема 14. Аналіз програмного забезпечення без доступу до вихідного коду програми Вивчення методів декомпіляції та аналізу мережевого трафіку.	4
Тема 15. Методи захисту програмного забезпечення та комп'ютерних ігор Огляд обфускації, підписування коду та захисту мережних ігор.	4
Тема 16. Захист програмного забезпечення на основі HMAC та електронного цифрового підпису Дослідження використання HMAC і електронного підпису для забезпечення цілісності та автентичності даних.	4
Загальна кількість годин	**74**

Тематика індивідуальних завдань

За результатами опрацювання тем 1-3 практичних (семінарських занять) студентам пропонується підготувати тези для участі у щорічній міжнародній науково-практичній конференції магістрантів та аспірантів "Теоретичні та практичні дослідження молодих вчених". Рекомендовані напрямки дослідження:

Аналіз проблем інформаційної безпеки у сфері комп'ютерної інженерії та сучасних кіберзагроз

Порівняльний аналіз вразливостей вебзастосунків на основі OWASP Top 10 за останні п'ять років.
Аналіз динаміки поширених уразливостей у базі CVE та виявлення ключових тенденцій розвитку кіберзагроз.

Дослідження відповідності між рекомендаціями OWASP та фактичними вразливостями, зафіксованими у CVE.
Аналіз джерел фішингових URL: статистичні характеристики та їх зміни у часовій перспективі.
Вивчення основних категорій фішингових атак на основі відкритих баз даних та наукових публікацій.
Аналіз кореляції між поширенням фішингових доменів та глобальними кіберзагрозами.
Огляд методологій та джерел даних для оцінки безпеки вебзастосунків: критичний аналіз підходів.
Загальна кількість годин **12**

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

CS50's Introduction to Cybersecurity (https://cs50.harvard.edu/cybersecurity/#how-to-take-this-course)
CS50: Вступ до кібербезпеки (https://prometheus.org.ua/prometheus-free/cs50-cybersecurity/)
Junior Cybersecurity Analyst (Cisco NetAcad, https://www.netacad.com/career-paths/cybersecurity?courseLang=en-US)
Цифрова безпека на персональному рівні (https://prometheus.org.ua/prometheus-free/personal-digital-security/)

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. В. Савченко, О. Мнушка "Сучасні технології безпечного програмування" : навч. посібник, Х.: НТУ "ХПІ", 2024, 180 с.
2. В. Савченко, О. Мнушка "Сучасні технології безпечного програмування. Практикум" : навч.-метод. посіб. / – Харків : НТУ "ХПІ", 2024. – 148 с. ISBN 978-617-8238-77-3.
3. Савченко В. М., Мнушка О. В. Сучасні технології безпечного програмування : навч.-метод. посібник для самостійної роботи студентів. – Харків : НТУ "ХПІ", 2025. – 112 с.– ISBN 978-617-05-0553-8. – URI: https://repository.kpi.kharkov.ua/handle/KhPI-Press/89754
4. Сучасні технології безпечного програмування : навч.-метод. посібник / В. В. Давидов [та ін.] ; Харків : НТУ "ХПІ", 2025. – Харків : Форт, 2021. – 117 с. URL: https://repository.kpi.kharkov.ua/handle/KhPI-Press/54747.
5. С.Е. Остапов, С.П. Євсеєв, О.Г. Король "Кібербезпека: сучасні технології захисту": навч. посібник, Новий світ, 2020, 678 с. URL: http://library.kpi.kharkov.ua/en/inftechnologies/кібербезпека-сучасні-технології-захисту
6. Ю.П. Лісовська "Кібербезпека: ризики та заходи" : навч. посібник. Київ, Видавничий дім «КОНДОР», 2019, 272 с. http://library.kpi.kharkov.ua/files/new_postupleniya/kibrtz.pdf
7. Ю. А. Тарнавський "Технології захисту інформації" : підручник, Київ : КПІ ім. Ігоря Сікорського, 2018, 162 с. https://ela.kpi.ua/handle/123456789/23896

8. J. N. Helfrich "Security for software engineers", CRC Press, Taylor & Francis Group: Boca Raton, 2020. URL: http://repo.darmajaya.ac.id/4635/1/Security%20for%20Software%20Engineers%20%28%20PDFDrive%20%29.pdf
9. I. Winkler, A. T. Gomes "Advanced persistent security", Syngress / Elsevier: Amsterdam, 2017. URL: https://www.sciencedirect.com/book/9780128093160/advanced-persistent-security
10. C. Paulsen, R. Byers "Glossary of key information security terms", National Institute of Standards and Technology, 2019. https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf
11. CNSS Glossary, Committee on National Security Systems, 2022, 252 pages. URL: https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf
12. ISO/IEC 27001 Information Security Management [Online], URL: https://www.iso27001security.com/html/27001.html
13. O. Mnushka and V. Savchenko, "Security Model of IOT-based Systems," 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 2020, pp. 398-401, doi: 10.1109/TCSET49122.2020.235462
14. О.В. Мнушка, В.М. Савченко "Модель безпеки інформаційної системи на базі технологій IoT" // Вісник НТУ «ХПІ». Серія: Інформатика і моделювання. – Харків: НТУ «ХПІ». – 2019. – № 28 (1353). – С. 78 – 86. DOI: 10.20998/2411-0558.2019.28.09
15. О.В. Мнушка, Б.О. Котенко, В.М. Савченко "Аналіз вимог та розробка прототипу навчаючого програмного забезпечення для мобільних платформ" // Вісник ХНАДУ : зб. наук. пр. – Вип. 92, т. 1. – Харків, 2021. – С. 51-59. DOI: 10.30977/BUL.2219-5548.2021.92.1.51
16. V. Savchenko, O. Mnushka, "Integrating secure coding practices and risk assessment in modern software development" // Problems of informatics and modeling (PIM-2023). Abstracts of the XXIII International Scientific and Technical Conference. - Kharkiv: NTU "KhPI", 2023. – p. 96.
17. J. Liu, O. Mnushka "Modern network intrusion detection systems" // Theoretical and practical research of young scientists. The abstracts of the XVIII International Scientific and Practical Conference of Undergraduate and Postgraduate Students (19-22 November 2024) / ed. by Prof. Y.I. Sokol – Kharkiv: NTU 'KhPI', 2024. pp.36-37
18. J. Zhao, O. Mnushka "Network cybersecurity situational awareness" // Theoretical and practical research of young scientists. The abstracts of the XVIII International Scientific and Practical Conference of Undergraduate and Postgraduate Students (19-22 November 2024) / ed. by Prof. Y.I. Sokol – Kharkiv: NTU 'KhPI', 2024. pp.38-39.

Система оцінювання

Підсумкова оцінка з освітнього компонента визначається відповідальним лектором за темами, видами занять тощо відповідно 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 (лабораторні роботи), k_1	Контрольні роботи (за наявності), k_2	Індивідуальне завдання (за наявності), k_3	Підсумковий контроль (для ОК з іспитом), k_4
0,6	0,15	0,15	0,1

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.

$$\text{П} = \frac{\text{П}_1 \cdot a_1 + \text{П}_2 \cdot a_2 + \ldots + \text{П}_n \cdot a_n}{\sum_{i=1}^{8} a_i},$$

де: a_i - ваговий коефіцієнт за лабораторне заняття.

$$K = \frac{K_1 \cdot b_1}{\sum_{i=1}^{1} b_i},$$

де: b_i - ваговий коефіцієнт за контрольну роботу.

Поточні оцінки за кожну складову (П, 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».

Підсумкова оцінка виставляється відповідно до розрахованої O 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	25.08.2025		**Завідувач кафедри** Олександр ЗАКОВОРОТНИЙ
	25.08.2025		**Гарант ОП** Світлана Гавриленко