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

"ЗАТВЕРДЖУЮ"
Проректор з навчально-методичної роботи
_____
Каріна ПЕМАШКАЛО

Безпека програм та даних
робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***126 Інформаційні системи та технології***
Освітній рівень	***перший (бакалаврський)***
Освітня програма	***Інформаційні системи та технології***

Статус дисципліни	***обов'язкова***
Мова викладання, навчання та оцінювання	***українська***

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	**екзамен**

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
КС 6 Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання	ПР 1. Знати лінійну та векторну алгебру, диференціальне та інтегральне числення, теорію функцій багатьох змінних, теорію рядів, диференціальні рівняння для функції однієї та багатьох змінних, операційне числення, теорію ймовірностей та математичну статистику в обсязі, необхідному для розробки та використання інформаційних систем, технологій та інфокомунікацій, сервісів та

функціональних завдань та обов'язків.	інфраструктури організації.
КС 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.	ПР 2. Застосовувати знання фундаментальних і природничих наук, системного аналізу та технологій моделювання, стандартних алгоритмів та дискретного аналізу при розв'язанні задач проектування і використання інформаційних систем та технологій.
КС 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.	ПР 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 професійної діяльності.

Програма навчальної дисципліни

Зміст навчальної дисципліни

Змістовий модуль 1. Основні послуги, механізми та засоби захисту даних
Тема 1. Основні поняття та визначення кібербезпеки
Тема 2. Основи криптографії. Прості алгоритми шифрування
Тема 3. Криптоалгоритми шифрування з ключем
Тема 4. Система PGP. Схема функціонування
Тема 5. Система PGP. Принципи застосування та алгоритми функціонування
Тема 6. Цілісність даних. Алгоритм Хемінга
Тема 7. Управління доступом.
Тема 8. Протоколи аутентифікації
Тема 9. Цифрові підписи
Тема 10. Антивірусний захист СПАМ. Методи боротьби зі СПАМом
Змістовий модуль 2. Мережева безпека
Тема 11. Трансляція мережних адрес. Комплексне використання трансляторів мережних адрес
Тема 12. IPSec.
Тема 13. Застарілі та сучасні технології для веб-додатків ключем
Тема 14. Збір інформації про веб-додатки
Тема 15. Мережі стандарту 802.11. Забезпечення послуг безпеки.

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 (Тема 15. Мережі стандарту 802.11. Забезпечення послуг безпеки.), презентації, бесіди, індивідуальні та групові проєкти (Тема 4. Система PGP. Схема функціонування. Тема 5. Система PGP. Принципи застосування та

алгоритми функціонування), майстер-класи (Тема 13. Застарілі та сучасні технології для веб-додатків ключем).

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 – 60 балів; мінімальна сума, що дозволяє студенту складати іспит, – 35 балів);

2) підсумковий/семестровий контроль, що проводиться у формі семестрового екзамену, відповідно до графіку навчального процесу.

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 крипостійкість 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 проведення семестрового екзамену, 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 60, а мінімальна – 40.

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 цій вид робіт не виділені.

Підсумковий контроль: проводиться з урахуванням іспиту.

Екзаменаційний білет охоплює програму дисципліни і передбачає визначення рівня знань та ступеня опанування студентами компетентностей.

Кожен екзаменаційний білет складається із 3 практичних ситуацій (одне стереотипне, одне діагностичне та одне евристичне завдання), які передбачають вирішення типових професійних завдань фахівця на робочому місці та дозволяють діагностувати рівень теоретичної підготовки студента і рівень його компетентності з навчальної дисципліни. Оцінювання кожного завдання екзаменаційного білету наступне: перше завдання – це 20 тестових завдань закритої форми, виконання його оцінюється 20 балами; друге завдання – присвячене розробленню схеми, що забезпечує аутентифікацію та достовірність інформації, що підготовлюється до передачі телекомунікаційними каналами зв'язку, виконання його оцінюється 10 балами; третє завдання – розрахункове, виконання його оцінюється 10 балами.

Результат семестрового екзамену оцінюється в балах (максимальна кількість – 40 балів, мінімальна кількість, що зараховується, – 25 балів) і проставляється у відповідній графі екзаменаційної "Відомості обліку успішності".

Студента слід вважати атестованим, якщо сума балів, одержаних за результатами підсумкової/семестрової перевірки успішності, дорівнює або перевищує 60. Мінімально можлива кількість балів за поточний і модульний контроль упродовж семестру – 35 та мінімально можлива кількість балів, набраних на екзамені, – 25.

Підсумкова оцінка з навчальної дисципліни розраховується з урахуванням балів, отриманих під час екзамену, та 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

Тема	**Форми та види навчання**		**Форми оцінювання**	**Max бал**
Тема 1.	***Аудиторна робота***			
	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
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема	***Аудиторна робота***			
	Лекція	Лекція №3. Протоколи автентифікації. Цифровий підпис		

2.	Лабораторне заняття	Лабораторна робота 2. Протоколи автентифікації. Цифровий підпис	Захист лабораторної роботи	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 3	***Аудиторна робота***			
	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
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 4.	***Аудиторна робота***			
	Лекція	Лекція №6. Алгоритми забезпечення цілісності даних		
	Лабораторне заняття	Лабораторна робота 5. Алгоритми забезпечення цілісності даних	Захист лабораторної роботи	10

	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 5.	***Аудиторна робота***			
	Лекція	Лекція №7. Забезпечення безпеки даних на мережевому рівні		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 6.	***Аудиторна робота***			
	Лекція	Лекція №8. Стек протоколів IPSec		
	Лабораторне заняття	Лабораторна робота 6. Стек протоколів IPSec	Захист лабораторної роботи	10
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 7.	***Аудиторна робота***			
	Лекція	Лекція №9. Сучасні файроволи		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		

Тема 8.	***Аудиторна робота***			
	Лекція	Лекція №10. Антивірусні системи		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 9.	***Аудиторна робота***			
	Лекція	Лекція №11. СПАМ. Методи боротьби зі СПАМом		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Тема 10.	***Аудиторна робота***			
	Лекція	Лекція 12. Застарілі та сучасні технології для веб-додатків ключем Лекція 13. Збір інформації про веб-додатки Лекція 14-15. Мережі стандарту 802.11. Забезпечення послуг безпеки.		
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою		
Іспит				40

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. Michael E. Whitman Principles of Information Security 6th Edition / Michael E. Whitman, Herbert J. Mattord - Cengage Learning; 6th edition (March 13, 2017) 656 p.
3. Richard E. Smith Elementary Information Security 3rd Edition / Jones & Bartlett Learning; 3rd edition (October 28, 2019) – 708 p.

Додаткова

4. Jason Andress Foundations of Information Security: A Straightforward Introduction / No Starch Press (October 7, 2019) – 248 p.
5. Якименко І.З. // Опорний конспект лекцій з дисципліни „Безпека програм та даних‖, для студентів спеціальності „Кібербезпека‖. – Тернопіль, 2019. – 50 с.
6. 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=8937