



СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КІБЕРФІЗИЧНА БЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

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-7)
Курс, семестр викладання	1 курс, 2 семестр
Трудовісткість навчальної дисципліни	4 кредити ЄКТС (120 академічних годин), з них: денна (очна) форма навчання: лекц. – 18 год., лаб.зан. – 14 год., практ. зан. – 12 год., самост. роб. – 76 год.; заочна форма навчання: лекц. – 10 год., лаб.зан. – 6 год., практ. зан. – 8 год., самост. роб. – 96 год.;
Форма підсумкового контролю	Екзамен
Мова викладання	Українська
Кафедра	Кібербезпеки та технічного захисту інформації
Факультет	Інформаційних технологій та кібербезпеки

Викладачі

Кононович Володимир Григорійвич,		Кільдишев Віталій Йосипович,	
	доцент кафедри кібербезпеки та технічного захисту інформації, кандидат технічних наук, доцент. чл.кор. Академії зв'язку України E-mail: vl_kononovich@ukr.net Консультації: щоп'ятниці з 17 ⁰⁰ до 18 ⁰⁰ год., лаб. 108 (лабораторний корпус)		доцент кафедри кібербезпеки та технічного захисту інформації, доктор технічних наук, доцент. E-mail v.y_kildishev@suitt.edu.ua, Консультації: щопонеділка з 14 ²⁰ до 15 ⁴⁰ год., лаб. 108 (лабораторний корпус)

Загальна інформація про дисципліну

Мета дисципліни

– формування у студентів компетенцій, знань і навичок з основних примітивів кіберфізичної безпеки, характерних для кібер-фізичних систем (КФС), із заходів безпеки та умінь застосування їх до широкого кола проблем з кіберфізичної безпеки. Основна увага приділяється таким типам КФС, як промислові системи управління, автоматизовані системи управління (АСУ ТП). Крім того, розглядатимуться концепції, які можна узагальнити для всіх інших КФС, включаючи телекомунікаційні, медичні, транспортні та енергетичні системи. Запропоновані в рамках курсу теми стосуються кіберфізичних атак, безпеки специфічних протоколів взаємодії КФС, захисту інформації та пристроїв, управління ключами та безпечного відновлення (виправлення).

Компетентності, формуванню яких сприяє дисципліна

Інтегральна компетентність:

Здатність особи розв'язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки.

ЗК-1. Здатність застосовувати знання у практичних ситуаціях.

ЗК-2. Здатність проводити дослідження на відповідному рівні.

ЗК-3. Здатність до абстрактного мислення, аналізу та синтезу.

ЗК-5. Здатність спілкуватися з представниками інших професійних груп різного рівня (з експертами з інших галузей знань / видів економічної діяльності).

СК-2. 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.

СК-3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

СК-4. 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.

СК-5. 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.

СК-8. Здатність досліджувати, розробляти, впроваджувати та супроводжувати методи і засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності та критичної інфраструктури, в інформаційних системах, а також здатність оцінювати ефективність їх використання, згідно встановленої стратегії і політики інформаційної безпеки та/або кібербезпеки організації.

СК-16. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації.

Програмні результати навчання (ПРН)

- ПРН2. Інтегрувати фундаментальні та спеціальні знання для розв'язування складних задач інформаційної безпеки та/або кібербезпеки у широких або мультидисциплінарних контекстах.
- ПРН3. Проводити дослідницьку та/або інноваційну діяльність в сфері інформаційної безпеки та/або кібербезпеки, а також в сфері технічного та криптографічного захисту інформації у кіберпросторі.
- ПРН4. Застосовувати, інтегрувати, розробляти, впроваджувати та удосконалювати сучасні інформаційні технології, фізичні та математичні методи і моделі в сфері інформаційної безпеки та/або кібербезпеки.
- ПРН6. Аналізувати та оцінювати захищеність систем, комплексів та засобів кіберзахисту, технології створення та використання спеціалізованого програмного забезпечення.
- 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.
- ПРН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.
- ПРН13. 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.
- ПРН26. Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації в системі або на об'єкті інформаційної діяльності.

Програма дисципліни**Тема 1*****Основи теорії, технік і технологій кіберфізичної безпеки кіберфізичних систем*****Лекція 1.** Дисципліна «Кіберфізична безпека об'єктів критичної інфраструктури»**Практичне заняття 1.** Класифікація та методика категоріювання безпеки систем та інформації**Лабораторна робота 1.** Гармонізована методика категоризації та розрахунок рівня критичності об'єктів критичної інфраструктури**Лекція 2.** Структура вимог до кіберфізичної безпеки АСУ ТП (автоматизованої системи управління технологічними процесами)**Практичне заняття 2.** Розрахунок та вимірювання показників функціональної безпеки кіберфізичних систем**Лабораторна робота 2.** Вибір заходів захисту інформації для інформаційної системи.**Лекція 3.** Концепція безпеки АСУ ТП промислових технологій**Практичне заняття 3.** Розробка політики та формування систем інформаційної безпеки**Лабораторна робота 3.** Концепція безпеки інформації та галузевого профілю безпеки. Загальні вимоги до системи кібербезпеки об'єкта критичної інфраструктури**Лекція 4.** Порядок впровадження конвергентної системи безпеки інформації та приватності

	Практичне заняття 4. Постулати та аксіоматичні основи теорії інформаційної безпеки. Лабораторна робота 4. Порядок оцінювання заходів захисту для інформаційної системи та інформації
Тема 2.	Задачі та заходи кіберфізичної безпеки об'єктів критичної інфраструктури Лекція 5. Порядок впровадження конвергентної системи безпеки інформації та приватності (Продовження) Практичне заняття 5. Огляд теорій захисту інформації, інформаційної та кібербезпеки, кіберфізичної безпеки Лабораторна робота 5. Самооцінка поточного та цільового профілю й підвищення рівня кібербезпеки ІКС та ОКП Лекція 6. Методи оцінки безпеки в мережах інформаційно-комунікаційних технологій Практичне заняття 6. Процес розробки показників кібербезпеки Лабораторна робота 6. Модель процесу оцінки безпеки інформаційних технологій за загальними критеріями Лекція 7. Протоколи індустріальних мереж Практичне заняття 7. Методи розрахунку показників надійності, відмово стійкості та безпеки кіберфізичних систем (Продовження Практичної роботи 2) Лабораторна робота 7. Методи розрахунку ризиків кіберфізичних систем. Якісний підхід Лекція 8. Криптологія у конвертованій безпеці АСУ ТП Практичне заняття 8. Безпека мережевих технологій для програмованих логічних контролерів Лекція 9. Вибір методів забезпечення інформаційної та функціональної безпеки Практичне заняття 9. Кібербезпека у пост воєнному новому майбутньому Лекція 10. (Факультативна) Проектування та реалізація життєвого циклу інформаційної та функціональної безпеки КФС
	Самостійна робота Служби інформаційної безпеки програмно-конфігурованої комунікаційної мережі
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 управління доступом до інформаційних ресурсів, включаючи теоретичні підходи, принципи, моделі (DAC, MAC, RBAC), етапи реалізації, а також регламенти й процедури адміністрування доступу, журналювання подій, впровадження єдиного входу (SSO) та аутентифікації. ▪ Уміння/навички – формується здатність проводити дослідження та впроваджувати інноваційні рішення в управлінні доступом на основі компетентнісного підходу, розв'язувати складні задачі у сферах налаштування політик доступу, оцінювання безпеки, впровадження SSO, а також забезпечувати захист інформаційних ресурсів через аналіз ризиків і застосування сучасних технологій. ▪ 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 в управлінні доступом, 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 навчальних 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 чотирьох тем та виконання завдань самостійної роботи. Семестровий (академічний) контроль передбачає проведення заліку, 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	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.

академічної доброчесності	
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	1. Кононович В.Г., Голев Д.В. «Кіберфізична безпека об'єктів критичної інфраструктури» .: Підручник та практикум. Одеса: ДУІТЗ, 2025. 406 с. 2. Юдін О.К., Корченко О.Г., Конахович І.Ф. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ «НВП» ІНІЕРСЕРВІС», 2009. 716 с. 3. МЕК 61508. Функціональна безпека систем електричних, електронних, програмованих електронних, пов'язаних з безпекою (ІЕС 61508-х “Functional safety of electrical/electronic/programmable electronic safety-related systems”). 600 с. 4. Лахно В.А., Васіліу Є.В. та ін. Методи та засоби захисту інформації [Навчальний посібник] – К.: ЦП «Компринт» О.В., 2021. 444 с. 5. Захарченко М.В., Онацький А.В., Йона Л.Г., Шинкарчук Т.М. Асиметричні методи шифрування в телекомунікаціях. – Одеса: ОНАЗ, 2011. 184 с. 6. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. <i>Затверджено наказом ДСТСЗІ СБ України № 123 від 8.11.2005.</i> (Серія видань «Нормативний документ»).
Методичні рекомендації та розробки викладачів дисципліни	1. Лабораторний практикум з «Кіберфізичної безпеки об'єктів критичної інфраструктури» Методичний посібник та методичні вказівки. – Одеса: ДУІТЗ. 40 с.
Інформаційні ресурси	1. http://www.dut.edu.ua/uploads/1_49183247.pdf . 2. http://www.dut.edu.ua/uploads/1_1066_65357958.pdf . 3. https://www.misra.org.uk/Activities/MISRAC/tabid/160/Default.aspx . 4. http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074&cat_id=38835 5. http://shop.uas.org.ua/ua/katalog-normativnih-dokumentiv/35-informatsiyi-tehnolohiyi-kontorski-mashyny/informacijni-tehnologii-metodi-zahistu-osnovni-polozhennja-schodo-zabezpechennja-nevtruchannja-v-osobiste-zhittja.html . 6. https://www.cisco.com/c/ru_ua/training-evens/netacd/training-courses/cisco-packet-traser.html .

	7. http://www.avispa-project.org . 8. https://www.dbn.co.ua/load/normativy/dstu/4145/5-1-0-1798 9. https://www.iso.org . 10. https://www.pdfdrive.com . 11. Packet Tracer. URL: https://www.cisco.com/c/ru_ua/training-evens/netacd/training-courses/cisco-packet-traser.html		
Рік введення силабусу - 2026 р	Затверджено рішенням кафедри кібербезпеки та технічного захисту інформації (Протокол від 22 травня 2025 р. №13)		
	Завідувача кафедри		Володимир КОРЧИНСЬКИЙ
	Гарант освітньої програми		Віталій КІЛЬДІШЕВ
	Викладач:		Володимир КОНОНОВИЧ
	Викладач:		Віталій КІЛЬДІШЕВ