СИЛАБУС

навчальної дисципліни «БЕЗПЕКА ДАНИХ ТА КРИПТОГРАФІЧНІ МЕТОДИ ЗАХИСТУ»

Спеціальність	051 Економіка
Рівень вищої освіти	перший (бакалаврський)
Статус навчальної дисципліни	вибіркова
Код навчальної дисципліни відповідно до освітньо-професійної програми	ВК 5
Семестр вивчення	5-й семестр
Кількість кредитів ЄКТС / годин	4/ 120
Розподіл за видами занять та годинами навчання	Лекції - 32 год.
	Лабораторні заняття – 32 год.
	Самостійна робота - 56 год.
Вид індивідуального завдання	Контрольна робота
Форма підсумкового контролю	залік
Кафедра (назва, № кабінету, контактний телефон, e-mail)	Економіки, обліку і оподаткування м. Черкаси, вул. Нечуя-Левицького, 16, каб.220., e-mail: kaf-oblik@suem.edu.ua
Викладач /і:	
Контактна інформація викладача/ів:	E-mail:
Дні занять	Згідно з розкладом
Консультації	Очні консультації: згідно з графіком Дистанційні: електронна пошта, групи у Вайбері, Телеграмі

Анотація навчальної дисципліни:

спрямована на розгляд широкого кола питань щодо принципів створення комплексних систем захисту інформації (КСЗІ) в інформаційно – телекомунікаційних системах (ІТС), здійснення комплексу заходів, спрямованих на розроблення і впровадження інформаційних технологій, які забезпечують обробку інформації в ІТС згідно з вимогами, встановленими нормативно – правовими документами у сфері захисту інформації.

Мета навчальної дисципліни:

формування системи теоретичних знань і придбання практичних умінь і навичок щодо процесів автоматизованого проєктування інформаційних систем з використанням САПР, сучасних технологій на основі структурно-функціонального підходу; побудови моделей для опису предметної області комп'ютерного проєктування – складних систем, об'єктів управління та бізнес-процесів підприємства.

Мета орієнтована на формування у студентів таких компетентностей:

ЗК4. Здатність застосовувати знання у практичних ситуаціях.

ЗК6. Здатність спілкуватися іноземною мовою.

ЗК7. Навички використання інформаційних і комунікаційних технологій.

СК8. Здатність проектувати та розробляти програмне забезпечення із застосуванням різних парадигм програмування: узагальненого, об’єктно-орієнтованого, функціонального, логічного, з відповідними моделями, методами й алгоритмами обчислень, структурами даних і механізмами управління.

СК10. Здатність застосовувати методології, технології та інструментальні засоби для управління процесами життєвого циклу інформаційних і програмних систем, продуктів і сервісів інформаційних технологій відповідно до вимог замовника.СК10. Здатність застосовувати методології, технології та інструментальні засоби для управління процесами життєвого циклу інформаційних і програмних систем, продуктів і сервісів інформаційних технологій відповідно до вимог замовника.

СК13. Здатність на основі інформаційного забезпечення та комп’ютерних технологій розробляти та застосовувати комп’ютерні моделі для прогнозування, оптимізації та планування економічної діяльності з використанням програмних додатків для мобільних пристроїв, Інтернет-додатків, оволодіти навичками будувати трендові і адаптивні моделі.

Програмні результати навчання:

ПРН8. Використовувати методологію системного аналізу об’єктів, процесів і систем для задач аналізу, прогнозування, управління та проектування динамічних процесів в макроекономічних, технічних, технологічних і фінансових об’єктах.

ПРН16. Застосовувати відповідні економіко-математичні методи та моделі для вирішення економічних задач, розробляти моделі бізнес-процесів в умовах невизначеності.

ПРН17. Використовувати інформаційні та комунікаційні технології для вирішення соціально-економічних завдань, підготовки та представлення аналітичних звітів, проектувати та розробляти класи та відношення між ними з використанням механізмів і технологій об'єктно-орієнтованого програмування.

ПРН18. Формувати цілісну систему інформаційно- аналітичного забезпечення ефективного оцінювання, створювати бізнес-додатки в рамках певної корпоративної інформаційної системи та управління економікою на мікро-, мезо- та макрорівнях.

Очікувані результати, досягнення яких забезпечує навчальна дисципліна:

У результаті засвоєння курсу здобувачі мають бути компетентними у таких *питаннях*:
вивчення основ використання криптографічних та стеганографічних засобів та методів захисту інформації у інформаційних системах, дослідження проблем зберігання, опрацювання, пошуку, передачі, перетворення, закриття та відновлення інформації в організаціях і на підприємствах різних напрямків діяльності та різних форм власності, способів захисту від несанкціонованого доступу до інформаційних ресурсів; сучасні погрози безпеки інформаційним системам; технічні методи і засоби захисту інформації; криптографічні методи захисту інформації; програмні методи і засоби захисту; технології забезпечення цілісності даних інформаційних систем; методи та процедури цифрової стеганографії.

У результаті вивчення навчальної дисципліни студенти повинні *вміти*:
аналізувати можливості несанкціонованого здобуття інформації потенційними порушниками;
аналізувати вплив комп’ютерних вірусів і шкідливих програм на безпеку комп’ютерних систем;
досліджувати стійкість секретних криптографічних систем;
досліджувати асиметричні криптосистеми;
забезпечувати обґрунтований підбір програмно-апаратних та програмних засобів для забезпечення необхідного рівня захисту інформації;
здатність забезпечувати захист програмного та інформаційного забезпечення від несанкціонованих дій.

Зміст навчальної дисципліни:

Змістовий модуль 1. Політика безпеки, механізми та протоколи забезпечення захисту інформації в інформаційних системах

Тема 1. Основи захисту інформації та життєвий цикл розробки систем безпеки

Роль інформації в сучасному світі, значення захисту. Основні поняття та визначення. Критична, конфіденційна, особиста, державна інформація. Державна таємниця. Роль захисту інформації в ІС. Аналіз основних видів атак, ризиків і вразливих елементів інформаційних систем. Вимоги щодо безпеки системи, ризики безпеки. Послуги безпеки: конфіденційність, цілісність, доступність, причетність, спостереженість. Розподіл послуг безпеки за рівнями моделі ISO/OSI. Документ політика безпеки в інформаційних системах. Критерії захищеності комп'ютерних систем. Розробка профілю захисту. Механізми реалізації послуг безпеки. Стандарт ISO 27001 та ISO 27002. Побу дова та впровадження систем захисту інформації.

Тема 2. Національні й міжнародні стандарти криптографічного захисту інформації в ІС

Міжнародні стандарти криптографічних методів захисту інформації. Стандарти безпеки банківської справи. Стандарти шифрування ANSI. Стандарти безпеки банківської справи ANSI.

Міжнародні стандарти стосовно засад безпеки інформації й архітектурі безпеки. Урядові стандарти США (FIPS). Державні стандарти колишнього СРСР, Російської федерації (ГОСТ) та нормативно правові документи. Державні стандарти України (ДСТУ) й інші та нормативно правові документи. Запити коментарів (Request for Comments, RFC). Стандарти науково-дослідницьких і промислових організацій: IEEE, ITU-T, PKCS. Стандарти безпеки НАТО. Галузеві стандарти.

Змістовий модуль 2 Методи і засоби захисту інформації в комп'ютерних системах

Тема 3. Криптографічні механізми захисту інформації в інформаційних системах

Компоненти криптосистеми та їх функціональні характеристики. Перестановка та підстановка. Прості шифри. Симетричне шифрування. Блочні симетричні шифри. Архітектура блочних симетричних шифрів. Характеристики і параметри сучасних блочних симетричних шифрів.

Режими шифрування: "Електронна кодова книга", "Зчеплення блоків шифру", "Зворотний зв'язок по шифру", "Зворотний зв'язок по виходу". Режим простої заміни. Режим гама шифрування. Режим шифрування зворотним зв'язком за виходим. Режим вироблення імітовставки. Автентифікація та імітозахист інформації. Потокові шифри. Сфера застосування симетричних алгоритмів і режимів шифрування. Односпрямовані функції.

Функція гешування. Важкозворотні функції, їх класифікація, еліптичні криві. Асиметричні криптоперетворення. Стійкість асиметричних криптоперетворень. Компоненти асиметричної системи. Генерування ключів. Загальносистемні. параметри. Спрямоване шифрування та цифровий підпис. Загрози й атаки на цифровий підпис. Формування та перевірка цифрового підпису. Стандарти спрямованого шифрування і цифрового підпису. ДСТУ 4145. Алгоритми ЦП: RSA, Ель Гамаля (EGSA), ECDSA. Протоколи керування ключами. Протокол Дефі-Хелмана. Напрямки стеганографії. Класифікація систем цифрової стеганографії та їх використання. Стеганографія з відкритим ключем. Атаки на стегасистеми та протидія їм.

Тема 4. Комплексні системи захисту в корпоративних ІС

Визначення і класифікація задач курування доступом до ресурсів. Поняття "держатель" та "власник" інформації. Класифікація суб'єктів і об'єктів доступу. Модель управління доступом. Типи порушників. Класифікація мережних загроз та атак. Захист інформації за рівнями ISO\OSI. Фільтрація трафіка. Захист інформації за допомогою міжмережних екранів. Захист інформації на мережному рівні. Протоколи IPSec, SSL, TLS, їх сутність. Захищена електронна пошта. Архітектура та основні вимоги. Система PGP. Криптографічні функції. Сумісність на рівні електронної пошти. Захищена електронна пошта. Компоненти та сервіси інфраструктури відкритих ключів. Архітектура і топологія PKI. Стандарти в галузі PKI. Сертифікати відкритих ключів X.509. Системи PKI. Документ політика за- хисту інформації, його сутність і структура. Профілі безпеки автоматизованих систем. Основні вимоги до політиці PKI.

Методи викладання, навчання:

Проблемні лекції.

Лабораторне заняття: виконання лабораторних робіт.

Виконання індивідуального навчально-дослідного завдання (ІНДЗ): виконання завдань з лабораторних робіт і оформлення їх в контрольну роботу, підготовка до захисту.

Форми контролю успішності навчання:

Контрольні заходи з перевірки успішності засвоєння навчального матеріалу з дисципліни включають: поточний контроль, виконання індивідуальних навчально-дослідних занять (ІНДЗ), підсумковий контроль.

Поточний контроль має на меті перевірку виконання завдань як аудиторної, так і самостійної роботи студентів та може проводитися в таких формах:

- перевірка підготовлених звітів лабораторних занять;
- усне опитування або письмовий експрес-контроль на аудиторних заняттях;
- перевірка виконання завдань СРС.

Контроль виконання *ІНДЗ* здійснюється у формі виконання завдань з лабораторних робіт і оформлення їх в контрольну роботу, підготовка до захисту.

Формою *підсумкового контролю* з навчальної дисципліни «Безпека даних та криптографічні методи захисту» є *залік*.

Рекомендована література:

1. Методологія захисту інформації. Аспекти кібербезпеки: підручник. К.: Видавництво НА СБ України, 2020. 256 с.. URL: http://www.immsp.kiev.ua/postgraduate/Biblioteka_trudy/Gulak_MetodolZahystuInfOsnKiberbezp_2020.pdf.
2. Щур Н.О., Покотило О.А. Основи криптології: навч. посібник. Житомир: Державний університет «Житомирська політехніка», 2021. 120 с. URL: https://eztuir.ztu.edu.ua/bitstream/handle/123456789/8092/%D0%A9%D1%83%D1%80.pdf?sequence=1&isAllowed=y.
3. Інформаційна безпека [Текст] : навч. посіб. / Ю.Я. Бобало, І.В. Горбатий, М.Д. Кіселичник та ін.; за заг. ред. Ю.Я. Бобала, І.В. Горбатого. Львів : Львівська політехніка, 2019. 580 с. URL: http://pdf.lib.vntu.edu.ua/books/2022/Bobalo_2019_580.pdf.
4. 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. URL: https://ela.kpi.ua/server/api/core/bitstreams/d99a0045-e907-4d17-afc1-5431f67d2444/content.

Система оцінювання результатів навчання:

Згідно з діючою в університеті системою комплексної діагностики знань студентів, з метою стимулювання планомірної та систематичної навчальної роботи, оцінка знань студентів здійснюється за 100-бальною системою.

Підсумкова оцінка (залік) виставляється на підставі суми накопичених балів студентом, отриманих у ході поточного контролю, виконання індивідуального завдання.

Схема розподілу балів:

70 балів (поточний контроль)	30 балів (контроль виконання індивідуального завдання)

Мінімальний пороговий рівень з кожного виду контролю:

45 балів (поточний контроль)	15 балів (контроль виконання індивідуального завдання)

Накопичування балів з навчальної дисципліни під час *поточного* контролю відбувається під час оцінювання таких видів робіт:

1) Усне опитування;
2) Виконання лабораторних завдань;
3) Проходження тестового контролю в електронній формі з засвоєння тем курсу;
4) Письмові роботи з засвоєння тем курсу;
5) Виконання завдань СРС.

Кожний вид поточної навчальної роботи студента оцінюються за 5-бальною шкалою.

Загальна семестрова оцінка за 100-бальною шкалою переводиться у національну шкалу відповідно до таблиці:

Сума балів за всі види навчальної діяльності	Шкала ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проєкту (роботи)	для заліку
90-100	A	відмінно	зараховано
82-89	B	добре	
74-81	C		
64-73	D	задовільно	
60-63	E		
35-59	FX	незадовільно з можливістю повторного складання	не зараховано з можливістю повторного складання
1-34	F	незадовільно з обов'язковим повторним вивченням дисципліни	не зараховано з обов'язковим повторним вивченням дисципліни

Політика курсу:

Політика дотримання академічної доброчесності

Викладання навчальної дисципліни ґрунтується на засадах академічної доброчесності. Порушеннями академічної доброчесності вважаються: академічний плагіат, фабрикація, фальсифікація, списування.

За порушення академічної доброчесності студенти можуть бути притягнені до такої академічної відповідальності: повторне проходження оцінювання (контрольна робота, іспит тощо); повторне проходження відповідного освітнього компонента освітньої програми.

Комунікаційна політика

Студенти повинні мати активовану університетську пошту.

Обов'язком студента є перегляд новин на Телеграм-каналі.

Протягом тижнів самостійної роботи обов'язком студента є робота з дистанційним курсом «Безпека даних та криптографічні методи захисту».

Політика щодо пропусків занять

Студенти мають відвідувати лекційні й практичні (семінарські) заняття. Відсутність студента на занятті може бути виправдана поважною причиною. Поважними причинами відсутності вважаються: хвороба, участь у Всеукраїнській студентській олімпіаді, Всеукраїнському конкурсі студентських наукових робіт чи будь-якому іншому заході, який можна віднести до заходів, що сприяють розвитку студентів і поліпшенню іміджу університету (факультету).

Політика щодо виконання навчальних завдань пізніше встановленого терміну

Студенти мають виконувати всі навчальні завдання у встановлені терміни. Студент, який не виконав ту чи іншу кількість навчальних завдань вчасно й хоче надолужити прогаяне, може звернутися по допомогу до викладача.

Політика щодо оскарження оцінювання

Якщо студент не згоден з оцінюванням його знань він може оскаржити виставлену викладачем оцінку у встановленому порядку.

Бонуси

Студенти, які регулярно відвідували лекції (мають не більше двох пропусків без поважних причин) та мають написаний конспект лекцій отримують додатково 2 бали до результатів оцінювання до підсумкової оцінки.