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

"ЗАТВЕРДЖУЮ"
Заступник керівника
(проректор з науково-педагогічної роботи)
_____
Микола АФАНАСЬЄВ

БЕЗПЕКА ПРОГРАМ ТА ДАНИХ

робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***121 Інженерія програмного забезпечення***
Освітній рівень	***перший (бакалаврський)***
Освітня програма	***Інженерія програмного забезпечення***

Статус дисципліни	***базова***
Мова викладання, навчання та оцінювання	***українська***

Завідувач кафедри
кібербезпеки та
інформаційних технологій _____ *Сергій ЄВСЕЄВ*

Харків
2020

ЗАТВЕРДЖЕНО
на засіданні кафедри *кібербезпеки та інформаційних технологій*
Протокол № 2 від 31.08.2020 р.

Розробник:
Євсеєв С. П., 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

Подано тематичний план навчальної дисципліни й її змістовність за модулями та темами, вміщено плани лекцій і лабораторних занять, матеріал щодо закріплення знань (завдання для самостійної роботи, контрольні запитання), методичні рекомендації та оцінювання знань студентів. Революційні зміни останнього десятиліття, що відбулися в Інтернет-ресурсах, зумовили до об'єднання інформаційних та комп'ютерних мереж в єдиний інформаційний та кібернетичний простір, що спонукало до створення інформаційно-корпоративних мереж на основі Інтернет-технологій, які істотно розширили спектр електронних послуг суспільства в цілому та людині окремо. Як на-слідок, суттєво трансформувалися і загрози такому інформаційному ресурсу, як Інтернет-ресурс (ІР). Загрози безпеці ІР набули ознак гібридності. Прояви ознак гібридності унаслідок одночасного впливу загроз інформаційній безпеці, кібернетичній безпеці (КБ) та безпеці інформації (БІ) на ІР призвели до виникнення явища синергізму, негативні прояви від якого потребують кардинального перегляду концепцій побудови діючих систем безпеки.

Розповсюдження Інтернет-технологій також, безперечно, вимагає добре поставленого захисту інформації яка циркулює і в кіберпросторі. Тому вивчення основних механізмів забезпечення безпеки, захисту програмного забезпечення на всьому циклі його існування приділяється багато уваги.

Мета – навчання студентів принципам захисту програмного забезпечення на всьому циклі його існування, дослідженню та використанню сучасних процедур забезпечення основних услуг безпеки інформації в інформаційно-комунікаційних ресурсах Інтернет-технологій та кіберпросторі, що засновані на використанні алгоритмів симетричної та несиметричної криптографії, цифровому підписі та протоколів інфраструктури відкритих ключів (ІВК).

Результатами навчання за дисципліною є придбання практичних навичок з визначення рівня захищеності програмного коду, сформованого за допомогою різних мов програмування та застосування новітніх способів захисту інформаційного контенту при розгортанні та функціонуванні додатків.

Характеристика навчальної дисципліни

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

Структурно-логічна схема вивчення дисципліни

Пререквізити	Постреквізити
Дискретна математика	Інженерія програмного забезпечення
Комп'ютерні системи та архітектура комп'ютерів	Програмування Інтернет
Комп'ютерні мережі	Архітектура та проектування програмного забезпечення

Компетентності та результати навчання за дисципліною

Компетентності	Результати навчання
Аналіз основ теорії захисту інформації щодо системного підходу до організації комплексних систем захисту даних на основі застосування криптографічних методів	Знати основні положення законодавства в галузі захисту інформації, основні міжнародні та національні стандарти з безпеки даних; основні терміни та визначення політики безпеки, принципи побудови профілю захисту інформації для забезпечення послуг безпеки

Здатність приймати участь у проектуванні програмного забезпечення, включаючи проведення моделювання (формальний опис) його структури, поведінки та процесів функціонування	Знати та вміти використовувати механізми та протоколи забезпечення конфіденційності, забезпечення автентичності (доступності) та цілісності даних
Знання і розуміння специфікацій, стандартів, правил і рекомендацій в професійній галузі, уміння оцінювати ступінь обґрунтованості їх застосування, здатність дотримуватися їх при реалізації процесів життєвого циклу	Знати моделі порушника, основні види атак, принципи лінійного та диференційного криптоаналізу. Методи та процедури захисту в банківських системах. Забезпечувати захист програмного та інформаційного забезпечення від несанкціонованих дій в програмному забезпечені IoT
Дослідження формування цифрового підпису за допомогою протоколів інфраструктури відкритих ключів (ІВК)	Знати та вміти використовувати механізми та протоколи керування ключами в ІВК інформаційної системи

Програма навчальної дисципліни

Змістовий модуль 1. Безпека і захист даних

Тема 1. *Механізми і політики розподіл прав доступу*
Тема 2. *Механізми шифрування. Симетричні та несиметричні криптосистеми*
Тема 3. *Протоколи автентифікації. Цифрові підписи*
Тема 4. *Комплексні системи захисту даних*
Тема 5. *Основні види атак на програмне забезпечення. Основи криптоаналізу*
Тема 6. *Основи цифрової стеганографії*

Змістовий модуль 2. Безпека в програмному забезпеченні

Тема 7. *Основи технології відкритих ключів (PKI)*
Тема 8. *Захист програмного забезпеченні в Інтернет-технологіях*
Тема 9. *Захист персональних даних*
Тема 10. *Основні принципи захисту програмного забезпечення*

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 лекції, презентації, бесіди, індивідуальні та групові міні-проєкти.

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, що дозволяє студенту поставити залік, – 60 балів);

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

Порядок здійснення поточного оцінювання знань студентів.

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

- аналізувати крипостійкість простих симетричних шифрів;
- застосовувати сучасні блочні симетричні шифри і режими шифрування;
- досліджувати сучасні асиметричні криптосистеми шифрування;
- досліджувати електронний цифровий підпис;
- застосовувати стеганографічні методи захисту інформації;
- аналізувати безпечність персональних конфіденційних даних на базі секретного диску та захищеної електронної пошти PGP;
- проводити статистичні дослідження генераторів випадкових і псевдовипадкових послідовностей за методикою NIST.

За дисципліною передбачені такі методи поточного формативного оцінювання: опитування та усні коментарі викладача за його результатами, настанови викладачів в процесі виконання лабораторних завдань, формування навичок самооцінювання та обговорення студентами виконаних лабораторних завдань, контроль самостійного виконання індивідуального завдання.

Всі роботи повинні бути виконані самостійно з метою розвитку творчого підходу до рішення задач.

Лекційні заняття: максимальна кількість балів становить 36 (робота на лекціях – 12, експрес-опитування – 24).

Лабораторні заняття: максимальна кількість балів становить 64 (захист лабораторних робіт – 40, контрольні роботи – 24), а мінімальна – 50.

Самостійна робота: складається з часу, який здобувач витрачає на підготовку до виконання лабораторних робіт та на підготовку до експрес-опитувань за лекціями та контрольних робіт за лабораторними роботами дисципліни, в технологічній карті бали на цій 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.

Виставлення підсумкової оцінки здійснюється за шкалою, наведено в таблиці "Шкала оцінювання: національна та ЄКТС".

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

Шкала оцінювання: національна та ЄКТС

Сума балів за всі види навчальної діяльності	Оцінка ЄКТС	Оцінка за національною шкалою	
		для екзамену, курсового проекту (роботи), практики	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	не зараховано

Рейтинг-план навчальної дисципліни

Тема	Форми та види навчання		Форми оцінювання	Max бал
Тема 1	***Аудиторна робота***			
	Лекція	Лекція *"Механізми і політики розподіл прав доступу"*	Робота на лекції	1
	Лабораторне заняття	*Лабораторна робота №1. Класичні симетричні системи. Дослідження крипостійкості простих симетричних шифрів*	виконання лабораторної роботи	
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 2	***Аудиторна робота***			
	Лекція	Лекція *"Механізми шифрування. Симетричні та несиметричні криптосистеми"*	Робота на лекції	1
			Експрес-опитування	3
	Лабораторне заняття	*Лабораторна робота №1. Класичні симетричні системи. Дослідження крипостійкості простих симетричних шифрів*	Захист лабораторних робіт № 1	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 3	***Аудиторна робота***			
	Лекція	Лекція *"Протоколи автентифікації. Цифрові підписи"*	Робота на лекції	2
			Експрес-опитування	3
	Лабораторне заняття	Лабораторна робота № 2.	Захист	5

		Дослідження сучасних блочних симетричних шифрів та режимів шифрування	лабораторних робіт № 2	
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 4	***Аудиторна робота***			
	Лекція	Лекція *"Комплексні системи захисту даних"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота №3. Дослідження сучасних асиметричних криптосистем шифрування. Стандарт ДСТУ ISO\IEC 15948-2	виконання лабораторної роботи	
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 5	***Аудиторна робота***			
	Лекція	Лекція*"Основні види атак на програмне забезпечення. Основи криптоаналізу"*	Робота на лекції	2
			Експрес-опитування	3
	Лабораторне заняття	Лабораторна робота №3. Дослідження сучасних асиметричних криптосистем шифрування. Стандарт ДСТУ ISO\IEC 15948-2 Лабораторна робота № 4. Дослідження електронного цифрового підпису. ЦП Ель Гамаля, ДСТУ 4145, ECDSA	Захист лабораторних робіт № 3	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 6	***Аудиторна робота***			
	Лекція	Лекція *"Основи цифрової стеганографії"*	Робота на лекції	1
			Експрес-опитування	3
	Лабораторне заняття	Лабораторна робота № 4. Дослідження електронного цифрового підпису. ЦП Ель	Захист лабораторної роботи № 4	5

		Гамаля, ДСТУ 4145, ECDSA	Контрольна робота 1	12
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 7	***Аудиторна робота***			
	Лекція	Лекція *"Основи технології відкритих ключів (PKI)"*	Робота на лекції	1
			Експрес-опитування	3
	Лабораторне заняття	Лабораторна робота № 5. Безпечність персональних конфіденційних даних на базі секретного диску та захищеної електронної пошти PGP	Захист лабораторної роботи № 5	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 8	***Аудиторна робота***			
	Лекція	Лекція *"Захист програмного забезпеченні в Інтернет-технологіях"*	Робота на лекції	1
	Лабораторне заняття	Лабораторна робота № 6. Стеганографічні методи захисту інформації	Експрес-опитування	3
			Захист лабораторної роботи № 6	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 9	***Аудиторна робота***			
	Лекція	Лекція *"Захист персональних даних"*	Робота на лекції	1
			Експрес-опитування	3
	Лабораторне заняття	Лабораторна робота № 7. Статистичні дослідження генераторів псевдовипадкових, випадкових і послідовностей за методикою NIS	Захист лабораторної роботи № 7	5
			Контрольна робота № 2	12
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		
Тема 10	***Аудиторна робота***			
	Лекція	Лекція *"Основні принципи захисту програмного забезпечення"*	Робота на лекції	1
			Експрес-опитування	3
	Лабораторне заняття	Лабораторна робота № 8. Розгортання та управління інфраструктурою відкритих ключів	Захист лабораторної роботи № 8	5
	Самостійна робота			
	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою. Підготовка до виконання лабораторних робіт. Виконання лабораторних завдань		

Рекомендована література

Основна

1. Технології захисту інформації. Мультимедійне інтерактивне електронне видання комбінованого використання / уклад. Євсеєв С. П., Король О. Г., Остапов С. Е., Коц Г. П. – Х.: ХНЕУ ім. С. Кузнеця, 2016. – 1013 Мб. ISBN 978-966-676-624-6

2. С. П. Євсеєв. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці. – Видавничий дом "Родовід", 2014. – 428 с.

3. Столлингс В. Криптография и защита сетей: принципы и практика, 2-е изд.: Пер. с англ. – М.: Издательский дом «Вильямс», 2001. – 672 с.: ил. – Парал. тит. англ.

Додаткова

4. Кузнецов О. О. Захист інформації в інформаційних системах. Методи традиційної криптографії / О. О. Кузнецов, С. П. Євсеєв, О. Г. Король. – Харків : Вид. ХНЕУ, 2010.– 316 с.

5 Хорошко В. А. Методы и средства зашиты информации. / В. А. Хорошко, А. А. Чекатков – К. : Юниор, 2003. – 504 с

Інформаційні ресурси.

6. Сайт персональних навчальних систем ХНЕУ ім. С. Кузнеця за дисципліною "Безпека програм та даних" https://pns.hneu.edu.ua/enrol/index.php?id=4941.