



СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Комплексні системи безпеки

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-6)
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. – 8 год., практ. зан. – 8 год., самост. роб. – 94 год.;
Мова викладання	Українська
Кафедра	Кібербезпеки та технічного захисту інформації
Факультет	Інформаційних технологій та кібербезпеки

Викладач

Стайкуца Сергій Володимирович



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

E-mail: s.v_staikutsa@suitt.edu.ua

Консультації: щоп'ятниці з 14³⁰ до 15³⁰ год., ауд. 218

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	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. СК-1.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. 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-11. 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). СК-16. Здатність аналізувати потреби та вимоги користувачів (замовників) щодо захисту інформації та кіберзахисту з метою впровадження систем та комплексів захисту інформації. СК-17. Здатність проводити оцінку відповідності (атестацію) комплексів технічного захисту інформації.
Програмні результати навчання	ПРН-2. 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. ПРН5. 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. 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.

Програма навчальної дисципліни

Тема 1. Методологія Основні цілі, задачі та вимоги замовника при побудові комплексних систем безпеки. Принципи системності та організації комплексної комплексності.

безпеки об'єктів.

Тема 2. Структура та Загальна структура інтегрованої системи безпеки, базові рівні мережевої взаємодії, принципи та стандарти рівні мережевої проектування ІСБ, основні вимоги до реалізації універсальної апаратної платформи ІСБ.

взаємодії при побудові КСБ.

Тема 3. Інженерно-технічні засоби та Про фізичний захист периметру: бар'єри, датчики, освітлення та реагування. Як виявити і затримати порушника та фізичний захист інтегрувати все в єдину систему безпеки.

периметру

Тема 4. Аналіз Загальні положення та можливості щодо платформи Building Integration System – системи збору та обробки можливостей інформації. Вивчення архітектури BIS, структури підключення різних підсистем до BIS, основні функції системи.

платформи Building Integration System.

Тема 5. Системи Цілі, задачі, та технології систем інтелектуального відеоспостереження.

інтелектуального відеоспостереження та відеоаналітика

Тема 6. Кібербезпека та Перехід систем безпеки до мережевих (IP) рішень і пов'язані з цим кіберзагрози. Концепція Zero Trust, захист каналів зв'язку в мікросегментація мережі та безперервна автентифікація користувачів і пристроїв.

інтегрованих системах

Тема 7. Програмно- Аналіз світового ринку рішень КСБ. Вітчизняні рішення - Ajax, Tiras. Технології, компонентний склад, функції.

апаратні рішення в масштабі комплексних систем безпеки

Тема 8. Ситуаційні Цілі, завдання та суб'єкти ситуаційних центрів. Масштаби та вимоги до інфраструктури.

центри комплексних систем безпеки.

Тема 9. Концепція ІАС “Безпечне місто”. Вимоги до побудови, оцінки відповідності та атестації комплексних систем безпеки, основні підсистеми, цілі та задачі, компоненти інфраструктури.

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 тощо.
- 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 дисципліни Результати навчання з даної дисципліни, які здобувач може продемонструвати та які можна ідентифікувати, оцінити і звиміряти, 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 концептуальних положень методології організації комплексної безпеки об’єктів, основних цілей та задач побудови комплексних систем безпеки (КСБ), принципів системності та комплексності, структури та рівнів мережевої взаємодії під час побудови інтегрованих систем безпеки (ІСБ). Передбачається розуміння архітектури інтегрованих платформ безпеки, зокрема систем збору та обробки інформації типу Building Integration System (BIS), принципів їх проектування, вимог до універсальних апаратних платформ, а також знання сучасних технологій інтелектуального відеоспостереження, відеоаналітики, програмно-апаратних рішень комплексних систем безпеки, включаючи світові та вітчизняні рішення (Ajax, Tiras). Також передбачається розуміння концепції ситуаційних центрів та інформаційно-аналітичних систем типу «Безпечне місто», їх функцій,

інфраструктури та основних підсистем

Уміння/навички – формується здатність аналізувати потреби та вимоги замовників, проектувати та впроваджувати комплексні системи безпеки об'єктів на основі системного підходу, здійснювати інтеграцію різних підсистем безпеки (контроль доступу, відеоспостереження, сигналізація, аналітичні модулі) у єдину інформаційну платформу. Здобувач набуває навичок аналізу архітектури інтегрованих систем безпеки, оцінювання можливостей програмно-апаратних платформ, використання систем відеоаналітики та моніторингу, а також здатності розв'язувати складні задачі у сфері організації ситуаційних центрів і побудови інфраструктури систем «Безпечне місто» з урахуванням сучасних технологій та вимог кібербезпеки.

Комунікація – здатність ефективно взаємодіяти з фахівцями у сфері інформаційної та технічної безпеки, брати участь у командній роботі під час проектування та впровадження комплексних систем безпеки, використовувати сучасні інформаційно-комунікаційні технології для обміну технічною інформацією, підготовки аналітичних матеріалів та презентації результатів досліджень

Відповідальність і автономія – очікується здатність самостійно приймати обґрунтовані рішення щодо проектування та впровадження комплексних систем безпеки, оцінювати ризики та ефективність застосованих технологічних рішень, розв'язувати нестандартні задачі у сфері інтеграції систем безпеки, організації ситуаційних центрів та управління інфраструктурою систем типу «Безпечне місто», демонструючи професійну відповідальність за прийняті рішення та результати діяльності.

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. 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.
Форма та методи контролю начальних досягнень	Політика навчальної дисципліни 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 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 різні програмні засоби.

Умови зарахування пропущених занять Інші умови	Відпрацювання академічної заборгованості з дисципліни можливо до початку екзаменаційної сесії. Процедура узгоджується з викладачем, згідно його розкладу консультацій. Навчально-методичні матеріали дисципліни розміщені на платформі Moodle
Базові підручники та навчальні посібники	Рекомендовані джерела інформації • Балтовський О. А., Форос А. В., Пядишев В. Г. (уклад.) Безпека технічних систем : навчально-методичні матеріали. — Одеса : ОДУВС, 2024. — 36 с. • Собченко В. А. та ін. Технічні засоби охорони кордону. Частина I. Технічні засоби спостереження : навчальний посібник (електр. навч. вид.). — Хмельницький : Видавництво НАДПСУ, 2024. — 218 с. • Андрієнко А. О. Упровадження концепції «Smart City» в управління великими містами України : монографія. — Вінниця, Україна : ГО «Європейська наукова платформа», 2023. — 196 с. • Кушнір А. П., Чалий Д. О. Системи пожежної та охоронної сигналізації : навч. посіб. — Львів : СПОЛОМ, 2022. — 298 с. • Батчаєв В. К., Шадська У. С. Відеоспостереження у публічних місцях: основи захисту персональних даних (посібник для органів місцевого самоврядування). — К. : Компринт, 2021. — 98 с. • Хорошко В. О. та ін. Проектування комплексних систем захисту інформації. — Л. : Львівська політехніка, 2020. — 320 с. • Козюра В. Д., Хорошко В. О., Шелест М. Є., Ткач Ю. М., Усов Я. Ю. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах : навчальний посібник. — Ніжин, 2019. — 144 с. • Дудикевич В. Б., Хорошко В. О., Яремчук Ю. Є. Основи інформаційної безпеки : навчальний посібник. — Вінниця : ВНТУ, 2018. — 316 с. • Субботін С. О. Інтелектуальні інформаційні системи : навчальний посібник. — Київ : КНТ, 2016.
Методичні рекомендації та розробки викладачів дисципліни	• Конспект лекцій з дисципліни “Комплексні системи безпеки”. Стайкуца С.В. ДУІТЗ, 2024 р. • Комплексні системи безпеки, навчально-методичні вказівки до виконання лабораторних робіт [для здобувачів другого (магістерський) рівня вищої освіти за спеціальністю «Кібербезпека та захист інформації»]. / Уклад., Стайкуца С.В., Заровський Р.В., Івахненко М.С., Одеса, ДУІТЗ, 2025, 90 с. • Стайкуца С.В., Заровський Р.В., Вихристюк О.А., Івахненко М.С., Комплексні системи безпеки. Сучасні системи відеоспостереження та відеоаналітики екосистеми Kobi Software: методичні вказівки до лабораторних робіт [для здобувачів другого (магістерський) рівня вищої освіти за спеціальністю F5 «Кібербезпека та захист інформації»]. — Одеса : ДУІТЗ, 2026. — 76 с.
Інформаційні ресурси	• Ajax Systems – Професійна система безпеки [Електронний ресурс]. URL: https://ajax.systems (дата звернення: 18.02.2023). • Тірас-12 – Український виробник систем безпеки [Електронний ресурс]. URL: https://tiras.technology (дата звернення: 13.02.2024).

- Bosch Security and Safety Systems I Global [Electronic resource]. URL: <https://www.boschsecurity.com/global/en/> (date of access: 08.03.2024).
- U-Prox – Системи безпеки та контролю доступу [Електронний ресурс]. URL: <https://u-prox.systems> (дата звернення: 08.03.2024).
- КОБІ – Дистриб'ютор систем відеоспостереження та безпеки [Електронний ресурс]. URL: <https://kobi.ua> (дата звернення: 22.05.2025).
- NIST Technical Series Publications. <https://www.nist.gov>. URL: <https://www.nist.gov/nist-research-library/nist-publications>.
- Zero Trust and Continuous Authentication: A Partnership for Network Security. <https://www.beyondidentity.com/>. URL: <https://www.beyondidentity.com/resource/zero-trust-and-continuous-authentication-a-partnership-for-network-security> (дата звернення: 23.04.2026).
- Затверджено оновлені вимоги до кіберзахисту об'єктів критичної інфраструктури. <https://cybersec.net.ua>. 17.11.2025. URL: <https://cybersec.net.ua/normatyvni-dokumenty/936-zatverdzheno-onovleni-vymohy-do-kiberzakhystu-obiektiv-krytychnoi-infrastruktury.html> (дата звернення: 26.11.2025).

**Рік введення
силабусу – 2026 р.**

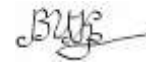
Затверджено рішенням кафедри кібербезпеки та технічного захисту інформації
(Протокол від 22 травня 2026 р. №13)

Завідувач кафедри



Володимир КОРЧИНСЬКИЙ

Гарант освітньої програми



Віталій КІЛЬДІШЕВ

Викладач:



Сергій СТАЙКУЦА