СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КІБЕРФІЗИЧНА БЕЗПЕКА ОБ'ЄКТІВ КРИТИЧНОЇ ІНФРАСТРУКТУРИ

Галузь знань	12 Інформаційні технології
Шифр та назва спеціальності	125 Кібербезпека та захист інформації
Назва освітньо-професійної програми	Кібербезпека та захист інформації
Рівень вищої освіти	Другого (магістерського) рівня
Факультет	Інформаційних технологій та кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	**ОК-7** ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладачі

Кононович Володимир Григорович
vl_kononovich@ukr.net

Доцент кафедри кібербезпеки та технічного захисту інформації, кандидат технічних наук, доцент.

Загальна інформація про дисципліну

Анотація до дисципліни	– Викладання дисципліни «Кіберфізична безпека об'єктів критичної інфраструктури» є навчання базовими знаннями з проблем безпеки кіберфізичних систем, телекомунікаційних систем і мереж, інших об'єктів критичних інфраструктур (Кібер-фізичні системи (КФС) – це системи управління, до яких інтегрують кібернетичні та фізичні компоненти для максимізації ефективності й надійності та застосовують в багатьох сферах). У першому змістовному модулі розглядаються теоретичні основи та архітектурні принципи побудови системи кіберфізичної безпеки КФС: моделі та характеристики КФС як об'єкта безпеки; індустріальні системи управління, АСУ ТП (SCADA) та їх

	елементи, безпечні мережні комунікаційні протоколи; термінологія, політика, механізми, послуги кіберфізичної безпеки КФС; атаки на КФС. Змістовний модуль 2 присвячено методикам і засобам проектування, побудові та експлуатації: технології проектування згідно МЕК 61508 та IEC 61850; проектування етапів життєвого циклу систем інформаційної, кібернетичної та функціональної безпеки; вимірюванням показників кіберфізичної безпеки.
Мета дисципліни	– Метою є формування у студентів знань і навичок з основними примітивами кіберфізичної безпеки, характерними для кібер-фізичних систем (КФС), із заходами безпеки та застосувати їх до широкого кола сучасних та майбутніх проблем з кіберфізичної безпеки. Основна увага приділяється таких типах КФС, як промислові системи управління, автоматизованим системам 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 стосуватимуться кіберфізичних атак, безпеці специфічних протоколів зв'язку КФС, захисту пристроїв, управлінню ключами та безпечного відновлення (виправлення). Цілі курсу: – ознайомити із теоретичними основами кіберфізичної безпеки; – визначити архітектурні та технічні характеристики об’єктів захисту кіберфізичних систем у критично важливих інфраструктурах, зокрема SCADA (АСУ ТП); – визначити види інформації, об’єктів та їх компонентів, кіберфізична безпека яких забезпечується; – окреслити принципи, засоби і етапи життєвого циклу систем кіберфізичної безпеки; – описати вимоги щодо кіберфізичної безпеки від загроз; – освоїти технології проектування систем кіберфізичної безпеки; – визначати послуги та механізми кіберфізичної безпеки; – застосовувати протоколи керування криптографічними ключами; – застосовувати протоколи ідентифікації та автентифікації; – застосовувати захищені телекомунікаційні протоколи; – враховувати особливості забезпечення інформаційної безпеки комп’ютерних систем управління (SCADA); – застосовувати засоби кіберфізичної безпеки систем на програмованих логічних інтегральних схемах.
Компетентності, формуванню яких сприяє дисципліна	КІ-1. Здатність особи розв’язувати задачі дослідницького та/або інноваційного характеру у сфері інформаційної безпеки та/або кібербезпеки. КЗ1. Здатність застосовувати знання у практичних ситуаціях. КЗ2. Здатність проводити дослідження на відповідному рівні. КЗ3. Здатність до абстрактного мислення, аналізу та синтезу. КЗ5. 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. КФ8. 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. КФ16. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації.
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. 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.

	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. 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. Розроблювати плани аварійного відновлення та безперервності операцій в інформаційних, електронних, комунікаційних та інформаційно-комунікаційних системах. РН25. Застосовувати сервіс-орієнтовані принципи архітектури безпеки, щоб задовольнити вимоги конфіденційності, цілісності та доступності організації. РН26. Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації в системі або на об'єкті інформаційної діяльності. РН30. Проводити сканування вразливостей і розпізнання вразливостей в ІКС і системах безпеки. РН31. Використовувати моделі та симуляції інформаційних, електронних комунікаційних та інформаційно-комунікаційних систем для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації.
Обсяг дисципліни	Загальний обсяг дисципліни: 4 кредитів ЄКТС 44 години). Для денної форми навчання: лекції – 16 годин, лабораторні роботи – 14 години, практичні заняття – 10 годин, самостійна робота – 52 години.
Форма підсумкового контролю	Залік
Терміни викладання дисципліни	Дисципліна викладається у 2-му семестрі (1–16 тижні)

Програма дисципліни

Тема 1.	***Теоретичні основи та архітектурні принципи побудови системи кіберфізичної безпеки кіберфізичних систем*** Розділ 1. Вступ. Поняття безпек та класифікація архітектур систем інформаційної безпеки інформаційної системи (ІС) та її задачі. **Лекція 1.** Аналітичний огляд теорій захисту інформації, інформаційної безпеки, кібербезпеки та кіберфізичної безпеки **Практичне заняття 1.** Система і формати команд віртуального операційного середовища Ubuntu, додаткових до команд Linux. **Лабораторна робота 1.** Інсталяція та використання віртуальної машини VirtualBox в середовищі Windows **Лекція 2.** Моделі та характеристики кібер-фізичних систем як об'єкта безпеки: , індустріальні системи управління, АСУ

	ТП (SCADA) та їх елементи, розширений кіберпростір, транспортні протоколи, функції **Практичне заняття 2.** Мереже-творення та протокол TCP/TP та інші **Лабораторна робота 2.** Налаштування віртуального операційного середовища Ubuntu. **Лекція 3.** Мережні комунікаційні протоколи для індустріальних систем управління **Практичне заняття 3.** Бібліотека GitHub та python для роботи з мережними комунікаційними протоколами **Лабораторна робота 3.** Мережний комунікаційний протокол ***Modbus*** для АСУ ТП, SCADA **Лекція 4.** Основи, термінологія, політика, механізми, послуги кіберфізичної безпеки кіберфізичних систем **Практичне заняття 4.** Використання бібліотеки OpenSSL Library, як набору криптографічних інструментів на основі UNIX **Лабораторна робота 4.** Модель створення спільного секретного ключа за алгоритмом Діффі-Хелмана **Практичне заняття 5.** Беграунд управління ключами. Центри розподілу ключів.**Лекція 5.** Атаки на кіберфізичні системи, на АСУ ТП. Вразливості комунікаційних протоколів. **Лабораторна робота 5.** Безпечна версія комунікаційного протоколу Modbus для забезпечення безпеки транспортного рівня TLS
Тема 2.	***Методи, засоби, заходи забезпечення кіберфізичної безпеки кіберфізичних систем*** **Лекція 6.** Безпечні версії сучасних протоколів для кіберфізичних систем. Транспортна телеметрія потоків повідомлень. **Практичне заняття 6.** Розрахунки та вимірювання показників функціональної безпеки кіберфізичних систем **Лабораторна робота 6.** Впровадження протоколу передачі потоку телеметрії (MQTT) на безпечному транспортному рівні (TLS) **Лекція 7.** Структура вимог до інформаційної та кіберфізичної безпеки комп'ютерних систем управління (АСУ ТП) **Практичне заняття 7.** Методи розрахунку показників надійності КФС **Лабораторна робота 7.** Розробка Технічного завдання на Комплексну систему захисту інформації типового робочого місця зовнішнього користувача автоматизованої інформаційної системи **Лекція 8.** Вибір методів забезпечення інформаційної та функціональної безпеки КФС **Практичне заняття 8.** Методи розрахунку ризиків кіберфізичної безпеки КФС **Лабораторна робота 8.** Розробка Технічних вимог до апаратного і програмного забезпечення Єдиної Державної Електронної Бази з питань освіти **Лекція 9.** Формування системи управління та менеджменту інформаційної та функціональної безпеки **Практичне заняття 9.** Метод розробки показників кіберфізичної безпеки телекомунікаційних систем і мереж **Лабораторна робота 9.** Розробка Календарного плану робіт із захисту інформації в Єдиній Державній Електронній Базі з питань Освіти **Лекція10.** Проектування та реалізація життєвого циклу інформаційної та функціональної безпеки КФС **Практичне заняття 10.** Метод оцінки ефективності систем захисту інформації від їх злочинного вивчення **Лабораторна робота 10.** Методика категоризації об'єктів критичної інфраструктури та розрахунок рівня критичності

	об’єкта

Список рекомендованих джерел

1. Конспект лекцій з дисципліни «Кіберфізична безпека об’єктів критичної інфраструктури». Одеса: ДУІТЗ, 2023.
2. Юдін О.К., Корченко О.Г., Конахович І.Ф. Захист інформації в мережах передачі даних. – К.: Вид-во ТОВ «НВП» ІНИЕРСЕРВІС», 2009. 716 с.
3. Скляр В. В. Обеспечение безопасности АСУТП в соответствии с современными стандартами: Методическое пособие. – М.: Инфра-Инженерия, 2018. 384 с.
4. Лахно В.А., Василіу Є.В. та ін. Методи та засоби захисту інформації [Навчальний посібник] – К.: ЦП «Компринт» О.В., 2021. 444 с.
5. Лабораторний практикум з «Кіберфізичної безпеки об’єктів критичної інфраструктури» Методичний посібник та методичні вказівки. – Одеса: ДУІТЗ. 40 с.
6. Захарченко М.В,, Онацький А.В., Йона Л.Г., Шинкарчук Т.М. Асиметричні методи шифрування в телекомунікаціях. – Одеса: ОНАЗ, 2011. 184 с.
7. Virtual Machine Oracle VirtualBoxR. User Manual. *Version* 6.1.22. Oracle Corporation: 2021. 401 p. URL: http://www.virtualbox.org .
8. Керівництво користувача операційної системи Linux (Ubuntu). URL: https://help.ubuntu.ru/wiki/%D0%BA%D0%BE%D%BC%D0%B0%D0%BD%D0%B4%D0%BD%D0%B0%D1%8F_%D1%81%D1%82%D1%80%D0%BE%D0%BA%D0%B0 .
9. НД ТЗІ 3.7-003-05 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі. *Затверджено наказом ДСТСЗІ СБ України* № 123 від 8.11.2005. (Серія видань «Нормативний документ»).
10. Packet Tracer. URL: https://www.cisco.com/c/ru_ua/training-evens/netacd/training-courses/cisco-packet-traser.html .
11. AVISPA, URL: http://www.avispa-project.org .
12. ДСТУ 4145-2002. URL: https://www.dbn.co.ua/load/normativy/dstu/4145/5-1-0-1798/ .

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.litmy.ru/knigi/seti/176809-kriptograficheskie-protokoly-osnovnye-svoystva-i-uyazvimosti.html .
4. http://www.dsszzi.gov.ua/control/uk/publish/article?art_id=46074&cat_id=38835
5. http://www.it-ebooks.ru/publ/it_security/it_security/15-1-0-526 .
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. http://www.virtualbox.org .

Інформація про консультації

Щопонеділка у січні-червні 2024 року з 11^{50} до 13^{10}год., TELEGRAM АМБ КБ 3.03, або ауд. 205 ДУІТЗ – доц. В. Г. Кононович

Загальна схема оцінювання

Сума балів за всівидинавчальноїдіяльності	Шкала ЄКТС	Оцінка за національною шкалою		Нарахування балів	Бали нараховуються таким чином:
		для іспиту	для заліку		
90-100	A	Відмінно	зараховано		***Оцінювання знань здобувачів фахової передвищої освіти здійснюється за 100-бальною шкалою*** і становить: за поточну успішність (участь у лабораторних роботах, практичних заняттях, виконання лабораторних робіт практичних завдань та контрольних робіт) – до 100 балів, за результати екзамену – до 0 балів.
82-89	B	Добре			
74-81	C				
64-73	D	Задовільно			
60-63	E				
35-59	FX	Незадовільно з можливістю повторного складання	Не зараховано з можливістю повторного складання		
0-34	F	Незадовільно з обов'язковим повторним вивченням дисципліни	Не зараховано з обов'язковим повторним вивченням дисципліни		

Політика опанування дисципліни

Відвідування:Здобувачі фахової перед вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на лабораторних роботах, практичних заняттях та контрольних заходах (екзамен/залік) є обов'язковою. При проведенні занять в онлайн режимі, присутність здобувача враховується у разі відкритого вікна.
Дотримання принципів академічної доброчесності: Підготовка усіх завдань, письмових робіт і т. ін., що виконуються в межах дисципліни, здійснюється здобувачем фахової перед вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт

застосовувати програму **Unicheck.**
Умови зарахування пропущених занять:
Інші умови:Навчально-методичні матеріали дисципліни розміщені на платформі Moodle, за посиланням Moodle Meet