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
«КРИПТОМЕХАНІЗМИ ІНФОРМАЦІЙНОЇ ТА КІБЕРБЕЗПЕКИ»

для студентів

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

2023 – 2024 навчальний рік

Розробник:

Бессалов Анатолій Володимирович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського університету імені Бориса Грінченка.

Викладач:

Бессалов Анатолій Володимирович, доктор технічних наук, професор, професор 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) (Скаржинський В.А.), «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	5 / 150	
Курс	4	
Семестр	7	
Кількість змістових модулів з розподілом:	5	
Обсяг кредитів	5	
Обсяг годин, в тому числі:	150	
Аудиторні	56	
Модульний контроль	8	
Семестровий контроль	30	
Самостійна робота	56	
Форма семестрового контролю	екзамен	

2. Мета та завдання навчальної дисципліни

Робоча навчальна програма з курсу «Криптомеханізми інформаційної та кібербезпеки» 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 навчального плану спеціальності 125 Кібербезпека та захист інформації, освітньої програми 125.00.01 Безпека інформаційних і комунікаційних систем.

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

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

Навчальна дисципліна ««Криптомеханізми інформаційної та кібербезпеки»» складається з 5 змістових модулів: 1.Основні поняття безпеки інформації. Математичні основи; 2.Асиметричні криптосистеми на базі кілець; 3.Асиметричні криптосистеми на базі полів. Обсяг дисципліни – 120 год (4 кредити).

Метою викладання навчальної дисципліни «Криптомеханізми інформаційної та кібербезпеки» є отримання компетентностей в області криптографічного захисту інформації у комп'ютерних мережах .

Завдання:

- надання студентам теоретичних знань про задачі та особливості криптографічного захисту інформації у комп'ютерних мережах .

– формування у студентів категоріальних понять з основ математики асиметричної криптографії;

– формування у студентів умінь обчислювати параметри цифрового підпису і розподілу ключів на основі відомих протоколів;

– стимулювання студентів до активної аналітико-пошукової роботи, що спрямована на визначення ефективних шляхів розвитку у сфері захисту інформації.

У результаті вивчення навчальної дисципліни формуються

загальні компетентності:

ЗК-1: Здатність до комплексного розв'язання проблем. Здатність виявляти наукову сутність проблем у професійній сфері, знаходити адекватні шляхи щодо їх розв'язання;

володіння системним, цілісним підходом до аналізу і оцінки ситуації.

ЗК-8: Когнітивна гнучкість. Здатність здобувати нові знання, уміння та інтегрувати їх з уже наявними; самостійного освоєння нових методів дослідження, зміни наукового й виробничого профілю своєї діяльності.

ЗК-10: Складання суджень і ухвалення рішень. Спроможність орієнтуватися у різних поглядах на проблему, формувати власну думку; уміти формулювати задачу, аргументовано обирати оптимальні шляхи розв'язання, аналізувати й осмислювати отриманий розв'язок.

фахові компетентності:

ФК-1: Здатність до ефективної реалізації себе як фахівця з комп'ютерних наук в інформаційному суспільстві; оцінки, аналізу та ефективного використання методів, технологій та інструментарію інформатики в усіх сферах суспільного життя; розуміння основних напрямків подальшого розвитку інформатики.

ФК-2: Здатність до формулювання та досліджування математичних моделей систем і процесів, обґрунтовування вибору методів і підходів для розв'язування теоретичних і прикладних задач в галузі комп'ютерних наук, інтерпретування отриманих результатів.

ФК-3: Здатність розробляти адекватні комп'ютерні моделі та алгоритми розв'язання професійних задачі з застосовуванням сучасних технологій і засобів (в т.ч. згідно обраної спеціалізації).

ДФК-1: Здатність прогнозувати, виявляти та оцінювати стан інформаційної безпеки об'єктів і систем; виконувати спеціальні дослідження технічних і програмних засобів захисту інформації в організаціях; здійснювати проектування (розробку) систем, технологій і засобів інформаційної безпеки, а також протидію несанкціонованому проникненню в систему і мережу.

3. Результати навчання за дисципліною

При вивченні курсу «Криптомеханізми інформаційної та кібербезпеки» студенти повинні ***знати:***

- про джерела і способи дії загроз на об'єкти інформаційної безпеки установ;
- про правові і нормативні акти, які визначають систему захисту інформації в державі;
- про основні методи, технологію, принципи і правила побудови захисту електронних обчислювальних машин, у тому числі персональних комп'ютерів, їх елементів і об'єктів комп'ютерних мереж;
- про алгоритми створення сучасних програм, алгоритми шифрування та застосування стандартного програмного забезпечення захисту;
- про методи та технології захисту операційних систем, текстових редакторів, табличних процесорів, системи управління базами даних в локальних, корпоративних та глобальних комп'ютерних мережах.

уміти:

- працювати з концептуальними моделями розробки, розподілу, обробки, використання та зберігання конфіденціальних документів;
- визначати системи й методи захищеності носіїв інформації;
- створювати засобами стандартного програмного забезпечення елементи захисту інформації.

та досягти наступних **програмних результатів навчання:**

ПРз-5: знання та розуміння концепцій, методів, інструментів і засобів, що застосовуються для проектування баз даних; основні моделі баз даних, архітектури СУБД, сучасні напрямки розвитку технологій баз даних; методику виконання розрахунків і критеріїв оцінювання альтернативних рішень на кожному етапі проектування; інформаційні вимоги як вихідні дані для процесу проектування; засоби опису вихідних даних і відображення результатів кожного етапу проектування.

ДПРз-1: знання та розуміння основ теорії інформаційної безпеки та ризиків на різних рівнях інформаційних процесів.

ДПРу-1: проектувати та реалізувати комплексні системи захисту інформації організацій (підприємств) відповідно до вимог нормативних документів системи захисту інформації.

4. Структура навчальної дисципліни

Тематичний план для денної форми навчання

Назва змістових модулів, тем	Усього	Розподіл годин між видами робіт					
		Аудиторна:					Самостійна
		Лекції	Семінари	Практичні	Лабораторні	Індивідуальні	
Змістовий модуль 1. Основні поняття і задачі безпеки інформації.							
Тема 1.Основні поняття безпеки інформації. Загрози безпеки інформації	6	2					4
Тема 2. Задачі технічного і криптографічного захисту інформації. Принципи криптографічного захисту інформації	6	2					4
Разом	12	4					8
Змістовий модуль 2. Сучасні симетричні криптосистеми							
Тема 3.Блочні шифри. Стандарт DES	12	2		2	2		6
Тема 4. Поточні шифри. Генератор Хафмена	12	2		2	2		6
Модульний контроль	2						
Разом	26	4		4	4		12
Змістовий модуль 3. Асиметричні криптосистеми на базі кінцевих полів							
Тема 5. Криптосистема Ель-Гамаля	12	2		2	2		6
Тема 6. Цифровий підпис DSA	12	2		2	2		6
Модульний контроль	2						
Разом	26	4		4	4		12
Змістовий модуль 4. Арифметика еліптичних кривих над кінцевим полем							
Тема 7. Еліптичні криві над полем R	14	4		2	2		6
Тема 8. Еліптичні криві над полем Fp	12	2		2	2		6
Модульний контроль	2						
Разом	28	6		4	4		12
Змістовий модуль 5. Асиметричні криптосистеми на базі еліптичних кривих							
Тема 9. Розподіл ключів за схемою Діфі-Хелмана	14	4		2	2		6
Тема 10. Цифровий підпис ECDSA	12	2		2	2		6
Модульний контроль	2						
Разом	28	6		4	4		12
Семестровий контроль	30						
Усього	**150**	**24**		**16**	**16**		**56**

5. Програма навчальної дисципліни

Змістовий модуль 1. Основні поняття безпеки інформації. Математичні основи

Тема 1. Вступ. Основні поняття безпеки інформації

Основні загрози інформаційній безпеці. Категорії безпеки інформації в комп'ютерних мережах та інформаційних системах. “Помаранчева книга” США. Методи захисту інформації.

Тема 2. Задачі т**ехнічного і криптографічного захисту інформації**.

Принципи криптографічного захисту інформації. Моделі симетричної і асиметричної криптосистем.

Змістовий модуль 2. Сучасні симетричні криптосистеми

Тема 3.Блочні шифри. Стандарт DES.

Класифікація симетричних шифрів. Принципи шифрування: підстановки і перестановки. Принцип побудови DES.

Тема 4. Поточні шифри. Генератор Хафмена

Принцип поточного шифрування. Циклічні коди. Код Хемінга. Дуальний код. Лінійний рекурентний регістр зі зворотними зв’язками. Генератор Хафмена.

Змістовий модуль 3. Асиметричні криптосистеми на базі кінцевих полів

Тема 5. Криптосистема Ель-Гамаля.

Функція шифрування Ель-Гамаля. Схеми шифрування і цифрового підпису.

Тема 6. Цифровий підпис DSA

Властивості хеш-функції повідомлення. Цифровий підпис RSA Безпека RSA. Складність факторизації модуля N = PQ.

Змістовий модуль 4. Арифметика еліптичних кривих над кінцевим полем

Тема 7. Еліптичні криві над полем R

Визначення ЕК. Закони додавання точок і формування абелевої групи. Порядок кривої і порядок точки. Точки малих порядків.

Тема 8. Еліптичні криві над полем Fp

Теорема Хасе. Структура групи точок кривої Е. Криптостійки криві у формі Вейерштраса.

Змістовий модуль 5. Асиметричні криптосистеми на базі еліптичних кривих

Тема 9. Розподіл ключів за схемою Діфі-Хелмана

Постанова задачі розподілу ключів. Інтерактивна і неінтерактивна схема розподілу ключів

Тема 10. Цифровий підпис ECDSA

Формування і перевірка ЦП за схемою ECDSA. Відомі атаки і безпека ECDSA

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 до 100.

Оцінка за кожний змістовий модуль включає бали за поточну роботу студента на практичних та лабораторних 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, 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.

Розрахунок рейтингових балів за видами поточного (модульного) контролю

Вид діяльності студента	Максимальна к-сть балів за одиницю	Модуль 1		Модуль 2		Модуль 3		Модуль 4		Модуль 5	
		кількість одиниць	максимальна кількість балів	кількість	максимальна кількість балів	кількість	максимальна кількість балів	кількість одиниць	максимальна кількість балів	кількість одиниць	максимальна кількість балів
Відвідування лекцій	1	2	2	2	2	2	2	3	3	3	3
Відвідування семінарських занять											
Відвідування практичних занять	1			2	2	2	2	2	2	2	2
Відвідування лабораторних занять	1			2	2	2	2	2	2	2	2
Робота на семінарському занятті											
Робота на практичному занятті	10			2	20	2	20	2	20	2	20
Лабораторна робота (в тому числі допуск, виконання, захист)	10			2	20	2	20	2	20	2	20
Виконання завдань для самостійної роботи	5	2	10	2	10	2	10	2	10	2	10
Виконання модульної роботи	25			1	25	1	25	1	25	1	25
Виконання ІНДЗ	30										
Разом		-	12	-	81	-	81	-	82	-	82
Максимальна кількість балів: 338											
Розрахунок коефіцієнта: 338/60=5,63											

Завдання для самостійної роботи та критерії її оцінювання

Самостійна робота є видом поза аудиторної 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
Змістовий модуль 1. Основні поняття і задачі безпеки інформації		**8**	**10**
1	Тема 1.Основні поняття безпеки інформації. Загрози безпеки інформації Тема 2. Задачі технічного і криптографічного захисту інформації. Принципи криптографічного захисту інформації	8	10
Змістовий модуль 2. Сучасні симетричні криптосистеми		**12**	**10**
2	Тема 3.Блочні шифри. Стандарт DES Тема 4. Поточні шифри. Генератор Хафмена	12	10
Змістовий модуль 3. Асиметричні криптосистеми на базі кінцевих полів		**12**	**10**
3	Тема 5. Криптосистема Ель-Гамаля Тема 6. Цифровий підпис DSA	12	10
Змістовий модуль 4. Арифметика еліптичних кривих над кінцевим полем		**12**	**10**
4	Тема 7. Еліптичні криві над полем R Тема 8. Еліптичні криві над полем Fp	12	10
Змістовий модуль 5. Асиметричні криптосистеми на базі еліптичних кривих		**12**	**10**
5	Тема 9. Розподіл ключів за схемою Діфі-Хелмана Тема 10. Цифровий підпис ECDSA	12	10
	Разом	**56**	**50**

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, обгрунтованість власної позиції, пропозиції щодо розв'язання проблеми, визначення перспектив дослідження	2 бали
3	Дотримання вимог щодо технічного оформлення	1 бал
	Разом	5 балів

Форми проведення модульного контролю та критерії оцінювання

Модульний контроль здійснюється відповідно до навчально-методичної карти дисципліни та перевіряє рівень досягнення результатів навчання студентів. Форма проведення – комп'ютерний тест, що складається 20 запитань закритої та відкритої форм.

Модульна контрольна робота оцінюється у 25 балів.

Форми проведення семестрового контролю та критерії оцінювання

Семестрове (підсумкове) оцінювання здійснюється у формі екзамену, умовою допуску до якого є отриманням студентом 35 балів (з врахуванням 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»

Питання до семестрового контролю

1. Загрози безпеки комп'ютерних мереж і систем.
2. Методи захисту комп'ютерних мереж і систем.
3. Методи захисту від несанкціонованого доступу
4. Задачі технічного захисту інформації
5. Задачі криптографічного захисту інформації
6. Блок-схема симетричної криптосистеми
7. Блок-схема асиметричної криптосистеми
8. Модульна арифметика.
9. Кінцеві структури: групи.
10. Зворотні елементи адитивної групи.
11. Зворотні елементи мультиплікативної групи.
12. Порядок групи і порядок елемента групи.
13. Підгрупи.
14. Генератори групи і підгрупи.
15. Кількість генераторів груп і підгруп.
16. Циклічні і нециклічні групи
17. Кінцеві структури: кільця.
18. Мультиплікативна група кільця.
19. Кінцеві структури: поля.
20. Функція Ейлера.
21. Узагальнена функція Ейлера, що вона визначає.
22. Визначення НОД (a,b) за допомогою алгоритму Евкліда.
23. Мультиплікативна група кільця за модулем N = PQ.
24. Структура МГ кільця за модулем N = PQ.
25. Розподіл ключів по схемі Діффі-Гелмана (над кінцевим полем). Неінтерактивний протокол.
26. Розподіл ключів по схемі Діффі-Гелмана (над кінцевим полем). Інтерактивний протокол.
27. Криптосистема RSA. Функції шифрування-дешифрування.
28. Напрямкові шифрування RSA.
29. Цифровий підпис RSA.
30. Криптосистема Ель-Гамаля. Напрямкове шифрування.
31. Цифровий підпис Ель-Гамаля.

32. Цифровий підпис DSA
33. Цифровий підпис ГОСТ Р34.310
34. Безпека асиметричних КС.
35. Безпека симетричних КС.

Шкала відповідності оцінок

Рейтингова оцінка	Сума балів за всі види навчальної діяльності	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

Навчально-методична карта дисципліни

Разом: 150 год., лекції – 24 год., практичні заняття – 16 год., лабораторні заняття – 16 год., модульний контроль – 8 год., самостійна робота – 56 год., семестровий контроль – 30 год.

Модулі (назви, бали)	**Змістовий модуль 1. Основні поняття і задачі безпеки інформації** (12 балів)	**Змістовий модуль 2. Сучасні симетричні криптосистеми** (81 бал)		**Змістовий модуль 3. Асиметричні криптосистеми на базі кінцевих полів** (81 бал)			**Змістовий модуль 4. Арифметика еліптичних кривих над кінцевим полем** (81 бал)		**Змістовий модуль 5. Асиметричні криптосистеми на базі еліптичних кривих** (81 бал)	
Лекції (теми, бали)	Задачі технічного і криптографічного захисту інформації. Моделі симетричної і асиметричної криптосистем (2 бали)	Блочні шифри. Стандарт DES (1 бал)	Поточні шифри. Генератор Хафмена (1 бал)	Побудова мультиплікативної групи кільця по модулю N = PQ, визначення порядку МГ кільця і максимального порядку елементів МГ. (2 бали)			Параметри в криптосистемі Ель-Гамаля. Вимоги до параметрів. Напрямкове шифрування Ель-Гамаля. Цифровий підпис Ель-Гамаля (3 бали)		Постанова задачі розподілу ключів. Інтерактивна і неінтерактивна схема розподілу ключів Формування і перевірка ЦП за схемою ECDSA. Відомі атаки і безпека ECDSA (3 бали)	
Практичні, лабораторні заняття (теми, бали)		Блочні шифри. Стандарт DES (22 бали)	Поточні шифри. Генератор Хафмена (22 бали)	Побудова мультиплікативної групи кільця по модулю N = PQ (22 бали)	Визначення ключової пари RSA. Секретні і відкриті ключі (11 балів)	Цифровий підпис RSA (11 балів)	Еліптичні криві над полем R (22 бали)	Еліптичні криві над полем Fp (22 бали)	Розподіл ключів за схемою Діфі-Хелмана (22 бали)	Цифровий підпис ECDSA (22 бали)
Самостійна робота	Самостійна робота (10 балів)	Самостійна робота (10 балів)		Самостійна робота (10 балів)			Самостійна робота (10 балів)		Самостійна робота (10 балів)	
Поточний контроль (вид, бали)		Модульна контрольна робота 1 (25 балів)		Модульна контрольна робота 2 (25 балів)			Модульна контрольна робота 3 (25 балів)		Модульна контрольна робота 4 (25 балів)	
Підсумковий контроль (вид, бали)	Екзамен (40 балів)									

8. Рекомендовані джерела

Основна

1. Бессалов А.В., Телиженко А.Б. Криптосистеми на еліптичних кривих. – К.: Вид. «Політехніка», 2004. – 224с.

2. Романець Ю.В., Тимофєєв П.А., Шаньгін В.Ф. Захист інформації у комп'ютерних системах та мережах. – Х.: Радіо та зв'язок, 1999. – 328с.

3. Задірака В.К., Олексюк О.С., Недашковський М.О. Методи захисту фінансової інформації. Навчальний посібник. – К.: Вища школа, 2000. – 460 с

4. Домарев В.В. Захист інформації та безпека комп'ютерних систем. – К.: Видавництво «Діасофт», 1999. – 480с.

5. Іванов М.А. Криптографичні методи захисту інформації у комп'ютерних системах та мережах. – К.:КУДИЦ-ОБРАЗ, 2001 – 368с.