Державний університет інтелектуальних технологій і зв'язку
Факультет інформаційних технологій та кібербезпеки
Кафедра кібербезпеки та технічного захисту інформації

"**ЗАТВЕРДЖУЮ**"
Ректор ДУІТЗ
_____ Олександр НАЗАРЕНКО
"____" _____ 2023 року

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОВПП-6 Комплексні системи безпеки

Рівень вищої освіти	другого (магістерського) рівня
Галузь знань	12 Інформаційні технології
Спеціальність	125 Кібербезпека та захист інформації
Спеціалізація (за наявності)	
Освітня програма	магістрів
Статус дисципліни	нормативна
Мова викладання	українська

Одеса 2023

Програма навчальної дисципліни Комплексні системи безпеки для студентів освітнього рівня другий (магістерський) за спеціальністю 125 Кібербезпека та захист інформації

Розробник: к.ф.н., доцент Стайкуца Сергій Володимирович

Навчальна програма затверджена на засіданні кафедри кібербезпеки та технічного захисту інформації

Протокол від "21" Березня 2023 року № 8

Завідувач кафедри _____ В.В. Корчинський

"21" Березня 2023 року

Програму погоджено з гарантом освітньо-професійних програми магістрів

Гарант освітньо-професійної програми _____ В.В. Корчинський

Програму погоджено з деканом факультету інформаційних технологій та кібербезпеки

Декан факультету _____ Є.В. Василіу

Програму схвалено навчально-методичною радою ДУІТЗ

Голова навчально-методичної ради ДУІТЗ,

Проректор з навчальної роботи _____ А.Г. Ложковський

Протокол № _____ від _____ "____" _____ 2023 р.

ВСТУП

Програма вивчення навчальної дисципліни "*Комплексні системи безпеки*" складена відповідно до освітньо-професійної програми підготовки *магістрів* спеціальності *125* «*Кібербезпека та захист інформації*».

Предметом вивчення навчальної дисципліни є комплексні системи безпеки, основою яких виступають підсистеми технічних засобів охорони (охоронно-пожежна сигналізація, система контролю та управління доступом, відеоспостереження та системи охорони периметру). Система розглядається як інтегрована (комплексна), основою якої виступають програмно-апаратні платформи, де дія в одній підсистемі викликає реакції в іншій, наприклад, Bosch BIS. Також розглядається автоматизація процесів при сумісному застосуванні підсистем (системи відеоаналітики, проекти типу "Безпечне місто", Smart City тощо.

Міждисциплінарні зв'язки:

- дисципліну забезпечують навчальні курси: Основи комп'ютерних технологій, Основи телекомунікацій і комп'ютерні мережі, матеріали та компоненти електроніки, архітектура та моделі безпеки, методи та засоби захисту інформації, фізична безпека та безпека оточення, безпека і експлуатація мережних і хмарних технологій;
- дисципліна забезпечує навчальні курси: Кіберфізична безпека об'єктів критичної інфраструктури, методологія забезпечення безперервності бізнес/операційних процесів сучасних підприємств.

1. Мета та завдання навчальної дисципліни

1.1. Метою викладання дисципліни «*Комплексні системи безпеки*» є формування знань щодо принципів побудови та оптимізації інтегрованих (автоматизованих) систем безпеки, аналіз принципів та варіантів складання технічного завдання на проектування автоматизованих систем безпеки, оволодіння методами рішення професійних завдань (оцінка рівнів демаркації при взаємодії систем, обстеження об'єкта з метою первинного збору інформації, оцінка рівнів та методики застосування автоматизованого інтелектуального обладнання).

1.2. Основними завданнями вивчення дисципліни «*Комплексні системи безпеки*» є вивчення класифікацій та компонентного складу інтегрованих систем безпеки, можливостей інтегрованих систем, структурних та функціональних схем обладнання, нормативних документів в галузі, ланки програмного забезпечення, відеоаналітики та інформаційно-аналітичних систем локального та глобального рівнів.

1.3. Згідно з вимогами освітньо-професійної програми студенти повинні:

знати:

Класифікацію і характеристики технічних засобів охорони різного призначення. Базові визначення в напрямку технічних засобів охорони, комплексних систем. Методологічні підходи до вирішення питань безпеки: системотехніку і комплексотехніку. Загальну структуру інтегрованих систем безпеки, базові рівні

мережевої взаємодії. Технічні засоби ІСБ та принципи проектування ІСБ, основні вимоги при реалізації універсальної апаратної платформи ІСБ. Інтеграцію на проектному, програмному, апаратному та апаратно-програмному рівнях (платформах) інтеграції. Загальні положення та можливості щодо платформи Building Integration System – системи збору та обробки інформації. Вивчення архітектури BIS, структури підключення різних підсистем до BIS, основні функції системи, інтерфейси користувачів. Системи інтелектуального відеоспостереження – задачі, можливості, принципи та технології, детектори тощо. Ситуаційні центри комплексних систем безпеки. Концепцію інформаційно-аналітичних систем типу "Безпечне місто" та Smart City;

вміти:

аналізувати державну та міжнародну нормативну базу щодо напрямку інтегрованих (комплексних) систем безпеки. Аналізувати тип та компонентний склад комплексних систем безпеки об'єктів в залежності від критеріїв масштабу та ТЗ. Розробляти технічне завдання на проектування з сукупними елементами. Вміти розраховувати технологічні параметри окремих підсистем КСБ, користуватися методиками та сервісами. Використовувати детектори систем інтелектуального відеоспостереження в залежності від завдання. Вміти ефективно використовувати технології та компоненти при розгортанні ситуаційних центрів при застосування комплексних та інтегрованих систем безпеки різного масштабу.

Вивчення навчальної дисципліни передбачає формування та розвиток у студентів **компетентностей**:

***Загальних*:**

ЗК 1. Здатність застосовувати знання у практичних ситуаціях;

ЗК 2. Знання та розуміння предметної області та розуміння професії;

4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням;

Фахових:

ФК2. Здатність формулювати, аналізувати та синтезувати рішення наукових задач і проблем на абстрактному рівні шляхом декомпозиції їх на складові, які можна дослідити окремо в їх більш та менш важливих аспектах

ФК7. Здатність розробляти та впровадити комплексну систему захисту інформації, що протидіє багатьом різним за природою загрозам (кібератаки з боку інсайдерів та хакерів, злам програм, віруси, перехоплення трафіку, помилки тощо).

ФК12. Здатність ефективно використовувати на практиці різні теорії в області навчання технологіям, засобам та організаційним аспектам безпеки інформаційних і комунікаційних систем та мереж.

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

А7.У10. Здатність впроваджувати (налаштовувати) апаратні засоби захисту інформації на об'єктах інформаційної діяльності

Результати навчання:

ПРН6 – Знання основ проектних процедури та принципів проектування складних технічних систем, принципів побудови систем автоматизованого проектування

Змістовний модуль: Управління доступом до інформаційних ресурсів: (кредитів ECTS – 5, 150 год).

2. Інформаційний обсяг навчальної дисципліни

Змістовий модуль. Комплексні системи безпеки

Тема 1. Введення в дисципліну. Методологія в питаннях безпеки. Визначення термінів функціональний ресурс системи, системотехніка та комплексотехніка, принципи комплексотехніки. Моделювання комплексної системи безпеки об'єкта.

Самостійно. Принципи системності та комплексності. Синергія та синергетичний ефект.

Тема 2. Визначення термінів АС, ІАС, ІСБ, КСБ тощо. Загальна структура інтегрованої системи безпеки, базові рівні мережевої взаємодії. принципів проектування ІСБ, основні вимоги при реалізації універсальної апаратної платформи ІСБ. Інтеграція на проектному, програмному, апаратному та апаратно-програмному рівнях (платформах) інтеграції.

Самостійно. Структурні схеми інтегрованих систем безпеки. Методи оцінки ефективності, швидкодія та залежність від масштабу

Тема 3. Загальні положення та можливості щодо платформи Building Integration System – системи збору та обробки інформації. Вивчення архітектури BIS, структури підключення різних підсистем до BIS, основні функції системи. Вивчення підсистем відеоспостереження, автоматизації та контролю доступу. Інтерфейс користувача, налаштування під вимоги замовника, інструментарій ActiveX. Приклади інтерфейсів користувачів системи BIS

Самостійно. Компонентний склад та сценарії роботи обладнання в екосистемі Bosch Building Integration System

Тема 4. Системи інтелектуального відеоспостереження та відеоаналітика. Базові відомості. Цілі, задачі, та технології систем. Функціональний склад типової системи відеоаналітики. Класифікація рішень в системах інтелектуального відеоспостереження. Детектори в системах інтелектуального відеоспостереження.

Самостійно. Дослідження рішень щодо сучасних систем відеоаналітики, представлених на ринку України та світу

Тема 5. Комплексні системи безпеки на основі екосистем Ajax та Tiras. Технології, компонентний склад, можливості застосування

Самостійно. Моделювання компонентного складу систему, складання специфікації в залежності від ТЗ на об'єкт. Використання спеціалізованих калькуляторів на корпоративних сайтах

Тема 6. Ситуаційні центри комплексних систем безпеки. Цілі, завдання та суб'єкти ситуаційних центрів. Масштаби ситуаційних центрів. Вимоги до фізичної та інформаційної інфраструктури, рівні оснащення ситуаційних центрів.

Самостійно. Загрози та ризики ситуаційних центрів, модель загроз, методи та засоби підвищення рівня безпеки ситуаційних центрів.

Тема 7. Концепція ІАС "Безпечне місто". Вимоги до побудови, основні підсистеми, приклади реалізації. Цілі та задачі при впровадженні системи безпеки міста, напрями впровадження, мета та переваги впровадження. Структура єдиної системи безпеки міста. Компоненти інфраструктури. Формування диспетчерських (ситуаційних) центрів

Самостійно. Вивчення досвіду щодо впровадження в містах України та світу КСБ в проектах типу "Безпечне місто". Технології, бренди, компонентний склад, результати.

3. Рекомендована література

1. Конспект лекцій з дисципліни Комплексні системи безпеки. Стайкуца С.В. ДУІТЗ, 2021 р.
2. Методичні вказівки для виконання курсу лабораторних робіт з дисципліни Комплексні системи безпеки. Стайкуца С.В., Бєлова Ю.В., Сєдов К.С., Севастєєв Є.О. ДУІТЗ, 2021 р.
3. Концепція комплексної системи безпеки. Робочий документ компанії Bosch

Інформаційні ресурси

1. Ajax [Електронний ресурс] // Корпоративний сайт Ajax. – 2023. – Режим доступу до ресурсу: https://ajax.systems/ua/.

2. Tiras [Електронний ресурс] // Корпоративний сайт Tiras. – 2023. – Режим доступу до ресурсу: https://tiras.technology/.

3. Bosch Security and Safety Systems [Електронний ресурс] // Корпоративний сайт компанії Bosch. – 2023. – Режим доступу до ресурсу: https://www.boschsecurity.com/pl/ru/.

4. Форма підсумкового контролю успішності навчання КП + залік

5. Оцінювання знань

(Шкала оцінювання: національна та ЄКТС)

Сума балів за всі види навчальної діяльності	Оцінка за національною шкалою	
	для екзамену, курсового проекту (роботи), практики	для заліку
90-100	відмінно	зараховано
82-89	добре	
74-81		
64-73	задовільно	
60-63		
35-59	незадовільно з можливістю	не зараховано з можливістю

	повторного складання	повторного складання
1-34	незадовільно з обов’язковим повторним вивченням дисципліни	не зараховано з обов’язковим повторним вивченням дисципліни

Засоби діагностики успішності навчання:
виконання лабораторних робіт, відповіді на практичних заняттях, виконання та захист курсового проекту.