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

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

ЗАТВЕРДЖУЮ
Гарант освітньої програми

О.О. Ілляшенко
(підпис) (ім'я, ПРІЗВИЩЕ)

«29» серпня 2025 р.

СИЛАБУС
ОБОВ'ЯЗКОВОЇ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

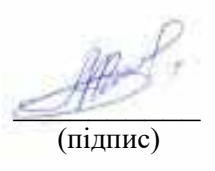
«СИСТЕМИ ТЕХІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ»

ГАЛУЗЬ ЗНАНЬ	12 «Інформаційні технології»
СПЕЦІАЛЬНІСТЬ	125 «Кібербезпека»
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	2 курс, 4 семестр
Обсяг дисципліни: кредити ЄКТС/ кількість годин	*денна*: 3,5 кредити ЄКТС / 105 годин (64 аудиторних, з яких: лекції – 32, практичні – 32; самостійна робота – 41)
Види занять	лекції, практичні заняття, семінари, самостійна робота
Види контролю	проміжний контроль – модульний; підсумковий (семестровий) контроль – залік
Пререквізити	Дисципліна є обов'язковим компонентом освітній програми і базується на знаннях, отриманих під час вивчення дисциплін у циклі загальної і професійної підготовки, передбачених навчальним планом спеціальності

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 регулювання 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 сформулювати 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:
Інтегральна компетентність:
Здатність розв'язувати складні спеціалізовані задачі і практичні завдання у галузі кібербезпеки та захисту інформації.

Загальні компетентності (ЗК):

ЗК 1. Здатність застосовувати знання у практичних ситуаціях.
ЗК 2. Знання та розуміння предметної області та розуміння професійної діяльності.
ЗКЗ. Здатність спілкуватися державною мовою як усно, так і письмово.
ЗК4. Здатність спілкуватися іноземною мовою.
ЗК5. Здатність вчитися і оволодівати сучасними знаннями.

Спеціальні компетентності спеціальності (СК):
СК1. Здатність застосовувати законодавчу та нормативно-правову базу, а також державні і міжнародні вимоги, практики і стандарти у професійній діяльності.

СК2. Здатність використовувати інформаційні технології, сучасні методи і моделі кібербезпеки та системи захисту інформації.

СК3. Здатність забезпечувати неперервність бізнес-процесів згідно встановленої політики кібербезпеки та захисту інформації.

СК4. Здатність забезпечувати захист інформації в інформаційних та інформаційно-комунікаційних системах згідно встановленої політики кібербезпеки й захисту інформації.

СК6. Здатність впроваджувати та забезпечувати функціонування комплексних систем захисту інформації (комплекси нормативно-правових, організаційних та технічних засобів і методів, процедур, практичних прийомів тощо.)

СК9. Здатність застосовувати методи та засоби технічного захисту інформації на об'єктах інформаційної діяльності.

СК10. Здатність виконувати моніторинг інформаційних процесів, аналізувати, виявляти, оцінювати можливі вразливості та загрози інформаційному простору й інформаційним ресурсам згідно встановленою політикою інформаційної безпеки.

Програмні результати навчання (ПРН):

РН1. Вільно спілкуватися державною мовою усно та письмово при виконанні професійних обов'язків.

РН2. Спілкуватися іноземною мовою з метою забезпечення ефективності професійної комунікації.

РН4. Організовувати власну професійну діяльність, обирати і використовувати оптимальні методи та способи розв'язання складних спеціалізованих задач і практичних проблем у професійній діяльності, оцінювати їхню ефективність.

РН5. Аналізувати, аргументувати, приймати рішення при розв'язанні складних спеціалізованих задач і практичних завдань у професійній діяльності, які характеризуються комплексністю та неповною визначеністю умов, відповідати за прийняті рішення.

РН6. Адаптуватися до нових умов і технологій професійної діяльності, прогнозувати кінцевий результат.

РН7. Застосовувати й адаптувати теорії інформації та кодування, математичної статистики, чисел, криптографії та стеганографії, оброблення і передачі сигналів тощо, принципи, методи, поняття кібербезпеки та захисту інформації у навчанні та професійній діяльності.

РН9. Знати та застосовувати законодавство України та міжнародні вимоги, практики і стандарти з метою здійснення професійної діяльності в галузі кібербезпеки та захисту інформації.

РН10. Використовувати сучасні інформаційні технології, методи і моделі кібербезпеки та систем захисту інформації для здійснення професійної діяльності.

РН12. Застосовувати методи та засоби захисту інформації в інформаційних та інформаційнокомунікаційних системах відповідно до встановленої політики інформаційної безпеки.

РН13. Впроваджувати, налаштовувати, супроводжувати та підтримувати функціонування програмних і програмно-апаратних комплексів і систем кібербезпеки та захисту інформації як необхідні процедури для функціонування

інформаційних й інформаційно-комунікаційних систем та або інфраструктури організації в цілому.

РН16. Вирішувати задачі впровадження та супроводу комплексних систем захисту інформації інформаційних системах;

РН18. Аналізувати, застосовувати методи та засоби криптографічного захисту інформації на об'єктах інформаційної діяльності.

РН19. Вирішувати задачі щодо організації та контролю стану криптографічного захисту інформації, зокрема відповідно до вимог нормативних документів.

РН20. Визначати загрози створення технічних каналів витоку інформації на об'єктах інформаційної діяльності; впроваджувати засоби і заходи технічного захисту інформації від витоку технічними каналами, проводити обслуговування і контроль стану апаратних засобів захисту інформації та комплексів технічного захисту інформації.

РН21. Виконувати впровадження, підтримку, аналіз ефективності систем виявлення несанкціонованого доступу, дій з інформацією в інформаційній системі, вразливостей, можливих загроз інформаційному простору й інформаційним ресурсам та використовувати комплекси захисту для забезпечення необхідного рівня захищеності інформації в інформаційних системах.

4. Зміст навчальної дисципліни

МОДУЛЬ 1

Змістовий модуль 1
Напрямки захисту інформації в системі технічного захисту інформації

Тема 1. Предмет, мета вивчення і задачі дисципліни. Структура та зміст дисципліни і методичні рекомендації щодо її вивчення

Стисла анотація. Характеристика рекомендованих під час вивчення дисципліни джерел інформації. Напрямки захисту інформації (далі - ЗІ) в системі технічного захисту інформації (далі - СТЗІ). Технічний захист інформації (далі - ТЗІ) від несанкціонованих дій на прикладному і програмному рівні. ТЗІ від несанкціонованих дій на апаратному рівні. ТЗІ на мережевому рівні. Засоби та заходи ТЗІ. Організаційні заходи ЗІ. Нормативно-методичне забезпечення СТЗІ.

Самостійна робота. Підготовка до лекції; підготовка до семінару; опрацювання матеріалів лекції.

Тема 2. Про нормативно-правове забезпечення технічного захисту інформації в Україні та основи побудови та функціонування системи технічного захисту інформації

Стисла анотація. Концепція технічного захисту інформації в Україні. Основи побудови та функціонування систем технічного захисту інформації. Концепція технічного захисту інформації в Україні.

Семінар. Головні завдання Концепції технічного захисту інформації в України.

Самостійна робота. Підготовка до лекції; підготовка до семінару відповідно до плана проведення семінару.

Тема 3. Методи вимірювань

Стисла анотація. Методи вимірювань (безпосередньої оцінки, порівняння з мірою, протиставлення, диференціальний, нульовий, заміщення збіги). Види вимірювань (прямі і непрямі, сукупні і спільні, абсолютні і відносні, одноразові і багаторазові, технічні та метрологічні, рівноточні і нерівноточні равно рассеяны і неравный рассеяны, статичні і динамічні). Характеристики датчиків (вимірювальних перетворювачів).

Семінар. Основи побудови системи технічного захисту інформації.

Самостійна робота. Підготовка до лекції; підготовка до семінару відповідно до плана проведення семінару.

Тема 4. Технічні канали витоку інформації

Стисла анотація. Основні об'єкти захисту інформації. Загальні відомості про технічні канали витоку інформації. Структура, класифікація та основні

характеристики. Технічні канали витоку інформації при передачі її по каналах зв'язку. Технічні канали витоку мовної інформації.

Практична робота 1. Методи вимірювань та обробки їх результатів

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

Тема 5. Вимірювальні перетворювачі. Загальні відомості про вимірювальних перетворювачах

Стисла анотація. Вимірювальні перетворювачі. Загальні відомості про вимірювальних перетворювачах. Ємнісні перетворювачі. Структура, класифікація та основні характеристики. Пристрій, принцип дії індуктивних перетворювачів. Пристрій, принцип дії індукційних перетворювачів.

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

Тема 6. Індуктивні та індукційні вимірювальні перетворювачі

Стисла анотація. Пристрій і принцип дії диференціального індуктивного перетворювача (датчика). Пристрій і принцип дії індукційного перетворювача.

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

Тема 7. Датчики руху

Стисла анотація. Природа і отримання ультразвукових коливань. Застосування ультразвуку. Властивості ультразвуку. Ультразвукові, мікрохвильові, інфрачервоні, комбіновані датчики руху. Принципи дії інфрачервоного, ультразвукового, мікрохвильового датчиків руху. Основні недоліки ультразвукових, інфрачервоних датчиків руху. Переваги інфрачервоних, ультразвукових, мікрохвильових, комбінованих датчиків руху.

Практична робота 2. Природа і отримання ультразвукових коливань. Застосування ультразвуку. Властивості ультразвуку. Ультразвукові, мікрохвильові, інфрачервоні, комбіновані датчики руху

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. Датчики систем ТЗІ

Стисла анотація. Пристрій, принципи дій тензорезисторів. Пристрій, принципи дій магнітопружних перетворювачів. Пристрій, принципи дій п'єзоелектричних перетворювачів.

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
Датчики контролю параметрів об’єктив інформаційної діяльності

Тема 1. Температура. Вимірювання і контроль температури.

Стисла анотація. Методи і засоби вимірювання температури. Загальні відомості про вимірювання і контроль температури.

Практична робота 3. Ультразвуковий датчик відстані.

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

Тема 2. Резистивних перетворювачі (реостатні, термістори, фоторезистори)

Стисла анотація. Пристрій, принципи дій резистивних перетворювачів (реостатні, термістори, фоторезистори).

Практична робота 4. Температура. Вимірювання і контроль температури об’єктів.

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

Тема 3. Інтелектуальні датчики.

Стисла анотація. Структура інтелектуальних датчиків. Функції, що реалізуються у інтелектуальних датчиках (перетворення, самодіагностики, інформаційні, конфігурації, форматування, що керують). Сучасні датчики електричних величин. Види перетворюючої апаратури в інтелектуальних датчиках. Сенсорно-комп'ютерні системи.

Практична робота 5. Принцип роботи мікроконтролерів на базі ммікроконтролера з відкритим вихідним кодом Arduino.

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

Тема 4. Сполучення перетворювачів з вимірювальної апаратурою.

Стисла анотація. Загальні вимоги до інформаційно-вимірювальних систем. Принципи забезпечення сумісності вимірювальних перетворювачів. Мостові схеми сполучення тензометрів і структури перетворювача. Температурна компенсація тензометрів. Способи компенсації температурних змін в тензометричної мостовій схемі. Проблема шумів та взаємних перешкод. Різні способи заземлення.

Практична робота 6. Системи доступу на об’єкт інформаційної діяльності. Підбір пароля.

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

Тема 5. Аналогові та цифрові системи перетворення.

Стисла анотація. Аналогово-цифрові та цифро-аналогові перетворювачі — це пристрої, що перетворюють аналогові сигнали на цифрові (аналогово-цифровий перетворювач, АЦП) і навпаки (цифро-аналоговий перетворювач, ЦАП). АЦП використовується для оцифрування сигналів, а ЦАП — для відновлення аналогового сигналу з цифрового, що є фундаментальним для роботи з аудіо, відео та іншими даними в електронних пристроях.

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

Тема 6. Сенсорний пристрій і влаштування протипожежних систем.

Стисла анотація. Характеристики пожежі та способи її виявлення. Класифікація і принципи функціонування пожежних сенсорних пристроїв. Теплові сенсорні пристрої. Оптичні сенсорні пристрої диму. Сенсорні пристрої відкритого полум'я. Ручні пожежні сповіщувачі.

Самостійна робота. Опрацювання матеріалів лекції. Підготовка до лекції.

Тема 7. Периметрова охорона об'єкта інформаційної діяльності

Стисла анотація. Функціональні зони охорони. Вимоги до системи периметрової охорони. Тепловізійні системи. Інфрачервоні системи. Ємнісні системи охорони периметрів. Радіопроменеві охоронні системи. Радіохвильові охоронні системи. Електрошокові системи охорони периметрів. Датчики різних систем охоронної сигналізації та деякі способи їх нейтралізації.

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

Тема 8. Датчики різних систем охоронної сигналізації та деякі способи їх нейтралізації

Стисла анотація. У нічний час, коли зазвичай і відбуваються проникнення, установи ставляться на охоронну сигналізацію, яку у разі порушення периметра, що охороняється, автоматично зобов'язані включати різні датчики. Датчики за принципом дії поділяються на такі види: електромеханічні, теплові, ємнісні, ультразвукові, оптико-електронні, мікрохвильові.

Самостійна робота. Опрацювання матеріалів лекції. Підготовка до лекції. Підготовка до модульного 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 заліку.

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 функціонування СТЗІ. 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 виконувати 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.