Міністерство освіти і науки України
Національний аерокосмічний університет
«Харківський авіаційний інститут»

Кафедра «Комп'ютерних систем, мереж і кібербезпеки» (№ 503)

ЗАТВЕРДЖУЮ
Гарант освітньої програми

_____ О. Ілляшенко
(підпис) (ініціали та прізвище)
«_29_» __серпня__ 2025 р.

СИЛАБУС
ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

«Нормативно-правове забезпечення інформаційної безпеки»

СТУПІНЬ ВИЩОЇ ОСВІТИ	Бакалавр
ГАЛУЗЬ ЗНАНЬ	12 «Інформаційні технології»
СПЕЦІАЛЬНІСТЬ	125 «Кібербезпека та захист інформації»
ОСВІТНЯ ПРОГРАМА	«Безпека інформаційних і комунікаційних систем»

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

Силабус введено в дію з 01.09.2025 року

Харків – 2025 р.

Розробник: доцент кафедри №503, к.т.н, снс, Олександр Піскачов _____
(посада, науковий ступінь і вчене звання, ім’я, ПРІЗВИЩЕ) (підпис)

Силабус навчальної дисципліни розглянуто на засіданні кафедри (№ 503)

«Комп’ютерних систем, мереж і кібербезпеки»
(назва кафедри)

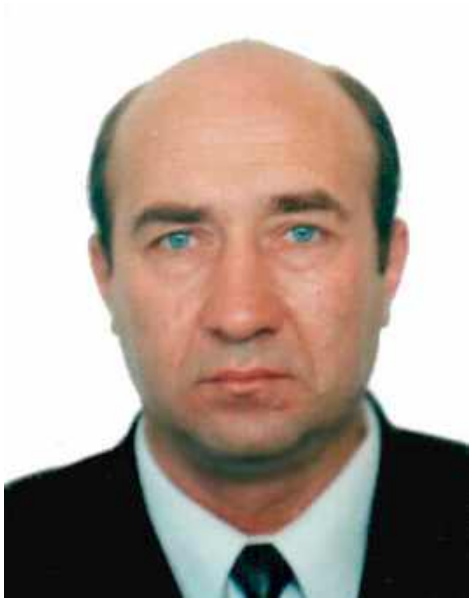
Протокол № 1 від « 29» серпня 2025 р.

Завідувач кафедри д.т.н, професор _____ Вячеслав Харченко
(науковий ступінь і вчене звання) (підпис) (ім’я, ПРІЗВИЩЕ)

Погоджено з представником здобувачів освіти:

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

1. Загальна інформація про викладача



ПІБ: Піскачов Олександр Іванович

Посада: доцент кафедри «Комп’ютерних систем, мереж і кібербезпеки»

Науковий ступінь: кандидат технічних наук

Вчене звання: старший науковий співробітник

Перелік дисциплін, які викладає: «Системи технічного захисту інформації», «Нормативно-правове забезпечення інформаційної безпеки», «Інтелектуальна власність», «Організація наукових досліджень і захист інтелектуальної власності», "Правова інформація та комп’ютерні технології в юридичній діяльності"

Напрями наукових досліджень:
Системи захисту інформації та безпеки безпілотних систем

Контактна інформація:
a.piskachev@csn.khai.edu

2. **Опис навчальної дисципліни**

Форма навчання	денна
Курс, семестр	3 курс, 6 семестр
Обсяг дисципліни: кредити ЄКТС/ кількість годин	*денна*: 4 кредита ЄКТС / 120 годин (64 аудиторних, з яких: лекції – 32, практичні – 32; самостійна робота – 56)
Види занять	лекції, практичні заняття, семінари, самостійна робота
Види контролю	проміжний контроль – модульний; підсумковий (семестровий) контроль – іспит
Пререквізити	ОК23 «Прикладна криптологія», ВК5 «Соціально-гуманітарна дисципліна за вибором»

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

Мета - отримання студентами необхідних знань та навиків для застосування їх з питань механізму правового врегулювання відносин, пов'язаних з використанням інформації і захистом останньої від неправомірного використання. А також в подальшому використанню отриманих знань стосовно розробки методів і засобів криптографічного, технічного захисту інформації та при проектування систем захисту інформації. Особлива увага в курсі приділяється вивченню законодавства, Указів Президента і Постанов Кабінету Міністрів України, нормативних документів технічного захисту інформації, вітчизняних та міжнародних стандартів в галузі захисту та безпеки інформації, здатності аналізувати сучасні стандарти та формувати загальні вимоги до інформаційної безпеки комп'ютерних систем і мереж.

Завдання:
-знати систему міжнародних і національних стандартів у галузі кібербезпеки;
-знати структуру нормативно-правового забезпечення кібербезпеки інформаційно-комунікаційних систем і мереж організацій і підприємств;
-знати методику оцінювання інформаційної безпеки на відповідність вимогам стандартів. А також:
-навчити студентів використанню нормативних документів ТЗІ, вітчизняних та міжнародних стандартів при розробці систем захисту інформації;
-надати студентам знання з методів сертифікації та оцінки якості технічних та криптографічних засобів захисту інформації;
-ознайомити студентів з базовими міжнародними стандартами в галузі забезпечення інформаційної безпеки.

Компетентності, які набуваються:

Загальні компетентності (ЗК):

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.
ЗК 2. Знання та розуміння предметної області та розуміння професії.
ЗК 3. Здатність професійно спілкуватися державною та іноземною мовами як усно, так і письмово.
ЗК 4. Вміння виявляти, ставити та вирішувати проблеми за професійним спрямуванням.
ЗК 5. Здатність до пошуку, оброблення та аналізу інформації.

Фахові компетентності спеціальності (КФ):

КФ 1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі інформаційної та/або кібербезпеки.
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 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):

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 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 12 Розробляти моделі загроз та порушника.

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

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 22 Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.

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).

ПНР 25 Забезпечувати введення підзвітності системи управління доступом до

електронних інформаційних ресурсів і процесів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах з використанням журналів реєстрації подій, їх аналізу та встановлених процедур захисту.

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 28 Аналізувати та проводити оцінку ефективності та рівня захищеності ресурсів різних класів в інформаційних та інформаційно-телекомунікаційних (автоматизованих) системах в ході проведення випробувань згідно встановленої політики інформаційної та\або кібербезпеки.

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 37. Вимірювати параметри небезпечних та завадових сигналів під час інструментального контролю процесів захисту інформації та визначати ефективність захисту інформації від витоку технічними каналами відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН 38. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН 40. Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.

ПРН 42. Впроваджувати процеси виявлення, ідентифікації, аналізу та реагування на інциденти інформаційної і/або кібербезпеки.

ПРН 43. Застосовувати національні та міжнародні регулюючі акти в сфері інформаційної безпеки та/ або кібербезпеки для розслідування інцидентів.

ПРН 44. Вирішувати задачі забезпечення безперервності бізнес-процесів організації на основі теорії ризиків та встановленої системи управління інформаційною безпекою, згідно з вітчизняними та міжнародними вимогами та стандартами.

ПРН 54. Усвідомлювати цінності громадянського (вільного демократичного) суспільства та необхідність його сталого розвитку, верховенства права, прав і свобод людини і громадянина в Україні.

4. Зміст навчальної дисципліни

МОДУЛЬ 1

Змістовний модуль 1

Тема 1. Правова основа забезпечення інформаційної безпеки в Україні.

Стисла анотація. Вступ. Загальні положення про інформаційну безпеку. Існуюча ієрархія нормативно-правових актів. Правова основа інформаційної безпеки України. Правові акти, які закріплюють концептуальні положення інформаційної безпеки України.

Практична робота 1. Пошук нормативно-правової інформації щодо захисту інформації в Інтернеті за допомогою пошукових систем.

Самостійна робота. Опрацювати: ст. УПК, Цивільного кодексу України та Кодексу про адміністративні порушення в інформаційній сфері. Підготовка до лекції; підготовка до практичної роботи; опрацювання матеріалів лекції.

Тема 2. Нормативно-правові акти, які визначають порядок охорони спеціальних та державної таємниці в Україні».

Стисла анотація. Правова основа забезпечення технічного захисту інформації в Україні, види правових актів та їх визначення, зміст та вимоги законів та кодексів України відповідно яких наступає відповідальність за правопорушення в інформаційній сфері. Порядок здійснення та забезпечення права кожного на доступ до інформації. Публічна інформація з обмеженим доступом. Доступ до інформації про особу. Види таємниць особистого життя з урахуванням чинного законодавства. Звід відомостей, що становлять державну таємницю.

Самостійна робота. Опрацювати: порядок обстеження об'єктів в яких циркулює інформація, що підлягає захисту від несанкціонованого доступу, та оформленням відповідних документів. Підготовка до лекції; підготовка до практичної роботи; опрацювання матеріалів лекції.

Тема 3. Системи захисту інформації в банківських установах. Закон України «Про захист персональних даних.

Стисла анотація. Зміст законів України: «Про банки та банківську діяльність», «Про платіжні системи та переказ коштів в Україні», «Про захист персональних даних». Системи захисту інформації в банківських установах. Інформаційна безпека електронного бізнесу.

Практична робота 2. Отримання практичних навичок з знаходження відмінностей в класифікації персональних даних в вітчизняних та закордонних юридичних практиках.

Практична робота 3. Отримання практичних навичок з знаходження відмінностей в визначенні терміну інформації в вітчизняних та закордонних юридичних практиках.

Самостійна робота. Порядок обстеження об'єктів в яких циркулює інформація, що підлягає захисту від несанкціонованого доступу, та оформленням відповідних документів. Підготовка до лекції.

Тема 4. Нормативно-правові акти, які закріплюють визначальні положення щодо забезпечення інформаційної безпеки України.

Стисла анотація. З точки зору подальшого розвитку концептуальних засад нормативно-правового регулювання забезпечення інформаційної безпеки України важливим нормативним актом є Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки». Стратегія розвитку інформаційного суспільства в Україні, яка визначає: мету, базові принципи, стратегічні цілі розвитку інформаційного суспільства в Україні, завдання, спрямовані на їх досягнення, а також основні напрями, етапи і механізм її реалізації. Пріоритети діяльності в галузі забезпечення інформаційної безпеки. Базовий закон у сфері інформатизації є Закон України «Про Національну програму інформатизації».

Самостійна робота. Ознайомитись з міжнародними стандартами в сфері технічного захисту інформації ISO/IEC. Підготовка до лекції; підготовка до практичних робіт; підготовка звітів до практичних робіт; підготовка відповідей на контрольні запитання до практичних робіт.

Тема 5. Нормативно-правові акти з інформаційної безпеки телекомунікаційних систем.

Стисла анотація. Державна система урядового зв’язку. Послуги конфіденційного зв'язку. Основний нормативно-правовий акт України щодо захисту інформації в комп’ютерних системах. З метою обміну інформацією з обмеженим доступом з використанням телекомунікаційної мережі загального користування всі країни створюють спеціальні телекомунікаційні мережі, які забезпечують технічний та криптографічний захист інформації.

Практична робота 4. Отримання практичних навичок з застосування міжнародного стандарту ISO 15408.

Самостійна робота. Підготовка до лекції; підготовка до практичних робіт; підготовка звітів до практичних робіт; підготовка відповідей на контрольні запитання до практичних робіт. Ознайомитись з міжнародними стандартами в сфері технічного захисту інформації ISO/IEC.

Тема 6. Забезпечення захисту інформації в автоматизованих системах.

Стисла анотація. Закон України «Про захист інформації в інформаційно-комунікаційних системах». Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу (НД ТЗІ 2.5-005 -99). Класифікація автоматизованих систем. Функціональні профілі захищеності та їхня семантика.

Практична робота 5. Отримання практичних навичок з застосування НД ТЗІ 2.5-005-99. Отримання практичних навичок з застосування механізмів сертифікації апаратних засобів захисту інформації в Україні.

Самостійна робота. Опрацювати: НД ТЗІ 2.5-005-99. Підготовка до лекції; підготовка до практичних робіт; підготовка звітів до практичних робіт; підготовка відповідей на контрольні запитання до практичних робіт.

Тема 7. Закон України «Про стандартизацію» та Закон України «Про

технічні регламенти та оцінку відповідності» щодо основних заходах розробки нормативно-правового забезпечення інформаційної безпеки.

Стисла анотація. Державна система стандартизації. Основні вимоги Закону України «Про стандартизацію» щодо діяльності у сфері стандартизації та застосуванням її результатів. Правові та організаційні засади розроблення, прийняття та застосування технічних регламентів і передбачених ними процедур оцінки відповідності та заходи щодо державної експертизи у сферах криптографічного та технічного захисту інформації. ДСТУ 1.2:2024 Національна стандартизація. Правила проведення робіт з національної стандартизації.

Самостійна робота. Підготовка до лекції; підготовка до практичних робіт; підготовка звітів до практичних робіт; підготовка відповідей на контрольні запитання до практичних робіт. Підготовка до модульного контролю.

Тема 8. Указ Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні».

Стисла анотація. Положення про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації. Стандарти в сфері криптографічного захисту інформації. Стандартизація національних криптографічних алгоритмів.

Практична робота 6. Отримання практичних навичок з застосування. ДСТУ 1.2:2024, ДСТУ 1.5:2015.

Самостійна робота. Підготовка до лекції; підготовка до практичних робіт; підготовка звітів до практичних робіт; підготовка відповідей на контрольні запитання до практичних робіт.

Змістовний модуль 2

Тема 9. Державні стандарти та будівельні норми України. Захист інформації.

Стисла анотація. Положення про порядок перевірки, перегляду, розроблення, прийняття і скасування галузевих нормативних документів зі стандартизації та галузевих будівельних норм. Про будівельні норми України, які використовуються при розробці комплексів та систем засобів захисту інформаційної структури. Національні стандарти України, які використовуються при розробці комплексів та систем засобів захисту інформаційної структури.

Самостійна робота. Підготовка до лекції; підготовка до практичних робіт; підготовка звітів до практичних робіт; підготовка відповідей на контрольні запитання до практичних робіт.

Тема 10. Міжнародний стандарт ISO 15408. Основні критерії.

Стисла анотація. Використання ДСТУ ISO/IEC 15408 (ISO 15408) у діяльності замовників, розробників та користувачів продуктів та систем інформаційних технологій (далі - ІТ) при формуванні ними вимог, розробці, придбанні та застосуванні продуктів та систем інформаційних технологій, призначених для обробки, зберігання або передачі інформації, що підлягає захисту відповідно до

вимог нормативних правових документів або вимог, що встановлюються власником інформації. На основі стандартів можуть розроблятися керівні та довідкові документи (оскільки стандарти копіювати не можна, а також вони можуть бути важкодоступними).

Самостійна робота. Підготовка до лекції; підготовка до практичних робіт; підготовка звітів до практичних робіт; підготовка відповідей на контрольні запитання до практичних робіт.

Тема 11. Основи захисту комп'ютерної інформації.

Стисла анотація. Загальне уявлення про інформаційну безпеку. Кримінальна відповідальність. Технологічні, організаційні, правові постулати захисту даних. Класифікація комп'ютерних злочинів. Засоби протидії загрозам для комп'ютерної інформації. Поняття про комп'ютерні злочини. Визначення, аналіз та фіксація слідів комп'ютерних злочинів.

Самостійна робота. Підготовка до лекції; підготовка до практичних робіт; підготовка звітів до практичних робіт; підготовка відповідей на контрольні запитання до практичних робіт.

Тема 12. Порядок створення, впровадження та супроводження засобів ТЗІ.

Стисла анотація. Забезпечення захисту інформації в АС. Методика комплексної оцінки профілів захищеності інформації в автоматизованих системах.

Практична робота 7. НД ТЗІ 3.7-003-2023 Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-комунікаційній системі (Наказ Адміністрації Держспецзв'язку від 28.10.2023 № 924). Отримання практичних навичок з застосування НД ТЗІ 3.7-003-2005 інформації в інформаційно-телекомунікаційній системі та НД ТЗІ 3.6-007-21 Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем).

Самостійна робота. Підготовка до лекції; підготовка до практичних робіт; підготовка звітів до практичних робіт; підготовка відповідей на контрольні запитання до практичних робіт.

Тема 13. Інформаційні системи державно-нормативного призначення.

Стисла анотація. Комп'ютерні технології у підготовці та технічного захисту нормативних документів. Сучасні підходи до автоматизації документообігу. Огляд сучасних систем електронного документообігу.

Самостійна робота. Підготовка до лекції; підготовка до практичних робіт; підготовка звітів до практичних робіт; підготовка відповідей на контрольні запитання до практичних робіт.

Тема 14. Нормативні документи ТЗІ щодо забезпечення захисту мовної інформації від витоку акустичним та віброакустичним каналами.

Стисла анотація. Захист мовної інформації – діяльність, спрямована на запобігання витоку інформації, яка циркулює у вигляді акустичних хвиль (голосу

людини). Якщо інформація існує у вигляди акустичних хвиль, які створюються за допомогою голосового апарату людини, вона називається мовною. Мовний сигнал – складний фізичний процес, пов'язаний зі зміною акустичних параметрів, які містять інформацію про зміст повідомлення.

Практична робота 7. Засоби активного захисту мовної інформації з акустичними та віброакустичними джерелами випромінювання. Класифікація та загальні технічні вимоги. РЕКОМЕНДАЦІЇ. Ознайомлення та вивчання нормативних документів ТЗІ щодо забезпечення захисту мовної інформації від витоку акустичним та віброакустичними каналами. Розроблення моделей загроз та порушника.

Самостійна робота. Підготовка до лекції; підготовка до практичних робіт; підготовка звітів до практичних робіт; підготовка відповідей на контрольні запитання до практичних робіт.

Тема 15. Організація та вимоги захисту конфіденційної інформації від несанкціонованого доступу під час оброблення в автоматизованих системах.

Стисла анотація. Ознайомлення та вивчання нормативних документів ТЗІ щодо захисту конфіденційної інформації від несанкціонованого доступу під час оброблення її в автоматизованих системах.

Самостійна робота. Опрацювання матеріалів лекції. Підготовка до лекції.

Тема 16. Нормативні документи ТЗІ щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.

Стисла анотація. Ознайомлення та вивчання нормативних документів ТЗІ щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Нормативні документи з технічного захисту інформації (ТЗІ) в Україні регулюють захист інформації в комп'ютерних системах і включають НД ТЗІ 3.6-001-2000 (створення засобів захисту), НД ТЗІ 2.5-004-99 (критерії захищеності від НСД).

Практична робота 8. Отримання практичних навичок з застосування механізмів сертифікації програмних засобів захисту інформації в Україні.

Самостійна робота. Опрацювання матеріалів лекції. Підготовка до лекції. Підготовка до підсумкового контролю.

5. Індивідуальні завдання

Не передбачено

6. Методи навчання

Проведення аудиторних лекцій, практичних робіт, консультацій, а також самостійна робота здобувачів з використанням відповідних матеріалів (п.11, 12).

7. Методи контролю

Проведення поточного контролю, підсумковий контроль у вигляді іспиту.

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

Таблиця 8.1 – Розподіл балів, які отримують здобувачі освіти

Складові навчальної роботи	Бали за одне заняття (завдання)	Кількість занять (завдань)	Сумарна кількість балів
Змістовний модуль 1			
Робота на лекціях	0…1	8	0…8
Виконання та захист практичних робіт	0...4	4	0...16
Модульний контроль	0…26	1	0…26
Змістовний модуль 2			
Робота на лекціях	0…1	8	0…8
Виконання та захист практичних робіт	0...4	4	0...16
Модульний контроль	0…26	1	0…26
Всього за семестр			**0…100**

Семестровий контроль (залік) проводиться у разі відмови здобувача освіти від балів підсумкового контролю й за наявності допуску до заліку. Під час складання семестрового заліку здобувач освіти має можливість отримати максимум 100 балів.

Таблиця 8.2 – Шкали оцінювання: бальна і традиційна

Сума балів	Оцінка за традиційною шкалою	
	Іспит, диференційований залік	Залік
90 – 100	Відмінно	Зараховано
75 – 89	Добре	
60 – 74	Задовільно	
0 – 59	Незадовільно	Не зараховано

Критерії оцінювання роботи студента протягом семестру

Задовільно (60-74). Захистити не менше 85% від усіх завдань практичних занять. Уміти використовувати правові та нормативні документи, вітчизняних та міжнародних стандартів для проведення робіт щодо розвитку та підтримки функціонування СТЗІ.

Добре (75-89). Твердо знати необхідний обсяг знань для одержання позитивної оцінки, захистити не менше 95% завдань практичних занять. Уміти використовувати сучасні методи теоретичних та експериментальних досліджень для організації та проведення робіт щодо розвитку та підтримки нормативної бази ТЗІ. Мати необхідний обсяг умінь для одержання позитивної оцінки.

Відмінно (90-100). Здати всі контрольні точки з оцінкою «відмінно». Досконально знати всі теми та вміти їх застосовувати. Уміти використовувати інформаційне забезпечення СТЗІ.

9. Політика навчального курсу

Відвідування занять. Інтерактивний характер курсу передбачає обов'язкове відвідування практичних занять. Здобувачі освіти, які за певних обставин не можуть відвідувати практичні 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 здобувачі 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. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших здобувачів освіти становлять, але не обмежують, приклади можливої академічної недоброчестності. Виявлення ознак академічної недоброчесності в письмовій роботі здобувача освіти є підставою для її незарахування викладачем.

Вирішення конфліктів. Порядок і процедури врегулювання конфліктів 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: https://mentor.khai.edu/course/view.php?id=3707

11. Рекомендована література

Базова

1. Конституція України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text.
2. Закон України «Про державну таємницю». URL https://zakon.rada.gov.ua/laws/show/3855-12#Text.
3. Закон України «Про основні засади забезпечення кібербезпеки України». URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.
4. Закон України «Про захист інформації в інформаційно-комунікаційних системах». URL:

5. https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.
6. Закон України «Про електронні комунікації» URL: https://zakon.rada.gov.ua/laws/show/1089-20#Text.
7. ДСТУ 3396.0-96 ТЗІ. Основні положення.
8. ДСТУ 3396.1-96 ТЗІ. Порядок проведення робіт.
9. Захист інформації в комп'ютерних системах від несанкціонованого доступу. Загальні положення. (НД ТЗІ 1.1-002-99).
10. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі (НД ТЗІ 3.7-003 -2005).

Допоміжна

1. Барило Г.І., Вісьтак М.В., Готра З.Ю., Лесінський В.В., Політанський Л.Ф. Електронні елементи та пристрої систем безпеки й охорони: Навчальний посібник .- За ред. Готри З.Ю. – Чернівці: Рута, 2017. 216 с.
2. Діордієв В. Т. Засоби автоматизації електротехнічних комплексів: навчальний посібник / В. Т. Діордієв, А. О. Кашкарьов, С. В. Дубініна, Г. В. Новіков. – Мелітополь: ФОП Однорог Т.В., 2020. 220 с.
3. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформации. Навчальний посібник / Іванченко С.О., Гавриленко О.В. та інші. – К.: ІСЗЗІ НТУУ «КПІ», 2016, 104 с.
4. Комплексні системи захисту інформації [Текст] : навч. посіб. / [Яремчук Ю. Є. Павловський П. В., Катаєв В. С., Сінюгін В. В.] ; Вінницький національний технічний університет. - Вінниця : ВНТУ, 2018, 118 с. - Бібліогр.: с. 116-117.
5. Афзель, С.С. Огляд сучасного стану та перспективи розвитку датчиків руху/ С.С. Афзель, М.О. Березанська // Ефективність інженерних рішень у приладобудуванні: матеріали доповідей XIV Всеукраїнської науково-практичної конференція студентів, аспірантів та молодих вчених, 2018. 16 с.

12. Інформаційні ресурси:

1. Конвенція Ради Європи про кіберзлочинність, ратифікована Законом України від 7.09.2005 року № 2824-IV. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.
2. Кормич Б. А. (2004) Організаційно-правові основи політики інформаційної безпеки України: дис... д-ра юрид. наук: 12.00.07 / Національний ун-т внутрішніх справ. Х., 2004. URL: http://www.disslib.org/orhanizatsiyno-pravovi-osnovy-polityky-informatsi.
3. Rabeya Islam Rima «Cyber security in modern world». 14.01.2024. URL: https://www.educative.io/answers/what-are-some-challenges-in-information.