Міністерство освіти і науки України
Київський національний торговельно-економічний університет
Харківський торговельно-економічний інститут КНТЕУ

Факультет економіки та управління
Кафедра інформаційних технологій

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Захист інформаційних систем і мереж
повна назва навчальної дисципліни

для підготовки студентів освітнього ступеня: бакалавр (молодший бакалавр, бакалавр чи магістр) року набору 2018

галузі знань: 12 Інформаційні технології
шифр і назва галузі знань

спеціальності: 126 Інформаційні системи та технології
шифр і найменування спеціальності

освітня програма / спеціалізація: Інформаційні технології у бізнесі
назва освітньої програми / спеціалізації

статус дисципліни: обов'язкова
обов'язкова чи вибіркова

Харків, 2019 рік

Розробник

Запорожцев Сергій Юрійович,
доцент кафедри інформаційних технологій,
кандидат технічних наук, доцент

прізвище, ім'я, по батькові повністю, посада повністю, науковий ступінь, вчене звання повністю

02.09.2019 р. _____ С. Ю. Запорожцев

підпис ініціали та прізвище

Гарант освітньої програми

Олійник Наталія Юріївна, заступник
директора з науково-педагогічної роботи,
доцент кафедри інформаційних технологій,
кандидат педагогічних наук, доцент

прізвище, ім'я, по батькові повністю, посада повністю, науковий ступінь, вчене звання повністю

02.09.2019 р. _____ Н. Ю. Олійник

підпис ініціали та прізвище

Програму обговорено та схвалено на засіданні кафедри
інформаційних технологій

назва кафедри

протокол від 02.09.2019 р. № 01.

Зав. кафедри _____ М. С. Синєкоп

підпис ініціали та прізвище

Програму розглянуто та затверджено на засіданні методичної комісії інституту, протокол від 02.09.2019 р. № 01.

Голова методичної комісії _____ Л. І. Літвін

підпис ініціали та прізвище

1. ОПИС НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Робоча програма навчальної дисципліни «Захист інформаційних систем і мереж» розроблена відповідно до освітньої програми підготовки студентів спеціальності 126 Інформаційні системи та технології галузі знань 12 Інформаційні технології.

Метою викладання навчальної дисципліни «Захист інформаційних систем і мереж» є навчання студентів принципам побудови комплексних систем захисту інформації, розробки, дослідженню та застосуванню механізмів захисту інформації, що засновані на використанні алгоритмів традиційної (симетричної) криптографії та криптографії з відкритим ключем для забезпечення автентичності, цілісності та конфіденційності інформаційних систем та технологій.

Предметом вивчення навчальної дисципліни є методи та алгоритми безпеки конфіденційних даних та принципи їх захисту.

Міждисциплінарні зв'язки. Дисципліна «Захист інформаційних систем і мереж» основана на попередньому вивченні дисциплін, таких як «Вища та прикладна математика», «Архітектура та проектування програмного забезпечення». Знання, що студенти отримають при вивченні дисципліни «Захист інформаційних систем і мереж», є основою для подальшого засвоєння професійних навчальних дисциплін, таких як «Технологія розподілених систем та паралельних обчислень», а також при проходженні практик та написанні випускного кваліфікаційного проекту.

Мова викладання – українська.

2. ЗАПЛАНОВАНІ РЕЗУЛЬТАТИ НАВЧАННЯ

Навчальна дисципліна забезпечує набуття студентами:

загальних компетентностей:

ЗК 4. Здатність спілкуватися іноземною мовою;

ЗК 5. Здатність вчитися і оволодівати сучасними знаннями;

ЗК 6. Здатність до пошуку, оброблення та узагальнення інформації з різних джерел;

ЗК 8. Здатність оцінювати та забезпечувати якість виконуваних робіт;

фахових компетентностей:

ФК 1. Здатність аналізувати об’єкт проектування або функціонування та його предметну область;

ФК 5. Здатність оцінювати та враховувати економічні, соціальні, технологічні та екологічні фактори на всіх етапах життєвого циклу інфокомунікаційних систем;

ФК 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов’язків;

ФК 10. Здатність вибору, проектування, розгортання, інтегрування, управління, адміністрування та супроводжування інформаційних систем, технологій та інфокомунікацій, сервісів та інфраструктури організації;

ФК 12. Здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями (у тому числі такими, що базуються на використанні Інтернет);

програмних результатів навчання:

ПРН 4. Проводити системний аналіз об’єктів проектування та обґрунтовувати вибір структури, алгоритмів та способів передачі інформації в інформаційних системах та технологіях;

ПРН 5. Аргументувати вибір програмних та технічних засобів для створення інформаційних систем та технологій на основі аналізу їх властивостей, призначення і технічних характеристик з урахуванням вимог до системи і експлуатаційних умов; мати навички налагодження та тестування програмних і технічних засобів інформаційних систем та технологій;

ПРН 6. Демонструвати знання сучасного рівня технологій інформаційних систем, практичні навички програмування та використання прикладних і спеціалізованих комп’ютерних систем та середовищ з метою їх запровадження у професійній діяльності;

ПРН 7. Обґрунтовувати вибір технічної структури та розробляти відповідне програмне забезпечення, що входить до складу інформаційних систем та технологій;

ПРН 9. Здійснювати системний аналіз архітектури підприємства та його ІТ-інфраструктури, проводити розроблення та вдосконалення її елементної бази і структури.

3. ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Тема 1. Визначення безпеки.

Роль захисту інформації в ІС, умови функціонування підсистеми безпеки в комп'ютерних мережах та системах. Вимоги щодо безпеки системи, ризики безпеки. Послуги безпеки: конфіденційність, цілісність, автентичність, причетність, спостереженість. Розподіл послуг безпеки за рівнями моделі ISO/OSI. Критерії захищеності комп'ютерних систем. Розробка профілю захисту. Механізми реалізації послуг безпеки. Побудування та впровадження систем захисту інформації.

Тема 2. Розмежування прав доступу

Засоби забезпечення захисту інформації в СУБД. Засоби ідентифікації й автентифікації об'єктів баз даних, управління доступом. Засоби контролю цілісності інформації, організація аудиту. Скасування прав доступу. Видача прав доступу до об'єктів баз даних.

Тема 3. Методи забезпечення безпеки

Компоненти криптосистеми та їх функціональні характеристики. Побудова класифікацій криптографічних засобів. Захист інформації за допомогою міжмережних екранів.

Тема 4. Захист, доступ та автентифікація

Загальні механізми забезпечення безпеки. Взаємозв'язок послуг та механізмів безпеки і взаємозв'язок послуг і рівнів моделі взаємодії відкритих систем. Автентифікація даних, механізми забезпечення та методи автентифікації.

Тема 5. Моделі захисту

Побудова моделі порушника безпеки. Організація захисту, захист окремих комірок пам'яті. Основні засоби захисту пам'яті при керуванні та з привілеями. Моделі безпеки, які застосовуються при побудові захисту в СУБД. Захист БД в системах з видаленим доступом. Інтерфейси CGI, API й FastCGI.

Тема 6. Шифрування даних

Математичні основи сучасної теорії захисту інформації. Методи булевої алгебри, елементи кореляційного та спектрального аналізу. Прості шифри. Симетричне шифрування даних. Криптографічні примітиви й типи структур симетричного шифрування. Блочні симетричні шифри. Архітектура блочних симетричних шифрів. Типові режими роботи криптосистеми: "Електронна кодова книга", "Зчеплення блоків шифру", "Зворотний зв'язок з шифру", "Зворотний зв'язок з виходу". Режим простої заміни. Режим гама шифрування. Режим шифрування зі зворотним зв'язком за виходом. Режим вироблення імітовставки. Потокові шифри. Регістри зсуву зі зворотнім зв'язком. Асиметричне шифрування даних. Математичні положення теорії скінченних

полів та систем класів лишків. Математичні положення теорії чисел. Асиметричні алгоритми шифрування даних RSA та Ель Гамаля.

Тема 7. Управління відновленням

Захист і відновлення даних. Формування служб резервного копіювання й відновлення даних для критично-важливих серверів. Кластерізація серверів. Етапи управління формуванням плану резервного відновлення. Типи та топології резервного копіювання.

Тема 8. Криптографія

Основні криптографічні примітиви. Математичні моделі нелінійних вузлів замін у термінах булевої алгебри. Основні напрями розвитку асиметричних криптоалгоритмів. Криптографія на еліптичних кривих. Теоретико-чисельні задачі, складність арифметики точок ЕК в різних формах і представленнях. Цифрова стеганографія з відкритим ключем.

Тема 9. Керування ключами

Компоненти та сервіси інфраструктури відкритих ключів. Архітектура і топологія PKI. Стандарти в галузі PKI. Сертифікати відкритих ключів X.509, управління сертифікатами. Системи PKI. Документ політика захисту інформації, його сутність та структура, управління ключами. Профілі безпеки автоматизованих систем. Основні вимоги до політиці PKI.

Тема 10. Криптоаналіз

Основи криптографії. Формальне математичне визначення криптосистеми. Критерії та показники ефективності. Аналіз основних видів атак, рисків та вразливих елементів інформаційних систем. Класифікація криптоаналітичних атак. Диференціальний криптоаналіз, диференціальний криптоаналіз на основі відмов пристрою. Лінійний криптоаналіз. Силова атака на основі розподілених розв’язань.

Тема 11. Алгоритми з секретним ключем

Захист інформації на мережному рівні. Протоколи захисту та цілісності IPSec, SSL, TLS, їх сутність.

Тема 12. Алгоритми з відкритим ключем

Системи захисту PGP та CS MIME. Криптографічні функції. Сумісність на рівні електронної пошти. Захищена електронна пошта.

Тема 13. Протоколи автентифікації

Класифікація механізмів автентифікації. MDC-коди, основні алгоритми. MAC-коди, основні способи формування. Методи побудови універсальних геш-функцій.

Тема 14. Цифрові підписи

Класифікація стандартів електронних цифрових підписів. Моделі цифрових підписів. Основні стандарти цифрового підпису.

4. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

4.1. Структура навчальної дисципліни за формами навчання

Теми дисципліни	Обсяг у годинах																							
	денна форма												заочна форма											
	повна						скорочена						повна						скорочена					
	усього	у тому числі					усього	у тому числі					усього	у тому числі					усього	у тому числі				
		Л	СЗ	ПЗ	ЛЗ	СРС		Л	СЗ	ПЗ	ЛЗ	СРС		Л	СЗ	ПЗ	ЛЗ	СРС		Л	СЗ	ПЗ	ЛЗ	СРС
Тема 1. Визначення безпеки	12	4		2		6	12	2		2		8							12	1				11
Тема 2. Розмежування прав доступу	12	4		2		6	12	2		2		8							12					12
Тема 3. Методи забезпечення безпеки	12	4		2		6	12	2		2		8							12	1		2		9
Тема 4. Захист, доступ та автентифікація	12	4		2		6	12	2		2		8							12	2		2		8
Тема 5. Моделі захисту	12	4		2		6	12	2		2		8							12					12
Тема 6. Шифрування даних	12	4		2		6	12	2		2		8							12					12
Тема 7. Управління відновленням	12	4		2		6	12	2		2		8							12					12
Тема 8. Криптографія	12	4		2		6	12	2		2		8							12					12
Тема 9. Керування ключами	14	4		2		8	14	2		2		10							14	2		2		10
Тема 10. Криптоаналіз	14	4		2		8	14	2		2		10							14					14
Тема 11. Алгоритми з секретним ключем	14	4		2		8	14	2		2		10							14					14
Тема 12. Алгоритми з відкритим ключем	14	4		2		8	14	2		2		10							14					14
Тема 13. Протоколи автентифікації	14	4		2		8	14	2		2		10							14					14
Тема 14. Цифрові підписи	14	4		2		8	14	2		2		10							14					14
Усього годин / кредитів ECTS	**180/6**	**56**		**28**		**96**	**180/6**	**28**		**28**		**124**							**180/6**	**6**		**6**		**168**

4.2. Обсяги та структура навчальної дисципліни за навчальними роками

Форма навчання	Вид навчальних занять	Навчальні роки					
		2019/2020		2020/2021		2021/2022	
		осінь	весна	осінь	весна	осінь	весна
Денна повна	Лекційні заняття					56	
	Семінарські заняття						
	Практичні заняття					28	
	Лабораторні заняття						
	Курсова робота						
	Самостійна робота студентів					96	
	Усього годин					**180**	
Денна скорочена	Лекційні заняття	28					
	Семінарські заняття						
	Практичні заняття	28					
	Лабораторні заняття						
	Курсова робота (проект)						
	Самостійна робота студентів	124					
	Усього годин	**180**					
Заочна повна	Лекційні заняття						
	Семінарські заняття						
	Практичні заняття						
	Лабораторні заняття						
	Курсова робота (проект)						
	Самостійна робота студентів						
	Усього годин						
Заочна скорочена	Лекційні заняття		4	2			
	Семінарські заняття						
	Практичні заняття		2	4			
	Лабораторні заняття						
	Курсова робота (проект)						
	Самостійна робота студентів		84	84			
	Усього годин		**90**	**90**			

5. ТЕМИ ЛЕКЦІЙНИХ ТА ПРАКТИЧНИХ ЗАНЯТЬ

5.1. Теми лекційних занять

Тема дисципліни	Тема лекції	Обсяг у годинах			
		денна форма		заочна форма	
		повна	скорочена	повна	скорочена
Тема 1. Визначення безпеки	Визначення дисципліни. Роль захисту інформації в ІС	4	2		1
Тема 2. Розмежування прав доступу	Засоби забезпечення захисту інформації в СУБД.	4	2		
Тема 3. Методи забезпечення безпеки	Компоненти криптосистеми та їх функціональні характеристики.	4	2		1
Тема 4. Захист, доступ та автентифікація	Автентифікація даних, механізми забезпечення та методи автентифікації.	4	2		2
Тема 5. Моделі захисту	Моделі безпеки, які застосовуються при побудові захисту в СУБД.	4	2		
Тема 6. Шифрування даних	Математичні основи теорії захисту інформації.	4	2		
Тема 7. Управління відновленням	Захист і відновлення даних.	4	2		
Тема 8. Криптографія	Основні криптографічні моделі	4	2		
Тема 9. Керування ключами	Компоненти та сервіси інфраструктури відкритих ключів.	4	2		2
Тема 10. Криптоаналіз	Математичне визначення криптосистеми.	4	2		
Тема 11. Алгоритми з секретним ключем	Захист інформації на мережному рівні.	4	2		
Тема 12. Алгоритми з відкритим ключем	Криптографічні функції.	4	2		
Тема 13. Протоколи автентифікації	Класифікація механізмів автентифікації.	4	2		
Тема 14. Цифрові підписи	Моделі цифрових підписів.	4	2		
Усього		**56**	**28**		**6**

Лекційний матеріал наведено у [1]- [3].

5.2. Теми практичних занять

Тема дисципліни	Тема практичного заняття	Обсяг у годинах			
		денна форма		заочна форма	
		повна	скорочена	повна	скорочена
Тема 1. Визначення безпеки	Класичні симетричні системи.	2	2		
Тема 2. Розмежування прав доступу	Дослідження крипостійкості простих симетричних шифрів	2	2		
Тема 3. Методи забезпечення безпеки	Дослідження сучасних блочних симетричних шифрів та режимів шифрування	2	2		2
Тема 4. Захист, доступ та автентифікація	Система блокового шифрування S-DES.	2	2		2
Тема 5. Моделі захисту	Дослідження розсіювальних властивостей S-DES	2	2		
Тема 6. Шифрування даних	Дослідження сучасних асиметричних криптосистем шифрування.	2	2		
Тема 7. Управління відновленням	Дослідження інтегрованих механізмів забезпечення вірогідності даних	2	2		
Тема 8. Криптографія	Стеганографічні методи захисту інформації	2	2		
Тема 9. Керування ключами	Розгортання та управління інфраструктурою відкритих ключів	2	2		2
Тема 10. Криптоаналіз	Статистичні дослідження генераторів випадкових та псевдовипадкових послідовностей	2	2		
Тема 11. Алгоритми з секретним ключем	Безпечність персональних конфіденціальних даних на базі секретного диску	2	2		
Тема 12. Алгоритми з відкритим ключем	Розгортання та управління інфраструктурою відкритих ключів	2	2		
Тема 13. Протоколи автентифікації	Безпечність персональних даних на базі захищеної електронної пошти PGP	2	2		
Тема 14. Цифрові підписи	Дослідження електронного цифрового підпису.	2	2		
Усього		**28**	**28**		**6**

6. ЗАВДАННЯ ДЛЯ САМОСТІЙНОЇ РОБОТИ

Основні види самостійної роботи, які запропоновані студентам:

- вивчення лекційного матеріалу.
- опрацювання першоджерел (навчальних видань, періодичної та наукової літератури, довідників, відео-матеріалів тощо) та Інтернет-ресурсів за темами навчальної дисципліни:

Тема 1. Визначення безпеки.
1. Розподіл послуг безпеки за рівнями моделі ISO/OSI.
2. Критерії захищеності комп'ютерних систем.

Тема 2. Розмежування прав доступу
1. Засоби контролю цілісності інформації, організація аудиту.
2. Скасування прав доступу.

Тема 3. Методи забезпечення безпеки
1. Захист інформації за допомогою міжмережних екранів.

Тема 4. Захист, доступ та автентифікація
1. Взаємозв'язок послуг та механізмів безпеки.
2. Взаємозв'язок послуг і рівнів моделі взаємодії відкритих систем.

Тема 5. Моделі захисту
1. Захист БД в системах з видаленим доступом.
2. Інтерфейси CGI, API й FastCGI.

Тема 6. Шифрування даних
1. Потокові шифри.
2. Асиметричне шифрування даних.

Тема 7. Управління відновленням
1. Кластерізація серверів.
2. Типи та топології резервного копіювання.

Тема 8. Криптографія
1. Цифрова стеганографія з відкритим ключем.

Тема 9. Керування ключами
1. Управління сертифікатами.
2. Профілі безпеки автоматизованих систем.

Тема 10. Криптоаналіз
1. Диференціальний криптоаналіз.
2. Лінійний криптоаналіз.

Тема 11. Алгоритми з секретним ключем
1. Протоколи захисту та цілісності IPSec, SSL, TLS.

Тема 12. Алгоритми з відкритим ключем
1. Захищена електронна пошта.

Тема 13. Протоколи автентифікації
1. Методи побудови універсальних геш-функцій.

Тема 14. Цифрові підписи
1. Основні стандарти цифрового підпису.

Організація самостійної роботи студентів регламентується наступними нормативними документами:

- Положенням про самостійну роботу студентів Харківського торговельно-економічного-інституту КНТЕУ;
- Положенням про організацію освітнього процесу у Харківському торговельно-економічному інституті КНТЕУ.

7. ІНДИВІДУАЛЬНІ ЗАВДАННЯ, ПЕРЕДБАЧЕНІ НАВЧАЛЬНИМ ПЛАНОМ

Не передбачено навчальним планом.

8. СХЕМА НАРАХУВАННЯ БАЛІВ

Схема нарахування балів для студентів денної форми навчання

Навчальні роки	Поточний контроль (максимум 60 балів, мінімум 36)															Підсумковий контроль	Сума
	усього	у тому числі за темами															
		Тема 1	Тема 2	Тема 3	Тема 4	Тема 5	Тема 6	Тема 7	Тема 8	Тема 9	Тема 10	Тема 11	Тема 12	Тема 13	Тема 14		
2019/2020	60	5	5	5	5	4	4	4	4	4	4	4	4	4	4	40	100
2021/2022	60	5	5	5	5	4	4	4	4	4	4	4	4	4	4	40	100

Схема нарахування балів для студентів заочної форми навчання

Навчальні роки	Поточний контроль (максимум 60 балів, мінімум 36)															Підсумковий контроль	Сума
	усього	у тому числі за темами															
		Тема 1	Тема 2	Тема 3	Тема 4	Тема 5	Тема 6	Тема 7	Тема 8	Тема 9	Тема 10	Тема 11	Тема 12	Тема 13	Тема 14		
2019/2020	60	5	5	5	5	4	4	4	4	4	4	4	4	4	4	40	100

Види активності студента з навчальної дисципліни протягом семестру:

1. Самостійне опрацювання тестів відповідно до тем курсу
2. Відвідування аудиторних занять

9. МЕТОДИ КОНТРОЛЮ

Для визначення рівня засвоювання студентами навчального матеріалу використовуються такі форми та методи оцінювання:

Поточний контроль:

- для студентів денної форми навчання: оцінювання роботи на практичних заняттях, поточне тестування в системі дистанційного навчання

ХТЕІ КНТЕУ, оцінювання відвідування аудиторних занять, виконання аудиторної контрольної роботи;

- для студентів заочної форми навчання: оцінювання виконання практичних завдань.

Умовою допуску до підсумкового контролю є виконання програми дисципліни (відпрацювання всіх практичних занять) і отримання оцінки за виконання завдань поточного контролю не менше 36 балів.

Підсумковий контроль:

- для студентів денної форми навчання: письмовий екзамен;
- для студентів заочної форми навчання: письмовий екзамен.

Організація та проведення контрольних заходів регламентується наступними нормативними документами:

- Положенням про оцінювання результатів навчання студентів;
- Положенням про організацію освітнього процесу у Харківському торговельно-економічному інституті КНТЕУ.

10. РЕКОМЕНДОВАНІ ДЖЕРЕЛА ІНФОРМАЦІЇ

10.1. Основні джерела інформації

1. Захист інформації в автоматизованих системах управління: навчальний посібник/ І. А. Пількевич, Н. М. Лобанчикова, К. В. Молодецька. – Житомир: ЖДУ ім. І. Франка, 2015. – 226 с.
2. Бем М. В. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник / М. В. Бем, І. М. Городиський, Г. Саттон, О. М. Родіоненко – Київ: К.І.С., 2015. – 220 с.
3. Грищук Р. В. Основи кібернетичної безпеки : монографія / Р. В. Грищук, Ю. Г. Даник ; під заг. ред. проф. Ю. Г. Даника. – Житомир : ЖНАЕУ, 2016. – 636 с.

10.2. Додаткові джерела інформації

4. Юдін О. К. Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія / О. К. Юдін, С. С. Бучик – Київ : НАУ, 2015. – 214 с.
5. Кормич Б. Інформаційна безпека: організаційно-правові основи: навчальний посібник / Б.Кормич. – Київ : Кондор, 2005. – 382 с.
6. Низенко Е. І. Забезпечення інформаційної безпеки підприємництва: навчальний посібник / Е.І. Низенко, В.П. Каленяк – Київ : МАУП, 2006. – 134 с.
7. Гуз А. М. Історія захисту інформації в Україні та провідних країнах світу: навчальний посібник / А. М. Гуз. – Київ : КНТ, 2011. – 260 с.
8. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Харків : ХНЕУ, 2010. – 316 с.