СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Загальна інформація про навчальну дисципліну

Повна назва навчальної дисципліни	Технічні заходи забезпечення інформаційної безпеки
Повна офіційна назва закладу вищої освіти	Сумський державний університет
Повна назва структурного підрозділу	Факультет електроніки та інформаційних технологій. Кафедра кібербезпеки
Розробник(и)	Коваль Віталій Вікторович
Рівень вищої освіти	Перший рівень вищої освіти, НРК – 6 рівень, QF-LLL – 6 рівень, FQ-EHEA – перший цикл
Тривалість вивчення навчальної дисципліни	один семестр
Обсяг навчальної дисципліни	Обсяг навчальної дисципліни становить 5 кредитів ЄКТС, 150 годин, з яких 56 годин становить контактна робота з викладачем (24 годин лекцій, 32 години лабораторних робіт), 94 години становить самостійна робота
Мова викладання	Українська

2. Місце навчальної дисципліни в освітній програмі

Статус дисципліни	Обов`язкова навчальна дисципліна для всіх освітніх програм спеціальності 125 "Кібербезпека"
Передумови для вивчення дисципліни	Фізичні основи кібербезпеки
Додаткові умови	Додаткові умови відсутні
Обмеження	Обмеження відсутні

3. Мета навчальної дисципліни

Вивчення процесів та явищ, пов'язаних з витоком інформації. Оволодіння методами захисту від витоку технічними каналами інформації. Формування навичок побудови, конфігурації та експлуатації інтелектуальних систем відеоспостереження, систем контролю і управління доступом, бездротових мереж.

4. Зміст навчальної дисципліни

Тема 1 Випромінювання та прийом хвиль та сигналів

Акустичні хвилі. Фізичні характеристики. Одиниці вимірювань. Розповсюдження звуку в відкритому просторі та приміщенні.. Прийом акустичних хвиль. Акустотехнічні методи виявлення та локалізації джерел звуку. Мікрофони та мікрофонні системи моніторингу та спостереження.

Тема 2 Основи технічного захисту інформації Поняття технічного захисту інформації, призначення та функції. Класифікація технічних каналів витоку інформації. Аналіз об’єкту захисту з метою впровадження СТЗІ.
Тема 3 Засоби захисту від витоку технічними каналами Класифікація загальних методів та засобів блокування каналів витоку інформації. Основні методи та засоби для практичного пошуку радіозакладних пристроїв. Особливості технічного захисту електронної інформації.
Тема 4 Інтелектуальні системи відеоспостереження Сучасне застосування систем відеоспостереження. Технологія Power-over-coaxial. Технологія Control over Coax. Технологія Dewarping. Технологія power-over-ethernet. Проектування систем відеоспостереження. Спектр можливостей застосування. Сучасні технології відеоспостереження. Сфери застосування систем відеоспостереження.
Тема 5 Системи контролю і управління доступом Основні завдання та функції СКУД. Сфера використання. Принципи роботи. Контролери СКУД: види, призначення, складові. Елементи СКУД : електричні замки , зчитувачі , датчики.
Тема 6 Безпека бездротових технологій Wi-Fi мережа. Wi-Fi роутер. Wi-Fi точка доступу. Сучасні стандарти Wi-Fi. Огляд стандартів безпеки. Їх класифікація по ступеню вразливості.

5. Очікувані результати навчання навчальної дисципліни

Після успішного вивчення навчальної дисципліни здобувач вищої освіти зможе:

РН1	Розуміти основні поняття, закони з теорії фізики, які лежать у принципах роботи, витоку та захисту інформації
РН2	Володіти методами фізичного дослідження з використанням вимірювальних приладів, фізичної апаратури і комп’ютерної техніки
РН3	Знати границі застосування методик та підходів
РН4	Планувати, конфігорувати обладнання для отримання поставлених результатів

6. Роль навчальної дисципліни у досягненні програмних результатів

Програмні результати навчання, досягнення яких забезпечує навчальна дисципліна.
Для спеціальності 125 Кібербезпека:

ПР22	Вирішувати задачі управління процедурами ідентифікації, автентифікації, авторизації процесів і користувачів в інформаційно-телекомунікаційних системах згідно встановленої політики інформаційної і\або кібербезпеки.
ПР25	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.

ПР36	Виявляти небезпечні сигнали технічних засобів.
ПР37	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.
ПР38	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик інформаційно-телекомунікаційних систем відповідно до вимог нормативних документів системи технічного захисту інформації.
ПР39	Проводити атестацію (спираючись на облік та обстеження) режимних територій (зон), приміщень тощо в умовах додержання режиму секретності із фіксуванням результатів у відповідних документах.
ПР40	Інтерпретувати результати проведення спеціальних вимірювань з використанням технічних засобів, контролю характеристик ІТС відповідно до вимог нормативних документів системи технічного захисту інформації.
ПР50	Забезпечувати функціонування програмних та програмно-апаратних комплексів виявлення вторгнень різних рівнів та класів (статистичних, сигнатурних, статистично-сигнатурних).
ПР51	Підтримувати працездатність та забезпечувати конфігурування систем виявлення вторгнень в інформаційно-телекомунікаційних системах.

7. Роль освітнього компонента у формуванні соціальних навичок

Компетентності та соціальні навички, формування яких забезпечує навчальна дисципліна:

8. Види навчальних занять

Тема 1. Випромінювання та прийом хвиль та сигналів
Лк1 "Випромінювання хвиль та сигналів" (денна) Акустичні хвилі. Фізичні характеристики. Одиниці вимірювань. Розповсюдження звуку в відкритому просторі та приміщенні.
Лк2 "Прийом хвиль та сигналів" (денна) Прийом акустичних хвиль. Акустотехнічні методи виявлення та локалізації джерел звуку. Мікрофони та мікрофонні системи моніторингу та спостереження.
Лб1 "Дослідження дальності прямої видимості як фактору впливу на доступність інформації." (денна) Експериментально дослідити розповсюдженість хвиль а також загасання та проходження через перешкоди.
Лб2 "Розрахунок параметрів екранів" (денна) Опираючись на теорію екранування розрахувати параметри простої конструкції для екранування джерела акустичних хвиль.

Тема 2. Основи технічного захисту інформації
Лк3 "Нормативно-правове забезпечення інформаційної безпеки" (денна) Поняття технічного захисту інформації, призначення та функції
Лк4 "Технічні канали витоку інформації" (денна) Класифікація технічних каналів витоку інформації. Аналіз об’єкту захисту з метою впровадження СТЗІ.
Лб3 "Аналіз технічних каналів витоку за їх класифікацією." (денна) Проведення порівняльного аналізу мохливих каналів витоку інформації та системи їх класифікації
Лб4 "Необхідність аналізу технічних каналів витоку на об’єкті ." (денна) Дослідження необхідності ідентифікації каналів витоку інформації на об'єкті з метою визначення заходів захисту.
Лб5 "Основні відмінності технічних каналів витоку" (денна) Аналіз досліджуваного об'єкту з пошуком можливих каналів витоку інформації
Тема 3. Засоби захисту від витоку технічними каналами
Лк5 "Методи та засоби блокування технічних каналів витоку інформації" (денна) Класифікація загальних методів та засобів блокування каналів витоку інформації.
Лк6 "Методи та засоби для пошуку радіозакладних пристроїв." (денна) Основні методи та засоби для практичного пошуку радіозакладних пристроїв. Особливості технічного захисту електронної інформації.
Лб6 "Порівняння технічних засобів блокування каналів витоку" (денна) Огляд сучасних засобів блокування каналів витоку інформації.
Лб7 "Порівняння методів та засобів пошуку радіозакладних пристроїв" (денна) Проведення вивчення та порівняння різних методів пошуку радіозакладних та акустичних каналів витоку інформації.
Лб8 "Пошук радіозакладних пристроїв" (денна) Моделювання на полігоні можливого закладання радіозакладного пристрою та методології його пошуку.
Тема 4. Інтелектуальні системи відеоспостереження
Лк7 "Основні компоненти систем відеоспостереження" (денна) Сучасне застосування систем відеоспостереження. Технологія Power-over-coaxial. Технологія Control over Coax. Технологія Dewarping. Технологія power-over-ethernet. Проектування систем відеоспостереження. Спектр можливостей застосування.

Лк8 "Огляд сучасних систем відеоспостереження" (денна) Сучасні технології відеоспостереження. Сфери застосування систем відеоспостереження.
Лб9 "Порівняльний аналіз складових систем спостереження" (денна) Провести пошукове дослідження необхідних елементів, які складають систему відеоспостереження. Дослідити чим визначаються параметри вибору відеокамер, реєстраторів.
Лб10 "Побудова системи відеоспостереження (частина 1)" (денна) Провести проектування обєкту з розподілом на відповідні зони та плануванням необхідного обладнання для поскриття зон контролю.
Лб11 "Побудова системи відеоспостереження (частина 2)" (денна) Конфігурація елементів, які входять в систему відеоспостереження, для її роботи відповідно до ТЗ.
Тема 5. Системи контролю і управління доступом
Лк9 "Основі принципи побудови систем контролю і управління доступом" (денна) Основні завдання та функції СКУД. Сфера використання. Принципи роботи.
Лк10 "Огляд систем контролю і управління доступом" (денна) Контролери СКУД: види, призначення, складові. Елементи СКУД : електричні замки , зчитувачі , датчики.
Лб12 "Побудова СКУД (частина 1)" (денна) Огляд об'єкту безпеки. Планування необхідного обладнання для виконання поставлених вимог по безпеці.
Лб13 "Побудова СКУД (частина 2)" (денна) Проектування для свого об'єкту елементів СКУД та їх розташування.
Лб14 "Побудова СКУД (частина 3)" (денна) Конфігурація обладнання та перевірка його функціонування відповідно до вимог.
Тема 6. Безпека бездротових технологій
Лк11 "Огляд бездротових технологій" (денна) Wi-Fi мережа. Wi-Fi роутер. Wi-Fi точка доступу.
Лк12 "Сучасні принципи побудови безпечних бездротових мереж" (денна) Сучасні стандарти Wi-Fi. Огляд стандартів безпеки. Їх класифікація по ступеню вразливості.

Лб15 "Перевірка безпеки Wi-Fi мережі" (денна) Проведення дослідження доступних роутерів на безпеку.
Лб16 "Побудова безшовних мереж" (денна) Проектування, конфігурація, налагодження та перевірка безшовної мережі.

9. Стратегія викладання та навчання

9.1 Методи викладання та навчання

Дисципліна передбачає навчання через:

МН1	Інтерактивні лекції
МН2	Дослідницька робота
МН3	Лекції-дискусії
МН4	Метод демонстрацій
МН5	Пошукова лабораторна робота

Під час проведення занять студенти отримують навички комунікації, вміння працювати в команді. Здатність розв’язувати типові та складні спеціалізовані задачі. Здатність обирати оптимальні методи досліджень, модифікувати та адаптувати існуючі, розробляти нові методи досліджень відповідно до існуючих технічних засобів та формувати методику обробки результатів. Зрозуміло, чітко і однозначно доносити власні знання, висновки та їх обґрунтованість.

9.2 Види навчальної діяльності

НД1	Індивідуальна робота, що передбачає самостійне виконання студентами завдання відповідно до рівня його навчальних можливостей
НД2	Фронтальна робота, що передбачає одночасне виконання всіма студентами одного і того ж завдання
НД3	Групова робота, що передбачає роботу студентів групою та бригадним методом для виконання лабораторних робіт за відповідними темами

10. Методи та критерії оцінювання

10.1. Критерії оцінювання

Визначення	Чотирибальна національна шкала оцінювання	Рейтингова бальна шкала оцінювання
Відмінне виконання лише з незначною кількістю помилок	5 (відмінно)	$90 \leq RD \leq 100$
Вище середнього рівня з кількома помилками	4 (добре)	$82 \leq RD < 89$
Загалом правильна робота з певною кількістю помилок	4 (добре)	$74 \leq RD < 81$

Непогано, але зі значною кількістю недоліків	3 (задовільно)	64 ≤ RD < 73
Виконання задовольняє мінімальним критеріям	3 (задовільно)	60 ≤ RD < 63
Можливе повторне складання	2 (незадовільно)	21 ≤ RD < 59
Можливе одноразове повторне складання	2 (незадовільно)	0 ≤ RD < 20

10.2 Методи поточного формативного оцінювання

	Характеристика	**Дедлайн, тижні**	**Зворотний зв'язок**
МФО1 оцінювання (захист) виконаних лабораторних робіт			
МФО2 оцінювання теоретичного матеріалу за формою колоквіуму або письмового чи тестового опитування.			

10.3 Методи підсумкового сумативного оцінювання

	Характеристика	**Дедлайн, тижні**	**Зворотний зв'язок**
МСО1 Виконання та захист лабораторних робіт			
МСО2 Поточні контрольні роботи (проміжний модульний контроль)			
МСО3 Звіт за результатами виконання обов’язкового домашнього завдання			

МСО4 Підсумковий контроль: екзамен			

Контрольні заходи:

	Максимальна кількість балів	Можливість перескладання з метою підвищення оцінки
Перший семестр вивчення	**100 балів**	
МСО1. Виконання та захист лабораторних робіт	**32**	
16x2	32	Ні
МСО2. Поточні контрольні роботи (проміжний модульний контроль)	**16**	
2x8	16	Ні
МСО3. Звіт за результатами виконання обов'язкового домашнього завдання	**12**	
	12	Ні
МСО4. Підсумковий контроль: екзамен	**40**	
	40	Ні

Рейтингові бали шкали оцінювання з навчальної дисципліни розподіляються між поточним оцінюванням, атестаціями та ДСК відповідно 60% і 40%. Студенти, які мають рейтинговий бал за результатами модульних атестацій менше 20 (20%) до заходу додаткового семестрового контролю (ДСК) не допускаються і їм призначається повторне вивчення дисципліни. Якщо студент не набрав загальний рейтинговий бал, який відповідає позитивній оцінці (60 балів і більше), вважається, що він має заборгованість з дисципліни з процедурою її ліквідації. Складання заходу ПСК за додатковою відомістю семестрової атестації. Студент має право на два складання заходу ПСК: викладачеві та комісії. У разі незадовільного складання заходу ПСК комісії студент отримує оцінку «незадовільно». ПСК являють собою іспит (за процедурою письмового іспиту), що передбачає 60 % балів від загальної кількості балів з дисципліни. За умови успішного складання заходу ПСК студент отримує оцінку «задовільно, 60 балів, «Е» за шкалою ECTS, яка засвідчує виконання студентом мінімальних вимог без урахування накопичених (рейтингових) балів та реальної кількості білів відведених на ПСК. У разі незадовільного складання заходу ПСК комісії студент отримує оцінку «незадовільно» з сумою балів, яка відповідає результату, набраному за підсумком роботи за семестр з урахуванням усіх доопрацювань, але не менш ніж сумарний рейтингових балів поточної атестації.

11. Ресурсне забезпечення навчальної дисципліни

11.1 Засоби навчання

ЗН1	Інформаційно-комунікаційні системи
ЗН2	Комп’ютери, комп’ютерні системи та мережи
ЗН3	Лабораторне обладнання (фізичні матеріали, генератори, осцилографи, тощо)
ЗН4	Мультимедіа, відео- і звуковідтворювальна, проєкційна апаратура (відеокамери, проєктори, екрани, смартдошки тощо)
ЗН5	Лабораторія технічного захисту зі специфічним обладнанням

11.2 Інформаційне та навчально-методичне забезпечення

Основна література	
1	Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. - К.: ІСЗЗІ НТУУ "КПІ", 2020. - 108с.
2	Браїловський В.В. Радіомоніторинг та радіопротидія на об’єктах інформаційної діяльності / Браїловський В.В., Гресь О.В., Косован Г.В. Чернівці ,Чернівецький національний університет, 2020 - 135с.
3	Технічний захист інформації в інформаційних та телекомунікаційних системах: Навчальний посібник / укл.: Г.І. Ластівка, П.М. Шпатар - Чернівці: Чернівецький національний університет, 2018 - 252 с.
4	4958 Методичні вказівки до лабораторної роботи на тему "Системи відеоспостереження" з дисципліни "Технічні заходи забезпечення інформаційної безпеки" [Текст] : для студ. спец. 125 "Кібербезпека" всіх форм навчання / В. В. Коваль, О. Б. Проценко, А. С. Москаленко. — Суми : СумДУ, 2020. — 24 с.
Допоміжна література	
1	Євграфов Д. В. Фізичні основи захисту інформації радіоелектронної апаратури. Навчальний посібник Київ: НТУУ «КПІ»,2020
2	Сучасні інформаційні технології в кібербезпеці [Текст] : монографія / А. С. Довбиш, В. К. Ободяк, І. В. Шелехов та ін. ; за ред. В. К. Ободяка, І. В. Шелехова. — Суми : СумДУ, 2021. — 348 с.