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

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

ЗАХИСТ ІНФОРМАЦІЇ

робоча програма навчальної дисципліни

Галузь знань	***12 Інформаційні технології***
Спеціальність	***122 Комп'ютерні науки***
Освітній рівень	***перший (бакалаврський)***
Освітня програма	***Комп'ютерні науки***

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. 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
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
дослідження сучасних протоколів і процедур щодо забезпечення основних послуг безпеки у відповідності до стандартів ISO-	Знати та вміти використовувати механізми та протоколи забезпечення конфіденційності, забезпечення автентичності (доступності) та цілісності даних

7498-2, ISO/IEC 10181	
дослідження основних протоколів захисту інформації в банківських системах відповідно до стандартів СОУ Н НБУ 65.1 СУІБ 1.0:2010, СОУ Н НБУ 65.1 СУІБ 2.0:2010, методів двофакторній автентифікації, дослідження відповідних атак на системи банківських транзакцій та вивчення методів протидії	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 АБС
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. *Огляд безпеки системи*
Тема 2. *Механізми і політики розмежування прав доступу*
Тема 3. *Методи та пристрої забезпечення захисту і безпеки*
Тема 4. *Захист, доступ та автентифікація*
Тема 5. *Моделі захисту. Захист пам'яті*
Тема 6. *Шифрування даних*
Тема 7. *Управління відновленням*
Тема 8. *Основні напрямки розвитку сучасної криптографії*
Тема 9. *Механізми та протоколи керування ключами в ІВК*

Змістовий модуль 2. Мережева безпека

Тема 10. *Основні види атак, принципи криптоаналізу*
Тема 11. *Алгоритми з секретним ключем*
Тема 12. *Алгоритми з відкритим ключем*
Тема 13. *Протоколи аутентифікації*
Тема 14. *Цифрові підписи*
Тема 15. *Використання паролів і механізмів контролю за доступом*

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, презентації, бесіди, індивідуальні та групові проєкти, майстер-класи.

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 сучасні блочні симетричні шифрі і режимиі шифрування;

– досліджувати сучасні асиметричні криптосистеми шифрування;

– досліджувати електронний цифровий підпис

– використовувати стеганографічні методи захисту інформації;

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

– проводити статистичні дослідження генераторів випадкових і псевдовипадкових послідовностей за методикою NIST.

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.

Лекційні заняття: максимальна кількість балів становить 20 (робота на лекціях – 12, експрес-опитування – 9).

Лабораторні заняття: максимальна кількість балів становить 40 (захист лабораторних робіт – 28, контрольні роботи – 12), а мінімальна – 30.

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.

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	Проблемна лекція *"Огляд безпеки системи"*	Робота на лекції	0,5
	Лабораторне заняття	Лабораторна робота №1. Класичні симетричні системи. Дослідження крипостійкості простих симетричних шифрів	виконання лабораторної роботи	
	Аудиторна 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 і політики розмежування прав доступу"*	Робота на лекції	0,5
	Лабораторне заняття	Лабораторна робота №1 *"Вивчення мережевих інструментів спільної роботи"*	захист лабораторної роботи № 1	4
	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		
Ма	***Аудиторна робота***			

	Лекція	Лекція *"Методи та пристрої забезпечення захисту і безпеки"*	Робота на лекції	0,5
			експрес-опитування	3
	Лабораторне заняття	Лабораторна робота №2 *Дослідження сучасних блочних симетричних шифрів та режимів шифрування*	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 4	***Аудиторна робота***			
	Лекція	Лекція *"Захист, доступ та автентифікація"*	Робота на лекції	0,5
	Лабораторне заняття	Лабораторна робота №2 *Дослідження сучасних блочних симетричних шифрів та режимів шифрування*	Захист лабораторної роботи № 2	4
	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 *"Моделі захисту. Захист пам'яті"*	Робота на лекції	0,5
	Лабораторне заняття	*Лабораторна робота №3. Дослідження сучасних асиметричних криптосистем шифрування. Стандарт ДСТУ ISO\IEC 15948-2*	виконання лабораторної роботи	
Тема 6	***Аудиторна робота***			
	Лекція	Лекція *"Шифрування даних"*	Робота на лекції	0,5
			експрес-опитування	3
	Лабораторне заняття	*Лабораторна робота №3. Дослідження сучасних асиметричних криптосистем шифрування. Стандарт ДСТУ ISO\IEC 15948-2*	Захист лабораторної роботи № 3	4
			контрольна робота 1	6
	Самостійна робота			

	Питання та завдання до самостійного опрацювання	Пошук, підбір та огляд літературних джерел за заданою тематикою, Підготовка до лабораторного заняття, до експрес-опитування, КР		
Тема 7	***Аудиторна робота***			
	Лекція	Лекція *"Управління відновленням"*	Робота на лекції	0,5
	Лабораторне заняття	*Лабораторна робота №4. Дослідження електронного цифрового підпису. ЦП Ель Гамаля, ДСТУ 4145, ECDSA*	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. Підготовка до екзамену		
Тема 8	***Аудиторна робота***			
	Лекція	Лекція *"Основні напрямки розвитку сучасної криптографії"*	Робота на лекції	0,5
	Лабораторне заняття	*Лабораторна робота №4. Дослідження електронного цифрового підпису. ЦП Ель Гамаля, ДСТУ 4145, ECDSA*	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. Підготовка до екзамену		
Тема 9	***Аудиторна робота***			
	Лекція	Лекція *"Механізми та протоколи керування ключами в ІВК"*	Робота на лекції	0,5
	Лабораторне заняття	*Лабораторна робота № 5. Безпечність персональних конфіденційних даних на базі секретного диску та захищеної електронної пошти PGP*	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. Підготовка до екзамену		
Тема 10	***Аудиторна робота***			
	Лекція	Лекція *"Основні види атак, принципи криптоаналізу"*	Робота на лекції	0,5
	Лабораторне заняття	*Лабораторна робота № 5.*	Захист	4

		Безпечність персональних конфіденційних даних на базі секретного диску та захищеної електронної пошти PGP	лабораторної роботи № 4	
	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. Підготовка до екзамену: виконання типових завдань за теорією		
Тема 11	***Аудиторна робота***			
	Лекція	Лекція *"Алгоритми з секретним ключем"*	Робота на лекції	0,5
	Лабораторне заняття	*Лабораторна робота № 6. Стеганографічні методи захисту інформації*	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. Підготовка до екзамену: виконання типових завдань за практичною складовою		
Тема 12	***Аудиторна робота***			
	Лекція	Лекція *"Алгоритми з відкритим ключем"*	Робота на лекції	0,5
			Експрес-опитування	3
	Лабораторне заняття	*Лабораторна робота № 6. Стеганографічні методи захисту інформації*	Захист лабораторної роботи № 5	4
	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. Підготовка до екзамену: виконання типових завдань за практичною складовою		
Тема 13	***Аудиторна робота***			
	Лекція	Лекція *"Протоколи автентифікації"*	Робота на лекції	0,5
	Лабораторне заняття	*Лабораторна робота № 7. Статистичні дослідження генераторів псевдовипадкових,*	Захист лабораторної роботи № 6	4

		випадкових і послідовностей за методикою NIST		
	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. Підготовка до екзамену: виконання типових завдань за практичною складовою		
Тема 14	***Аудиторна робота***			
	Лекція	Лекція *"Протоколи автентифікації"*	Робота на лекції	0,5
			Експрес-опитування	3
	Лабораторне заняття	*Лабораторна робота № 7. Статистичні дослідження генераторів псевдовипадкових, випадкових і послідовностей за методикою NIST*	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. Підготовка до екзамену: виконання типових завдань за практичною складовою		
Тема 15	***Аудиторна робота***			
	Лекція	Лекція *"Використання паролів і механізмів контролю за доступом"*	Робота на лекції	1
	Лабораторне заняття	*Лабораторна робота № 8. Розгортання та управління інфраструктурою відкритих ключів*	Захист лабораторної роботи № 7, 8	4
			контрольна робота 2	6
	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. Підготовка до екзамену: виконання типових завдань за практичною складовою		
Екзамен				40

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 "Захист інформації" https://pns.hneu.edu.ua/course/view.php?id=4777.