Силабус освітнього компонента
Програма навчальної дисципліни

Моделі та технології забезпечення безпеки інтелектуальних систем

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

ЄВСЕЄВ Сергій Петрович

serhii.yevseiev@khpi.edu.ua
Доктор технічних наук, професор, завідувач кафедри кібербезпеки НТУ «ХПІ».

Лауреат національної премії імені Бориса Патона.
Кількість наукових публікацій: понад 351, з них патентів на корисну модель 44, 11 монографій, з яких 10 колективних монографій, 31 навчальний посібник, з яких 4 з грифом Міністерства освіти і науки України, 149 статтей у закордонних виданнях та фахових виданнях України, з них 61 у наукометричній базі Scopus. Гарант освітньо-професійної програми "Кібербезпека" першого (бакалаврського) рівня вищої освіти. Провідний лектор з дисциплін: Математичні основи криптології, Комп`ютерні мережі, Основи криптографічного захисту, Методи криптоаналізу, Основи кібербезпеки, Сучасні проблеми постквантової криптографії, Основи наукових досліджень, Цифрова криміналістика, Етичний хакінг у студентів бакалавріата та магістратури, Методологія наукової та педагогічної діяльності в науках кіберзахисту для аспірантів.

Детальніше про викладача на сайті кафедри

ХВОСТЕНКО Владислав Сергійович

vladyslav.khvostenko@khpi.edu.ua
Кандидат економічних наук, доцент кафедри кібербезпека НТУ «ХПІ».

Автор понад 170 наукових і навчально-методичних праць (за даними Google Scholar, h-індекс – 12), у тому числі 3 монографій та навчального посібника з грифом.
Має у своєму доробку 10 патентів та 10 авторських свідоцтв.
Провідний лектор з дисциплін: «Інтелектуальна власність систем безпеки», «Правове регулювання кібербезпеки», «Авторське право у цифровому суспільстві».
Сфера наукових інтересів охоплює питання інтелектуальної власності, правового регулювання кіберпростору, інформаційної безпеки, криптографічних методів захисту, цифрові активи.

Детальніше про викладача на сайті кафедри

Загальна інформація

Анотація

Навчальна дисципліна "Моделі та технології забезпечення безпеки інтелектуальних систем" є вибірковою навчальною дисципліною. Дисципліна спрямована на засвоєння теоретичних основ, формування умінь з організації безпеки інтелектуальних систем та отримання знання технологій побудови систем рівня сучасного центру обробки даних, формування компетентностей щодо засвоєння основних способів захисту конфіденційної інформації, протидії несанкціонованому доступу та кіберзагроз.

Мета та цілі дисципліни

Знайомство з новітніми моделями та методами захисту інтелектуального кіберпростору; формування компетентностей щодо засвоєння основних способів захисту конфіденційної інформації, протидії несанкціонованому доступу та кіберзагроз.

Формат занять

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

Компетентності

КЗ–2. Здатність проводити дослідження на відповідному рівні.
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.
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.
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.
РН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
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.
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.
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.
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)

Комп'ютерні мережі, Основи машинного навчання для кібербезпеки, Інформаційна безпека держави, Основи криптографічного захисту, Виявлення вторгнень у комп'ютерні мережі (мережеві аномалії).

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. Правові аспекти інформаційної безпеки. Напрямки забезпечення інформаційної безпеки інтелектуальних систем. Законодавча та нормативно-правова база України у галузі інформаційної та /або кібербезпеки. Канали несанкціонованого отримання даних. вимикачі електромагнітних коливань. оптичні вимикачі. Елекричне поле. Способи захисту. Магнітне поле. Способи захисту. Класифікація акустичних каналів витоку інформації. Середовище поширення і спосіб перехвату. Напрямки забезпечення інформаційної безпеки. Завдання служби безпеки. Фізичні засоби захисту. Правовий і технічний захист інформації. Аналіз ризиків.	2
Тема 2. Методи захисту інформації інтелектуальних систем. Основні моделі інформаційної безпеки інтелектуальних систем. Забезпечення інформаційної безпеки. Організаційні заходи. організаційно-технічні заходи. Характеристика захисних дій. Основні визначення. захист інформації. Моделі секретних систем симетричні криптосистеми. Нелінійні вузли замін симетричних криптоалгоритмів. Блочні алгоритми. Поточні алгоритми. Асиметричні схеми шифрування. Класифікація цифрових підписів. Концептуальна модель. Дискреційне розмеження доступу. Модель адепт-50. Модель дискретного доступу Хартсона. Моделі на основі матриці доступу. Модель Харисона-Руззо-Ульмана Модель take-grant . Модель Белла-Лападули. Моделі безпеки на основі тематичної політики. Формальна специфікація та різновиди рольових моделей. Дискреційна модель Кларка-Вільсона. Теоретико-графові моделі комплексної оцінки захищеності.	2
Тема 3. Внутрішні та зовнішні загрози. Використання IDS та IPS. Ключові критерії для класифікації кіберінцидентів від легких до складних. Вразливості IP. Вразливості TCP та UDP. IP-сервіси. Корпоративні сервіси. Можливі наслідки для організації або системи при кожному рівні класифікації. Класифікатор загроз. Системи виявлення та запобігання вторгнень. Оцінювання сповіщень Security Onion. Інструменти аналізу. Генерація сповіщень. Структура правил Snort .	2
Тема 4. Управління кризовими ситуаціями та ліквідація їх наслідків.	2

Організація ефективного управління кризовими ситуаціями в критичній інфраструктурі. Реалізація концепції на прикладі ОБС України. Класифікатор загроз. Удосконалена модель інфраструктури АБС. Концептуальна та синергетична моделі безпеки. Удосконалення моделі оцінювання рівня захищеності . Координація дій різних агентів під час кризової ситуації.	
Тема 5. Підходи до побудови моделі загроз та порушника. Механізм деструктивного впливу на інформаційну систему. Джерела загроз інформації. Модель порушника інформаційної безпеки . Можливі типи порушників. Основні канали витоку інформації. Тип інсайдера. Класифікації інсайдерів за рівнем ризику. Класифікації зовнішнього порушника за наявними у нього знань про інформаційну систему організації.	2
Тема 6. Політика системи менеджменту. Система менеджменту інформаційної безпеки. (Загальна) політика інформаційної безпеки. План забезпечення безперебійної діяльності організації в разі нештатних ситуацій.	2
Тема 7. Аналіз логів. Збір, агрегація, інтерпретація. Інструменти для збору лог-даних з різних компонентів мережі та систем. Методи для агрегації лог-файлів з різних джерел в одне централізоване сховище. Нормалізація лог-даних. Техніки та алгоритми для виявлення аномалій в логах. Результати аналізу лог-файлів. Профілювання мережі та сервера. Загальна система оцінки вразливостей (CVSS). Профілювання мережі та сервера. Безпечне керування пристроями.	2
Тема 8. Управління інцидентами інформаційної безпеки інтелектуальних систем. Взаємозв'язок понять. Зміст процесу управління інцидентами. Причини виникнення інцидентів. Планування і підготовка. Принципи ефективної політики реагування на інциденти інформаційної безпеки. Ресурси і інструментарій розслідування інцидентів інформаційної безпеки. Превентивні заходи. Виявлення та аналіз інцидентів інформаційної безпеки. Ознаки інциденту. Аналіз інцидентів. Документування інциденту. Пріоритезація інцидентів. Розсилка повідомлень про інцидент. Протидія поширенню інциденту. Збір свідчень інциденту і їх обробка. Ідентифікація порушника. Процедура ліквідації наслідків інциденту. Зберігання матеріалів розслідування інцидентів.	2
Загальна кількість годин	**16**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Розгортання операційної системи для проведення аудиту інформаційної безпеки комп'ютерних мереж та інформаційних систем. Вивчення процесу встановлення та налаштування спеціалізованої ОС (наприклад, Kali Linux) для проведення аудиту ІБ. Ознайомлення з базовими інструментами тестування безпеки та принципами організації середовища аудиту.	4	0,1
Тема 2. Інструменти прихованого збору технічної інформації з інформаційної системи або комп'ютерної мережі.	4	0,1

Дослідження засобів пасивного сканування та збору даних про структуру мережі, служби, відкриті порти, конфігурації систем. Аналіз застосування reconnaissance-інструментів для етичного хакінгу.		
Тема 3. Дослідження сучасних блочних симетричних шифрів та режимів шифрування. Дослідження сучасних асиметричних криптосистем шифрування. Ознайомлення з алгоритмами AES, DES, RSA, ECC та їх режимами роботи. Порівняльний аналіз безпеки, швидкодії та застосувань симетричних і асиметричних криптосистем.	4	0,1
Тема 4. Дослідження електронного цифрового підпису. ЦП Ель Гамаля, ДСТУ 4145, ECDSA. Дослідження вразливостей системи або мережі за допомогою сканера вразливостей Nessus. Вивчення принципів побудови та перевірки цифрового підпису. Практичне дослідження реалізацій сучасних алгоритмів ЦП. Використання Nessus для виявлення вразливостей та оцінювання рівня захищеності IT-інфраструктури.	4	0,1
Тема 5. Стеганографічні методи захисту інформації. Аналіз методів приховування інформації в цифрових носіях — зображеннях, аудіо, відео. Практична реалізація стеганографічних алгоритмів та оцінювання їх стійкості до виявлення.	4	0,1
Тема 6. Статистичні дослідження генераторів випадкових та псевдовипадкових послідовностей за методикою NIST. Оцінювання якості та ентропії генераторів випадкових чисел, що використовуються у криптографії. Проведення тестів NIST STS для визначення рівня випадковості послідовностей.	4	0,1
Тема 7. Визначення вразливостей веб ресурсів та веб додатків. Сканер вразливостей – Vega. Дослідження безпеки веб-додатків, виявлення поширених вразливостей (SQL injection, XSS, CSRF). Застосування Vega для автоматизованого аналізу безпеки веб-ресурсів.	4	0,1
Тема 8. Збір технічної та чуттєвої інформації за допомогою ПЗ класу – сніфери. Засіб дослідження вразливостей безпровідних мереж Wi-Fi – Aircrack-ng. Використання мережевих аналізаторів (Wireshark, tcpdump) для перехоплення та аналізу трафіку. Практичне застосування Aircrack-ng для оцінювання захисту бездротових мереж та виявлення слабких точок у Wi-Fi безпеці.	4	0,1
Загальна кількість годин	**32**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. Правові аспекти, методи захисту інформації, моделі інформаційної безпеки, внутрішні та зовнішні загрози.. Охоплює вивчення нормативно-правової бази України у сфері кібербезпеки, основних каналів витоку інформації, моделей захисту даних, криптосистем та принципів роботи систем IDS/IPS.	0,1

Тема 2. Управління кризовими ситуаціями, моделі загроз і порушників, політика безпеки, аналіз логів, управління інцидентами.. Включає розгляд процесів реагування на кіберінциденти, побудову моделі порушника, методів аналізу логів, формування політики інформаційної безпеки та плану відновлення діяльності.	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,2

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріалу

Теми для самостійного вивчення	Кількість годин
Тема 1 Правові та нормативні основи інформаційної безпеки інтелектуальних систем. Вивчення законодавства України, міжнародних стандартів та нормативних документів у сфері кібербезпеки та захисту інформації інтелектуальних систем.	8
Тема 2. Моделі загроз та порушників інформаційної безпеки. Аналіз можливих типів внутрішніх і зовнішніх атакувальників, джерел загроз та їх класифікації для інтелектуальних систем.	8
Тема 3. Основні моделі та політики інформаційної безпеки. Дослідження концепцій дискретного та мандатного контролю доступу, моделей Белла-Лападули, Хартсона, Кларка-Вільсона, RBAC та MAC, а також їх застосування в ІС.	7
Тема 4. Методи захисту інформації інтелектуальних систем. Огляд організаційних, технічних та криптографічних заходів захисту, включно із симетричним та асиметричним шифруванням, цифровими підписами та стеганографією.	7
Тема 5. Системи виявлення та запобігання вторгнень (IDS/IPS). Принципи роботи систем виявлення та запобігання атак, налаштування правил, аналіз сповіщень та інтеграція в корпоративні середовища.	7
Тема 6. Управління кризовими ситуаціями та ліквідація наслідків інцидентів. Організація реагування на інциденти, координація дій персоналу та відновлення функціонування інтелектуальної системи.	7
Тема 7. Аналіз логів та моніторинг безпеки. Збір, агрегація, нормалізація та інтерпретація лог-файлів із різних компонентів ІС. Методи виявлення аномалій і профілювання системи.	7
Тема 8. Статистичні та криптографічні методи оцінки безпеки. Дослідження генераторів випадкових і псевдовипадкових чисел, криптографічних алгоритмів та їх стійкості до атак.	7
Тема 9. Безпека мережевих та веб-компонентів інтелектуальних систем. Оцінка вразливостей веб-додатків і мережевих сервісів, використання сканерів вразливостей (Nessus, Vega), рекомендації щодо підвищення безпеки.	7
Тема 10. Стратегії управління інформаційною безпекою в інтелектуальних системах. Розробка політик безпеки, планів забезпечення безперебійної роботи та превентивних заходів для захисту критичних компонентів ІС.	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 CISCO «DevNet»
https://www.netacad.com/catalogs/learn?category=course.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Євсеєв С.П. Кібербезпека: сучасні технології захисту. / Євсеєв С.П, Остапов С.Е., Король О.Г. // Навчальний посібник для студентів вищих навчальних закладів. Львів: “Новий Світ- 2000”, 2019. – 678. [Електронний ресурс]. – Режим доступу: http://ns2000.com.ua/wp-content/uploads/2019/11/Kiberbezpeka-suchasni-tekhnolohii-zakhystu.pdf.
2. Bonaventure O. Computer Networking: Principls, Protocols and Practice. - Louvain-la-Neuve: Universite catholique de Louvain (Belgium), 2019. - 272 p. [Електронний ресурс]. – Режим доступу: https://resources.saylor.org/wwwresources/archived/site/wp-content/uploads/2012/02/Computer-Networking-Principles-Bonaventure-1-30-31-OTC1.pdf.
3. С. П. Євсеєв, О. Ю. Йохов, та О. Г. Король Гешування даних в інформаційних системах. Монографія. Харків, Україна: Вид. ХНЕУ, 2013. [Електронний ресурс]. – Режим доступу: http://repository.hneu.edu.ua/jspui/bitstream/123456789/6813/1/%D0%93%D0%B5%D1%88%D1%83%D0%B2%D0%B0%D0%BD%D0%BD%D1%8F%20%D0%B4%D0%B0%D0%BD%D0%B8%D1%85%20%D0%B2%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B8%D1%85%20%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0%D1%85%20%D0%BC%D0%BE%D0%BD%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D1%96%D1%8F.pdf
4. Євсєев С.П. Кібербезпека: основи кодування та криптографії/ С.П. Євсеєв, О.В. Мілов, С.Е. Остапов, О.В. Сєвєрінов. – Харків: Вид. “Новий Світ-2000”, 2023. – 657 с. [Електронний ресурс]. – Режим доступу: https://acrobat.adobe.com/id/urn%3Aaaid%3Asc%3AEU%3A3c427761-01ab-4365-88f6-37f76ca508c5/?x_api_client_id=chrome_extension_viewer&bookmarkAcrobat=true&x_api_client_location=bookmark&filetype=application%2Fpdf&viewer%21megaVerb=group-discover
5. Енсон С. Реагування на комп'ютерні інциденти. Прикладний курс / . Стив Енсон. ДМК Пресс, 2021. - 436 с. [Електронний ресурс]. – Режим доступу:
6. Johnson, Leighton. Computer incident response and forensics team management: conducting a successful incident response / Leighton Johnson. Elsevier Inc., 2014. – 349 p. [Електронний ресурс]. – Режим доступу: https://www.google.com.ua/books/edition/Computer_Incident_Response_and_Forensics/6lJxGXfLWkYC?hl=ru&gbpv=1&dq=Johnson,+Leighton.+Computer+incident+response+and+forensics+team+management:+conducting+a+successful+incident+response+/+Leighton+Johnson.+Elsevier+Inc.,+2014.+%E2%80%93+349+p.&printsec=frontcover
7. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p. [Електронний ресурс]. – Режим доступу: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
8. Models of socio-cyber-physical systems security: monograph / S. Yevseiev, Yu. Khokhlachova, S. Ostapov, O.Laptiev and others. - Kharkiv: PC TECHNOLOGY CENTER, 2023. - 168 p. [Електронний ресурс]. – Режим доступу: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju

9. Modeling of security systems for critical infrastructure facilities: monograph / S. Yevseiev, R. Hryshchuk, K. Molodetska, M. Nazarkevych and others. - Kharkiv: PC TECHNOLOGY CENTER, 2022. - 196 p. [Електронний ресурс]. – Режим доступу: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

Додаткова література

10. ISO/IEC 15408-1:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 1: Introduction and general model. URL: https://www.iso.org/search.html?q=15408-1.
11. ISO/IEC 15408-2:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 2: Security functional components. URL: https://www.iso.org/search.html?q=15408-2&hPP=10&idx=all_en&p=0.
12. ISO/IEC 15408-3:2022 Information security, cybersecurity and privacy protection – Evaluation criteria for IT security – Part 3: Security assurance components. URL: https://www.iso.org/search.html?q=15408-3&hPP=10&idx=all_en&p=0.
13. ISO/IEC 31010:2019 Risk management — Risk assessment techniques
5. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
14. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls
15. ISO/IEC 27003:2017 Information technology — Security techniques — Information security management systems — Guidance
16. ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks.
17. ISO/IEC 27032:2023 Cybersecurity — Guidelines for Internet security

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:

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

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