Силабус освітнього компонента
Програма навчальної дисципліни

Комплексний тренінг

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
Обов'язкова

Рівень освіти
Перший (бакалаврський)

Форма навчання
Денна, заочна

Семестр
8

Мова викладання
Українська, англійська

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

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 дисципліна "Комплексний тренінг" є обов`язковою навчальною дисципліною. Дисципліна спрямована на набуття студентами практичних навичок щодо виявлення та протидії сучасним загрозам в кіберпросторі.

Мета та цілі дисципліни

Формування у студентів практичних навичок щодо виявлення та протидії сучасним загрозам в кіберпросторі на основі відпрацювання практичних завдань.

Формат занять

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

Компетентності

ЗК1. Здатність застосовувати знання у практичних ситуаціях.
ЗК2. Знання та розуміння предметної області і розуміння професійної діяльності.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.
ЗК8. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.
СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації
СК2. Здатність використовувати інформаційні технологій, сучасні методи і моделей кібербезпеки та систем захисту інформації.
СК4. Здатність забезпечувати захист інформації в інформаційних системах згідно встановленої політики кібербезпеки та захисту інформації.
СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо).
СК7. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та кібербезпекою.

СК8. Здатність застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.
СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно з встановленою політикою інформаційної безпеки.

Результати навчання

РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.
РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.
РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.
РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення та передачі сигналів тощо, принципи, методи і поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.
РН8. Застосовувати знання й розуміння математики та фізики в професійній діяльності, формалізувати задачі предметної галузі кібербезпеки та захисту інформації, формулювати їх математичну постановку та обирати раціональний метод вирішення.
РН9. Вміти застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.
РН10. Вміти використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.
РН12. Застосовувати методи захисту інформації в інформаційних системах згідно встановленої політики інформаційної безпеки.
РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних та програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування інформаційних систем та\або інфраструктури організації в цілому.
РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації в інформаційних системах.
РН17. Забезпечувати функціонування системи управління кібербезпекою та захистом інформації організації, включаючи персонал та управління наслідками реалізації загроз інформаційній безпеці в кризових ситуаціях, на основі здійснення процедур кількісної і якісної оцінки ризиків.
РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.
РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.
РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування та контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.
РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору та інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

Обсяг дисципліни

Загальний обсяг дисципліни 120 год. (4 кредити ECTS): лекції – 24 год., лабораторні роботи – 24 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Антивірусний захист інформації, Комплексні системи захисту інформації.

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. Впровадження коду. Некоректна автентифікація і управління сесією. Виявлення ін'єкцій, таких як SQL, NoSQL, ОС та ін'єкція LDAP, які виникають, коли ненадійні дані надсилаються інтерпретатору як частина команди чи запиту. Виявлення функцій іплікації, які пов'язані з автентифікацією та керуванням сеансом, що дозволяє зловмисникам компрометувати паролі, ключі або скельні маркери або використовувати інші недоліки впровадження, щоб тимчасово або назавжди припустити особистість інших користувачів.	3
Тема 2. Міжсайтовий скриптинг (XSS). Виявлення веб-додатків та API, які не захищені належним чином. Зловмисники можуть вкрасти або змінити такі слабко захищені дані, щоб вчинити шахрайство з кредитною карткою, крадіжку особи або інші злочини.	3
Тема 3. Небезпечні прямі посилання на об'єкти. Небезпечна конфігурація. Аналіз старих або погано налаштованих процесорів XML оцінюють посилання зовнішніх об'єктів у документах XML. Зовнішні об'єкти можуть використовуватися для розкриття внутрішніх файлів за допомогою обробника URI файлів, обміну внутрішніми файлами, сканування внутрішніх портів, віддаленого виконання коду та відмови в атаці служби. Аналіз обмеження щодо дозволених користувачів, які дозволено робити, часто не виконуються належним чином. Зловмисники можуть використовувати ці недоліки для доступу до несанкціонованих функціональних можливостей та / або даних, таких як доступ до облікових записів інших користувачів, перегляд конфіденційних файлів, зміна даних інших користувачів, зміна прав доступу тощо.	3
Тема 4. Витік чутливих даних – оцінка конфігурації безпеки. Зазвичай це результат небезпечних конфігурацій за замовчуванням, неповних або спеціальних конфігурацій, відкритого хмарного сховища, неправильно налаштованих заголовків HTTP та багатослівних повідомлень про помилки, що містять конфіденційну інформацію. Не тільки всі операційні системи, рамки, бібліотеки та додатки повинні бути надійно налаштовані, але вони повинні бути виправлені / модернізовані своєчасно.	3

Тема 5. Відсутність контролю доступу до функціонального рівня. Визначення недоліків XSS, які виникають щоразу, коли програма включає недовірені дані на новій веб-сторінці без належної валідації або не відкриття, або оновлює наявну веб-сторінку за допомогою наданих користувачем даних за допомогою API браузера, який може створювати HTML або JavaScript. XSS дозволяє зловмисникам виконувати скрипти в браузері жертви, які можуть захоплювати сеанси користувачів, знищувати веб-сайти або перенаправляти користувача на шкідливі сайти.	3
Тема 6. Підробка міжсайтових запитів (CSRF). Оцінка небезпечної десеріалізації, яка часто призводить до віддаленого виконання коду. Навіть якщо дефери дезаріалізації не призводять до віддаленого виконання коду, їх можна використовувати для виконання атак, включаючи атаки відтворення, атаки ін'єкції та напади ескалації привілеїв.	3
Тема 7. Використання компонентів з відомими уразливостями. Аналіз компонент, таких як бібліотеки, рамки та інші програмні модулі, які працюють із тими ж привілеями, що і додаток. Якщо використовується вразливий компонент, така атака може полегшити серйозні втрати даних або захоплення сервера. Програми та API, що використовують компоненти з відомою вразливістю, можуть підірвати захисні програми та включити різні атаки та впливи.	3
Тема 8. Невалідовані редіректи. Виявлення недостатнього обліку та моніторингу у поєднанні з відсутньою або неефективною інтеграцією з реакцією на інцидент дозволяє зловмисникам надалі атакувати системи, підтримувати стійкість, перетворювати на більші кількості систем, а також підробляти, витягувати або знищувати дані. Більшість досліджень щодо порушення виявляють час виявлення порушення понад 200 днів, як правило, виявляються зовнішніми сторонами, а не внутрішніми процесами чи моніторингом.	3
Загальна кількість годин	**24**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Впровадження коду (Injection). Огляд видів ін'єкцій: SQL, NoSQL, OS-команди, LDAP, XPath. Налаштування тестового додатку та бази даних для ін'єкцій. Виявлення вразливостей через ручні запити та автоматизовані сканери. Експлуатація: прості SQL-ін'єкції (логін, витяг даних), Blind SQL. Захист: підготовлені запити (prepared statements), ORM, валідація вводу, параметризація. Логування та моніторинг спроб ін'єкцій.	2	0,1
Тема 2. Некоректна автентифікація і управління сесією. Механізми автентифікації: паролі, багатофакторна автентифікація, OAuth/OpenID Connect. Налаштування сесійного середовища (cookies, JWT). Виявлення проблем: слабкі паролі, відновлення паролю, brute-force, незахищені токени. Експлуатація: підбір паролів, маніпуляція сесіями, крадіжка cookies. Захист: політики паролів, MFA, secure/HttpOnly cookies, регенерація сесій після логіну, TTL для токенів. Тестування відновлення пароля та	2	0,1

механізмів блокування облікових записів. Контроль: аудит сесій, інструменти для тестування автентифікації.		
Тема 3. Міжсайтовий скриптинг (XSS). Типи XSS: Stored, Reflected, DOM-based. Підготовка середовища з уразливими полями. Виявлення XSS ручними ін'єкціями та сканерами. Демонстрація експлуатації: відображення скрипта в різних контекстах (HTML, attribute, JS). Захист: правильної ескейпінг/енкодинг, CSP, валідація та санітизація вводу на боці сервера і клієнта. Тестування політик Content Security Policy (CSP).	2	0,1
Тема 4. Небезпечні прямі посилання на об'єкти (IDOR / Insecure Direct Object References). Пояснення моделі доступу до об'єктів і шляхів доступу (ID, шляхи файлів). Налаштування середовища з ресурсами, доступ до яких контролюється ID. Виявлення: тестування змінних ID, некоректні посилання, вертикальне/горизонтальне підміни. Експлуатація: доступ до чужих ресурсів шляхом зміни параметрів. Захист: авторизаційні перевірки, непрямі посилання/токени, перевірки прав доступу на сервері.	2	0,1
Тема 5. Небезпечна конфігурація. Перелік поширених помилок конфігурації (debug режим, default credentials, verbose errors). Налаштування вразливого сервера/додатку для тестування. Виявлення: сканування відкритих портів, небезпечні заголовки, неправильні права доступу. Експлуатація: використання відкритих сервісів, отримання метаданих, доступ до конфігфайлів. Захист: мінімізація привілеїв, закриття непотрібних сервісів, безпечні заголовки (HSTS, X-Frame-Options), hardening серверів. Контроль змін конфігурацій та управління секретами (секрет-менеджери).	2	0,1
Тема 6. Витік чутливих даних – оцінка конфігурації безпеки. Ідентифікація «чутливих» даних (PII, кредити, ключі API). Методи витоку: логування, резервні копії, неправильні ACL, відкриті S3/страти. Виявлення: пошук секретів у репозиторіях, огляд логів, аудит баз даних і хмарних сховищ. Експлуатація прикладів витоків (експортування секретів у тестовому середовищі). Захист: шифрування у спокої та при передачі, обмеження доступу, ротація ключів, DLP-політики. План реагування на витік і повідомлення постраждалих.	2	0,1
Тема 7. Відсутність контролю доступу до функціонального рівня (Broken Function Level Authorization). Різниця між контролем доступа на ресурсному і функціональному рівні. Побудова сценаріїв: привілеї адміністратора vs користувача. Виявлення: доступ до API-ендівпойнтів без належної перевірки ролей. Експлуатація: виклик прихованих/адмінських функцій через API. Захист: централізовані перевірки прав, ролевий контроль доступу (RBAC), тестування авторизації. Автоматизовані тести для перевірки функціональних прав.	2	0,1
Тема 8. Підробка міжсайтових запитів (CSRF). Механізм CSRF і вразливі шаблони (state-changing requests без токена). Налаштування середовища з формами/запитами, що змінюють стан. Виявлення: аналіз відсутніх CSRF-токенів,	2	0,1

реферальні/Origin-перевірки. Експлуатація: створення PoC сторінки, яка виконує небажану дію. Захист: використання CSRF-токенів, SameSite cookies, перевірка Origin/Referer, double-submit cookie. Тест-кейси і автоматизоване сканування на CSRF.		
Тема 9. Використання компонентів з відомими уразливостями. Інвентаризація компонентів (бібліотеки, фреймворки, контейнерні образи). Налаштування проєкту з вразливими версіями залежностей. Виявлення: SCA-інструменти (наприклад, OWASP Dependency-Check), пошук CVE. Експлуатація: демонстрація відомої вразливості у тестовому середовищі. Захист: регулярні оновлення, політики прийняття патчів, використання SBOM, фіксація версій. Процес реагування: швидке виправлення, тестування регресій.	4	0,1
Тема 10. Невалідовані редіректи (Open Redirects). Пояснення ризику та сценарії використання (фішинг, втручання в довіру). Налаштування тестового додатку з параметризованими редіректами. Виявлення: сканування параметрів redirect/return_to, перевірка синтаксису URL. Експлуатація: створення посилання для фішингу в тестовому домені. Захист: білдлістинг дозволених доменів, відмова від редіректів на зовнішні URL, валідація та ескейпінг.	4	0,1
Загальна кількість годин	**24**	$\sum_{i=1}^{n} a_i = 1$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b
Тема 1. еоретичні основи безпеки веб-додатків та уразливості OWASP Top 10. Класифікація основних уразливостей за OWASP Top 10. Ін'єкційні атаки (SQL, OS, NoSQL): механізм, приклади, методи захисту. Некоректна автентифікація та управління сесіями – типові проблеми. Міжсайтовий скриптинг (XSS) – види, приклади експлуатації.	0,1
Тема 2. Практичні аспекти тестування і захисту веб-додатків. Виявити потенційні проблеми конфігурації безпеки (debug mode, заголовки, доступ до ресурсів). Проаналізувати приклад коду з уразливістю IDOR (небезпечні прямі посилання на об'єкти). Запропонувати механізми захисту від CSRF. Оцінити ризики використання застарілих компонентів у проєкті.	0,1
Тема 3. Управління доступом і захист чутливих даних. Моделі контролю доступу: DAC, MAC, RBAC, ABAC – порівняння. Приклади порушень контролю доступу на функціональному рівні. Методи запобігання витоку чутливих даних (шифрування, токенізація, DLP).	0,1
Загалом	$\sum_{i=1}^{m} b_i$=0,3

Самостійна робота

До самостійної роботи відноситься самостійне опрацювання теоретичного матеріалу

Опрацювання теоретичного матеріал

Теми для самостійного вивчення	Кількість годин
Тема 1. Основи інформаційної безпеки та загальні принципи захисту систем.	8
Тема 2. Модель загроз OWASP Top 10. Класифікація, ризики та приклади атак.	8
Тема 3. Ін'єкційні атаки (SQL, NoSQL, OS, LDAP). Механізми, інструменти пошуку, методи захисту.	7
Тема 4. Автентифікація та управління сесіями. Сучасні методи, слабкі місця, рекомендації OWASP.	7
Тема 5. Міжсайтовий скриптинг (XSS). Види XSS, приклади експлуатації, CSP як метод захисту.	7
Тема 6. Контроль доступу. Принципи RBAC, ABAC; типові помилки у веб-додатках.	7
Тема 7. Захист конфігурацій та секретів. Керування паролями, ключами, змінними середовища.	7
Тема 8. Витік даних і безпечна робота з чутливою інформацією. PII, GDPR, методи захисту.	7
Тема 9. Захист від CSRF та атак на довіру користувача. Приклади експлуатації, практичні рішення.	7
Тема 10. Компоненти з відомими уразливостями та практики DevSecOps. Інвентаризація залежностей, оновлення, SBOM.	7
Загалом	**72**

Тематика індивідуальних завдань

Реферат передбачає виконання індивідуального звіту, розкривати обрану тематику, демонструвати вміння аналізувати інформацію та оформлювати текстові документи відповідно до мети навчальної дисципліни. Здобувач обирає конкретну тему в межах загальної тематики за погодженням з викладачем. Обсяг звіту: 8–12 сторінок основного тексту. Звіт має бути оформлений відповідно до вимог, наведених у літературному джерелі [2]. Завдання виконується протягом навчальних тижнів і подається на перевірку до екзамену.

Теми індивідуального завдання	
Тема 1. Сучасні методи захисту інформаційних систем	
Тема 2. Вплив соціальної інженерії на безпеку інформації	
Тема 3. Аналіз кіберзагроз та кіберінцидентів у критичній інфраструктурі	
Тема 4. Методи оцінки вразливостей інформаційних систем	
Тема 5. Сучасні стандарти та нормативи інформаційної безпеки	
Тема 6. Шифрування та криптографічний захист інформації	
Тема 7. Роль комплексних тренінгів у підвищенні кібербезпеки організацій	
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. Kali Linux Web Penetration Testing Cookbook, Second Edition (Packt Publishing) URL: https://www.packtpub.com/product/kali-linux-web-penetration-testing-cookbook-second-edition/9781788991513.
2. Система стандартів з організації навчального процесу. ТЕКСТОВІ ДОКУМЕНТИ У СФЕРІ НАВЧАЛЬНОГО ПРОЦЕСУ. Загальні вимоги до виконання. СТЗВО-ХПІ-3.01-2025. https://blogs.kpi.kharkov.ua/v2/metodotdel/wp-content/uploads/sites/28/2025/06/STZVO-HPI-3.01-2025-2.pdf
3. Зразок звіту з тестування на проникнення URL: https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf.
4. Зразок технічного звіту з проникнення URL: https://tbgsecurity.
5. OWASP Top 10: issues in the 10 most critical security risk categories in your web applications URL: https://www.sonarqube.org/features/security/owasp/?gads_campaign=Europe-1-Generic&gads_ad_group=OWASP&gads_keyword=owasp%20top%2010&gclid=CjwKCAiAsNKQBhAPEiwAB-I5zQywzTKai6fcrilMphlAn21CRehrI0q9DEjUZNpHUoDt5V_bVpLm4RoClIkQAvD_BwE.
6. Технології захисту інформації./ С. Е. Остапов, С. П. Євсєєв, О.Г. Король. – Чернівці : Чернівецький національний університет, 2013. – 471 с.
http://kist.ntu.edu.ua/textPhD/tzi.pdf
7. Євсєєв 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.
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

Додаткова література

8. Встановлення Metasploitable 2 URL: https://metasploit.help.rapid7.com/docs/metasploitable-2.
9. Збірка Metasploitable 3 URL: https://github.com/rapid7/metasploitable3.
10. Synergy of building cybersecurity systems: monograph / S. Yevseyev, V. Ponomarenko, O. Laptiev, O. Milov and others. - Kharkiv: PC TECHNOLOGY CENTER, 2021. - 188 p. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
11. 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. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju
12. 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. URL: https://drive.google.com/drive/u/1/folders/1wOTN8N-GBGO06AnvjQHU1SdBl3xCaUju.

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
0,7	0,3		

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** Сергій ЄВСЕЄВ