Міністерство освіти і науки України
Національний аерокосмічний університет ім. М.Є. Жуковського
«Харківський авіаційний інститут»

Кафедра комп'ютерних систем, мереж і кібербезпеки (№503)

ЗАТВЕРДЖУЮ

Гарант освітньої програми


_____ Олег ІЛЛЯШЕНКО
(підпис) (ім'я та ПРІЗВИЩЕ)

« 29 » серпня 2025 р.

СИЛАБУС ОБОВ'ЯЗКОВОЇНАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Комплексні системи захисту інформації: проектування, впровадження, супровід»
(назва навчальної дисципліни)

Галузь знань: 12 "Інформаційні технології"
(шифр і найменування галузі знань)

Спеціальність: 125 "Кібербезпека"
(код та найменування спеціальності)

Освітня програма: Безпека інформаційних і комунікаційних систем
(найменування освітньої програми)

Рівень вищої освіти:***перший (бакалаврський)***

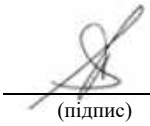
Силабус введено в дію з 01.09.2025 року

Харків – 2025р.

Розробник:  Брежнєв Є.В., проф., д.т.н
(прізвище та ініціали, посада, науковий ступінь та вчене звання) (підпис)

Силабус розглянуто на засіданні кафедри комп'ютерних систем, мереж і кібербезпеки
(назва кафедри)

Протокол №1 від «29» 08 2025р.

Завідувач кафедри д.т.н., професор  ВячеславХАРЧЕНКО
(науковий ступінь та вчене звання) (підпис) (ім'я таПРІЗВИЩЕ)

Погоджено з представником здобувачів освіти:

 Ілля МІЦИК
(підпис) (ім'я та ПРІЗВИЩЕ)

1. Загальна інформація про викладача

Брежнєв Євген Віталійович
професор кафедри комп'ютерних систем, мереж і кібербезпеки
доктор технічних наук, професор
Викладає дисципліни: «Комплексні системи захисту інформації: проектування, впровадження, супровід», «Методи дослідження комп'ютерних систем та мереж», «Технології бізнес аналітики».
Напрями наукових досліджень: застосування інформаційних технологій щодо побудови захисту складних технічних систем, методи забезпечення гарантоздастності систем що базуються на штучному інтелекті, безпека критичних інфраструктур.
Контактна інформація:
e-mail: e.brezhnev@csn.khai.edu

2. Опис навчальної дисципліни

Форма здобуття освіти	*Денна*
Семестр	7 семестр
Мова викладання	Українська
Тип дисципліни	*Обов'язкова*
Обсяг дисципліни: кредити ЄКТС/ кількість годин	4 кредити ЄКТС / 120 годин (64 аудиторних, з яких: лекції - 32, практичні роботи – 32, самостійна робота – 56)
Види навчальної діяльності	Лекції, практичні заняття.
Види контролю	Модульний контроль, семестровий контроль – іспит
Пререквізити	«Захист інформації в інформаційно-комунікаційних системах», «Прикладна криптологія», «Надійність та функціональна безпека інформаційно-управляючих систем», «Системи технічного захисту інформації».

3. Мета та завдання навчальної дисципліни, переліки компетентностей та очікуваних результатів навчання

Мета: є формування у студентів теоретичних знань та практичних навичок у галузі проектування, впровадження та експлуатації комплексних систем захисту інформації; застосування системного підходу до забезпечення інформаційної безпеки, включаючи комплекс організаційних заходів.

Завдання:

– вивчити основні поняття комплексної системи захисту інформації;

– застосовувати знання до вирішення задач інформаційної безпеки;

– обирати потрібні організаційні та інженерно-технічні заходи, засоби і методи захисту інформації;

– аналізувати вхідні дані та обирати методи оцінки якості.

Компетентності, які набуваються:

а) загальні компетентності:

КЗ 1. Здатність застосовувати знання у практичних ситуаціях.

КЗ 2. Знання та розуміння предметної області та розуміння професії.

КЗ 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.

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

КЗ 5. Здатність до пошуку, оброблення та аналізу інформації

б) фахові компетентності:

КФ 4. Здатність забезпечувати неперервність бізнесу згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 5. Здатність забезпечувати захист інформації, що обробляється в інформаційно-телекомунікаційних (автоматизованих) системах з метою реалізації встановленої політики інформаційної та/або кібербезпеки.

КФ 6. Здатність відновлювати штатне функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем після реалізації загроз, здійснення кібератак, збоїв та відмов різних класів та походження.

КФ 7. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів та ін.).

КФ 8. Здатність здійснювати процедури управління інцидентами, проводити розслідування, надавати їм оцінку.

КФ 9. Здатність здійснювати професійну діяльність на основі впровадженої системи управління інформаційною та/або кібербезпеки.

КФ 10. Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об’єктах інформаційної діяльності.

КФ 11. Здатність виконувати моніторинг процесів функціонування інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем згідно встановленої політики інформаційної та/або кібербезпеки.

КФ 12. Здатність аналізувати, виявляти та оцінювати можливі загрози, уразливості та дестабілізуючі чинники інформаційному простору та інформаційним ресурсам згідно з встановленою політикою інформаційної та/або кібербезпеки.

Програмні результати навчання:

ПРН 1 Застосовувати знання державної та іноземних мов з метою забезпечення ефективності професійної комунікації.

ПРН 2 Організовувати власну професійну діяльність, обирати оптимальні методи та способи розв'язування складних спеціалізованих задач та практичних проблем у професійній діяльності, оцінювати їхню ефективність.

ПРН 3 Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел для ефективного рішення спеціалізованих задач професійної діяльності.

ПРН 4 Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач та практичних проблем у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

ПРН 5 Адаптуватися в умовах частої зміни технологій професійної діяльності, прогнозувати кінцевий результат.

ПРН 6 Критично осмислювати основні теорії, принципи, методи і поняття у навчанні та професійній діяльності.

ПРН 7 Діяти на основі законодавчої та нормативно-правової бази України та вимог відповідних стандартів, у тому числі міжнародних в галузі інформаційної та /або кібербезпеки.

ПРН 8 Готувати пропозиції до нормативних актів щодо забезпечення інформаційної та /або кібербезпеки.

ПРН 9 Впроваджувати процеси, що базуються на національних та міжнародних стандартах, виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної та/або кібербезпеки.

ПРН 10 Виконувати аналіз та декомпозицію інформаційно-телекомунікаційних систем.

ПРН 12 Розробляти моделі загроз та порушника.

ПРН 13 Аналізувати проекти інформаційно-телекомунікаційних систем базуючись на стандартизованих технологіях та протоколах передачі даних.

ПРН 14 вирішувати завдання захисту програм та інформації, що обробляється в інформаційно-телекомунікаційних системах програмно-апаратними засобами та давати оцінку результативності якості прийнятих рішень.

ПРН 16 Реалізовувати комплексні системи захисту інформації в автоматизованих системах (АС) організації (підприємства) відповідно до вимог нормативно-правових документів.

ПРН 17 Забезпечувати процеси захисту та функціонування інформаційно-телекомунікаційних (автоматизованих) систем на основі практик, навичок та знань, щодо структурних (структурно-логічних) схем, топології мережі, сучасних архітектур та моделей захисту електронних інформаційних ресурсів з

відображенням взаємозв’язків та інформаційних потоків, процесів для внутрішніх і віддалених компонент.

ПРН 19 Застосовувати теорії та методи захисту для забезпечення безпеки інформації в інформаційно-телекомунікаційних системах.

ПРН 21 Вирішувати задачі забезпечення та супроводу (в.т. числі: огляд, тестування, підзвітність) системи управління доступом згідно встановленої політики безпеки в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 23 Реалізовувати заходи з протидії отриманню несанкціонованого доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах.

ПРН 24 Вирішувати задачі управління доступом до інформаційних ресурсів та процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах на основі моделей управління доступом (мандатних, дискреційних, рольових).

ПРН 26 Впроваджувати заходи та забезпечувати реалізацію процесів попередження отриманню несанкціонованого доступу і захисту інформаційних, інформаційно-телекомунікаційних (автоматизованих) систем на основі еталонної моделі взаємодії відкритих систем.

ПРН 29 Здійснювати оцінювання можливості реалізації потенційних загроз інформації, що обробляється в інформаційно-телекомунікаційних системах та ефективності використання комплексів засобів захисту в умовах реалізації загроз різних класів.

ПРН 30 Здійснювати оцінювання можливості несанкціонованого доступу до елементів інформаційно-телекомунікаційних систем.

ПРН 31 Застосовувати теорії та методи захисту для забезпечення безпеки елементів інформаційно-телекомунікаційних систем.

ПРН 33 Вирішувати задачі забезпечення безперервності бізнес процесів організації на основі теорії ризиків.

ПРН 34 Приймати участь у розробці та впровадженні стратегії інформаційної безпеки та/або кібербезпеки відповідно до цілей і завдань організації.

ПРН 35 Вирішувати задачі забезпечення та супроводу комплексних систем захисту інформації, а також протидії несанкціонованому доступу до інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах згідно встановленої політики інформаційної і\або кібербезпеки.

Пререквізити

Дисципліна базується на: ОК15 «Курс на вибір 1 Захист інформації в інформаційно-комунікаційних системах», ОК23 «Прикладна криптологія», ОК24 «Надійність та функціональна безпека інформаційно-управляючих систем», ОК25 «Системи технічного захисту інформації». Дисципліна є базовою для: ВБ1.7 «Комплексні системи захисту інформації: проектування, впровадження, супровід», ВБ1.15 «Комплексні системи захисту інформації:

проектування, впровадження, супровід (КП)», ОК36 «Дипломний робота (проект) бакалавра».

4. Зміст навчальної дисципліни

Змістовний модуль 1. Основи теорії захисту інформації.

ТЕМА 1. Вступ до дисциплини

Інформація. Інформаційна безпека. Визначення комплексної системи захисту інформації. Етапи побудови КСЗІ. Принципи побудови КСЗІ. Рекомендована література.

Тема Лекції 1: *«Вступ до дисциплини».*

Тема практичної роботи 1: Визначення вартості інформації

ТЕМА 2. Архітектура безпеки ІТС

Загрози безпеки для ІТС. Застосування сервісів безпеки до рівнів безпеки ІТС. Поняття архітектури безпеки ІТС. Основні компоненти архітектури. Типи атак на ІТС. Системи захисту інформації.

Тема Лекції 2: *«Архітектура безпеки інформаційно-телекомунікаційних систем ».*

ТЕМА 3. Моделі захисту інформації

Визначення суб'єктів та об'єктів в моделях ЗІ. Мандатні моделі ЗІ. суб'єктно-об'єктні моделі ЗІ. Політика безпеки.

Тема Лекції 3: *«Моделі захисту інформації».*

Тема практичної роботи 2: Вивчення моделей аналізу інцидентів, загроз та правопорушника

ТЕМА 4. Моделювання впливу на інформацію

Загрози інформації. Модель загроз. Модель Порушника.

Тема Лекції 4: *«Моделювання впливу на інформацію».*

Тема практичної роботи 3: Ознайомлення з ПЗ аналізу ризиків інформаційної безпеки. SecuriTree

ТЕМА 5. Системи фізичного захисту об'єктів критичної інфраструктури

Критична інфраструктура. Категоризація об’єктів критичної інфраструктури. Особливості задач охорони об'єктів. Принципи забезпечення безпеки. Завдання систем захисту. Приклади.

Тема Лекції 5: *«Системи фізичного захисту об'єктів критичної інфраструктури»*.

Тема практичної роботи 4: Визначення показника ефективності засобів охорони території обєктів

ТЕМА 6. Визначення інформації яка потребує захисту.

Методика визначення інформації яка потребує захисту. Класифікація інформації. Проблеми визначення інформації.

Тема Лекції 6: *«Визначення інформації що потрібно захищати»*.

ТЕМА 7. Побудова КСЗІ периметру важливого об’єкту.

Приклади загроз важливого об’єкту. Інтегрований комплекс безпеки (ІКБ). Архітектура ІКБ. Склад ІКБ. Аналіз ефективності ІКБ. Методи аналізу ефективності ІСБ.

Тема Лекції 7: *«Побудова КСЗІ периметру важливого об’єкту»*.

Тема практичної роботи 5: Застосування інструментальних засобів для оцінювання інформаційної безпеки промислового об’єкту

ТЕМА 8. Аудит інформаційної безпеки

Аудит інформаційної безпеки (мета, завдання, класификація). Види аудиту. Основні етапи аудиту безпеки. Доументи аудиту.

Тема Лекції 8: *«Аудит інформаційної безпеки»*.

Модульний контроль.

Змістовний модуль 2. Канали витоку інформації. Засоби контролю.

ТЕМА 9. Системи відео спостереження

Основні визначення. Основні завдання системи відео спостереження (СВВ). Класифікація СВВ. Аналогові та цифрові системи. Переваги та недоліки. Гібридні системи.

Тема Лекції 9: *«Системи відео спостереження»*.

ТЕМА 10. Системи пожежогасіння на об'єктах з ОЕТ

Визначення та призначення. Класифікація. Сповіщувачі. Оповіщувачи. Система автоматичного пожежогасіння.

Тема Лекції 10: *«Системи пожежогасіння на об'єктах з ОЕТ».*

ТЕМА 11. Система контролю та управління доступом

Класифікація СКУД. Призначення СКУД. Електронна прохідна. Датчики СКУД.

Тема Лекції 11: *«Система контролю та управління доступом».*

ТЕМА 12. Канали контролю доступу. Засоби контролю

Визначення та призначення. Зони охорони. Оптимізація побудови охорони периметру. Системи охорони периметру.

Тема Лекції 12: *«Канали контролю доступу. Засоби контролю».*

Тема практичної роботи 6: Застосування штучного інтелекту для розробки специфікації системи фізичного захисту

ТЕМА 13. Аспекти соціальної інженерії в КСЗІ. Аспекти не благочестя та корупції в контексті кібербезпеки

Концепції соціальної інженерії. Техніки соціальної інженерії. Соціальна інженерія у соціальних мережах. Крадіжка особистих даних. Контрзаходи соціальної інженерії. Роль та вплив кібербепеки в боротьбі з корупцією в державі.

Тема Лекції 13: *«Аспекти соціальної інженерії в КСЗІ».*

ТЕМА 16. Підсумок вивченого матеріалу

Тема Лекції 13: *«Підсумкова лекція».*

Модульний контроль.

5. Індивідуальні завдання

№ з/п	Назва теми	Кількість годин
...	*Не передбачено*	

6. Методи навчання

Словесні (пояснення, розповідь, проблемний виклад), наочні (ілюстрування, демонстрація, презентація), практичні.

7. Методи контролю

Проведення поточного контролю, письмового модульного контролю, підсумковий контроль у вигляді іспиту.

8. Критерії оцінювання та розподіл балів, які отримують здобувачі освіти

Таблиця 1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовий модуль 1,2			
Виконання і захист лабораторних робіт	0…5	3	0…15
Модульний контроль	0…25	1	0…25
Змістовий модуль 3,4			
Виконання і захист лабораторних робіт	0...5	5	0…25
Виконання і захист розрахунково-графічного завдання	0...10	1	0…10
Модульний контроль	0…25	1	0…25
Усього за семестр			**0…100**

Семестровий контроль у вигляді іспиту проводиться у разі відмови студента від балів поточного тестування й за наявності допуску до іспиту. Під час складання семестрового іспиту студент має можливість отримати максимум 100 балів.

Білет для іспиту складається із двох теоретичних та одного практичного запитання, максимальна кількість балів за кожне теоретичне запитання, складає 34 балів, а за практичне – 32 балів.

Таблиця 2 – Шкали оцінювання: бальна та традиційна

Сума балів	Оцінка за традиційною шкалою
	Іспит
90-100	Відмінно
75-89	Добре
60-74	Задовільно
0-59	Незадовільно

Критерії оцінювання роботи здобувач освіти протягом семестру

Задовільно (60 – 74). Мати мінімум знань та умінь. Відпрацювати та захистити всі лабораторні роботи.

Знати визначення комплексної системи захисту інформації, етапи побудови КСЗІ, принципи побудови КСЗІ. Розуміти архітектуру безпеки ІТС, загрози безпеки для ІТС. Знати моделі захисту інформації, модель порушника та модель загроз. Знати категоризацію об’єктів критичної інфраструктури. Особливості задач охорони об'єктів. Принципи забезпечення безпеки. Завдання систем захисту.

Вміти обґрунтувати основні компоненти комплексної системи захисту, формулювати загрози об’єктів та будувати модель загроз, порушника та КСЗІ.

Добре (75 – 89). Твердо знати матеріал дисципліни, виконати всі завдання. Показати вміння виконувати та захищати всі лабораторні роботи в обумовлений викладачем строк з обґрунтуванням рішень та заходів, які запропоновано у роботах.

Окрім знань, необхідних для отримання задовільної оцінки, студент повинен знати методи визначення вартості інформації. Розуміти категорії об’єктів захисту. Особливості охорони різних типів об’єктів та структуру системи забезпечення безпеки об’єктів. Студент також повинен знати загальні принципи забезпечення безпеки об’єктів, системи охоронно-тривожної сигналізації, охоронні сповіщувачі. Знати основні етапи аудиту інформаційної безпеки.

Вміти формулювати вимоги до систем контролю доступу та системи охоронно-тривожної сигналізації, розраховувати вартість інформації, базуючись на основних методах.

Відмінно (90 – 100). Повністю знати основний та додатковий матеріал. Знати всі теми. Орієнтуватися у підручниках та посібниках. Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та уміти застосовувати їх. Безпомилково виконувати та захищати всі роботи в обумовлений викладачем строк з докладним обґрунтуванням рішень та заходів, які запропоновано у роботах.

Окрім знань, необхідних для отримання оцінки добре, студент повинен знати методи класифікації СКУД, призначення СКУД. Визначення та призначення системи телевізійного спостереження. Визначення та призначення системи пожежної сигналізації. Визначення та призначення каналів контролю доступу. Аспекти соціальної інженерії в КСЗІ. Аспекти недоброчесності та корупції в контексті кібербезпеки.

Вміти створювати та документувати специфікацію (ТЗ) КСЗІ із застосуванням сучасних інформаційних технологій (штучного інтелекту).

9. Політика навчального курсу

Відвідування занять. Регуляція пропусків. Характер курсу передбачає необхідність відвідування занять. Здобувачі освіти, які за певних обставин не

можуть відвідувати заняття регулярно, повинні протягом тижня узгодити із викладачем графік індивідуального відпрацювання пропущених занять. Окремі пропущені заняття мають бути відпрацьовані на найближчій консультації протягом тижня після їх пропуску. Відпрацювання занять здійснюється усно у формі співбесіди за питаннями, визначеними планом заняття. В окремих випадках дозволяється письмове відпрацювання пропущених занять шляхом виконання індивідуального письмового завдання.

Дотримання вимог академічної доброчесності здобувачами освіти під час вивчення навчальної дисципліни. Під час вивчення навчальної дисципліни здобувані освіти мають дотримуватися загальноприйнятих морально-етичних норм і правил поведінки, вимог академічної доброчесності, передбачених Положенням про академічну доброчесність Національного аерокосмічного університету«Харківський авіаційний інститут» (https://khai.edu/assets/files/polozhennya/polozhennya-pro-akademichnu-dobrochesnist.pdf). Очікується, що роботи здобувачів освіти будуть їх оригінальними дослідженнями або міркуваннями. Списування, втручання в роботу інших здобувачів освіти становлять, але не обмежують, приклади можливої академічної недоброчестності. Виявлення ознак академічної недоброчесності в письмовій роботі здобувана освіти є підставою для її незарахування викладачем незалежно від масштабів плагіату чи обману.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів, пов'язаних із корупційними діями, зіткненням інтересів, різними формами дискримінації, сексуальними домаганнями, міжособистісними стосунками та іншими ситуаціями, що можуть виникнути під час навчання, а також правила етичної поведінки регламентуються Кодексом етичної поведінки в Національному аерокосмічному університеті «Харківський авіаційний інститут» (https://khai.edu/ua/university/normativna-baza/ustanovchi-dokumenti/kodeks-etichnoi-povedinki/).

10. Методичне забезпечення

Сторінка дисципліни у системі дистанційного навчання «Ментор» [Ел. ресурс]. URL: httpshttps://mentor.khai.edu/course/view.php?id=3718, на якому розміщено навчально-методичний комплекс дисципліни.

11. Рекомендована література

Базова

1. Комплексні системи захисту інформації : навчальний посібник / [Яремчук Ю. Є., Павловський П. В., Катаєв В. С., Сінюгін В. В.] – Вінниця : ВНТУ, 2018. – 118 с.

2. Хорошко В. О. та ін Проектування комплексних систем захисту інформації - Л.: Львівська політехніка, 2020. - 320с

3. Комплексні системи захисту інформації в інформаційно-телекомунікаційних системах: Навчальний посібник / В. Д. Козюра, В. О. Хорошко, М. Є. Шелест, Ю. М. Ткач, Я.Ю. Усов. – Ніжин, 2019. – 144 с.

Допоміжна

1. Яремчук Ю. Є. Комплексні системи захисту інформації: навч. пос. [Електронний ресурс] / Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін. – Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41 yaremchuk _kompleksni_systemy_zahystu_informaciyi/index.html

2. Integrated Security Systems Design: A Complete Reference for Building Enterprise-Wide Digital Security Systems / Thomas L. Norman

3. Physical Security Systems Handbook: The Design and Implementation of Electronic Security systems / Michael Khairallah

12. Інформаційні ресурси

1. Вадим Гребенніков Комплексні системи захисту інформації. Проектування, впровадження, супровід [Электрон. ресурс]. - Режим доступа: https://www.academia.edu/40525032/Комплексні_системи_захисту_інформації_проектування_впровадження_супровід

2. Microsoft IT Academy Program [Электрон. ресурс]. - Режим доступа: https://itacademy.microsoftelearning.com/

3. Cisco Networking Academy [Электрон. ресурс]. - Режим доступа: https://www.netacad.com/, http://www.cisco.com/web/learning/netacad/