Силабус освітнього компонента
Програма навчальної дисципліни

Цифрова криміналістика

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
1

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

Загальна інформація

Анотація

Вивчення дисципліни спрямовано на освоєння основних понять та методів цифрової криміналістики, навиків збору цифрової криміналістичної інформації за допомогою інструментів з відкритим кодом з операційних систем Windows та Linux.

Мета та цілі дисципліни

Формування знань і вмінь проводити первинні криміналістичні розслідування порушень кібербезпеки. Основними завданнями вивчення дисципліни "Цифрова криміналістика" є отримання знань щодо криміналістичних досліджень сучасних інформаційних систем і носіїв даних, а також формування вмінь проводити первинні криміналістичні розслідування порушень кібербезпеки. Предметом навчальної дисципліни є основні поняття та методи цифрової криміналістики, навики збору цифрової криміналістичної інформації за допомогою інструментів з відкритим кодом з операційних систем Windows та Linux.

Формат занять

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

Компетентності

КЗ–3. Здатність до абстрактного мислення, аналізу та синтезу.
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.
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.

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.
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 роботи – 16 год., самостійна робота – 72 год.

Передумови вивчення дисципліни (пререквізити)

Математичні основи криптології, Основи криптографічного захисту, Основи програмування, Аналіз шкідливих програм.

Особливості дисципліни, методи та технології навчання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються презентації, бесіди, індивідуальні групові проєкти, майстер-класи.

Програма навчальної дисципліни

Навчальні заняття

Лекції

Теми лекцій	Кількість годин
Тема 1. Вступ. Цілі та завдання навчальної дисципліни «Цифрова криміналістика». Місце дисципліни у навчальному процесі підготовки спеціаліста з кібербезпеки. Структура, зміст тематичного плану вивчення дисципліни; навчально-методична література. Особливості вивчення дисципліни; форми контролю знань, умінь та навичок учнів. Напрями науково-дослідної роботи студентів.	2
Тема 2. Електронні (цифрові) докази. Цифрові дані як докази: визначення, роль, типи, характеристика, законодавчі вимоги. Характеристика криміналістичних досліджень. Типи кіберзлочинів, проблеми розслідувань, загальні правила криміналістичних досліджень. Правила поводження із електронними доказами. Типи електронних доказів. Криміналістичні дослідження як складова реагування на інциденти порушення кібербезпеки. Ролі та обов'язки осіб, що проводять криміналістичні дослідження.	2
Тема 3. Процес первинних цифрових криміналістичних досліджень. Фази первинних цифрових криміналістичних досліджень. Вимоги до обладнання, ролі учасників первинних цифрових криміналістичних досліджень. Пошук, виявлення, збір, фіксація і збереження електронних доказів. Порядок передачі та зберігання (chain of custody) електронних доказів. Створення дублікатів, відновлення даних і первинна експертиза електронних доказів. Звіт про криміналістичні дослідження і свідчення у суді.	2
Тема 4. Структура жорсткого диску та файлових систем. Типи жорстких дисків зберігання даних, їх характеристики. Фізична та логічна структура жорстких дисків. Розділи жорстких дисків. Завантаження з диску ОС Windows, Linux, Mac. Файлові системи ОС Windows, Linux, Mac. Відмінності різноманітних RAID систем зберігання. Порядок аналізу файлових систем.	2

Тема 5. Вилучення даних та створення дублікатів носіїв даних. Загальний опис процесу вилучення даних. Вилучення динамічних даних (live data). Вилучення статичних даних (static data). Послідовність у вилученні та дублюванні даних. Забезпечення незмінності оригінальних носіїв даних. Визначення підходящих методів і засобів вилучення даних. Вилучення даних з Windows і Linux комп'ютерів. Найкращі практики вилучення даних.	2
Тема 6. Методи протидії криміналістичним дослідженням. Поняття протидії криміналістичним дослідженням. Методи протидії криміналістичним дослідженням. Отримання доказів з видалених файлів і розділів, зашифрованих файлів, стеганографічних об'єктів. Ідентифікація обфускації, витирання залишків, перезапису даних та метаданих, шифрування. Криптографічні мережні протоколи, програмні пакувальники, руткіти як методи протидії криміналістичним дослідженням. Контрзаходи протидії криміналістичним дослідженням. Основні виклики у подоланні протидії криміналістичним дослідженням.	2
Тема 7. Криміналістичні дослідження операційних систем. Порядок збору і огляду летючих і нелетючих даних з Windows комп'ютерів. Аналіз пам'яті і реєстру Windows. Огляд кешу, куків та історії веб-браузерів Windows.. Огляд файлів і метаданих в Windows. Аналіз журналів подій Windows. Аналіз журналів подій Linux. Збір і огляд летючих і нелетючих даних з Linux комп'ютерів. Аналіз файлів і журналів подій Mac комп'ютерів.	2
Тема 8. Криміналістичні дослідження комп'ютерних мереж. Сутність криміналістичного дослідження комп'ютерних мереж. Протоколювання трафіку комп'ютерної мережі. Принципи взаємозв'язків подій. Підготовка і етапи проведення криміналістичного дослідження комп'ютерних мереж. Огляд маршрутизатору, міжмережного екрану, системи виявлення вторгнень, DHCP-сервера, баз даних. Огляд трафіку. Документування отриманих із мережі доказів. Реконструкція доказів.	2
Тема 9. Криміналістичні дослідження веб-атак. Сутність криміналістичного дослідження веб-атак. Архітектура веб-застосунків і виклики їх криміналістичного дослідження. Індикатори веб-атак і визначення загроз веб-застосункам. Етапи проведення криміналістичного дослідження веб-атак. Криміналістичне дослідження веб-атак на Windows сервери. Архітектура IIS веб-сервера і криміналістичний аналіз його лог- файлів. Архітектура Apache веб-сервера і криміналістичний аналіз його лог-файлів. Розслідування різноманітних атак на веб-застосунки.	2
Тема 10. Криміналістичні дослідження баз даних. Сутність криміналістичного дослідження баз даних. Криміналістичне дослідження MS SQL. Виявлення репозиторіїв баз даних і збір файлів-доказів. Огляд файлів з використанням SQL Management Studio і ApexSQL DBA. Криміналістичне дослідження MySQL. Архітектура MySQL і визначення структури тек даних. Інструменти криміналістичного дослідження MySQL. Криміналістичне дослідження MySQL на WordPress.	2
Тема 11. Криміналістичні дослідження хмарних сервісів. Технології хмарних обчислень. Відомі атаки на технології хмарних обчислень. Сутність криміналістичного дослідження технології хмарних обчислень. Завдання криміналістичного дослідження хмарних сервісів. Відмінності різних типів криміналістичного дослідження хмарних сервісів. Ролі зацікавлених сторін у криміналістичному дослідженні хмарних сервісів. Виклики, що виникають під час проведення криміналістичного дослідження хмарних сервісів. Криміналістичне дослідження хмарних сховищ Dropbox та Google Drive	2

Тема 12. Криміналістичні дослідження шкідливого програмного забезпечення. Шкідливе програмне забезпечення (ШПЗ) та шляхи його впровадження в систему. Методи розповсюдження ШПЗ. Основні складові ШПЗ. Принципи криміналістичного дослідження ШПЗ. Ідентифікація і вилучення ШПЗ з включеної і виключеної системи. Створення лабораторії і середовища з аналізу шкідливих програм. Правила лабораторного аналізу ШПЗ. Динамічний і статичний аналіз. Виклики, що виникають під час проведення криміналістичного дослідження ШПЗ.	2
Тема 13. Криміналістичні дослідження електронної пошти. Архітектура системи електронної пошти, сервери і клієнти, їх характеристики. Важливість електронних повідомлень. Злочини, де використовується електронна пошта. Складові листа електронної пошти, службові заголовки листа. Етапи криміналістичного дослідження електронних листів зловмисників і потерпілих. Інструменти криміналістичного дослідження електронної пошти.	2
Тема 14. Криміналістичні дослідження мобільних пристроїв. Необхідність криміналістичного дослідження мобільних пристроїв. Роль апаратних і програмних платформ у криміналістичного дослідження мобільних пристроїв. Рівні архітектури оточення мобільних пристроїв. Стек архітектури Android і процеси завантаження системи. Стек архітектури iOS і процеси завантаження системи. Визначення місць збереження доказових даних. Підготовка до криміналістичного дослідження мобільних пристроїв. Криміналістичні дослідження мобільних пристроїв.	2
Тема 15. Складання звіту і представлення результатів криміналістичних досліджень. Важливість оформлення звіту щодо результатів криміналістичних досліджень. Узагальнений шаблон звіту криміналістичних досліджень. Види звітів та методика їх складання. Спеціаліст з первинних криміналістичних досліджень як свідок. Порівняння ролей експертів і технічних спеціалістів. Свідчення спеціаліста у суді.	2
Тема 16. Використання державних інформаційних систем під час вирішення криміналістичних завдань. Криміналістична реєстрація як інформаційна система. Обліки Міністерства внутрішніх справ України. Обліки інформаційно-довідкової служби. Обліки митної служби. Криміналістичні обліки міжнародних організацій. Використання інформації криміналістичних реєстраційних систем.	2
Загальна кількість годин	**32**

Лабораторні заняття

Теми лабораторних занять	Кількість годин	Вагові коефіцієнти a
Тема 1. Встановлення та настройка спеціалізованого програмного забезпечення. Практична робота з інсталяції та початкового налаштування інструментів цифрової криміналістики (аналізатори образів дисків, інструменти для зняття пам'яті, утиліти для створення хешів, SIEM-клієнти). Відпрацювання конфігурацій безпечного робочого середовища (ізольовані лабораторії, налаштування мережевих правил, збереження логів).	2	-

Тема 2. Збір та аналіз цифрової криміналістичної інформації в ОС Windows. Методика збору летючих і нелетючих даних із Windows-систем: створення образів диска, експорту реєстру, збір журналів подій, аналіз браузерних артефактів і тимчасових файлів. Практичні вправи з використанням інструментів для вилучення та первинного аналізу.	2	0,1
Тема 3. Збір та аналіз цифрової криміналістичної інформації в ОС Linux. Збір і аналіз даних у Linux-середовищі: вилучення логів (syslog, auth), знімки процесів, мережеві логи, дослідження файлових систем і прав доступу. Практика створення образів і аналізу слідів у сервісах та демонах.	2	0,1
Тема 4. Відновлення видаленого розділу та відновлення RAID. Методи виявлення та відновлення видалених розділів і таблиць розділів, підходи до реконструкції RAID-масивів (RAID0, RAID1, RAID5) та відновлення даних із пошкоджених масивів. Практичні кейси — відновлення структури та вилучення файлів.	2	0,1
Тема 5. Аналіз файлової системи NTFS. Детальний огляд NTFS: MFT, записів файлів, атрибутів, журналу транзакцій, метаданих та їх ролі як джерела доказів. Практичні вправи з витяганням артефактів (відновлення видалених файлів, аналіз часів змін, зв'язки між MFT-записами).	2	0,1
Тема 6. Аналіз артефактів прикладних програм у Windows. Дослідження артефактів відомих прикладних програм — веб-браузерів, поштових клієнтів, месенджерів, пакету Office — і способів отримання доказових даних (історія, кеші, локальні бази, метадані документів). Практичні вправи з інструментами витягання артефактів.	2	0,1
Тема 7. Криміналістичний аналіз мережі. Збір і аналіз мережевих доказів: захоплення трафіку (pcap), аналіз мережевих сесій, відновлення передачі файлів, кореляція подій мережевого обладнання (маршрутизатори, міжмережеві екрани, IDS). Практичні завдання з реконструкції інциденту за мережевими даними.	2	0,1
Тема 8. Аналіз оперативної пам'яті. Методи збору та аналізу оперативної пам'яті (RAM): створення дампів, пошук процесів, відкритих з'єднань, ключів ідентифікації шкідливого ПЗ, витяг метаданих і об'єктів у пам'яті. Практична робота з інструментами для статичного й динамічного аналізу пам'яті.	2	0,1
Загальна кількість годин	**16**	$\sum_{i=1}^{n} a_i = 0{,}8$

Контрольні роботи

Теми контрольних робіт	Вагові коефіцієнти b

Тема 1. Електронні докази: пошук, вилучення, документообіг (chain of custody). Аналіз правових та практичних аспектів поводження з електронними доказами: правила пошуку й вилучення, створення дублікатів, забезпечення незмінності даних, оформлення ланцюга зберігання (chain of custody) та підготовка звіту про первинні криміналістичні дослідження.	0,1
Тема 2. Розслідування шкідливого програмного забезпечення та мережевих інцидентів. Дослідження методів виявлення, вилучення та криміналістичного аналізу шкідливого ПЗ та мережевих інцидентів: статичний і динамічний аналіз зразків, відтворення ланцюга зараження, робота з мережевими логами та реконструкція подій.	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. Основні принципи цифрової криміналістики. Вивчення базових понять, принципів збереження доказів, непорушності даних та етичних норм у криміналістичній практиці.	8
Тема 2. Міжнародні стандарти цифрової криміналістики. Ознайомлення з міжнародними стандартами (ISO/IEC 27037, 27041, 27042, 27043), їхнім призначенням та використанням у практиці розслідувань.	8
Тема 3. Цифрові докази та ланцюг зберігання (Chain of Custody). Дослідження процедур документування, передачі та зберігання цифрових доказів, що забезпечують їхню достовірність у суді.	7
Тема 4. Криміналістичні інструменти з відкритим кодом. Вивчення найпопулярніших безкоштовних засобів криміналістичного аналізу (Autopsy, FTK Imager, Volatility, Wireshark) та принципів їх роботи.	7
Тема 5. Особливості дослідження мобільних пристроїв. Аналіз архітектури Android та iOS, методів вилучення даних, резервних копій, а також виявлення цифрових артефактів у смартфонах.	7
Тема 6. Методи виявлення шкідливого програмного забезпечення. Розгляд методів динамічного та статичного аналізу шкідливих програм, створення безпечного середовища для досліджень.	7
Тема 7. Особливості криміналістики хмарних обчислень. Вивчення процесів збору цифрових доказів у хмарних середовищах, обмежень, що виникають через віртуалізацію та розподілення даних.	7
Тема 8. Криміналістичний аналіз мережевого трафіку. Розгляд принципів збору, збереження та аналізу мережевого трафіку з метою відтворення дій користувача або зловмисника.	7
Тема 9. Електронна пошта як джерело доказів. Вивчення структури електронних листів, методів аналізу заголовків (headers), визначення джерела повідомлення та перевірки достовірності.	7
Тема 10. Судова експертиза у сфері кіберзлочинів.	7

Ознайомлення з етапами проведення судової експертизи цифрових доказів, ролями експертів і процедурою представлення результатів у суді.	
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. За даним компонентом врахування тем, у разі успішного завершення курсів, не передбачено.

Література, навчальні матеріали та інформаційні ресурси

Основна література

1. Davidoff, Sherri. Network forensics: tracking hackers through cyberspace / Sherri Davidoff, Jonathan Ham. Pearson Education, Inc. 2012.
https://ptgmedia.pearsoncmg.com/images/9780132564717/samplepages/0132564718.pdf
2 Євсеєв С.П. КІБЕРБЕЗПЕКА: ЛАБОРАТОРНИЙ ПРАКТИКУМ З ОСНОВ КРИПОГРАФІЧНОГО ЗАХИСТУ / С.П. Євсеєв, О.В. Мілов, О.Г. Король – Львів: «Новий Світ- 2000», 2020 . – 241 с.
http://library.hneu.edu.ua/storage/new-arrivals-books/December2020/Yevseiev.pdf.

Додаткова література

3. Aaron Philipp, David Cowen, Chris Davis. Hacking exposed computer forensics. Second edition. The McGraw-Hill Companies, 2010.
https://needuxnworkplace.wordpress.com/wp-content/uploads/2014/01/hacking-exposed-computer-forensics-secrets-solutions.pdf
4. Бобало Ю.Я., Горбатий І.В. (ред.) Інформаційна безпека. Навчальний посібник. — Львів : Видавництво Львівської політехніки, 2019. — 580 с. — ISBN 978-966-941-339-0
https://pdf.lib.vntu.edu.ua/books/2021/Bobalo_2019_580.pdf.

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: $a_і$ - 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: $b_і$ - 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