



СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Моніторинг та аудит інформаційно-комунікаційних систем

Рівень вищої освіти	Другий (магістерський)
Код та назва спеціальності, галузь знань	F5. Кібербезпека та захист інформації; F. Інформаційні технології
Тип та назва освітньої програми	Освітньо-професійна програма «Кібербезпека та захист інформації»
Статус навчальної дисципліни	Обов'язкова компонента (ОК-9)
Курс, семестр викладання	1 курс, 1 семестр
Трудовісткість навчальної дисципліни	5 кредити ЄКТС (150 академічних годин), з них: денна (очна) форма навчання: лекц. – 20 год., лаб.зан. – 18 год., практ. зан. – 18 год., самост. роб. – 94 год.; заочна форма навчання: лекц. – 14 год., лаб.зан. – 8 год., практ. зан. – 8 год., самост. роб. – 120 год.;
Мова викладання	Українська
Кафедра	Кібербезпеки та технічного захисту інформації
Факультет	Інформаційних технологій та кібербезпеки

Викладачі

КІЛЬДІШЕВ Віталій Йосипович,



доцент кафедри кібербезпеки та технічного захисту інформації,
доктор технічних наук, доцент

E-mail: v.y_kildishev@suitt.edu.ua

Консультації: щоп'ятниці з 14²⁰ до 15⁴⁰ год.,
каб. 205 (головний корпус)

Мета дисципліни	– формування знань щодо способів сканування та розпізнавання вразливостей у системах безпеки для інформації в інформаційних системах і мережах та компетенції щодо здатності здійснювати постійний моніторинг та аудит загроз для інформації та відповідну модернізацію систем і комплексів захисту інформації.
Компетентності, формуванню яких сприяє дисципліна	ЗК1 Здатність застосовувати знання у практичних ситуаціях. ЗК2 Здатність проводити дослідження на відповідному рівні. ЗК3 Здатність до абстрактного мислення, аналізу та синтезу. ЗК4 Здатність оцінювати та забезпечувати якість виконуваних робіт. СК9 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. СК14 Здатність здійснювати постійний моніторинг та аудит загроз для інформації та відповідну модернізацію (доробку) систем і комплексів захисту інформації. СК15 Здатність проводити процедури сканування вразливостей і розпізнавання вразливостей в системах безпеки.
Програмні результати навчання	ПРН7 Обґрунтовувати використання, впроваджувати та аналізувати кращі світові стандарти, практики з метою розв’язання складних задач професійної діяльності в галузі інформаційної безпеки та/або кібербезпеки. ПРН14 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. ПРН27 Здійснювати моніторинг та аудит загроз для інформації в інформаційних системах та мережах та оцінку ризиків безпеки інформації. ПРН29 Використовувати інструменти та технології безперервного моніторингу з метою оцінки ризиків, користуватися прикладними програмами моніторингу та аудиту загроз для інформації в інформаційних системах та мережах. ПРН30 Проводити сканування вразливостей і розпізнавання вразливостей в ІКС і системах безпеки. ПРН31 Використовувати моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації.
Програма навчальної дисципліни	
Тема 1. Загальні принципи аудиту інформаційної безпеки	Основні цілі та задачі моніторингу та аудиту інформаційних систем. Основи проведення аудиту безпеки інформаційно-комунікаційних систем. Цілі та метод проведення зовнішнього аудиту.
Тема 2. Безперервний внутрішній аудит	Загальні принципи аудиту інформаційної безпеки. Оцінка інформаційної безпеки. Здійснення збирання та

<i>інформаційної безпеки інформаційно-комунікаційних систем</i>	попередній аналіз даних, планування заходів з підготовки та проведення аудиту.
Тема 3. Аналіз і оцінка ризиків інформаційної безпеки	Методи оцінки ризиків інформаційної безпеки. Удосконалення системи інформаційної безпеки інформаційно-комунікаційних систем за допомогою страхування ризиків.
Тема 4. Відповідність аудиту інформаційної безпеки міжнародним стандартам	Характеристика сучасної національної та міжнародної нормативної бази у сфері інформаційної безпеки. Аудит інформаційної безпеки на відповідність міжнародному стандарту ISO/IEC 27001, 27002.
Тема 5. Тестування вразливостей	Етапи тестування на проникнення. Оформлення аудиторського звіту, аналіз відповідних ризиків та рекомендації щодо їх усунення.

Методи навчання

При вивченні навчальної дисципліни використовуються наступні методи навчання:

Інтерактивні	▪ Наочно-демонстраційні дидактичні комплекси до тем, що вивчаються в межах дисципліни (схеми, таблиці, графіки, діаграми; зображення, картини, зарисовки, фотографії; відеоролики; стрічки новин чи подій; гіфки, меми; комікси; квести, кросворди, ребуси тощо). ▪ Відповіді на запитання і опитування думок здобувачів освіти (дискусії). ▪ Відпрацювання навичок та робота в групах. Організовується групова робота (2–6 осіб) із конкретними завданнями, що виконуються спільно з взаємодопомогою, після чого результати презентуються в аудиторії для розвитку професійних і командних навичок.
Практичні	▪ Вправи. Різні практичні завдання, які застосовуються на будь-якому етапі навчального процесу і допомагають задіювати інтелектуальні, комунікативні та пошукові здібності здобувачів освіти. Вони можуть включати відповіді на запитання, розв’язання задач, виправлення помилок, складання порівняльних таблиць, графіків і т.п. ▪ Творчі роботи (проекти). Мета таких робіт – розвиток творчого мислення, підвищення технічних навичок роботи з необхідним програмним забезпеченням та обладнанням.

Методи дистанційного навчання	- Відеоконференції в форматі лекцій або семінарів. Зв'язок здобувачів освіти з викладачем забезпечують різноманітні сучасні платформи, такі як: Zoom, Moodle, Google Meet та ін. - Онлайн дискусії; - Індивідуальне і групове консультування (викладач дає додаткові роз'яснення щодо виконання завдань через чати та e-mail-надсилання);
--------------------------------------	---

Стратегія оцінювання результатів навчання

Змістовий контент результатів навчання з дисципліни	Результати навчання з даної дисципліни, які здобувач може продемонструвати та які можна ідентифікувати, оцінити і виміряти, розглядаються у вимірах 7 рівня Національної рамки кваліфікацій, що відповідає другому циклу вищої освіти Рамки кваліфікацій Європейського простору вищої освіти, а саме: Знання – очікується засвоєння базових концептуальних положень щодо методів створення систем моніторингу безпеки в інфокомунікаційних системах та основ проведення аудиту безпеки інформаційних і комунікаційних систем; Уміння/навички – формується здатність розробки автоматизованої системи моніторингу інформаційної безпеки та її основних складових, рекомендацій щодо удосконалення системи інформаційної безпеки, застосування яких дозволить мінімізувати ризики та формулювати перелік уразливостей та міждержавними та вітчизняними стандартами при створенні системи моніторингу інформаційної безпеки; Комунікація – здатність ефективно спілкуватися та взаємодіяти з командою проєкту, застосовуючи сучасні методи інформаційно-комунікаційних систем та технологій; Відповідальність і автономія – очікується здатність самостійно розв'язувати нестандартні ситуації при моніторингу та аудиту інформаційно-комунікаційних систем, що потребують нових стратегічних підходів.
Критерії оцінювання	Академічні успіхи здобувачів освіти в межах даної дисципліни оцінюються за бально-рейтинговою шкалою (максимальна кількість – 100 балів), що прийнята в ДУІТЗ, з обов'язковим переведенням кількості балів в оцінки за національною шкалою та за шкалою ECTS. Відмінно (А) – від 90 до 100 балів – здобувач у повному обсязі володіє навчальним матеріалом, вільно самостійно та аргументовано його викладає під час усних виступів та письмових відповідей, глибоко та всебічно розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову та додаткову літературу. Правильно вирішив усі або не менше 90% завдань, передбачених програмою навчальної дисципліни. Дуже добре (В) – від 82 до 89 балів – здобувач досить повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Однак під час викладання деяких питань допускаються при цьому окремі несуттєві неточності. Правильно вирішив 80-89% письмових завдань. Добре (С) – від 74 до 81 балів – здобувач достатньо повно володіє навчальним матеріалом, обґрунтовано його викладає під час усних виступів та письмових відповідей, в основному розкриває зміст теоретичних питань та практичних завдань, використовуючи при цьому обов'язкову літературу. Однак під час викладання деяких питань

	не вистачає достатньої глибини та аргументації, допускаються при цьому окремі несуттєві неточності та незначні помилки. Правильно вирішив 74-81% письмових завдань. Задовільно (D) – від 64 до 73 балів – здобувач в цілому володіє навчальним матеріалом, викладає його основний зміст під час усних та письмових відповідей, але з не зовсім глибоким та всебічним аналізом, обґрунтуванням та аргументацією, з недостатнім використанням необхідної літератури, допускаючи при цьому окремі неточності та помилки. Правильно вирішив 64-73% письмових завдань. Задовільно (E) – від 60 до 63 балів – здобувач в цілому володіє навчальним матеріалом, викладає його основний зміст під час усних та письмових відповідей, але без глибокого всебічного аналізу, обґрунтування та аргументації, без використання необхідної літератури, допускаючи при цьому окремі суттєві неточності та помилки. Правильно вирішив 60-63% письмових завдань. Незадовільно з можливістю повторного складання (FX) – від 35 до 59 балів – здобувач не в повному обсязі володіє навчальним матеріалом. Фрагментарно, стисло без аргументації та обґрунтування викладає його під час усних виступів та письмових відповідей, поверхово розкриває зміст теоретичних питань та практичних завдань, допускаючи при цьому суттєві неточності. Правильно вирішив 35-59% письмових завдань. Незадовільно з обов'язковим повторним вивченням дисципліни (F) – від 0 до 34 балів – Здобувач частково володіє навчальним матеріалом, не у змозі викласти зміст більшості питань теми під час усних виступів та письмових відповідей, допускаючи при цьому суттєві помилки. Правильно вирішив 1-34% письмових завдань.
Форма та методи контролю початкових досягнень	В межах даної дисципліни передбачено три види контролю: поточний, підсумковий та семестровий/академічний. Поточний контроль здійснюється під час проведення практичних занять і має на меті перевірку рівня підготовленості здобувачів до виконання конкретної роботи з теми, що вивчається. При поточному контролі оцінюється: активність роботи здобувача на практичних заняттях, результати виконання ним індивідуальних завдань, контрольних робіт, якість підготовлених завдань, що виконувались під час самостійної роботи. У концепції викладу навчальної дисципліни застосовуються такі форми проведення поточного контролю: тестування, опитування. Підсумковий контроль – це накопичена здобувачем сума балів за результатами вивчення п'яти тем та виконання завдань самостійної роботи. Семестровий (академічний) контроль передбачає проведення екзамену, під час якого здобувачу виставляється остаточна оцінка за навчальну дисципліну, яка виводиться із суми балів за результатами підсумкового контролю та складання екзаменаційного тесту. Оцінювання навчальних досягнень здобувачів здійснюється за 100-бальною шкалою.
Політика навчальної дисципліни	
Відвідування	Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях та контрольних заходах (залік) є обов'язковою. Важливим є своєчасне виконання індивідуальних завдань в межах самостійної роботи, передбачених програмою дисципліни.

Дотримання принципів академічної доброчесності	Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати різні програмні засоби.
Умови зарахування пропущених занять	Відпрацювання академічної заборгованості з дисципліни можливо до початку екзаменаційної сесії. Процедура узгоджується з викладачем, згідно його розкладу консультацій.
Інші умови	Навчально-методичні матеріали дисципліни розміщені на платформі Moodle
Рекомендовані джерела інформації	
Базові підручники та навчальні посібники	• Тестування на проникнення: навч. посіб. Ч.1 / [Є.О. Живило]; за ред. Є.О. Живило. – П.: ПНТУ “Полтавська політехніка ім. Юрія Кондратюка”, 2024. – 134 с. • Основи управління інформаційною безпекою: навч. посібник / А.М. Гребенюк, Л.В. Рибальченко. Дніпро: Дніпроп. держ. ун-т внутріш. справ, 2020. – 144 с. • Методи та засоби захисту інформації [Навчальний посібник] / В.А. Лахно, Є.В. Васіліу, В.М. Гладких, В.М. Домрачев, Н.М. Сивкова. – К. : ФОП Ямчинський О.В., 2020. – 445 с. • Гулак Г.М. Методологія захисту інформації. Аспекти кібербезпеки: підручник/ Г.М. Гулак – К.: Видавництво НА СБ України, 2020. – 256 с.
Методичні рекомендації та розробки викладачів дисципліни	▪ Моніторинг та аудит інформаційно-комунікаційних систем: методичні вказівки до лабораторних робіт [для здобувачів другого (магістерський) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації] / Уклад.: Кільдішев В.Й., Севастєєв Є.О.. Одеса: ДУІТЗ, 2026. 38 с. ▪ Моніторинг та аудит інформаційно-комунікаційних систем: методичні вказівки до практичних занять [для здобувачів другого (магістерський) рівня вищої освіти за спеціальністю F5 Кібербезпека та захист інформації] / Уклад.: Кільдішев В.Й.. Одеса: ДУІТЗ, 2026. 46 с.
Інформаційні ресурси	▪ Kali Linux: історія, встановлення, налаштування, огляд [Електронний ресурс]. – 2024. – Режим доступу до ресурсу: https://kr-labs.com.ua/blog/kali-linux-istoriya-vstanovlennya-nalashtuvannya-oglyad/. ▪ Oracle VM Virtualbox: що це за програма, хто розробники, ресурсомісткість, виконувані функції, особливості установки і настройки [Електронний ресурс] – Режим доступу до ресурсу: https://hi-news.pp.ua/kompyuteri/13386-oracle-vm-virtualbox-scho-ce-za-programa-hto-rozrobniki-resursomstkst-vikonuvan-funkcyi-osoblivost-ustanovki-nastroyki.html.
Рік введення силабусу – 2026 р.	Затверджено рішенням кафедри кібербезпеки та технічного захисту інформації (Протокол від 22 травня 2026 р. №13)
	Завідувача кафедри Володимир КОРЧИНСЬКИЙ Гарант освітньої програми Віталій КІЛЬДІШЕВ Викладач: Віталій КІЛЬДІШЕВ