КИЇВСЬКИЙ СТОЛИЧНИЙ УНІВЕРСИТЕТ ІМЕНІ БОРИСА ГРІНЧЕНКА

Факультет інформаційних технологій та математики
Кафедра інформаційної та кібернетичної безпеки
імені професора Володимира Бурячка

«ЗАТВЕРДЖУЮ»
Проректор з наукової роботи
_____ Наталія ВІННІКОВА
«__5__» _____2024 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ПРИКЛАДНІ АСПЕКТИ СТВОРЕННЯ ТА ЗАСТОСУВАННЯ СИСТЕМ КРИПТОГРАФІЧНОГО ЗАХИСТУ

для аспірантів

спеціальності 125 Кібербезпека та захист інформації

освітнього рівня третього (освітньо-наукового)

освітньо-наукової програми «Інформаційна безпека держави»

Київ – 2024

Розробник:

Гулак Геннадій Миколайович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.

Викладач:

Гулак Геннадій Миколайович, доктор технічних наук, професор, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка Факультету інформаційних технологій та математики Київського столичного університету імені Бориса Грінченка.

Робочу програму розглянуто і затверджено на засіданні кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Протокол від 03.01.2024 № 1

Завідувач кафедри _____ Павло СКЛАДАННИЙ
(підпис)

Робочу програму погоджено з гарантом освітньо-наукової програми «Інформаційна безпека держави»

03.01.2024

Гарант освітньо-наукової програми _____ Наталія КОРШУН
(підпис)

Робочу програму перевірено

11.01.2024

Завідувач аспірантури, докторантури _____ Ілона ТРИГУБ
(підпис)

Пролонговано:

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

на 20__/20__ н.р. _____ (_____), «____»____ 20___ р., протокол № ___
(підпис) (ПІБ)

1. Опис навчальної дисципліни

Найменування показників	Характеристика дисципліни	
	денна	заочна
Вид дисципліни	вибіркова	
Мова викладання, навчання та оцінювання	українська	
Загальний обсяг кредитів / годин	3 / 90	
Рік навчання	2	2
Семестр	4	4
Кількість змістових модулів з розподілом:	3	3
Обсяг кредитів	3	3
Обсяг годин, в тому числі:	90	90
Аудиторні	24	12
Самостійна робота	60	78
Модульний контроль	6	
Форма семестрового контролю	залік	залік

2. Мета та завдання навчальної дисципліни

Мета: формування у аспірантів фундаментальних знань теорії та практики забезпечення криптографічного захисту інформації і відповідних професійних компетенцій.

Завдання: вивчення теоретичних положень і практики взаємодії держави, бізнесу, суспільства та людини у сфері криптографічного захисту інформації як умови сталого розвитку суспільства.

У результаті вивчення навчальної дисципліни відповідно до освітньо-наукової програми спеціальності формуються фахові компетентності:

Програмні компетентності	**Код**	**Значення компетентності**
Спеціальні компетентності	СК 1	Здатність оцінювати фізичні, технологічні, інформаційні, соціологічні, етичні та інші процеси інформаційного і кіберпросторів.
	СК 3	Здатність застосовувати сучасні ІТ технології при створенні систем інформаційної та/або кібербезпеки і захисту інформації, електронні інформаційні ресурси, спеціалізоване програмне забезпечення у науковій та навчальній діяльності; здійснювати проєктну діяльність на засадах лідерства.
	СК 5	Здатність робити оцінки та в умовах припущень і обмежень знаходити відповідні рішення щодо систем інформаційної та/або кібербезпеки і захисту інформації.
	СК 6	Здатність до удосконалення, модернізації та уніфікації систем, засобів і технологій забезпечення безпеки ІТ систем та мереж, обробки та перетворення інформації.
	СК 7	Здатність до планування і реалізації заходів із захисту інформації на об'єктах критичної інфраструктури, проведення моніторингу, аудиту та відновлення процесів штатного функціонування ІТ систем та мереж після збоїв та відмов різних класів і походження.

3. Результати навчання за дисципліною.

У результаті вивчення навчальної дисципліни аспірант повинен:

знати:

- задачі, класифікацію, історію, розвідку, концепції і стандарти, моделі та рівні безпеки криптосистем;
- базові математичні поняття і визначення при побудові криптосистем;
- алгоритми найбільш поширених асиметричних криптосистем;
- нормативно-правові документи і закони у сфері КЗІ;

вміти:

- сформулювати задачу безпечного електронного документообігу;
- визначати сутність роботи крипто алгоритму за допомогою простих прикладів;
- оцінювати необхідний за стандартом рівень безпеки криптосистем.

Програмні результати навчання:

Код	Значення програмного результату
РН 4	Забезпечувати неперервність бізнес процесів на базі системи управління інформаційною та/або кібербезпекою, згідно вітчизняних та міжнародних вимог і стандартів; здійснювати професійну діяльність на основі знань сучасних інформаційно-комунікаційних технологій, вміти застосовувати їх як в побуті, так і в професійній діяльності; проводити або керувати проведенням наукових і науково-технічних досліджень з питань захисту інформації, організації й забезпечення інформаційної та/або кібербезпеки ОІД; обґрунтовувати раціональні шляхи щодо захисту інформації на ОІД та інформації, що циркулює в ІТ системах та мережах; використовувати сучасні техніки для проведення досліджень за напрямом захисту інформації, організації й забезпечення безпеки мережевої інфраструктури об'єктів інформаційної діяльності, а також наукових досліджень вищих рівнів, зокрема дотичних міждисциплінарних напрямів.
РН 5	Розробляти та аналізувати проєкти ІКС базуючись на стандартизованих технологіях та протоколах передачі даних; аналізувати та визначати можливість застосування технологій, методів та засобів КТЗІ в ІКС; проєктувати та реалізувати комплексні системи КТЗІ в ІКС відповідно до вимог чинних нормативно-правових документів системи захисту інформації; вирішувати задачі впровадження, супроводу та управління комплексними системами захисту інформації в ІКС, проведення їх експертизи та випробувань; забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту; використовувати для обґрунтування висновків належні докази, наявні літературні дані.
РН 6	Розробляти та впроваджувати науково-дослідницькі та інноваційні проєкти в сфері захисту інформації, інформаційної та кібербезпеки; розробляти алгоритми, моделі, методи та складні програмні комплекси оцінки характеристик і стану систем інформаційної та кібербезпеки; здійснювати захист ресурсів і процесів в ІКС на основі моделей безпеки та встановлених режимів їх безпечного функціонування; забезпечувати процеси захисту інформаційно-комунікаційних систем шляхом встановлення та коректної експлуатації програмних та програмно-апаратних комплексів засобів захисту, виконувати розробку експлуатаційної документації на КЗЗ; забезпечувати функціонування системи управління інформаційною та/або кібербезпекою організації на основі керування інформаційними ризиками з врахуванням можливих конфліктів і катастроф.
РН 7	Вирішувати задачі централізованого і децентралізованого адміністрування доступом до ІР і процесів в ІКС та реалізовувати заходи з протидії отриманню несанкціонованого доступу до них; володіти науково-організаційними основами проведення аудиту безпеки ІКС, а також науковими методами та практичними навичками щодо створення систем моніторингу безпеки в ІТ системах та мережах.

4. Структура навчальної дисципліни

Тематичний план для *денної* форми навчання

Назви теоретичних розділів	Усього	Розподіл годин за видами робіт			
		Аудиторні			
		Лекцій	Практ.	Семін.	Самост. робота
Змістовий модуль І. Базові аспекти безпеки криптосистем					
Тема 1. Стандарти про криптографічний захист	14	2		2	10
Тема 2. Фізико-математичні основи безпеки криптосистем	14	2	2		10
Модульний контроль	2				
Разом за змістовим модулем	28	4	2	2	20
Змістовий модуль ІІ. Криптосистеми спеціального зв'язку					
Тема 3. Криптографічні протоколи комп'ютерних систем	14	2	2		10
Тема 4. Апаратні засоби криптографічного захисту	14	2	2		10
Модульний контроль	2				
Разом за змістовим модулем	28	4	4		20
Змістовий модуль ІІІ. Криптосистеми електронних довірчих послуг					
Тема 5. Математичні моделі асиметричних криптосистем	14	2	2		10
Тема 6. Архітектура електронних довірчих послуг	14	2		2	10
Модульний контроль	2				
Разом за змістовим модулем	28	4	2	2	20
Разом	**90**	**12**	**8**	**4**	**60**

Тематичний план для *заочної* форми навчання

Назви теоретичних розділів	Усього	Розподіл годин за видами робіт			
		Аудиторні			
		Лекцій	Практ.	Семін.	Самост. робота
Змістовий модуль І. Базові аспекти безпеки криптосистем					
Тема 1. Стандарти про криптографічний захист	14				14
Тема 2. Фізико-математичні основи безпеки криптосистем	16	2	2		12
Модульний контроль					
Разом за змістовим модулем	30	2	2		26
Змістовий модуль ІІ. Криптосистеми спеціального зв'язку					
Тема 3. Криптографічні протоколи комп'ютерних систем	16	2	2		12
Тема 4. Апаратні засоби криптографічного захисту	14				14
Модульний контроль	2				
Разом за змістовим модулем	30	2	2		26
Змістовий модуль ІІІ. Криптосистеми електронних довірчих послуг					
Тема 5. Математичні моделі асиметричних криптосистем	14				14
Тема 6. Архітектура електронних довірчих послуг	16	2		2	12
Модульний контроль	2				
Разом за змістовим модулем	30	2		2	26
Разом	**90**	**6**	**4**	**2**	**78**

5. Програма навчальної дисципліни

ЗМІСТОВНИЙ МОДУЛЬ І. Базові аспекти безпеки криптосистем

Тема 1. Стандарти про криптографічний захист

Основні задачі, принципи і поняття криптографії. Рівняння шифрування у загальному вигляді. Конфіденційність, автентифікація, цілісність. Секретний та відкритий ключі. Однобічна функція м стійкість. Схема взаємної недовіри. Стандартизація криптосистем.

Ключові слова: симетрична криптосистема, асиметрична криптосистема, цифровий підпис, розподіл ключів.

Література:

1. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія, практика, застосування : монографія / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Видавництво «Форт», 2012. – 870 с.
2. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації Вінниця: Вид-во ВНТУ, 2011. – 198с.
3. Бессалов А. В., Теліженко А. Б. Криптосистеми на еліптичних кривих: посібник, –К. : ІВЦ «Політехніка», 2004 – 224 с.
4. Про електронні довірчі послуги [Електронний ресурс] : Закон України: // База даних «Законодавство України» / ВР України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#n534

Тема 2. Фізико-математичні основи безпеки криптосистем

Поняття криптографічного та інженерно криптографічного аналіза та спеціальних досліджень. Елементи теорії чисел. Алгоритм Евкліда, функція Ейлера. Алгебраїчні структури: група, кільце, поле. Порядок групи і елемента групи. Збої та відмови шифраторів, помилки операторів. Технічні (фізичні) канали витоку інформації.

Ключові слова: алгоритм Евкліда, функція Ейлера, група, кільце, поле, просте число, модуль.

Література:

1. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія, практика, застосування : монографія / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Видавництво «Форт», 2012. – 870с.
2. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації Вінниця: Вид-во ВНТУ, 2011. – 198с.
3. Гулак Г.М. Моделювання на етапі оцінки безпеки шифраторів конфіденційної інформації / Сучасна спеціальна техніка», 2011. № 1(24). С. 73–81.

ЗМІСТОВНИЙ МОДУЛЬ ІІ. Криптосистеми спеціального зв'язку

Тема 3. Криптографічні протоколи комп'ютерних систем

Історична довідка ECC. Стандартизація ECC. Визначення еліптичної кривої у формі Вейерштраса. Закон додавання точок. Порядок кривої, порядок точки кривої. Межі Хассе порядку кривої над кінцевим полем.

Ключові слова: форма Вейерштраса, закон додавання точок, порядок кривої, порядок точки, межі Хассе.

Література:

1. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації Вінниця: Вид-во ВНТУ, 2011. – 198с.
2. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія, практика, застосування : монографія / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Видавництво «Форт», 2012. – 870с.

3. Бессалов А. В., Теліженко А. Б. Криптосистеми на еліптичних кривих: посібник, –К. : ІВЦ «Політехніка», 2004 – 224 с.

Тема 4. Апаратні засоби криптографічного захисту

Розподіл ключів за схемою Діфі-Хеллмана. Історична довідка. Алгоритм КЕР на еліптичних кривих.

Ключові слова: розділення секретів, інтерактивний протокол.

Література:

1. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації Вінниця: Вид-во ВНТУ, 2011. – 198с.
2. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія, практика, застосування : монографія / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Видавництво «Форт», 2012. – 870с.
3. Гулак Г.М. Моделювання на етапі оцінки безпеки шифраторів конфіденційної інформації / Сучасна спеціальна техніка», 2011. № 1(24). С. 73–81.
4. Сайт ТОВ «Автор». Продукти. [Електронний ресурс] https://avtor.ua/products
5. Сайт ТОВ ІІТ. Користувач центру сертифікації ключів. [Електронний ресурс] https://www.iit.com.ua
6. Сайт ТОВ «Трител». Продукція. [Електронний ресурс] http://www.tritel.ua/index.php/uk/produktsiya

ЗМІСТОВНИЙ МОДУЛЬ ІІІ. Криптосистеми електронних довірчих послуг

Тема 5. Математичні моделі асиметричних криптосистем

Однобічна функція з секретом. Відкритий і секретний ключі. Сертифікат відкритого ключу.

Ключові слова: цифровий підпис, цифровий конверт, атаки на асиметричні криптосистеми, постквантова криптографія, кубіт.

Інтернет-ресурс:

1. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія, практика, застосування : монографія / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Видавництво «Форт», 2012. – 870с.
2. Бессалов А. В., Теліженко А. Б. Криптосистеми на еліптичних кривих: посібник, –К. : ІВЦ «Політехніка», 2004 – 224 с.
3. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації Вінниця: Вид-во ВНТУ, 2011. – 198с.

Тема 6. Архітектура електронних довірчих послуг

Теоретичні, методологічні та практичні аспекти побудови та функціонування системи електронних довірчих послуг

Ключові слова: електронні довірчі послуги, стійкість.

Інтернет-ресурс:

1. Про електронні довірчі послуги [Електронний ресурс] : Закон України: // База даних «Законодавство України» / ВР України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#n534
2. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації Вінниця: Вид-во ВНТУ, 2011. – 198с.
3. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія, практика, застосування : монографія / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Видавництво «Форт», 2012. – 870с.
4. Сайт ТОВ «Автор». Продукти. [Електронний ресурс] https://avtor.ua/products
5. Сайт ТОВ ІІТ. Користувач центру сертифікації ключів. [Електронний ресурс] https://www.iit.com.ua

6.Контроль навчальних досягнень

6.1.1. Система оцінювання навчальних досягнень аспірантів (денна форма)

№ з/п	Вид діяльності аспіранта	Макс. кількість балів за одиницю	Модуль 1		Модуль 2		Модуль 3	
			Кількість одиниць	Максимальна кількість	Кількість одиниць	Максимальна кількість	Кількість одиниць	Максимальна кількість
1	Відвідування лекцій	1	2	2	2	2	2	2
2	Відвідування практичних занять	1	1	1	2	2	1	1
3	Відвідування семінарських занять	1	1	1			1	1
4	Виконання завдань для самостійної роботи	5	2	10	2	10	2	10
5	Робота на практичних заняттях	10	1	10	2	20	1	10
6	Робота на семінарських заняттях	10	1	10			1	10
7	Виконання модульної контрольної роботи	25	1	25	1	25	1	25
Разом				**59**		**59**		**59**
Максимальна кількість балів: **177**								
Розрахунок коефіцієнта: 100/177 = **0.56**								

6.1.1. Система оцінювання навчальних досягнень аспірантів (денна форма)

№ з/п	Вид діяльності аспіранта	Макс. кількість балів за одиницю	Модуль 1		Модуль 2		Модуль 3	
			Кількість одиниць	Максимальна кількість	Кількість одиниць	Максимальна кількість	Кількість одиниць	Максимальна кількість
1	Відвідування лекцій	1	1	1	1	1	1	1
2	Відвідування практичних занять	1	1	1	1	1		
3	Відвідування семінарських занять	1					1	1
4	Виконання завдань для самостійної роботи	5	2	10	2	10	2	10
5	Робота на практичних заняттях	10	1	10	1	10		
6	Робота на семінарських заняттях	10					1	10
7	Виконання модульної контрольної роботи	25						
Разом				**22**		**22**		**22**
Максимальна кількість балів: **66**								
Розрахунок коефіцієнта: 100/66=**1.51**								

Умовою зарахування кожного змістовного модулю та отримання аспірантом заліку є здобуття не менше 35% балів (Бал min / Бал max = 35:100=0,35) за результатами всіх видів означених діяльностей в кожному змістовному модулі.

6.2. Завдання для самостійної роботи та критерії її оцінювання

№ з/п	Назва теми	Кількість годин (денна/ заочна)	Бали
Змістовий модуль І. Базові аспекти безпеки криптосистем			
1	Класифікація криптосистем	10/14	5
2	Канали витоку інформації з криптосистем	10/12	5
Змістовий модуль ІІ. Криптосистеми спеціального зв'язку			
3	Захищені протоколи стеку TCP/IP	10/12	5
4	Класифікація атак на симетричні криптосистеми	10/14	5
Змістовий модуль ІІІ. Криптосистеми електронних довірчих послуг			
5	Класифікація атак на схеми електронного підпису	10/14	5
6	Стандарти електронного підпису	10/12	5
	Разом	60/78	30

Критерії оцінювання самостійної роботи

№ 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 аспіранта на практичних заняттях, за виконання домашніх завдань, за модульну контрольну роботу. Модульний контроль знань аспіранта здійснюється після завершення вивчення навчального матеріалу модуля. Форма проведення – комп'ютерний тест, що складається з 20 питань закритої та відкритої форм. Модульна контрольна робота оцінюється у 25 балів. Критерії оцінювання модульного контролю наведено у таблиці.

Критерії оцінювання модульного контролю

Сума балів	Значення оцінки
22-25	аспірант виявив повне знання програмного матеріалу, успішно виконує передбачені програмою завдання, засвоїв основну літературу рекомендовану програмою, виявив систематичний характер знань з дисципліни і здатний до самостійного доповнення
13-21	аспірант виявив знання основного програмного матеріалу в обсязі, необхідному для подальшого навчання та майбутньої роботи за професією, вміє виконувати завдання, передбачені програмою, знайомий з основною рекомендованою літературою
0-13	аспірант, що виявив часткове знання основного програмового матеріалу, не завжди вміє виконувати завдання, передбачені програмою, знайомий лише частково з основною рекомендованою літературою.

6.4. Форми проведення семестрового контролю

Семестровий контроль проводиться у вигляді заліку за результатами поточної успішності з усіх змістових модулів дисципліни «Прикладні аспекти створення та застосування систем криптографічного захисту». Підсумкова семестрова (залікова) рейтингова оцінка аспіранта є сумою підсумкових фактичних оцінок аспіранта за змістовими модулями.

6.5. Оцінювання освітніх досягнень аспірантів за системою ECTS

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

7. Рекомендовані джерела

Основна (базова) література:

1. Гулак Г.М., Мухачов В.А., Хорошко В.О., Яремчук Ю.Є. Основи криптографічного захисту інформації Вінниця: Вид-во ВНТУ, 2011. – 198с.
2. Горбенко І. Д., Горбенко Ю. І. Прикладна криптологія. Теорія, практика, застосування : монографія / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Видавництво «Форт», 2012. – 870с.
4. Бессалов А. В., Теліженко А. Б. Криптосистеми на еліптичних кривих: посібник, –К. : ІВЦ «Політехніка», 2004 – 224 с.
5. Гулак Г.М. Моделювання на етапі оцінки безпеки шифраторів конфіденційної інформації / Сучасна спеціальна техніка», 2011. № 1(24). С. 73–81.
6. Про електронні довірчі послуги [Електронний ресурс] : Закон України: // База даних «Законодавство України» / ВР України. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2155-19#n534

Додаткова література:

1. Державний стандарт України ДСТУ ISO/IEC 14888-1:2014. Інформаційні технології. МЕТОДИ ЗАХИСТУ. ЦИФРОВІ ПІДПИСИ З ДОПОВНЕННЯМ. Частина 1. Загальні положення. 2014.
2. Державний стандарт України ДСТУ ISO/IEC 14888-3:2014. Інформаційні технології. МЕТОДИ ЗАХИСТУ. ЦИФРОВІ ПІДПИСИ З ДОПОВНЕННЯМ. Частина 3. Механізми, що грунтуються на дискретному логарифмі. 2014.
3. Blahut R. E. Cryptography and Secure Communication. Cambridge University Press, 2014.
4. Handbook of elliptic and hyperelliptic curve cryptography / Scientific editors, Henri Cohen & Gerard Frey ; authors, Roberto M Avanzi Roberto Avanzi, Christophe Doche, Tanja Lange, Kim Nguyen, and Frederik Vercauteren. Chapman & Hall/CRC, Taylor & Francis Group, London, New York, Singapur, 2006.
7. Koblitz N. Introduction to elliptic curves and modular forms. - Springer Science & Business Media, 2012.
5. Washington L. C.. Elliptic Curvres. Number Theory and Cryptography. Second Edition. CRC Press, 2008.