Київський університет імені Бориса Грінченка

Факультет інформаційних технологій та математики

Кафедра інформаційної та кібернетичної безпеки

імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з науково-методичної
та навчальної роботи
_____ Олексій ЖИЛЬЦОВ
«_01_» ____09_____ 2023 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ПРИКЛАДНА КРИПТОЛОГІЯ»

для студентів
спеціальності 125 Кібербезпека
освітнього рівня першого (бакалаврського)
освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем

2023 – 2024 навчальний рік

КИЇВСЬКИЙ УНІВЕРСИТЕТ
ІМЕНІ БОРИСА ГРІНЧЕНКА
Ідентифікаційний код 02136554
Начальник відділу
моніторингу якості освіти
Програма № 0085/23
(підпис) (прізвище, ініціали)
«___» _____ 2023 р.

Розробник:
Жданова Юлія Дмитрівна, кандидат фізико-математичних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка;

Викладач:
Жданова Юлія Дмитрівна, кандидат фізико-математичних наук, доцент, доцент кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка;

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка
Протокол від 01.09.2022 р. № 12

Завідувач кафедри _____ (підпис) Павло СКЛАДАННИЙ

Робочу програму погоджено з гарантом освітньої програми (керівником освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем)

___.___. 2022 р.
Керівник освітньої програми _____ (підпис) Артем ПЛАТОНЕНКО

Робочу програму перевірено
___.___. 2022 р.
Заступник декана _____ (підпис) Євген ІВАНІЧЕНКО

Пролонговано:
на 2023/2024 н.р. _____ (підпис) Бурячинський С.В. (ПІБ), «23» 08 2023 р., протокол № 8
на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___
на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___
на 20__/20__ н.р. _____ (підпис) (_____ (ПІБ)), «____»____ 20___ р., протокол № ___

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни за формами навчання		
	денна		заочна
Вид дисципліни	обов'язкова		
Мова викладання, навчання та оцінювання	українська		
Загальний обсяг кредитів / годин	7 / 210		
Курс	3		
Семестр	5	6	
Кількість змістових модулів з розподілом:	6		
Обсяг кредитів	3	4	
Обсяг годин, в тому числі:	90	120	
Аудиторні	42	42	
Модульний контроль	6	6	
Самостійна робота	42	42	
Семестровий контроль		30	
Форма семестрового контролю	Залік	Екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Прикладна криптологія» є нормативним документом Київського університету імені Бориса Грінченка, який розроблено кафедрою інформаційної та кібернетичної безпеки імені професора Володимира Бурячка на основі освітньо-професійної програми підготовки здобувачів першого (бакалаврського) рівня відповідно до навчальних планів спеціальності 125 Кібербезпека .

Робочу навчальну програму укладено згідно з вимогами Європейської кредитної трансферно-накопичувальної системи (ЄКТС) організації навчання.

Програма визначає обсяги знань, якими повинен опанувати здобувач першого (бакалаврського) рівня відповідно до вимог освітньо-кваліфікаційної характеристики, алгоритму вивчення навчального матеріалу дисципліни «Прикладна криптологія» та необхідне методичне забезпечення, складові і технологію оцінювання навчальних досягнень студентів.

Мета:

- надання знань, умінь, компетенції в області системного підходу до організації і практичного застосування стандартних методів забезпечення належного рівня криптографічного захисту інформації у мережі зв'язку;
- формування вмінь володіння математичним апаратом, який повинен бути достатнім для опрацьовування математичних моделей, пов'язаних із розробкою та функціонуванням сучасних криптоалгоритмів та криптопротоколів.

Завдання: отримання теоретичних знань та практичних умінь з побудови та дослідження систем криптографічного захисту інформації та набуття наступних компетентностей:

Фахові компетентності спеціальності

КФ-10: Здатність застосовувати методи та засоби криптографічного та технічного захисту інформації на об'єктах інформаційної діяльності.

3. Результати навчання за дисципліною

У результаті вивчення навчальної дисципліни студент повинен

знати:

- загальні принципи побудови систем криптографічного захисту інформації;
- загальні підходи щодо вибору параметрів криптосистем, алгоритми їх побудови та тестування.

вміти:

– характеризувати принципи побудови сучасних криптографічних систем та орієнтуватися в термінології і формулюваннях теоретичних результатів щодо їхньої стійкості;
– застосовувати стандартні криптографічні алгоритми та протоколи для захисту інформації;
– застосовувати типові методи криптографічного аналізу;
– застосовувати стандартні криптографічні алгоритми для побудови та використання електронних цифрових підписів;
– характеризувати сучасні системи криптографічного захисту інформації.

та досягти наступних **програмних результатів навчання**:

ПРз-10: аналізувати та визначати можливість застосування технологій, методів та засобів криптографічного захисту інформації.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назви змістових модулів і тем	Усього	Розподіл годин між видами робіт			
		Аудиторна			Самостійна
		Лекції	Практичні	Лабораторні	
СЕМЕСТР 5					
Змістовий модуль 1. Основи криптології					
Тема 1. Основні поняття криптології	12	2	2		4
Тема 2. Математичні основи криптології	16	2	4	4	10
Модульний контроль 1	2				
Разом за змістовим модулем 1	**30**	**4**	**6**	**4**	**14**
Змістовий модуль 2. Традиційні та блокові криптосистеми					
Тема 3. Традиційні криптосистеми	16	2	4	2	4
Тема 4. Блокові симетричні шифри	12	2		4	6
Модульний контроль 2	2				
Разом за змістовим модулем 2	**30**	**4**	**4**	**6**	**14**
Змістовий модуль 3. Потокові шифри					
Тема 5. Псевдовипадкові послідовності та методи їх генерації	12	2	2	2	6
Тема 6. Потокові симетричні шифри	16	2	4	2	8
Модульний контроль 3	2				
Разом за змістовим модулем 3	**30**	**4**	**6**	**4**	**14**
Разом за 5 семестр	**90**	**12**	**16**	**14**	**42**
СЕМЕСТР 6					
Змістовий модуль 4. Асиметричні криптосистеми					
Тема 7. Основи асиметричної криптографії	28	4	4	6	14
Модульний контроль 4	2				
Разом за змістовим модулем 4	**30**	**4**	**4**	**6**	**14**
Змістовий модуль 5. Тестування на простоту та факторизація цілих чисел					
Тема 8. Тестування на простоту та факторизація цілих чисел	28	4	6	4	14
Модульний контроль 5	2				
Разом за змістовим модулем 5	**30**	**4**	**6**	**4**	**14**
Змістовий модуль 6. Застосування асиметричних криптосистем					
Тема 9. Криптографічні хеш-функції. Аутентифікація	10	2	2	2	6

Назви змістових модулів і тем	Усього	Розподіл годин між видами робіт			
		Аудиторна			Самостійна
		Лекції	Практичні	Лабораторні	
Тема 10. Електронний цифровий підпис. Елементи еліптичної криптографії	10	2	2	2	8
Модульний контроль 6	**2**				
Разом за змістовим модулем 6	**30**	**4**	**4**	**6**	**14**
Разом за 6 семестр	**120**	**12**	**14**	**16**	**42**
Семестровий контроль	**30**				
Усього годин	**210**	**24**	**30**	**30**	**84**

5. Програма навчальної дисципліни

5 СЕМЕСТР

Змістовий модуль 1. Основи криптології

Тема 1. Основні поняття криптології

Предмет криптології. Роль криптологічних методів в побудові систем захисту інформації. Актуальність проблеми надійності реальних систем криптографічного захисту інформації. Історичний огляд розвитку криптології. Основні поняття, терміни і позначення криптології. Кодування відкритого тексту. Основні характеристики шифрів. Вимоги до криптографічних систем.

Модель секретного зв'язку К. Шеннона. Короткі відомості про криптоаналіз. Атаки на симетричні і асиметричні криптосистеми. Теоретична та практична стійкість криптосистем.

Тема 2. Математичні основи криптології

Алгебраїчні операції та алгебраїчні структури. Групи; циклічні групи, групи підстановок. Кільця, поля. Скінченні поля. Поля Галуа. Векторні простори. Базис і розмірність векторного простору. Лінійні перетворення та матриці над полем. Підстановочні матриці.

Подільність цілих чисел. Алгоритм Евкліда. Лінійні діофантові рівняння з двома невідомими. Прості числа і основна теорема арифметики.

Конгруентність цілих чисел. Класи лишків за даним модулем та їх властивості. Функція Ейлера та її властивості. Лінійні конгруенції. Системи лінійних конгруенцій. Китайська теорема про остачі.

Змістовий модуль 2. Традиційні та блокові криптосистеми

Тема 3. Традиційні симетричні криптосистеми

Основні типи шифрів заміни: проста заміна, гомофонічна підстановка, складна заміна, поліграмний шифр. Статистичний підхід до аналізу шифрів заміни. Основні типи шифрів перестановки. Криптоаналіз шифрів перестановки. Афінні шифри.

Загальна характеристика блокових складених шифрів. Принципи побудови блокових шифрів. Компоненти сучасного блокового шифру. Режими роботи блокових шифрів. Мережа Фейстеля. Блокові симетричні шифри на основі мережі Фейстеля: блоковий шифр *DES*; стандарт криптографічного перетворення даних ДСТУ ГОСТ 28147:2009. Стандарт симетричного шифрування AES на основі алгоритму *Rijndael*. Огляд алгоритму блокового симетричного шифрування ДСТУ 7624:2014/Калина.

Змістовий модуль 3. Потокові шифри

Тема 5. Псевдовипадкові послідовності та методи їх генерації

Шифри гамування. Шифр Вернама. Принципи побудови та властивості генераторів псевдовипадкових чисел. Криптографічні генератори псевдовипадкових чисел. Лінійні конгруентні генератори. Статистичні тести для перевірки псевдовипадкових послідовностей.

Тема 6. Потокові симетричні шифри

Загальні відомості про потокові шифри. Структура синхронного потокового шифратора. Класифікація потокових шифрів. Генерування потоку бітів за допомогою регістра зсуву з лінійним зворотним зв'язком. Запис станів двійкового регістру через супроводжуючу матрицю. Атаки на регістри зсуву з лінійним зворотним зв'язком Комбінування регістрів зсуву. Класифікація криптоатак на потокові шифри. Потоковий шифр A5. Потоковий шифр RC4. Державний стандарт України потокового симетричного перетворення ДСТУ 8845:2019/Струмок.

6 СЕМЕСТР

Змістовий модуль 4. Асиметричні криптосистеми

Тема 7. Основи асиметричної криптографії

Алгебраїчні конгруенції другого степеня. Квадратичні лишки і нелишки. Критерій Ейлера. Символ Лежандра. Символ Якобі. Добування квадратних коренів за простим модулем. Добування квадратних коренів за модулем складеного числа, що є добутком двох простих чисел. Первісний корінь за модулем p^a. Дискретні логарифми (індекси).

Задачі криптології, які привели до поняття асиметричних шифрів. Поняття про однонапрямлені функції та однонапрямлені функції з лазівками. Задачі, які приводять до однонапрямлених функцій. Принципи побудови асиметричної криптосистеми. Змішані криптосистеми. Асиметричні системи шифрування: протокол узгодження ключів Діффі-Хеллмана, криптосистема Ель-Гамаля, криптосистема RSA, криптосистема Рабіна.

Генератори псевдовипадкових чисел на основі однонапрямлених функцій з лазівкою. Генератор Блюма–Блюм–Шуба (BBS). Застосування генераторів псевдовипадкових послідовностей при ймовірнісному шифруванні. Криптосистема Блюма-Гольдвассер, криптосистема Гольдвассер-Мікалі.

Змістовий модуль 5. Тестування на простоту і факторизація цілих чисел

Тема 8 Тестування на простоту і факторизація цілих чисел

Тестування на простоту та факторизація чисел. Детерміновані тести: метод пробних ділень, тест Поклінгтона. Числа Кармайкла. Ймовірнісні тести. Тест Ферма та псевдопрості числа. Тест Соловея-Штрассена та ейлерові псевдопрості числа. Тест Міллера–Рабіна та сильні псевдопрості числа. Метод Гордона побудови сильно простих чисел.

Задача і методи факторизації цілих чисел. Огляд сучасних методів факторизації. Загальні вимоги до вибору параметрів криптосистеми RSA. Атаки на криптосистему RSA: методом Ферма, методом безключового читання, повторним шифруванням, на основі китайської теореми про остачі.

Змістовий модуль 6. Застосування асиметричних криптосистем

Тема 9. Криптографічні хеш-функції. Аутентифікація.

Проблема захисту від модифікування даних. Означення та властивості хеш-функцій, побудованих на однокрокових стискуючих функціях. Типи криптографічних хеш-функцій. Хеш-функції на основі блокових шифрів. Застосування хеш-функцій у криптографії. Стандартизовані хеш-функції. Державний стандарт України ДСТУ 7564:2014. Аутентифікація та цілісність повідомлень. *MAC*-коди.

Тема 10. Електронний цифровий підпис. Елементи еліптичної криптографії

Поняття про електронний цифровий підпис. Призначення, застосування, властивості і вимоги до електронного цифрового підпису. Загальна схема побудови електронного цифрового підпису. Схеми електронного цифрового підпису: Ель-Гамаля, *DSA, RSA*. Стандартизовані схеми ЕЦП. Цифрові сертифікати. Атаки на електронний цифровий підпис.

Арифметика на еліптичних кривих. Використання еліптичних кривих в криптографії: обмін ключами з використанням еліптичних кривих; шифрування з використанням еліптичних кривих;

електронний цифровий підпис на еліптичних кривих. Державний стандарт України ДСТУ 4145-2002.

6. Контроль навчальних досягнень

Навчальні досягнення студентів з дисципліни оцінюються за модульно-рейтинговою системою, в основу якої покладено принцип поопераційної звітності, обов'язковості модульного контролю, накопичувальної системи оцінювання рівня знань, умінь та навичок, розширення кількості підсумкових балів з урахуванням балів за екзамен до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних заняттях, за виконання індивідуальних завдань, за модульну контрольну роботу. Виконання модульних контрольних робіт здійснюється в електронному вигляді. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу змістового модуля.

У процесі оцінювання навчальних досягнень студентів застосовуються такі методи:

- *Методи усного контролю*: індивідуальне опитування, фронтальне опитування, співбесіда, екзамен.
- *Комп'ютерного контролю:* тестові програми.
- *Методи самоконтролю:* уміння самостійно оцінювати свої знання, самоаналіз.

Кількість балів за роботу з теоретичним матеріалом, на практичних заняттях, під час виконання самостійної роботи залежить від дотримання таких вимог:

- систематичність відвідування занять;
- своєчасність виконання навчальних і індивідуальних завдань;
- повний обсяг їх виконання;
- якість виконання навчальних і індивідуальних завдань;
- самостійність виконання;
- творчий підхід у виконанні завдань;
- ініціативність у навчальній діяльності;
- виконання тестових завдань.

Контроль успішності студентів з урахуванням поточного і підсумкового оцінювання здійснюється відповідно до навчально-методичної карти дисципліни (п.7), де зазначено види контролю і кількість балів за видами. Систему рейтингових балів для різних видів контролю та порядок їх переведення у національну (4-бальну) та європейську (ECTS) шкалу подано нижче у таблицях.

6.1 Система оцінювання навчальних досягнень студентів

Поточний контроль здійснюється під час оцінювання в балах знань та вмінь студента з кожного практичного заняття, опитування теорії, результатів самостійної роботи.

5 СЕМЕСТР

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	2	2	2	2	2	2
Відвідування практичних занять	1	3	3	2	2	3	3
Відвідування лабораторних занять	1	2	2	3	3	2	2
Робота на практичних заняттях	10	3	30	2	20	3	30
Лабораторне заняття (допуск, виконання, захист)	10	2	20	3	30	2	20
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25	1	25
Макс. кількість балів за видами поточного контролю (МВ)			87		87		87
Максимальна кількість балів: 261							
Розрахунок коефіцієнта: k=261/100=2,61							

Модульний контроль здійснюється під час проведення модульної контрольної роботи з кожного модуля і визначається викладачем у балах контрольної модульної рейтингової оцінки.

Підсумковий контроль здійснюється за результатами підсумкової семестрової модульної рейтингової оцінки (суми підсумкових модульних оцінок).

6 СЕМЕСТР

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 4		Модуль 5		Модуль 6	
		кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	2	2	2	2	2	2
Відвідування практичних занять	1	2	2	3	3	2	2
Відвідування лабораторних занять	1	3	3	2	2	3	3
Робота на практичних заняттях	10	2	20	3	30	2	20
Лабораторне заняття (допуск, виконання, захист)	10	3	30	2	20	3	30
Виконання завдань для самостійної роботи	5	1	5	1	5	1	5
Виконання модульної роботи	25	1	25	1	25	1	25
Макс. кількість балів за видами поточного контролю (МВ)			87		87		87
Максимальна кількість балів: 261							
Розрахунок коефіцієнта: k=261/60=4,35							

Модульний контроль здійснюється під час проведення модульної контрольної роботи з кожного модуля і визначається викладачем у балах контрольної модульної рейтингової оцінки.

Підсумковий контроль здійснюється за результатами підсумкової семестрової модульної рейтингової оцінки (суми підсумкових модульних оцінок) і екзамену.

6.2 Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом позааудиторної індивідуальної діяльності студента, результати якої використовуються у процесі вивчення програмового матеріалу навчальної дисципліни та містить результати дослідницького пошуку, відображає певний рівень його навчальної компетентності.

Перелік тем та оцінювання самостійної роботи студента

№ з/п	Назва теми	Кількість годин	Бали
5 семестр			
Змістовий модуль 1. Основні поняття криптології		**14**	**5**
1	Математичні основи криптології - виконання завдань відповідно до теми; - опрацювання фахових видань.	14	5
Змістовий модуль 2. Традиційні та блокові криптосистеми		**14**	**5**
2	Традиційні симетричні криптосистеми, сучасні блокові шифри: - виконання завдань відповідно до теми; - опрацювання фахових видань.	14	5
Змістовий модуль 3. Симетричні криптосистеми 2		**14**	**5**
3	Сучасні потокові шифри: - виконання завдань відповідно до теми; - опрацювання фахових видань.	14	5
	Разом за 5 семестр	**42**	**15**
6 семестр			
Змістовий модуль 4. Асиметричні криптосистеми		**14**	**5**
4	Аспекти практичного застосування окремих асиметричних криптоалгоритмів: - виконання завдань відповідно до теми; - опрацювання фахових видань.	14	5
Змістовий модуль 5. Тестування на простоту та факторизація цілих чисел		**14**	**5**
5	Сучасні методи тестування на простоту та факторизації - виконання завдань відповідно до теми; - опрацювання фахових видань.	14	5
Змістовий модуль 6. Застосування асиметричних криптосистем		**14**	**5**
6	Аспекти практичного застосування окремих криптоалгоритмів та криптопротоколів: - виконання завдань відповідно до теми; - опрацювання фахових видань.	14	5
	Разом за 6 семестр	**42**	**15**
	Разом	**84**	**30**

Критерії оцінювання самостійної роботи студента

№ п/п	Критерії оцінювання роботи	Максимальна кількість балів за кожним критерієм
1	Критичний аналіз суті та змісту першоджерел. Виклад фактів, ідей, результатів досліджень в логічній послідовності. Аналіз сучасного стану дослідження проблеми, розгляд тенденцій подальшого розвитку даного питання.	2 бали
2	Доказовість висновків, обґрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

6.3 Форми проведення модульного контролю та критерії оцінювання

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних заняттях, за виконання домашніх завдань, за виконання завдань самостійної роботи, за модульну контрольну роботу. Модульний контроль знань студентів здійснюється після завершення вивчення навчального матеріалу модуля. Форма проведення – виконання тестових завдань в середовищі MOODLE. Модульна контрольна робота оцінюється у 25 балів.

6.4 Форми проведення семестрового контролю та критерії оцінювання

Семестровий (підсумковий) контроль знань студентів у 5 семестрі здійснюється після завершення вивчення навчального матеріалу дисципліни у формі заліку, умовою допуску до якого є отримання студентом 25 балів (з урахуванням коефіцієнту) за результатами поточного контролю.

Підсумкова семестрова (залікова) рейтингова оцінка студента є сумою підсумкових фактичних оцінок студента за змістовими модулями.

Семестрове (підсумкове) оцінювання у 6 семестрі здійснюється у формі екзамену, умовою допуску до якого є отриманням студентом 35 балів (з урахуванням коефіцієнту) за результатами поточного контролю.

Форма проведення екзамену – комбінована. Екзамен оцінюється у 40 балів за розподілом: 20 балів – комплексний комп'ютерний тест з дисципліни; 20 балів – виконання практико-орієнтованого завдання.

Виконання практичного завдання передбачає перевірку рівня оволодіння студентом теоретичними знаннями та практичними вміннями.

Оцінювання практичного завдання відбувається в межах від 0 до 20 балів, згідно критеріїв оцінювання, й здійснюється з урахуванням: рівнів сформованості аналітико-синтетичних, творчих та методичних умінь необхідних для побудови ІТ-інфраструктури освітнього закладу.

Бали за виконання тесту та бали за виконання практичного завдання додаються. Оцінювання результатів засвоєння теоретичних знань та оцінювання сформованості практичних навичок володіння цифровими технологіями студентами, продемонстровані на екзамені, представлене у таблиці.

Підсумкова кількість балів (max – 40)	Оцінка за 4-бальною шкалою
1 – 23	«незадовільно»
24 – 29	«задовільно»
30 – 35	«добре»
36 – 40	«відмінно»

6.5 Орієнтовний перелік питань для семестрового контролю

Змістовий модуль 1. Основи криптології

Тема 1. Основні поняття криптології

1. Роль криптологічних методів і систем криптографічного захисту інформації в сучасному суспільстві.
2. Актуальність проблеми надійності реальних систем криптографічного захисту інформації.
3. Історичний огляд розвитку криптології.
4. Основні поняття, терміни і позначення криптології.
5. Моделі відкритого тексту
6. Поняття криптосистеми. Види криптосистем.
7. Основні характеристики шифрів.
8. Вимоги до криптографічних систем.
9. Короткі відомості про криптоаналіз.
10. Формальна модель загроз безпеки криптосистем.
11. Атаки на симетричні і асиметричні криптосистеми.
12. Модель секретного зв'язку К. Шеннона.
13. Абсолютно стійкий шифр.
14. Поняття практичної стійкості.

Тема 2. Математичні основи криптології

15. Алгебраїчні операції та алгебраїчні структури.
16. Групи; циклічні групи, групи підстановок.
17. Кільця, поля.
18. Скінченні поля. Поля Галуа.
19. Поняття векторного простору.
20. Лінійна залежність векторів. Базис і розмірність векторного простору.
21. Лінійні перетворення та матриці над полем.
22. Підстановки. Цикли і транспозиції. Підстановочні матриці.
23. Означення і основні властивості подільності цілих чисел.
24. Алгоритм Евкліда.
25. Взаємно прості числа та їх основні властивості
26. Найменше спільне кратне цілих чисел
27. Лінійні діофантові рівняння з двома невідомими**.**
28. Прості числа і основна теорема арифметики.
29. Означення і властивості конгруенцій.
30. Класи лишків за даним модулем та їх властивості.
31. Кільце класів лишків.
32. Повна і зведена системи лишків
33. Функція Ейлера та її властивості.
34. Теореми Ейлера та Ферма.
35. Лінійні конгруенції. Способи розв’язування лінійних конгруенцій.
36. Китайська теорема про остачі.

Змістовий модуль 2. Симетричні криптосистеми 1

Тема 3. Традиційні симетричні криптосистеми

37. Шифр заміни (підстановки).
38. Шифри багатозначної заміни (гомофонічної підстановки).
39. Шифри складної заміни (багатоалфавітної підстановки).
40. Криптосистема Віжінера.
41. Поліграмні шифри.
42. Статистичний підхід до аналізу шифрів заміни.
43. Шифрування з використанням підстановок степеня n .
44. Шифри маршрутної перестановки. Шифр вертикальної перестановки.

45. Лінійний шифр
46. Аффінний шифр
47. Шифр зсуву *l*-го порядку
48. Лінійний шифр *l*-го порядку

Тема 4. Блокові симетричні шифри

49. Загальна характеристика блокових складених шифрів.
50. Принципи побудови блокових шифрів.
51. Компоненти сучасного блокового шифру.
52. Мережа Фейстеля.
53. Режими роботи блокових шифрів.
54. Атаки на блокові шифри.
55. Загальна характеристика блокового шифру *DES*.
56. Побудова раундових ключів шифру *DES*.
57. Функція DES.
58. Режими роботи *DES*.
59. Атаки на *DES*.
60. Області застосування DES.
61. Модифікації *DES*.
62. Загальна характеристика ДСТУ ГОСТ 28147:2009.
63. Ключова інформація алгоритму ГОСТ 28147-89.
64. Основний крок криптоперетворення алгоритму ГОСТ 28147-89.
65. Базові цикли криптоперетворень алгоритму ГОСТ 28147-89.
66. Режими роботи алгоритму ГОСТ 28147-89.
67. Атаки на ГОСТ 2 8147-89.
68. Математичні основи AES на основі алгоритму Rijndael.
69. Представлення даних в криптоалгоритмі AES.
70. Загальна структура AES.
71. Один раунд шифрування AES.
72. Формування ключових елементів AES.
73. Вибір вузлів замін і констант AES.
74. Показники стійкості, продуктивність і зручність реалізації.
75. Порівняння характеристик алгоритмів ДСТУ ГОСТ 28147:2009 і AES/Rijndael.
76. Огляд стандарту ДСТУ 7624:2014.

Змістовий модуль 3. Потокові шифри

Тема 5. Псевдовипадкові послідовності та методи їх генерації

77. Шифри гамування.
78. Шифр Вернама.
79. Принципи побудови та властивості генераторів псевдовипадкових чисел.
80. Криптографічні генератори псевдовипадкових чисел.
81. Лінійні конгруентні генератори.
82. Статистичні тести для перевірки псевдовипадкових послідовностей.

Тема 6. Потокові симетричні шифри

83. Загальні відомості про потокові шифри.
84. Генерування потоку бітів за допомогою регістра зсуву з лінійним зворотним зв'язком (РЗЛЗЗ).
85. Вираз елементів рекуренти, що генерується РЗЛЗЗ, через елементи початкового стану.
86. Атаки на регістри зсуву з лінійним зворотним зв'язком.
87. Комбінування регістрів зсуву.
88. Класифікація криптоатак на потокові шифри.
89. Потоковий шифр А5.

Змістовий модуль 4. Асиметричні криптосистеми

Тема 7. Основи асиметричної криптографії

90. Алгебраїчні конгруенції другого степеня. Квадратичні лишки і нелишки. Критерій Ейлера.
91. Означення і властивості символів Лежандра і Якобі.
92. Добування квадратних коренів за простим модулем.
93. Добування квадратних коренів за модулем складеного числа, що є добутком двох простих чисел.
94. Означення порядків чисел та класів чисел за даним модулем.
95. Первісні корені.
96. Індекси (дискретні логарифми).
97. Задача дискретного логарифмування в скінченному полі.
98. Задачі криптології, які привели до створення асиметричних шифрів.
99. Загальна схема асиметричної криптосистеми.
100. Поняття про однонапрямлені функції і функції з лазівками.
101. Задачі, які приводять до однонапрямлених функцій
102. Принципи побудови асиметричної криптосистем, їх застосування, переваги і недоліки
103. Змішані криптосистеми
104. Алгоритми дискретного логарифмування.
105. Протокол обміну ключами Діффі–Хеллмана.
106. Криптосистема Ель-Гамаля.
107. Криптосистема Райвеста–Шаміра–Адлемана (RSA).
108. Криптосистема Рабіна.

Змістовий модуль 5. Тестування на простоту та факторизація цілих чисел

Тема 8. Тестування на простоту і факторизація цілих чисел

109. Детерміновані тести перевірки на простоту та їх властивості.
110. Ймовірнісні тести перевірки на простоту та їх властивості.
111. Застосовування алгоритму пробного ділення для факторизації цілого числа.
112. Метод решета Ератосфена для перевірки цілого числа на простоту.
113. Алгоритм Ферма перевірки на простоту.
114. Числа Кармайкла.
115. Сутність ймовірнісних тестів на перевірку простоти непарного цілого числа.
116. Тест Соловея–Штрассена перевірки непарного цілого числа на простоту.
117. Тест Рабіна–Міллера перевірки непарного цілого числа на простоту.
118. Метод Гордона побудови сильних простих чисел.
119. Задача факторизації цілих чисел.
120. Метод пробних ділень факторизації цілих чисел.
121. Метод Ферма факторизації цілих чисел.
122. Метод квадратичного решета факторизації цілих чисел.
123. Огляд сучасних методів факторизації.
124. Загальні вимоги до вибору параметрів КС *RSA*.

Змістовий модуль 6. Застосування асиметричних криптосистем

Тема 9. Криптографічні хеш-функції. Аутентифікація

125. Означення і властивості хеш-функцій.
126. Узагальнена модель побудови хеш-функций за допомогою однокрокових стискуючих функцій
127. Типи криптографічних хеш-функцій.
128. Хеш-функції на основі блокових шифрів
129. Застосування хеш-функций для аутентифікації повідомлень.
130. Стандартизовані хеш-функції.
131. *MAC*-коди. *MAC*-код на основі блокового шифру в режимі CBC
132. Алгоритм аутентифікації повідомлень H-MAC.
133. ГПВП на основі однонапрямлених функцій з лазівкою.

134. Принцип роботи генератора псевдовипадкових чисел BBS.
135. Застосування генераторів псевдовипадкових послідовностей при ймовірнісному шифруванні.

Тема 10 Електронний цифровий підпис. Елементи еліптичної криптографії

136. Поняття про ЕЦП.
137. Призначення, застосування, властивості і вимоги до ЕЦП.
138. Класифікація ЕЦП.
139. Загальна схема побудови ЕЦП.
140. Електронний цифровий підпис *RSA*.
141. Електронний цифровий підпис Ель-Гамаля.
142. Електронний цифровий підпис *DSA*.
143. Стандартизовані схеми ЕЦП.
144. Цифрові сертифікати.
145. Атаки на електронний цифровий підпис.
146. Арифметика на еліптичних кривих.
147. Обмін ключами з використанням еліптичних кривих.
148. Шифрування з використанням еліптичних кривих.
149. Електронний цифровий підпис на еліптичних кривих.

6.6 Шкала відповідності оцінок

Рейтингова оцінка	Оцінка за стобальною шкалою	Значення оцінки
A	90-100	**Відмінно** — відмінний рівень знань (умінь) в межах обов'язкового матеріалу з, можливими, незначними недоліками
B	82-89	**Дуже добре** – достатньо високий рівень знань (умінь) в межах обов'язкового матеріалу без суттєвих (грубих) помилок
C	75-81	**Добре** – в цілому добрий рівень знань (умінь) з незначною кількістю помилок
D	69-74	**Задовільно** – посередній рівень знань (умінь) із значною кількістю недоліків, достатній для подальшого навчання або професійної діяльності
E	60-68	**Достатньо** – мінімально можливий допустимий рівень знань (умінь)
FX	35-59	**Незадовільно з можливістю повторного складання** – незадовільний рівень знань, з можливістю повторного перескладання за умови належного самостійного доопрацювання
F	1-34	**Незадовільно з обов'язковим повторним вивченням курсу** - досить низький рівень знань (умінь), що вимагає повторного вивчення дисципліни

7.1 Навчально-методична картка дисципліни на 5 семестр

Разом: 90 год., лекції – 12 год., практичні заняття – 16 год., лабораторні заняття – 14 год., модульний контроль – 6 год., самостійна робота – 42 год.

Модулі (назви, бали)	**1. Основні поняття криптології (87 балів)**			**2. Традиційні та блокові криптосистеми (87 балів)**					**3. Потокові шифри (87 балів)**		
Теми	1	2		3		4			5	6	
Лекції (теми, бали)	1. Основні поняття і задачі крипт (1бал)	2. Математичні основи криптографії (1 бал)		3. Класичні шифри (1 бал)		4. Блокові симетричні .шифри. (1 бал)			5. Шифри гамування. Псевдовипадкові послідовності та методи їх генерації (1 бал)	6. Потокові симетричні шифри .(1 бал)	
Практичні заняття (теми, бали)	1..Кодування відкритого тексту та двійкових даних (11 баліv0	2. Підстановки. Дії в скінченних полях (11 балів)	3. Арифметика остач (11 балів)	4. Шифри заміни і перестановки (11 балів)	5. Афінні шифри (11 балів)				6. Шифри гамування (11 балів)	7. Регістри зсуву з лінійним зворотним зв'язком (11 балів)	8. Система потокового шифрування на основі РЗЛЗ3 (11 балів)
Лабораторні заняття (теми, бали)		1.Подільність в кільці цілих чисел та в кільці многочленів. (11 балів)	2.Лінійні конгруенції за простим та складеним модулем (11 балів)			3. Стандарт шифрування даних DES (11 балів)	4. Стандарт ДСТУ ГОСТ 28147:2009 (11 балів)	5. Криптоалгоритм AES-128 (11 балів)	6. Побудова та дослідження лінійного конгруентного генератора псевдовипадкових чисел (11 балів)		7. Вивчення властивостей моделі алгоритму А5/1 (11 балів)
Самостійна робота	Самостійна робота (5 балів)			Самостійна робота (5 балів)					Самостійна робота (5 балів)		
Поточний контроль (вид, бали)	Модульна контрольна робота 1 (25 балів)			Модульна контрольна робота 2 (25 балів)					Модульна контрольна робота 3 (25 балів)		
Підсумковий контроль (вид, бали)	Залік										

7.2 Навчально-методична картка дисципліни на 6 семестр

Разом: 120 год., лекції – 12 год., практичні заняття – 14 год., лабораторні заняття – 16 год., модульний контроль – 6 год., самостійна робота – 42 год., семестровий контроль – 30 год.

Модулі (назви, бали)	4. Асиметричні криптосистеми (87 балів)				5. Тестування на простоту та факторизація цілих чисел (87 балів)			6. Застосування асиметричних криптосистем (87 балів)			
Теми	7				8			9	10		
Лекції (теми, бали)	7. Алгебраїчні контруенції другого степеня. Дискретні логарифми (1 бал)		8. Асиметричні криптосистеми. (1 бал)		9. Тестування на простоту (1 бал)	10. Факторизація цілих чисел (1 бал)		11. Криптографічні хеш-функції. Аутентифікація (1 бал)	12. Електронний цифровий підпис. Елементи еліптичної криптографії (1 бал)		
Практичні заняття (теми, бали)	9. Добування квадратних коренів за модулем. (11 балів)	10. Задача дискретного логарифмування в скінченному полі (11 балів)			11. Тестування на простоту (11 балів)	12. Факторизація цілих чисел (11 балів)	13. Вибір параметрів КС RSA (11 балів)	14. Контроль цілісності повідомлень за допомогою MAC-коду DES-CBC (11 балів)	15. Арифметика на еліптичних кривих (11 балів)		
Лабораторні заняття (теми, бали)		8. Протокол узгодження ключів Діффі-Хеллмана, криптосистема Ель-Гамаля (11 балів)	9. Криптосистема RSA (11 балів)	10. Криптосистема Рабіна (11 балів)	11. Метод Гордона побудови сильних простих чисел і тест Міллера-Рабіна (11 балів)		12. Метод квадратичного решета факторизації цілих чисел (11 балів)	13. Схеми ймовірнісного шифрування. (11 балів)	14. Електронний цифровий підпис (11 балів)	15. Еліптичні криві в криптографії (11 балів)	
Самостійна робота	Самостійна робота (5 балів)				Самостійна робота (5 балів)			Самостійна робота (5 балів)			
Поточний контроль (вид, бали)	Модульна контрольна робота 4 (25 балів)				Модульна контрольна робота 5 (25 балів)			Модульна контрольна робота 6 (25 балів)			
Підсумковий контроль (вид, бали)	Екзамен (40 балів)										

8. Рекомендовані джерела

Базова література

1. Бабенко Т.В., Гулак Г.М., Сушко С. О., Фомичова Л.Я. Криптологія у прикладах, тестах і задачах: навч. посіб. Дніпропетровськ: Національний гірничий університет, 2013. 318 с.
2. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації: підручник. Вінниця : ВНТУ, 2011. 198 с.
3. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. Вид. офіц. Чинний від 01.07.2015. Київ: ДП «УкрНДНЦ», 2015. 228 с.
4. ДСТУ 8845:2019 Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного потокового перетворення. Вид. офіц. Чинний від 01.10.2019. Київ: ДП «УкрНДНЦ», 2019. 50 с.
5. ДСТУ 7564:2014. Функція хешування. Вид. офіц. Чинний від 01.04.2015. Київ: Мінекономрозвитку України, 2015. 33 с.
6. ДСТУ 4145-2002 Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. / розроб. О. Шаталов, Кочубінський А. Вид офіц. Чинний від 01.07.2003. К.: Державний комітет України з питань технічного регулювання та споживчої політики, 2003. 31 с.
7. Закон України «Про електронні довірчі послуги», від 14. 01.2020 № 440-IX; станом на 01.12.2022.
8. Корченко О. Г., Сіденко В. П., Дрейс Ю.О. Прикладна криптологія: системи шифрування: підручник. К.: ДУТ, 2014. –448 с.
9. Кузнецов Г. В., Фомичов В. В., Сушко С.О., Фомичова Л. Я. Математичні основи криптографії: навч. посіб. Дніпропетровськ: Національний гірничий університет, 2004. 391 с.
10. Оглобліна О. І., Сушко Т.С., Шрамко Ю. В. Елементи теорії чисел: навч. посіб. Суми: Сумський державний університет, 2015. 186 с.
11. Сушко С. О., Кузнецов Г. В., Фомичова Л. Я., Корабльов А. В. Математичні основи криптоаналізу: навч. посіб. Дніпропетровськ: Національний гірничий університет, 2010. 466 с.
12. Фільштінський В. А., Бережний А. В. Математичні основи криптографії: конспект лекцій. Суми: Сумський державний університет, 2011. 138 с.

Допоміжна література

1. Богуш В.М., Мухачов В.А. Криптографічні застосування елементарної теорії чисел. Навчальний посібник. – Київ: ДУІКТ, 2006. – 125 с.
2. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч. посібник / Г. Л. Козіна. – Запоріжжя: НУ «Запорізька політехніка», 2020. – 192 с.
3. Menezes A. Elliptic Curve Public Key Cryptosystems, Kluwer Academic Publishers, 1993. 141 p.
4. Schneier B. Applied Cryptography: Protocols, Algorithms and Source Code in C, 20th Anniversary Edition edition. New York: Wiley, 2015. 784 p.
5. Steinberg J., Beaver K., Winkler I., Coombs T. Cybersecurity All-in-One For Dummies. New York: Wiley, 2022. 700 p.

9. Додаткові ресурси (інформаційні ресурси)

1. Тарнавський Ю.А. Технології захисту інформації [Електронний ресурс]: підручник. – К.: КПІ ім. Ігоря Сікорського, 2018. – 162 с. Режим доступу: https://ela.kpi.ua/bitstream/123456789/23896/1/TZI_book.pdf
2. Wenbo Mao. Modern Cryptography: Theory and Practice. Hewlett-Packard Company. Published Prentice Hall PTR. 2003. 648 p. [Електронний ресурс] – Режим доступу: https://docs.google.com/file/d/0Bxy7_wFLYLfSYlpUdHhVQUU5Rnc/view?resourcekey=0-8Xf78RyrE1DuU8XA8xQHTA
3. Український ресурс з безпеки. [Електронний ресурс] – Режим доступу: http://kiev-security.org.ua
4. Криптографічний захист інформації. [Електронний ресурс] – Режим доступу:

http://www.bezpeka.com/ru/lib/spec/cript.html

5. Державна служба спеціального зв'язку та захисту інформації України. [Електронний ресурс] – Режим доступу: http://www.dsszzi.gov.ua