СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

КОМПЛЕКСНІ СИСТЕМИ БЕЗПЕКИ

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 і кібербезпеки
Кафедра	Кібербезпеки та технічного захисту інформації
Статус навчальної дисципліни	**ОК-6** ОПП «Кібербезпека та захист інформації»
Форма навчання	Денна

Викладач

Стайкуца Сергій Володимирович
s.v_staikutsa@suitt.edu.ua

Доцент кафедри кібербезпеки та технічного захисту інформації (КБ та ТЗІ), кандидат філософських наук, доцент

Загальна інформація про дисципліну

Анотація до дисципліни	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 використанні підсистем (системи відеоаналітики, проекти типу ”Безпечне місто”, Smart City тощо.

Мета дисципліни	– 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).
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. КФ1.Здатність обґрунтовано застосовувати, інтегрувати, розробляти та удосконалювати сучасні інформаційні технології, фізичні та математичні моделі, а також технології створення та використання прикладного і спеціалізованого програмного забезпечення для вирішення професійних задач у сфері інформаційної безпеки та/або кібербезпеки. 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/ КФ11. Здатність розробляти та впроваджувати комплексну систему захисту інформації, що протидіє багатьом різним за природою загрозам (кібератаки з боку інсайдерів та хакерів, злам програм, віруси, перехоплення трафіку, помилки тощо). КФ16. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації. КФ17. Здатність проводити оцінку відповідності (атестацію) комплексів технічного 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. 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. РН16. Приймати обґрунтовані рішення з організаційно-технічних питань інформаційної безпеки та/або кібербезпеки у складних і непередбачуваних умовах, у тому числі із застосуванням сучасних методів та засобів оптимізації, прогнозування та прийняття рішень. РН19. Обирати, аналізувати і розробляти придатні типові аналітичні, розрахункові та експериментальні методи кіберзахисту, розробляти, реалізовувати та супроводжувати проекти з захисту інформації у кіберпросторі, інноваційної діяльності та захисту інтелектуальної власності. РН22. Планувати та виконувати експериментальні і теоретичні дослідження, висувати і перевіряти гіпотези, обирати для цього придатні методи та інструменти, здійснювати статистичну обробку даних, оцінювати достовірність результатів досліджень, аргументувати висновки. 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.
Обсяг дисципліни	Загальний обсяг дисципліни: 5 кредитів ЄКТС 150 годин). Для денної форми навчання: лекції – 14 годин, практичні заняття –14 години, лабораторні заняття –24 години, самостійна робота – 98 годин.
Форма підсумкового контролю	Залік
Терміни викладання дисципліни	Дисципліна викладається у 1-му семестрі

Програма дисципліни	
Тема 1.	***Методологія організації комплексної безпеки об'єктів.*** Основні цілі та задачі при побудові комплексних систем безпеки. Принципи системності та комплексності.
Тема 2.	***Структура та*** рівні мережевої взаємодії при побудові КСБ. Загальна структура інтегрованої системи безпеки, базові рівні мережевої взаємодії, принципи проектування ІСБ, основні вимоги при реалізації універсальної апаратної платформи ІСБ.
Тема 3.	***Аналіз можливостей платформи Building Integration System.*** 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.
Тема 4.	***Системи інтелектуального відеоспостереження та відеоаналітика*** Цілі, задачі, та технології систем інтелектуального відеоспостереження.
Тема 5.	***Програмно-апаратні рішення в масштабі комплексних систем безпеки*** Аналіз світового ринку рішень КСБ. Вітчизняні рішення - Ajax, Tiras. Технології, компонентний склад, функції.
Тема 6.	***Ситуаційні центри комплексних систем безпеки.*** Цілі, завдання та суб'єкти ситуаційних центрів. Масштаби та вимоги до інфраструктури.
Тема 7.	***Концепція ІАС "Безпечне місто".*** Вимоги до побудови, основні підсистеми, цілі та задачі, компоненти інфраструктури.

Список рекомендованих джерел

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
4. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека: Термінологічний навчальний довідник / За ред. Кривуци В.Р – Київ.: ООО "Д.В.К.", 2004. – 508 с.
5. Ajax [Електронний ресурс] // Корпоративний сайт Ajax. – 2023. – Режим доступу до ресурсу: https://ajax.systems/ua/.
6. Tiras [Електронний ресурс] // Корпоративний сайт Tiras. – 2023. – Режим доступу до ресурсу: https://tiras.technology/.
7. Bosch Security and Safety Systems [Електронний ресурс] // Корпоративний сайт компанії Bosch. – 2023. – Режим доступу до ресурсу: https://www.boschsecurity.com/pl/ru/.

Інформація про консультації

Щосереди у вересні-грудні 2024 року з 14.30 до 15.30 год., ауд. 250 або зум – доц. С.В. Стайкуца

Загальна схема оцінювання

<table>
<tr><td rowspan="2">Сума балів за всі види навчальної діяльності</td><td rowspan="2">Шкала ЄКТС</td><td colspan="2">Оцінка за національною шкалою</td><td rowspan="2">Нарахування балів</td><td>Бали нараховуються таким чином:</td></tr>
<tr><td>для іспиту</td><td>для заліку</td><td rowspan="8">Оцінювання знань здобувачів вищої освіти здійснюється
за 100-бальною шкалою і становить:
за поточну успішність (участь у практичних заняттях, виконання практичних завдань та контрольних робіт) – до 60 балів,
за результати екзамену – до 40 балів.</td></tr>
<tr><td>90-100</td><td>A</td><td>Відмінно</td><td rowspan="5">зараховано</td></tr>
<tr><td>82-89</td><td>B</td><td rowspan="2">Добре</td></tr>
<tr><td>74-81</td><td>C</td></tr>
<tr><td>64-73</td><td>D</td><td rowspan="2">Задовільно</td></tr>
<tr><td>60-63</td><td>E</td></tr>
<tr><td>35-59</td><td>FX</td><td>Незадовільно з можливістю повторного складання</td><td>Не зараховано з можливістю повторного складання</td></tr>
<tr><td>0-34</td><td>F</td><td>Незадовільно з обов’язковим повторним вивченням дисципліни</td><td>Не зараховано з обов’язковим повторним вивченням дисципліни</td></tr>
</table>

Політика опанування дисципліни

Відвідування: Здобувачі вищої освіти самостійно планують відвідування лекційних занять, що проводяться в межах дисципліни. Присутність на практичних заняттях, лабораторних 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 вищої освіти самостійно, на засадах академічної доброчесності. Викладач має право для перевірки робіт застосовувати програму **Unicheck.**