РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

СИЛАБУС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

1. Загальна інформація про навчальну дисципліну

Повна назва навчальної дисципліни	Інформаційна безпека в комп'ютерних системах
Повна офіційна назва закладу вищої освіти	Сумський державний університет
Повна назва структурного підрозділу	Факультет електроніки та інформаційних технологій. Кафедра електроніки і комп`ютерної техніки
Розробник(и)	Бережна Ольга Володимирівна
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 становить 5 кред. ЄКТС, 150 год. Для денної форми навчання 48 год. становить контактна робота з викладачем (16 год. лекцій, 32 год. лабораторних занять), 102 год. становить самостійна робота.
Мова викладання	Українська

2. Місце навчальної дисципліни в освітній програмі

Статус дисципліни	Вибіркова навчальна дисципліна для освітньої програми "Електронні системи та компоненти"
Передумови для вивчення дисципліни	Необхідні базові знання з вищої математики та базове володіння комп'ютером
Додаткові умови	Додаткові умови відсутні
Обмеження	Обмеження відсутні

3. Мета навчальної дисципліни

Метою вивчення дисципліни є досягнення студентами конструктивного мислення у фундаментальних питаннях та системи спеціальних знань у галузі захисту інформації в телекомунікаційних технологіях та сучасних методів створення комплексної системи захисту інформації для електронних систем.

4. Зміст навчальної дисципліни

Тема 1 Проблеми інформаційної безпеки розподілених комп’ютерних систем та мереж Предмет та об’єкт захисту інформації. Класифікація та аналіз загроз безпеки інформації. Аудит інформаційної безпеки комп’ютерних систем. Загрози та уразливості IP-мереж. Забезпечення інформаційної безпеки.
Тема 2 Стандарти інформаційної безпеки Міжнародні та вітчизняні стандарти інформаційної безпеки. Загальні критерії безпеки інформаційних технологій (IT). Забезпечення конфіденційності, цілісності, обмежень в доступі. Мережеві механізми безпеки. Шифрування. Електронний цифровий підпис (ЕЦП). Механізми управління доступом, контролю цілісності даних, аутентифікації.
Тема 3 Принципи криптографічного захисту даних Основні поняття криптографічного захисту даних. Симетричні та асиметричні криптосистеми шифрування. Комбінована криптосистема шифрування. ЕЦП та функція хешування. Управління криптоключами.
Тема 4 Криптографічні алгоритми Класифікація криптографічних алгоритмів. Блочні алгоритми шифрування даних. Симетричні та асиметричні криптоалгоритми. Алгоритм шифрування RSA. Алгоритм ЕЦП.
Тема 5 Технології аутентифікації Аутентифікація, авторизація та адміністрування дій користувачів. Методи аутентифікації, що використовують паролі та PIN-коди. Аутентифікація, що заснована на симетричних алгоритмах. Аутентифікація, що заснована на асиметричних алгоритмах.
Тема 6 Технології захисту міжмережевого обміну даними в розподілених комп’ютерних системах Архітектура та функції підсистеми захисту ОС. Ідентифікація, аутентифікація та авторизація суб’єктів доступу. Технології міжмережевих екранів (МЕ). Протоколи формування захищених каналів. Протокол управління криптоключами IKE. Організація захищеного віддаленого доступу. Інфраструктура управління відкритими ключами PKI.
Тема 7 Технології виявлення вторгнень Технології аналізу захищеності та виявлення атак. Захист від вірусів. Побудова системи антивірусного захисту.
Тема 8 Захист інформації від витоку по технічним каналам Методи та засоби захисту від електромагнітних випромінювань та наведень. Пасивні та активні методи захисту від побічних випромінювань та наведень.

5. Очікувані результати навчання навчальної дисципліни

Після успішного вивчення навчальної дисципліни здобувач вищої освіти зможе:

РН1	Знати аналітичні, кодові, технічні та організаційні заходи щодо забезпечення інформаційної безпеки в комп'ютерних системах та мережах.
РН2	Володіти методами рішення задач захисту комп'ютерних систем та мереж.

РН3	Вміти будувати систему безпеки комп'ютерних систем та мереж, проводити організаційні заходи із захисту даних.

7. Роль освітнього компонента у формуванні соціальних навичок

Компетентності та соціальні навички, формування яких забезпечує навчальна дисципліна:

СН1	Здатність виявляти, ставити та вирішувати проблеми.
СН2	Здатність до абстрактного мислення, аналізу та синтезу.
СН3	Здатність до навчання впродовж життя (прагнення постійного особистого та професійного розвитку, активний пошук нових знань, набуття нових навичок та адаптація до нових тенденцій і технологій)
СН4	Здатність планувати та управляти часом.

8. Види навчальних занять

Тема 1. Проблеми інформаційної безпеки розподілених комп’ютерних систем та мереж
Лк1 "Проблеми інформаційної безпеки розподілених комп’ютерних систем та мереж" Предмет та об’єкт захисту інформації. Джерела загроз. Класифікація та аналіз загроз безпеки інформації. Методи оцінки уразливості інформації. Аудит інформаційної безпеки комп’ютерних систем. Вступ до мережевого інформаційного обліку. Аналіз загроз мережевої безпеки. Загрози та уразливості IP-мереж. Забезпечення інформаційної безпеки.
Лб1 "Аудит інформаційної безпеки комп’ютерних систем." Аналіз стану комп’ютерної системи у сфері інформаційної безпеки.
Тема 2. Стандарти інформаційної безпеки
Лк2 "Стандарти інформаційної безпеки" Міжнародні та вітчизняні стандарти інформаційної безпеки та їх роль. Загальні критерії безпеки інформаційних технологій (ІТ). Методологія оцінки безпеки ІТ. Види вимог безпеки. Забезпечення конфіденційності, цілісності, обмежень в доступі. Мережеві механізми безпеки. Шифрування. Електронний цифровий підпис (ЕЦП). Механізми управління доступом, контролю цілісності даних, аутентифікації.
Лб2 "Програмні продукти захисту інформації." Аналіз різних програмних продуктів захисту інформації, їх функціональності та ступеня забезпечення конфеденційності даних.
Тема 3. Принципи криптографічного захисту даних
Лк3 "Принципи криптографічного захисту даних" Основні поняття криптографічного захисту даних. Симетричні криптосистеми шифрування. Асиметричні криптосистеми шифрування. Комбінована криптосистема шифрування. ЕЦП та функція хешування. Управління криптоключами.

Лб3 "Методи генерування простих чисел." Генерування простих чисел для використання в асиметричних системах шифрування.
Лб4 "Шифрувальна машина «Енігма»." Вивчення структури та принципу роботи шифрувальної машини «Енігма». Застосування імітаційної моделі «Енігми» для захисту конфеденційної інформації.
Лб5 "Стандарт симетричного шифрування AES RIJNDAEL." Вивчення структури та функціональності стандарту симетричного шифрування AES RIJNDAEL. Застосування імітаційної моделі шифрування.
Лб6 "Електронний цифровий підпис." Вітчизняний алгоритм електронного цифрового підпису. Застосування імітаційної моделі формування електронного цифрового підпису.
Тема 4. Криптографічні алгоритми
Лк4 "Криптографічні алгоритми" Класифікація криптографічних алгоритмів. Симетричні алгоритми шифрування. Блочні алгоритми шифрування даних. Асиметричні криптоалгоритми. Алгоритм шифрування RSA. Алгоритм ЕЦП.
Лб7 "Шифрування методом ковзної перестановки." Формування шифрограм методом ковзної перестановки.
Лб8 "Класичні криптоалгоритми заміни для захисту інформації." Використання класичних криптоалгоритмів заміни для захисту текстової інформації. Формування шифрограм методом заміни.
Лб9 "Класичні криптоалгоритми перестановки для захисту інформації." Використання класичних криптоалгоритмів перестановки для захисту текстової інформації. Формування шифрограм методом перестановки.
Лб10 "Методи захисту текстової інформації на основі підбору ключів. Методи заміни та перестановки." Дослідження методів захисту текстової інформації та їх стійкості на основі підбору ключів. Формування шифрограм методами заміни та перестановки.
Лб11 "Методи захисту текстової інформації на основі підбору ключів. Метод гамування та таблиця Віженера." Дослідження методів захисту текстової інформації та їх стійкості на основі підбору ключів. Формування шифрограм методами гамування та Віженера.
Тема 5. Технології аутентифікації

Лк5 "Технології аутентифікації" Аутентифікація, авторизація та адміністрування дій користувачів. Методи аутентифікації, що використовують паролі та PIN-коди. Аутентифікація, що заснована на симетричних алгоритмах. Аутентифікація, що заснована на асиметричних алгоритмах.
Тема 6. Технології захисту міжмережевого обміну даними в розподілених комп'ютерних системах
Лк6 "Технології захисту міжмережевого обміну даними в розподілених комп'ютерних системах" Архітектура та функції підсистеми захисту ОС. Ідентифікація, аутентифікація та авторизація суб'єктів доступу. Технології міжмережевих екранів (МЕ). Протоколи формування захищених каналів на канальному та сеансовому рівнях. Архітектура засобів безпеки IPSec. Захист даних за допомогою протоколів AH та ESP. Протокол управління криптоключами IKE. Особливості реалізації засобів IPSec. Організація захищеного віддаленого доступу. Управління доступом за схемою однократного входу з авторизацією Single Sign-On (SSO). Протокол Kerberos. Інфраструктура управління відкритими ключами PKI.
Лб12 "Основи захвата та аналіза мережевого трафіку." Аналіз методів захвата та аналіза мережевого трафіку.
Лб13 "Методи виявлення мережевих атак." Виявлення мережевих атак шляхом аналізу трафіка в комп'ютерних мережах.
Лб14 "Міжмережеві екрани." Захист комп'ютерної мережі з використанням міжмережевих екранів.
Лб15 "Протокол Kerberos." Організація системи єдиного входу до мережі на основі протоколу Kerberos.
Тема 7. Технології виявлення вторгнень
Лк7 "Технології виявлення вторгнень" Технології аналізу захищеності та виявлення атак. Засоби аналізу захищеності та методи реагування. Захист від вірусів. Побудова системи антивірусного захисту.
Лб16 "Системи виявлення атак." Виявлення атак в комп'ютерній мережі.
Тема 8. Захист інформації від витоку по технічним каналам
Лк8 "Захист інформації від витоку по технічним каналам" Методи та засоби захисту від електромагнітних випромінювань та наведень. Пасивні методи захисту від побічних випромінювань та наведень. Активні методи захисту від побічних випромінювань та наведень.

9. Стратегія викладання та навчання

9.1 Методи викладання та навчання

Дисципліна передбачає навчання через:

МН1	Лекційне навчання
МН2	Практикоорієнтоване навчання
МН3	Самостійне навчання

Лекції надають студентам теоретичні знання аналітичних, кодових, технічних та організаційних заходів щодо забезпечення інформаційної безпеки в комп'ютерних системах та мережах, що є основою для самостійного навчання здобувачів вищої освіти (РН1). Лекції доповнюються пошуковими лабораторними роботами, що надають студентам можливість застосовувати теоретичні знання на практичних прикладах та комп'ютерних моделях та сформувати вміння застосовувати методи рішення задач захисту комп'ютерних систем та мереж та будувати систему безпеки комп'ютерних систем та мереж, проводити організаційні заходи із захисту даних (РН2, РН3). Самостійному навчанню сприятиме підготовка до лекцій та лабораторних робіт, підготовча робота до виконання розрахунково-графічної роботи з практичної реалізації криптографічних алгоритмів (РН1, РН2, РН3).

Робота в невеликих групах для підготовки презентацій програмних моделей алгоритмів інформаційної безпеки комп'ютерних систем, що будуть представлені іншим групам, будуть стимулювати формування навичок командної роботи та лідерських якостей, а аналіз, подання та захист результатів виконання лабораторних робіт та результатів виконання розрахунково-графічної роботи розвиватимуть у студентів навички вести дискусію, аргументувати свою позицію, критичного мислення та нестандартного підходу до розв'язування задач.

9.2 Види навчальної діяльності

НД1	Інтерактивні лекції
НД2	Виконання практичних завдань
НД3	Виконання індивідуальних розрахунково-аналітичних завдань

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)	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 Опитування та усні коментарі викладача за його результатами	Призначене для закріплення знань, отриманих протягом лекційного заняття.	Протягом аудиторного заняття	Google Meet, Telegram, e-mail
МФО2 Настанови викладача в процесі виконання практичних завдань	Призначене для визначення здобувачами вищої освіти своїх проміжних досягнень та їх покращення надалі.	Протягом аудиторного заняття	Google Meet, Telegram, e-mail
МФО3 Проміжне оцінювання виконання індивідуального пошуково-дослідницького завдання (підготовка, презентація, захист)	Призначене для обговорення проблемних питань протягом виконання розрахунково-графічної роботи.	Протягом семестру	Google Meet, Telegram, e-mail

10.3 Методи підсумкового сумативного оцінювання

	Характеристика	**Дедлайн, тижні**	**Зворотний зв'язок**
МСО1 Проміжний модульний контроль у формі тестування	Тестові питання направлені на перевірку знань, отриманих протягом модулю.	Атестаційні тижні, згідно графіку навчального процесу	Google Meet, Telegram, e-mail
МСО2 Звіт за результатами виконання пошукових лабораторних робіт	Для зарахування лабораторної роботи необхідно виконати мінімальний обсяг завдання згідно методичних вказівок.	До наступного лабораторного заняття	Google Meet, Telegram, e-mail
МСО3 Виконання індивідуальних розрахунково-аналітичних завдань	Зарахування розрахунково-графічної роботи відбувається після її виконання, оформлення згідно методичних вказівок та захисту.	Згідно графіку навчального процесу перед другим модульним тижнем	Google Meet, Telegram, e-mail

Контрольні заходи:

		Максимальна кількість балів	Можливість перескладання з метою підвищення оцінки
Семестр викладання		**100 балів**	
МСО1. Проміжний модульний контроль у формі тестування		**40**	
	2х20	40	Ні
МСО2. Звіт за результатами виконання пошукових лабораторних робіт		**30**	
		30	Так
МСО3. Виконання індивідуальних розрахунково-аналітичних завдань		**30**	
		30	Так

Звіти з лабораторних робіт і розрахунково-графічну роботу треба оформлювати згідно ДСТУ 3008:2015 "Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлювання".

11. Ресурсне забезпечення навчальної дисципліни

11.1 Засоби навчання

ЗН1	Мультимедіа, відео- і звуковідтворювальна, проєкційна апаратура (відеокамери, проєктори, екрани, смартдошки тощо)
ЗН2	Комп’ютери, комп’ютерні системи та мережі
ЗН3	Програмне забезпечення для дистанційного навчання (Google Meet, Google Forms)

11.2 Інформаційне та навчально-методичне забезпечення

Основна література	
1	Полторак В.П. Інформаційна безпека та захист даних в комп’ютерних технологіях і мережах [Електронний ресурс]: навч. посіб. для студ. спеціальності 126 «Інформаційні системи та технології» / В.П. Полторак. – Київ: КПІ ім. Ігоря Сікорського, 2020. – 78 с.
2	Гапак О.М. Захист інформації в комп’ютерних системах: підручник / О.М. Гапак, С.І. Балога. – Ужгород: ДВНЗ «УжНУ», 2021. – 184 с.
Допоміжна література	
3	4636 Методичні вказівки до лабораторних робіт із дисциплін «Інформаційна безпека телекомунікаційних мереж», «Основи кібербезпеки в інформаційних мережах» /О.В. Бережна, Т.О. Протасова, О.В. Д’яченко. – Суми: СумДУ, 2019. – Ч. 1. – 15 с.

4	4637 Методичні вказівки до лабораторних робіт із дисципліни «Захист інформації в комп'ютерних системах» / укладачі: О.В. Бережна, Т.О. Протасова, О.В. Д'яченко. – Суми: Сумський державний університет, 2019. – Ч. 1. – 22 с.
5	Smith, Sean. The Internet of Risky Things: Trusting the devices that surround us. O'Reilly Media, Inc., 2017. – 229 pp.

ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

№ з/п	Програма навчальної дисципліни	Усього годин	Навчальна робота, аудиторних годин				Самостійна робота здобувача вищої освіти за видами, годин					
			Усього, ауд. год.	Лекції	Практичні заняття	Лабораторні роботи	Усього, год.	Самостійне опрацювання матеріалу	Підготовка до практичних занять	Підготовка до лабораторних робіт	Підготовка до контрольних заходів	Виконання самостійних позааудиторних завдань
1	2	3	4	5	6	7	8	9	10	11	12	13
денна форма навчання												
1	Проблеми інформаційної безпеки розподілених комп’ютерних систем та мереж	5.5	4	2	0	2	1.5	0.5	0	1	0	0
2	Стандарти інформаційної безпеки	5.5	4	2	0	2	1.5	0.5	0	1	0	0
3	Принципи криптографічного захисту даних	14.5	10	2	0	8	4.5	0.5	0	4	0	0
4	Криптографічні алгоритми	17.5	12	2	0	10	5.5	0.5	0	5	0	0
5	Технології аутентифікації	2.5	2	2	0	0	0.5	0.5	0	0	0	0
6	Технології захисту міжмережевого обміну даними в розподілених комп’ютерних системах	14.5	10	2	0	8	4.5	0.5	0	4	0	0
7	Технології виявлення вторгнень	5.5	4	2	0	2	1.5	0.5	0	1	0	0
8	Захист інформації від витоку по технічним каналам	2.5	2	2	0	0	0.5	0.5	0	0	0	0
Контрольні заходи												
1	диференційний залік	6	0	0	0	0	6	0	0	0	6	0
Індивідуальні завдання												
1	інші індивідуальні завдання	76	0	0	0	0	76	0	0	0	0	76
Всього з навчальної дисципліни (денна форма навчання)		*150*	*48*	*16*	*0*	*32*	*102*	*4*	*0*	*16*	*6*	*76*