СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Загальна інформація про навчальну дисципліну

Повна назва навчальної дисципліни	Технології захисту інформації
Повна офіційна назва закладу вищої освіти	Сумський державний університет
Повна назва структурного підрозділу	Факультет електроніки та інформаційних технологій. Кафедра кібербезпеки
Розробник(и)	Ободяк Віктор Корнелійович
Рівень вищої освіти	Перший рівень вищої освіти, НРК – 6 рівень, QF-LLL – 6 рівень, FQ-EHEA – перший цикл
Семестр вивчення навчальної дисципліни	8 тижнів протягом 8-го семестру
Обсяг навчальної дисципліни	Обсяг становить 5 кред. ЄКТС, 150 год. Для денної форми навчання 40 год. становить контактна робота з викладачем (16 год. лекцій, 24 год. лабораторних занять), 110 год. становить самостійна робота.
Мова викладання	Українська

2. Місце навчальної дисципліни в освітній програмі

Статус дисципліни	Обов`язкова навчальна дисципліна для всіх освітніх програм спеціальності 122 "Комп`ютерні науки"
Передумови для вивчення дисципліни	Обслуговування комп’ютерної техніки
Додаткові умови	Додаткові умови відсутні
Обмеження	Обмеження відсутні

3. Мета навчальної дисципліни

Метою дисципліни є формування здобувачами теоретичних знань щодо основних концепцій інформаційної безпеки, принципів безпечного проєктування програмного забезпечення та набуття практичних вмінь забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних.

4. Зміст навчальної дисципліни

Тема 1 Проблеми захисту інформації Основні положення теорії захисту інформації. Періоди розвитку теорії захисту інформації у комп’ютерних системах та мережах. Основні підходи до розгляду питань теорії захисту інформації та інформаційних систем. Забезпечення виконання вимог конфіденційності, цілісності, достовірності та доступності інформації. Мережева модель OSI. Загальна характеристика проблем безпеки в розподілених комп'ютерних системах. Моделі розподілених систем в процесах розмежування доступу
Тема 2 Характеристика загроз безпеки інформації. Несанкціонований доступ. Порушники безпеки Класифікація загроз безпеки інформації. Загроза розкриття. Загроза порушення цілісності. Загроза відмови в обслуговуванні. Способи несанкціонованого доступу. Модель порушника
Тема 3 Шляхи забезпечення безпеки інформації Концепція захисту інформації. Стратегія та архітектура захисту інформації. Види забезпечення безпеки інформації. Основні принципи створення безпечного програмного забезпечення. Запобігання появи і усунення вразливостей програм
Тема 4 Політика безпеки інформації Політики безпеки інформації. Заходи політики безпеки. Реалізація політики безпеки. Підтримка політики безпеки. Дискреційна, мандатна та рольова політики безпеки. Монітор безпеки
Тема 5 Криптографічні методи захисту інформації Основні положення та визначення. Характеристика алгоритмів шифрування. Поняття блочних шифрів та принципи їх побудови. Схеми Фейстеля. Розширений стандарт шифрування (AES). Асиметричне шифрування даних (алгоритм RSA та функції Діффі-Хеллмана)
Тема 6 Оцінювання захищеності інформаційно-комунікаційних систем Система стандартів комплексних систем захисту інформації та управління інформаційною безпекою. Використання стандартів для проектування та оцінювання комплексних систем захисту інформації. Загальні критерії оцінювання безпеки інформаційних технологій. Методики оцінювання надійності систем захисту інформації від несанкціонованого доступу в автоматизованих системах

5. Очікувані результати навчання навчальної дисципліни

Після успішного вивчення навчальної дисципліни здобувач вищої освіти зможе:

РН1	Розробляти документи зі створення політики інформаційної безпеки використовуючи методологію системного аналізу об’єктів, процесів і систем для задач аналізу, прогнозування, управління та проектування динамічних процесів в різних об’єктах
РН2	Розробляти програмне забезпечення з підвищеною стійкістю до комп'ютерних загроз, а також управляти життєвим циклом цього програмного забезпечення

РН3	Забезпечувати захист інформації, розуміючи концепцію інформаційної безпеки та принципи безпечного проектування програмного забезпечення в умовах неповноти та невизначеності вихідних даних

6. Роль навчальної дисципліни у досягненні програмних результатів

Програмні результати навчання, досягнення яких забезпечує навчальна дисципліна. Для спеціальності 122 Комп`ютерні науки:

ПР8	Використовувати методологію системного аналізу об’єктів, процесів і систем для задачаналізу, прогнозування, управління та проектування динамічних процесів в макроекономічних, технічних, технологічних і фінансових об’єктах.
ПР11	Володіти навичками управління життєвим циклом програмного забезпечення, продуктіві сервісів інформаційних технологій відповідно до вимог і обмежень замовника, вміти розробляти проектну документацію (техніко-економічне обґрунтування, технічне завдання,бізнес-план, угоду, договір, контракт).
ПР16	Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп’ютерних мереж в умовах неповноти та невизначеності вихідних даних.

7. Роль освітнього компонента у формуванні соціальних навичок

Загальні компетентності та соціальні навички, формування яких забезпечує навчальна дисципліна:

СН1	Здатність діяти на основі етичних міркувань (мотивів).
СН2	Здатність застосовувати знання у практичних ситуаціях.

8. Види навчальних занять

Тема 1. Проблеми захисту інформації
Лк1 "Проблеми теорії захисту інформації" Періоди розвитку теорії захисту інформації у комп’ютерних системах та мережах. Основні підходи до розгляду питань теорії захисту інформації безпеки
Лк2 "Базові принципи захисту інформації" Забезпечення виконання вимог конфіденційності, цілісності, достовірності та доступності інформації. Мережева модель OSI. Загальна характеристика проблем безпеки в розподілених комп'ютерних системах. Моделі розподілених систем в процесах розмежування доступу.
Лб1 "Ідентифікація загроз для об’єктів господарської діяльності" Ідентифікація загроз для об’єктів господарської діяльності
Тема 2. Характеристика загроз безпеки інформації. Несанкціонований доступ. Порушники безпеки

Лк3 "Характеристика загроз безпеки інформації. Порушення конфіденційності, цілісності та доступності інформації" Класифікація загроз безпеки інформації. Загроза розкриття. Способи несанкціонованого доступу. Загроза порушення цілісності. Загроза відмови в обслуговуванні
Лк4 "Порушники безпеки" Модель порушника
Лб2 "Розроблення моделей загроз" Розроблення моделей загроз інформаційної безпеки
Лб3 "Розроблення моделей порушника" Розроблення моделей порушника в інформаційному середовищі
Тема 3. Шляхи забезпечення безпеки інформації
Лк5 "Шляхи забезпечення безпеки інформації. Принципи створення безпечного програмного забезпечення" Концепція захисту інформації. Стратегія та архітектура захисту інформації. Використання сукупностей заходів, спрямованих на запобігання появи і усунення вразливостей програм
Лб4 "Система управління безпекою підприємства" Управління безпекою підприємства (структура системи безпеки та структура концепції безпеки)
Лб5 "Методи безпечного програмування" Використання методів безпечного програмувння. Їх поєднання з безпечним середовищем виконання
Лб6 "Виявлення та усунення недоліків безпеки" Використання інструментів статичного та динамічного аналізу для виявлення та усунення недоліків безпеки
Тема 4. Політика безпеки інформації
Лк6 "Політика безпеки інформації. Моделі політики безпеки" Політики безпеки інформації. Заходи політики безпеки. Реалізація політики безпеки. Підтримка політики безпеки. Дискреційна політика безпеки. Мандатна політика безпеки. Рольова політика безпеки. Монітор безпеки
Лб7 "Політика безпеки інформації- складова безпеки інформаційно-комунікаційних систем інформації" Розробка політики безпеки інформації
Лб8 "Моделі політики безпеки" Захист програмного забезпечення від несанкціонованого доступу

Тема 5. Криптографічні методи захисту інформації
Лк7 "Основи теорії шифрування. Блочні шифри. Асиметричне шифрування даних" Основні положення та визначення. Характеристика алгоритмів шифрування. Поняття блочного шифру та принципи його побудови. Схеми Фейстеля. Розширений стандарт шифрування (AES). Впровадження AES. Режими роботи блочних шифрів. Математичні основи RSA-шифрування. Генерація RSA-ключів. Електронні підписи на основі RSA. Реалізація RSA. Функції Діффі-Хеллмана
Лб9 "Блочні шифри" Моделювання атаки кодової книги. Раунди блочного шифру. Мережі підстановки-перестановки та схеми Фейстеля.
Лб10 "RSA-алгоритм шифрування" Генерація RSA-ключів
Тема 6. Оцінювання захищеності інформаційно-комунікаційних систем
Лк8 "Оцінювання захищеності інформаційно-комунікаційних систем" Система стандартів комплексних систем захисту інформації та управління інформаційною безпекою. Використання стандартів для проектування та оцінювання комплексних систем захисту інформації. Загальні критерії оцінювання безпеки інформаційних технологій. Методики оцінювання надійності систем захисту інформації від несанкціонованого доступу в автоматизованих системах
Лб11 "Захищеність систем від порушень конфіденційності" Методика оцінювання ефективності системи захисту інформації від несанкціонованого доступу для забезпечення конфіденційності даних
Лб12 "Захищеність систем від порушень доступності" Методика оцінювання рівня готовності систем захисту інформації від несанкціонованого доступу для забезпечення доступності даних

9. Стратегія викладання та навчання

9.1 Методи викладання та навчання

Дисципліна передбачає навчання через:

МН1	Лекційне навчання
МН2	Практикоорієнтоване навчання
МН3	Самостійне навчання

Лекційне навчання, а саме мультимедійні лекції з докладним викладенням навчального матеріалу із застосуванням пасивного методу навчання з елементами активного та інтерактивного методів є основою для самостійного навчання здобувачів вищої освіти (РН1 - РН3). Лекції доповнюються практикоорієнтованим навчанням (включно з лабораторними заняттями з виконанням завдань на персональних комп’ютерах), що надає студентам можливість застосовувати теоретичні знання для конкретних ситуацій (РН1 - РН3).

Самостійному навчанню сприятиме підготовка до лекцій, лабораторних занять, а також врахування коментарів викладача при аналіз робіт інших студентів (РН1 - РН3).

Засвоїти навички самонавчання, покращити здатність розподіляти час, виділяти головне і другорядне. Використовувати результати самостійного пошуку, аналізу та синтезу інформації з різних джерел.

9.2 Види навчальної діяльності

НД1	Лекції-дискусії
НД2	Виконання лабораторних робіт
НД3	Робота з підручниками та релевантними інформаційними джерелами

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)	$64 \leq RD < 73$
Виконання задовольняє мінімальним критеріям	3 (задовільно)	$60 \leq RD < 63$
Можливе повторне складання	2 (незадовільно)	$35 \leq RD < 59$
Необхідний повторний курс з навчальної дисципліни	2 (незадовільно)	$0 \leq RD < 34$

10.2 Методи поточного формативного оцінювання

	Характеристика	**Дедлайн, тижні**	**Зворотний зв'язок**
МФО1 Опитування та усні коментарі викладача за його результатами	Теоретичні знання	0	Безпосередньо в аудиторії або через Meet

МФО2 Настанови викладача в процесі виконання практичних завдань	Безпосередньо в аудиторії або через Meet	0	Безпосередньо в аудиторії або через Meet

10.3 Методи підсумкового сумативного оцінювання

	Характеристика	**Дедлайн, тижні**	**Зворотний зв'язок**
МСО1 Підсумковий контроль: екзамен	Проводиться екзамен в формі тестування	В день проведення екзамену	Безпосередньо в аудиторії
МСО2 Звіт за результатами виконання лабораторних робіт	Перевіряється виконання лабораторних робіт	1	Через Mix
МСО3 Модульний контроль	Проводиться тестування	В день проведення тестування	Безпосередньо в аудиторії або через MIX
МСО4 Виконання індивідуальної контрольної роботи	Перевіряється виконання	1	Безпосередньо в аудиторії або через MIX

Контрольні заходи:

		Максимальна кількість балів	Мінімальна кількість балів	Можливість перескладання з метою підвищення оцінки
8 семестр		**100 балів**		
МСО1. Підсумковий контроль: екзамен		**40**		
		40	Не передбачено	Ні
МСО2. Звіт за результатами виконання лабораторних робіт		**32**		
		32	Не передбачено	Ні
МСО3. Модульний контроль		**12**		

		12	Не передбачено	Ні
МСО4. Виконання індивідуальної контрольної роботи		**16**		
		16	Не передбачено	Ні

При здійсненні семестрової атестації повинні виконуватись такі положення: а) студент, який протягом навчального періоду виконав всі заплановані види нав-чальної роботи та за наслідками цієї роботи та модульних атестацій набрав необ-хідну, яка відповідає позитивній оцінці, кількість рейтингових балів (не менше 20% від визначених шкалою оцінювання), отримує допуск до здачі іспиту; при отриманні рейтингового балу за наслідками роботи на протязі семестру та мо-дульних атестацій менше 20 балів, студент допуск до здачі іспиту не отримує і йому призначається повторне вивчення дисципліни; Складання додаткових заходів підсумкового семестрового контролю з метою підвищення позитивної оцінки не здійснюється; б) іспит (ДСК) є обов'язковим й на нього виділяється 40% від визначених шкалою оцінювання; в) повторне вивчення дисциплін планується за рахунок власного часу студента і не фінансується з бюджетних коштів. При повторному вивчені відповідний навчальний компонент відноситься до індивідуального навчального плану наступного навчального періоду. У разі неуспішного повторного вивчення дисципліни студент відраховується з університету. Якщо студент, який отримав доступ до іспиту, за всі види робіт, включно іспит, набрав загальний рейтинговий бал, що відповідає позитивній оцінці (60 балів і більше), цей результат заноситься в залікову екзаменаційну відомість без можливості його покращення. Якщо студент, який отримав доступ до іспиту, не набрав загальний рейтинговий бал, який відповідає позитивній оцінці (60 балів і більше), вважається, що він має заборгованість з дисципліни з процедурою її ліквідації.

11. Ресурсне забезпечення навчальної дисципліни

11.1 Засоби навчання

ЗН1	Мультимедіа, відео- і звуковідтворювальна, проєкційна апаратура (відеокамери, проєктори, екрани, смартдошки тощо)
ЗН2	Комп'ютерний клас для лабораторних занять, комп'ютери, комп'ютерні системи та мережі
ЗН3	Програмне забезпечення для підтримки дистанційного навчання

11.2 Інформаційне та навчально-методичне забезпечення

Основна література	
1	Жилін А. В. Технології захисту інформації в інформаційно-телекомунікаційних системах : навч. посіб. / А. В. Жилін, О. М. Шаповал, О. А. Успенський ; ІСЗЗІ КПІ ім. Ігоря Сікорського. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2021. – 213 с. https://ela.kpi.ua/bitstream/123456789/45723/1/NP_TZI_ITS.pdf

2	Демчинський В. В. Основи технологій захисту інформації [електронний ресурс]: В. В. Демчинський, М.В. Грайворонський, О.В. Кіреєнко/Навчальний посібник/ Київ: КПІ, 2022. 107 с. https://ela.kpi.ua/bitstream/123456789/53203/1/OTZI_Practices_plan_v115.pdf
3	Кушнерьов, О. С. Безпека інформації [Електронний ресурс] : конспект лекцій / О. С. Кушнерьов. — Суми : СумДУ, 2021. — 99 с.https://essuir.sumdu.edu.ua/bitstream-download/123456789/85989/3/Kushnerov.pdf
Допоміжна література	
4	Cyber Security. Simply. Make it Happen. : Monograph / edit. Abolhassan. – Springer International Publishing, 2017. – ISBN 978-3-319-46528-9 (print); 978-3-319-46529-6 (online). 127 p.
5	Тарнавський Ю.А. Технології захисту інформації [електронний ресурс]: підручник для студентів спеціальності 122 «Компютерні науки»/ Київ: КПІ, 2018. 162 с. https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
Інформаційні ресурси в Інтернеті	
1	Державна служба спеціального зв'язку та захисту інформації України - https://cip.gov.ua/ua
2	Ободяк В.К. Матеріали навчального курсу "Технології захисту інформації" на платформі MIX - https://mix.sumdu.edu.ua/textbooks/66503/index.html