

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ СЕМЕНА КУЗНЕЦЯ



Проректор з навчально-методичної роботи

Каріна НЕМАШКАЛО

ЗАХИСТ ІНФОРМАЦІЇ
робоча програма навчальної дисципліни

Галузь знань	<i>12 Інформаційні технології</i>
Спеціальність	<i>122 Комп'ютерні науки</i>
Освітній рівень	<i>перший (бакалаврський)</i>
Освітня програма	<i>Комп'ютерні науки</i>
Статус дисципліни	<i>обов'язкова</i>
Мова викладання, навчання та оцінювання	<i>українська</i>

Завідувач кафедри
кібербезпеки
та інформаційних технологій

Ольга СТАРКОВА

Харків
2022

ЗАТВЕРДЖЕНО

на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 1 від 30.08.2022 р.

Розробник:

Семенов С.Г., д.т.н., проф. кафедри КІТ.

**Лист оновлення та перезатвердження
робочої програми навчальної дисципліни**

Навчальний рік	Дата засідання кафедри – розробника РПНД	Номер протоколу	Підпис завідувача кафедри

Анотація навчальної дисципліни

Захист інформації перетворюється сьогодні на одну з найактуальніших задач внаслідок надзвичайно широкого розповсюдження як власне різноманітних систем обробки інформації, так і розширення локальних та глобальних комп'ютерних мереж, якими передаються величезні об'єми інформації державного, військового, комерційного, приватного характеру, власники якої часто були б категорично проти ознайомлення з нею сторонніх осіб. Проблема набуває особливої гостроти після прийняття урядом України закону про захист персональних даних, який зобов'язує зберігати та передавати персональні дані працівників лише у захищеному вигляді в інформаційних системах (ІС).

Не менш важливим завданням вважається широке впровадження інформаційних технологій у різні сфери людської діяльності в Україні: стрімке зростання обігу пластикових карток, майбутнє введення електронних паспортів та медичних карт, студентських квитків та залікових книжок; зрештою все більше державних установ та приватних підприємств переходять на електронний документообіг, який до того ж, вимагає юридичної чинності підпису фізичної або юридичної особи. Розповсюдження таких технологій також, безперечно, вимагає добре поставленого захисту інформації.

Метою викладання дисципліни є навчання студентів принципам побудови комплексних систем захисту інформації, дослідженню та використанню сучасних процедур забезпечення основних услуг безпеки інформації в банківських системах, що засновані на використанні алгоритмів симетричної та несиметричної криптографії в комунікаційних системах, протоколів інфраструктури відкритих ключів (ІВК).

Результатами вивчення даної дисципліни є придбання навичок з використання методів шифрування інформації для подальшої передачі її телекомунікаційними каналами зв'язку.

Характеристика навчальної дисципліни

Курс	4
Семестр	7
Кількість кредитів ECTS	5
Форма підсумкового контролю	залік

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Комп'ютерні системи	Дипломне проектування
Дискретна математика	Технології тестування ПЗ
Комп'ютерні мережі	Кросплатформене програмування

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
ЗК1. Здатність до абстрактного мислення, аналізу та синтезу. ЗК2. Здатність застосовувати знання у практичних ситуаціях. ЗК4. Здатність спілкуватися державною мовою як усно, так і письмово ЗК5. Здатність спілкуватися іноземною мовою. ЗК6. Здатність вчитися й оволодівати сучасними знаннями. ЗК8. Здатність генерувати нові ідеї (креативність). ЗК9. Здатність працювати в команді ЗК13. Здатність діяти на основі етичних міркувань. СК15. Здатність до аналізу та функціонального моделювання бізнеспроцесів, побудови та практичного застосування функціональних моделей організаційно-економічних і виробничо-технічних систем, методів оцінювання ризиків їх проектування.	ПР16. Розуміти концепцію інформаційної безпеки, принципи безпечного проектування програмного забезпечення, забезпечувати безпеку комп'ютерних мереж в умовах неповноти та невизначеності вихідних даних.
СК14. Здатність застосовувати методи та засоби забезпечення інформаційної безпеки, розробляти й експлуатувати спеціальне програмне забезпечення захисту інформаційних ресурсів об'єктів критичної інформаційної інфраструктури	ПР17. Виконувати паралельні та розподілені обчислення з використанням програмного забезпечення кластерних обчислювальних систем, застосовувати чисельні методи та алгоритми для їх застосування в паралельних архітектурах високопродуктивних систем, мови паралельного програмування при розробці та експлуатації паралельного та розподіленого програмного забезпечення в цих системах.

Програма навчальної дисципліни

Змістовий модуль 1. Безпека і захист даних

- Тема 1. Основні поняття та визначення кібербезпеки
- Тема 2. Основи криптографії. Прості алгоритми шифрування
- Тема 3. Протоколи автентифікації. Цифровий підпис
- Тема 4. Система PGP
- Тема 5. Алгоритми забезпечення цілісності даних

Змістовий модуль 2. Мережева безпека

- Тема 6. Забезпечення безпеки даних на мережевому рівні

Перелік лабораторних занять, а також питань та завдань до самостійної роботи наведено у таблиці "Рейтинг-план навчальної дисципліни".

Методи навчання та викладання

В ході викладання дисципліни викладачем застосовуються пояснювально-ілюстративний (інформаційно-рецептивний) та репродуктивний методи навчання. В якості методів викладання, які направлені на активізацію та стимулювання навчально-пізнавальної діяльності здобувачів, застосовуються проблемні лекції (теми 1-6), презентації (теми 1-6), бесіди (теми 1-2), індивідуальні та групові проекти (теми 3-6), майстер-класи (теми 3-6).

Порядок оцінювання результатів навчання

Система оцінювання сформованих компетентностей у студентів враховує види занять, які згідно з програмою навчальної дисципліни передбачають лекційні та лабораторні заняття, а також виконання самостійної роботи. Оцінювання сформованих компетентностей у студентів здійснюється за накопичувальною 100-бальною системою. Контрольні заходи включають:

1) поточний контроль, що здійснюється протягом семестру під час проведення лекційних та лабораторних занять і оцінюється сумою набраних балів (максимальна сума – 100 балів; мінімальна сума – 60 балів);

2) підсумковий/семестровий контроль, що проводиться у формі заліку.

Порядок здійснення поточного оцінювання знань студентів.

Оцінювання знань студента під час лекційних і лабораторних занять проводиться за такими критеріями:

– знання принципів класичних симетричних систем;

– досліджувати криптостійкість простих симетричних шифрів;

– досліджувати електронний цифровий підпис

– оцінювати безпечність персональних конфіденційних даних на базі секретного диску та захищеної електронної пошти PGP;

– проводиться оцінка засобів забезпечення безпеки даних на мережевому рівні

Підсумковий контроль знань та компетентностей студентів з навчальної дисципліни здійснюється на підставі заліку, завданням якого є перевірка розуміння студентом програмного матеріалу в цілому, логіки та взаємозв'язків між окремими розділами, здатності творчого використання накопичених знань, вміння формулювати своє ставлення до певної проблеми навчальної дисципліни тощо.

Лабораторні заняття: максимальна кількість балів становить 100, а мінімальна – 60.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до екзамену з дисципліни, в технологічній карті бали на цей вид робіт не виділені.

Підсумковий контроль: проводиться з урахуванням отриманих балів у продовж семестру. Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час поточного контролю за накопичувальною системою. Сумарний результат у балах за семестр складає: "60 і більше балів – зараховано", "59 і менше балів – не зараховано" та заноситься у залікову "Відомість обліку успішності" навчальної дисципліни.

Форми оцінювання та розподіл балів наведено у таблиці "Рейтинг-план навчальної дисципліни".

Рейтинг-план навчальної дисципліни

Т е м а	Форми та види навчання	Форми оцінювання	Мак бал
Т е м а 1.	<i>Аудиторна робота</i>		
	Лекція	Лекція №1. Основні поняття та визначення кібербезпеки	
	Лекція	Лекція №2. Основи криптографії. Прості алгоритми шифрування	

	Лабораторне заняття	Лабораторна робота 1. Прості алгоритми шифрування	Захист лабораторної роботи	10
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т е м а 2.	<i>Аудиторна робота</i>			
	Лекція	Лекція №3. Протоколи автентифікації. Цифровий підпис		
	Лабораторне заняття	Лабораторна робота 2. Протоколи автентифікації. Цифровий підпис	Захист лабораторної роботи	10
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т е м а 3	<i>Аудиторна робота</i>			
	Лекція	Лекція №4. Система PGP		
	Лабораторне заняття	Лабораторна робота 3. Моделювання системи PGP	Захист лабораторної роботи	10
	Лекція	Лекція №5. Дослідження системи PGP		
	Лабораторне заняття	Лабораторна робота 4. Дослідження системи PGP	Захист лабораторної роботи	10

	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
	<i>Аудиторна робота</i>			
Т е м а 4.	Лекція	Лекція №6. Алгоритми забезпечення цілісності даних		
	Лабораторне заняття	Лабораторна робота 5. Алгоритми забезпечення цілісності даних	Захист лабораторної роботи	10
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
	<i>Аудиторна робота</i>			
Т е м а 5.	Лекція	Лекція №7. Забезпечення безпеки даних на мережевому рівні		
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
	<i>Аудиторна робота</i>			
Т е м а 6.	Лекція	Лекція №8. Стек протоколів IPSec		
	Лабораторне заняття	Лабораторна робота 6. Стек протоколів IPSec	Захист лабораторної роботи	10

			Контрольна робота	20
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т е м а 7.	<i>Аудиторна робота</i>			
	Лекція	Лекція №9. Сучасні файровони		
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т е м а 8.	<i>Аудиторна робота</i>			
	Лекція	Лекція №10. Антивірусні системи		
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т е м а 9.	<i>Аудиторна робота</i>			
	Лекція	Лекція №11. СПАМ. Методи боротьби зі СПАМом		
	<i>Самостійна робота</i>			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Т е м а 1 0.	<i>Аудиторна робота</i>			
	Лекція	Лекція №12. Методи стеганографічного захисту		
			Контрольна робота	20
	<i>Самостійна робота</i>			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		

Рекомендована література

Основна

1. Лісовська, Ю. П. Інформаційна безпека України : навчальний посібник для студентів вищих навчальних закладів / Ю. П. Лісовська. - Київ : Кондор, 2020. - 170 с.
2. Richard E. Smith Elementary Information Security 3rd Edition / Jones & Bartlett Learning; 3rd edition (October 28, 2019) – 708 p.

Додаткова

3. Jason Andress Foundations of Information Security: A Straightforward Introduction / No Starch Press (October 7, 2019) – 248 p.
4. Якименко І.З. // Опорний конспект лекцій з дисципліни „Безпека програм та даних», для студентів спеціальності „Кібербезпека». – Тернопіль, 2019. – 50 с.
5. Основи інформаційної безпеки : навч. посібник / В. Б. Вишня, О. С. Гавриш, Е. В. Рижков. Дніпро : Дніпроп. держ. ун-т внутріш. справ, 2020. 128 с.

Інформаційні ресурси.

7. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Захист інформації" <https://pns.hneu.edu.ua/course/view.php?id=8940>