ДЕРЖАВНИЙ УНІВЕРСИТЕТ ІНТЕЛЕКТУАЛЬНИХ ТЕХНОЛОГІЙ І ЗВ'ЯЗКУ

Факультет інформаційних технологій і кібербезпеки

Кафедра кібербезпеки та технічного захисту інформації

"**ЗАТВЕРДЖУЮ**"

Ректор ДУІТЗ

_____ Олександр НАЗАРЕНКО

"____" _____ 2023 року

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ООК-5 Кіберфізична безпека об'єктів критичної інфраструктури

(шифр і назва навчальної дисципліни)

Рівень вищої освіти __другого (магістерського) рівня_____

Галузь знань __12 – Інформаційні технології_____

Спеціальність __125 – Кібербезпека та захист інформації

Спеціалізація (за наявності)_____

Освітня програма __Кібербезпека_____

Статус дисципліни __нормативна_____

Мова викладання __українська_____

Одеса 2023

Програма навчальної дисципліни Кіберфізична безпека об'єктів критичної інфраструктури для студентів освітнього рівня магістр за спеціальністю 125 – Кібербезпека та захист інформації

Розробник(и): к.т.н., доцент Кононович Володимир Григорійович

Навчальна програма затверджена на засіданні кафедри Кібербезпеки та технічного захисту інформації

Протокол від "21" березня 2023 року № 8

Завідувач кафедри _____ В.В. Корчинський
(підпис) (ініціали та прізвище)

"21" березня 2023 року

Програму погоджено з гарантом освітньо-професійної програми магістрів

Гарант освітньо-професійної програми _____ В.В. Корчинський
(підпис) (ініціали та прізвище)

Програму погоджено з деканом факультету Інформаційних технологій і кібербезпеки

_____ Є.В. Василіу
(підпис) (ініціали та прізвище)

Програму схвалено навчально-методичною радою ДУІТЗ

Голова навчально-методичної ради ДУІТЗ,

Проректор з навчальної роботи _____ А.Г. Ложковський
(підпис) (ініціали та прізвище)

Протокол № ____ від _____ «____» _____ 2023 р.

Вступ

Програма вивчення навчальної дисципліни «Кіберфізична безпека об'єктів критичної інфраструктури» складена відповідно до освітньо-професійної програми підготовки магістрів спеціальності 125 «Кібербезпека та захист інформації»

Предметом вивчення навчальної дисципліни є: знайомство із теоретичними основами кіберфізичної безпеки; визначення архітектурних та технічних характеристик 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; описання вимог щодо кіберфізичної безпеки від загроз; технології проектування систем кіберфізичної безпеки; 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.

Міждисциплінарні зв'язки:

Дана дисципліна базується на наступних дисциплінах:

– Спеціальні вимірювання в галузі ТЗІ.

– Керування доступом в інтелектуальних мережах.

– Система менеджменту інформаційної безпеки.

– Комплексні системи безпеки.

– Криптологія.

Програма навчальної дисципліни складається з таких змістовних модулів.

Змістовний модуль 1: Теоретичні основи та архітектурні принципи побудови системи кіберфізичної безпеки кіберфізичних систем (кредитів ECTS – 2,5; 75 год)

Змістовний модуль 2: Методи, засоби, заходи забезпечення кіберфізичної безпеки кіберфізичних систем: (кредитів ECTS – 2,5; 75 год)

1. Мета та завдання навчальної дисципліни

1.1. Метою курсу Кіберфізична безпека об’єктів критичної інфраструктури 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).

1.2. Основні завдання 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.

1.3. Згідно з вимогами професійного стандарту «фахівець сфери захисту інформації» та освітньо-професійної програми студенти повинні:

Набути професійні компетенції:

А. Впровадження систем та комплексів захисту інформації

А1. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації.

А2. Здатність виявляти, досліджувати (оцінювати) системно аналізувати загрози для інформації, аналізувати ризики безпеки інформації та кібербезпеки інформації у разі реалізації загроз.

А3. Здатність формувати стратегію і політики безпеки інформації в інформаційно-комунікаційних системах.

А4. Здатність аналізувати, розробляти та супроводжувати систему управління інформаційною безпекою підприємства/організації.

А5. Здатність виконувати передпроєктні роботи щодо систем та комплексів захисту інформації.

А7. Здатність впроваджувати (активізувати) програмні та апаратні засоби захисту інформації в системах і на об'єктах.

А9. Здатність розробляти, впроваджувати та аналізувати технічні документи, положення, інструкції щодо систем і комплексів захисту інформації.

В. Експлуатація та обслуговування систем і комплексів захисту інформації, моніторинг та аудит загроз для інформації

В2. Здатність проводити періодичне обслуговування інформаційних систем та мереж , комплексних систем захисту інформації та комплексів технічного захисту інформації.

В6. Здатність проводити процедуру сканування вразливостей і розпізнавання вразливостей в системах безпеки.

Д. Унормування систем технічного та криптографічного захисту інформації

Д1. Здатність аналізувати, інтегрувати і використовувати кращі світові практики та стандарти при розробці нормативних документів системи технічного та криптографічного захисту інформації.

Д2. Здатність розробляти, впроваджувати та аналізувати нормативні документи, положення, інструкції й вимоги технічного та організаційного спрямування щодо системи технічного та криптографічного захисту інформації.

Е. Координація діяльності з технічного та криптографічного захисту інформації

Е2. Здатність взаємодіяти з керівництвом і фахівцями технологічних та інших підрозділів підприємства/ організації з технологічних та інших питань, пов'язаних із забезпеченням захисту інформації та кіберзахисту.

Е3. Здатність взаємодіяти із зовнішніми партнерами в межах визначених повноважень.

Забезпечити набуття професійних компетенцій:

Загальні компетенції

КЗ-1. Здатність застосовувати знання у практичних ситуаціях.

КЗ-2. Здатність проводити дослідження на відповідному рівні.

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

Фахові компетенції

КФ3. Здатність досліджувати, розробляти і супроводжувати методи та засоби інформаційної безпеки та/або кібербезпеки на об’єктах інформаційної діяльності та критичної інфраструктури.

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.

знати:

А. Впровадження систем та комплексів захисту інформації

А1.33. Концепції і протоколи комп’ютерних мереж, методики забезпечення мережевої безпеки та захисту інформації в автоматизованих (інформаційних) системах і на об’єктах інформаційної діяльності.

А1.311. Моделі та симуляції інформаційних, електронних, комунікаційних та інформаційно-комунікаційних систем, призначених для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації.

А2.32. Методи (способи) та методики виявлення. Дослідження та системного аналізу загроз для інформації та кіберзагроз.

А2.36. Класифікація операційних наслідків, спричинених помилками в системі кібербезпеки.

А2.32. Методи (способи) та методики виявлення. Дослідження та системного аналізу загроз для інформації та кіберзагроз

А2.36. Класифікація операційних наслідків, спричинених помилками в системі кібербезпеки.

А3.31. Поняття стратегії і політики безпеки інформації в інформаційних, електронних, комунікаційних та інформаційно-комунікаційних системах.

А3.32. Концепції архітектури безпеки мережі, включаючи технологію, протоколи, компоненти і принципи ешелонованого захисту (прикладна система ешелонованого захисту).

А3.35. Поняття профілю безпеки інформації та функціональних послуг безпеки.

А4.33. Принципи створення систем інформаційної безпеки (NIST SP 800-160).

А5.31. Середовища функціонування автоматизованих систем.

А6.318. Концепції та протоколи комп’ютерних мереж.

А7.32. Методології забезпечення мережевої безпеки.

А7.35. Методи програмування мікроконтролерів і контролерів відповідно до норм IEC 61131-3.

А7.39. Процедури підключення до локальної мережі підприємства (організації) та до глобальних мереж, процедури активізації (настроювання) програмних мережевих механізмів захисту інформації.

А7.310. Концепції управління послугами для мереж і відповідних стандартів (бібліотека інфраструктури інформаційних технологій (ITIL)

А9.34. Сучасні підходи по формуванню вимог до захисту інформації в інформаційно-комунікаційних системах і на об'єктах інформаційної діяльності.

В. Експлуатація та обслуговування систем і комплексів захисту інформації, моніторинг та аудит загроз для інформації

В2.31. Типи та періодичність планової підтримки апаратного забезпечення, періодичність підтримки та оновлення програмного забезпечення.

В6.32. Способи сканування та розпізнавання вразливостей у системах безпеки для інформації в інформаційних системах і мережах.

Д. Унормування систем технічного та криптографічного захисту інформації

Д2.31. Система нормативних документів (нормативна база) системи технічного та криптографічного захисту інформації.

Д2.31. Порядок розробки та впровадження нормативних документів системи технічного та криптографічного захисту інформації.

Е. Координація діяльності з технічного та криптографічного захисту інформації

Е2.32. Положення про структурні підрозділи підприємства (організації), що задіяні в спільному виконанні технологічних та функціональних завдань.

Е3.34. Порядок розроблення та виконання договірних робіт для зовнішніх партнерів.

забезпечувати знання:

– теоретичних основ систем інформаційної безпеки та кіберфізичної безпеки КФС у критично важливих інфраструктурах;

– етапів життєвого циклу систем інформаційної, кібернетичної та функціональної безпеки;

– формування вимог до кіберфізичної безпеки КФС;

– технології проектування систем кіберфізичної безпеки згідно МЕК 61508 та IEC 61850;

– послуг та механізмів кіберфізичної безпеки;

– організаційних, технічних, програмних та соціоінженерних методів забезпечення інформаційної та кіберфізичної безпеки;

– управління та менеджмент інформаційної та кіберфізичної безпеки;

– видів телекомунікаційних та криптографічних протоколів.

вміти:

А1.У4. Визначити (формулювати) вимоги щодо захисту інформації та кіберзахисту в інформаційно-комунікаційних системах та на об’єктах інформаційної діяльності підприємства (організації).

А2.У1. Виявляти загрози для інформації та кіберзагрози в інформаційних, електронних, комунікаційних та інформаційно-комунікаційних системах.

А2.У3. Досліджувати (оцінювати) та системно аналізувати загрози для інформації та вразливості комп’ютерної системи (систем) для розробки профілю безпеки.

А3.У1. Обґрунтовувати та розробляти політику безпеки інформації в інформаційних, електронних, комунікаційних та інформаційно-комунікаційних системах.

А3.У4. Визначати (розробляти, обґрунтовувати) профіль безпеки інформації в автоматизованих системах різного класу.

А4.У6. Створення системи (брати участь у створенні систем) інформаційної безпеки.

А5.У7. Розробляти проекти комплексних систем захисту інформації та комплексів технічного захисту інформації багаторівневими вимогами безпеки або вимогами для обробки кількох рівнів класифікації даних (відкрита інформація, службова інформація, секретна інформація з різними ступенями секретності).

А6.У3. Визначати вимоги до показників (характеристик) апаратних засобів технічного захисту інформації, які необхідні для забезпечення захищеності інформації в системі.

А7.У2. Визначати та групувати за пріоритетами основні системні функції або підсистеми, необхідні для підтримки основних можливостей або бізнес функцій з метою відновлення або поновлення після відмови системи, або під час відновлення системи на основі загальних системних вимог щодо безперервності та доступності.

А9.У1. Формулювати (брати участь у форму ванні) вимог до захисту інформації в інформаційно-комунікаційних системах і на об’єктах інформаційної діяльності.

В2.У6. Здійснювати оновлення баз даних, антивірусних програм, програмних механізмів захисту інформації.

В5.У6. Використовувати відповідні інструменти для відновлення програмного та апаратного периферійного обладнання системи.

Д2.У2. Писати та публікувати методики та настанови з кібербезпеки та інструктивні матеріали

Е2.У1. Взаємодіяти з керівництвом та працівниками технологічних та інших підрозділів підприємства (організації) з технологічних та інших питань, пов’язаних із забезпеченням захисту інформації та кіберзахисту (організовувати та отримувати від технологічних та інших підрозділів інформацію, необхідну для організації захисту інформації та кіберзахисту, узгоджувати та погоджувати технічну документацію на системи та комплекси захисту інформації, доводити до керівництва підрозділів недоліки у захисті інформації та пропозицій до їх

усунення, пропозицій про удосконалення систем та комплексів захисту інформації.

забезпечувати вміння:

– розроблення та впровадження заходів забезпечення кіберфізичної безпеки;

– оцінювати показники інформаційної та кіберфізичної безпеки, ризиків та надійності;

– застосовувати порядок створення системи кіберфізичної безпеки відповідно до стандартів та нормативних документів;

– виконувати захист мережі та захищати від відмов апаратних засобів та програмного забезпечення;

– виконувати розрахунки для показників кіберфізичної безпеки та надійності;

– виконувати розрахунки для протоколів ідентифікації;

– виконувати розрахунки для протоколів ключів та виконувати їх крипто аналіз;

– виконувати розрахунки для аналізу видів наслідків та критичності відмов апаратних засобів та програмного забезпечення.

Результати навчання:

А1.У8. Використовувати моделі та симуляції інформаційних, електронних, комунікаційних та інформаційно-комунікаційних систем, призначених для аналізу вразливості та прогнозування продуктивності таких систем за різних умов експлуатації.

А3.У6. Застосовувати політики безпеки інформації в інформаційно-комунікаційних системах для досягнення цілей безпеки системи.

А4.У7. Застосовувати сервіс-орієнтовані принципи архітектури безпеки, щоб задовольнити вимоги конфіденційності, цілісності та доступності організації.

А7.У3. Аналізувати проектні обмеження та можливі компроміси системи безпеки інформації (комплексної системи захисту інформації).

А7.У8. Впроваджувати (налаштовувати) програмно-апаратні засоби захисту мережних комунікацій.

А9.У5. Розроблювати плани аварійного відновлення та безперервності операцій. В інформаційних, електронних, комунікаційних та інформаційно-комунікаційних системах.

В2.З5. Відновлювати системи/сервери після виявленого збою (програмне забезпечення для відновлення, відмово стійкі кластери, дублювання/»зеркалювання».

В5.У8. Співпрацювати із системними аналітиками ,інженерами, програмістами, з метою отримання інформації про обмеження та можливості системи, вимог до продуктивності та інтерфейсів, шляхів модернізації системи і комплексів технічного захисту інформації.

Д1.У3. Проводити системний аналіз світових практик, стандартів із захисту інформації.

Е3.У1. Співпрацювати із зовнішніми партнерами доступними засобами комунікації стосовно питань захисту інформації та кіберзахисту.

Забезпечувати результати навчання

РН8. Досліджувати, розробляти і супроводжувати системи та засоби інформаційної безпеки та/або кібербезпеки на об'єктах інформаційної діяльності та критичної інфраструктури.

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.

2. Інформаційний обсяг навчальної дисципліни

Змістовний модуль 1: Теоретичні основи та архітектурні принципи побудови системи кіберфізичної безпеки кіберфізичних систем (кредитів ECTS – 2, 60 год)

Тема 1. Основи, термінологія, політика, механізми, послуги кіберфізичної безпеки кіберфізичних систем

Тема 2. Аналітичний огляд теорій захисту інформації, інформаційної безпеки, кібербезпеки та кіберфізичної безпеки

Тема 3. Моделі та характеристики кіберфізичних систем як об'єкта безпеки: , індустріальні системи управління, АСУ ТП (SCADA) та їх елементи, розширений кіберпростір, транспортні протоколи, функції

Тема 4 Мережні комунікаційні протоколи для індустріальних систем управління

Тема 5. Атаки на кіберфізичні системи, на АСУ ТП. Вразливості комунікаційних протоколів.

Змістовний модуль 2: Методи, засоби, заходи забезпечення кіберфізичної безпеки кіберфізичних систем: (кредитів ECTS – 2, 60 год)

Тема 6. Безпечні версії сучасних протоколів для кіберфізичних систем. Транспортна телеметрія потоків повідомлень

Тема 7. Структура вимог до інформаційної та кіберфізичної безпеки комп'ютерних систем управління (АСУ ТП)

Тема 8. Вибір методів забезпечення інформаційної та функціональної безпеки КФС

Тема 9. Формування системи управління та менеджменту інформаційної та функціональної безпеки

Тема 10. Проектування та реалізація життєвого циклу інформаційної та функціональної безпеки КФС

3 Рекомендована література

ОСНОВНА

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.

ДОДАТКОВА

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 .

4. Форма підсумкового контролю успішності навчання

Поточний контроль знань, ККР екзамен. Оцінювання проводиться шкалою ОНАЗ (100 балів).

5. Засоби діагностики успішності навчання

Поточний контроль знань здійснюється шляхом проведення контрольних робіт наприкінці лекцій, тестування, щомісячної атестації з урахуванням захисту лабораторних робіт та практичних занять, оцінками за комплексне завдання, заліку в термін залікового тижня.

Оцінювання проводиться за шкалою ESNS, національною та за шкалою ДУІТЗ (100 бал).