КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА
ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ
Кафедра прикладної статистики

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи
_____ Кашпур О.Ф.
«28» ____08_____ 2020 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
«Математичні моделі страхування та асиметрична криптографія»
Модуль 2. «Асиметрична криптографія та криптосистеми з відкритим ключем»

для студентів

галузь знань	**12 «Інформаційні технології»**
спеціальність	**124 «Системний аналіз»**
освітній рівень	**бакалавр**
освітня програма	**«Системний аналіз»**
вид дисципліни	**вибіркова**

Форма навчання	**денна**
Навчальний рік	**2022/2023**
Семестр	**8**
Кількість кредитів ECTS	**2**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**іспит**

Викладачі: **член-кор. НАН України, доктор фіз.-мат.наук Савчук М.М.**

Пролонговано: на 20__/20__ н.р. _____(_____) «__»____20__р.

на 20__/20__ н.р. _____(_____) «__»____20__р.

КИЇВ – 2020

Розробник: Савчук Михайло Миколайович, член-кор. НАН України, доктор фіз.-мат. наук, професор кафедри Прикладної Статистики

ЗАТВЕРДЖЕНО
Завідувач кафедри Прикладної Статистики

_____ (Лебєдєв Є.О.)

Протокол № 1 від «27» серпня 2020 р.

Схвалено Гарантом освітньо-професійної програми першого рівня вищої освіти

«Системний аналіз» _____ М.М. Шарапов

«28» серпня 2020 року

Схвалено науково-методичною комісією факультету комп'ютерних наук та кібернетики

Протокол від «28» серпня 2020 року № 1

Голова науково-методичної комісії _____ **(Омельчук Л.Л.)**
(підпис) (прізвище та ініціали)

«28» серпня 2020 року

1 Мета дисципліни – одержання студентами базових знань в галузі криптографії з відкритими ключами, в теорії складності функцій та алгоритмів, в методах побудови важкооборотних функцій та їх застосувань для побудови асиметричних криптосистем, освоєння методів побудови різноманітних криптографічних протоколи, зокрема, протоколів автентифікації, цифрового підпису тощо.

2 Попередні вимоги до опанування або вибору навчальної дисципліни

знати: базові поняття математичного аналізу, дискретної математики, лінійної та загальної алгебри, теорії чисел, теорії ймовірностей, математичної теорії інформації, теорії алгоритмів, теорії складності обчислень, основні поняття симетричної криптографії.

вміти: програмувати на мові високого рівня, вміти розробляти математичні моделі інформаційних процесів та алгоритмів.

володіти елементарними навичками: розв'язування задач дискретної математики, математичного аналізу, теорії ймовірностей та математичної статистики, лінійної алгебри, теорії інформації та кодування, теорії чисел, теорії скінченних полів.

3 Анотація навчальної дисципліни

Дисципліна «Асиметрична криптографія і криптосистеми з відкритим ключем» є складовою частиною циклу професійної підготовки фахівців за першим (бакалаврським) освітньо-кваліфікаційним рівнем галузі знань 12 Інформаційні технології за спеціальністю 124 «Системний аналіз» освітньо-професійної програми «Системний аналіз»; вона включає вивчення теоретичних основ криптографії з відкритим ключем, асиметричних систем шифрування, основних алгоритмів та схем систем цифрового підпису, автентифікації, різноманітних криптографічних протоколів, способів їх застосування у системах захисту інформації в різних сферах, де використовуються інформаційні технології.

Викладається у 8-му семестрі, обсяг 60 год. (2 кредити ECTS), з них лекції – 20 год.., самостійна робота – 40 год. Передбачено 2 змістовні частини та іспит.

4 Завдання (навчальні цілі)

набуття знань, умінь та навичок (компетентностей) відповідно до освітньої кваліфікації бакалавра з системного аналізу. Зокрема, розвивати:

- **К18.** Здатність формалізувати проблеми, описані природною мовою, у тому числі за допомогою математичних методів, застосовувати загальні підходи до математичного моделювання конкретних процесів, в тому числі, в інформаційних системах.
- **ФКСАС 1.** Здатність проводити факторний аналіз на предмет виявлення як детермінованих так і стохастичних слабких та сильних чинників у процесах різної природи; здатність встановлювати зв'язки між виявленими факторами.
- **ФКСАС 2.** Здатність проводити аналітично обґрунтоване планування експериментів і спостережень, здійснювати статистичний аналіз отриманих результатів та коректно їх інтерпретувати

5 Результати навчання за дисципліною

Результат навчання (РН) **(1 – знати; 2 – вміти; 3. комунікація; 4. автономність та відповідальність)**		**Форми викладання та навчання**	**Методи оцінювання**	**Відсоток у підсумковій оцінці з дисципліни**
Код	**Результат навчання**			
РН.1	Знати і розуміти методи і способи побудови криптографічних систем з		Поточне оцінювання	45

	відкритим ключем, основні алгоритми, протоколи і стандарти асиметричної криптографії	Лекції, самостійна робота	(ПО), іспит, контрольні роботи	
РН.2	Вміти розраховувати та застосовувати важкооборотні функції при побудови асиметричних криптосистем, володіти методами побудови і застосування різних асиметричних криптографічних протоколів і алгоритмів			
РН.3	Виявляти здатність до самонавчання та продовження професійного розвитку	Самостійна робота	ПО, іспит	45
РН.3.1	Уміти організувати власну діяльність та одержувати результат у рамках обмеженого часу	Самостійна робота	ПО, іспит	5
РН.4	Демонструвати навички взаємодії з іншими людьми, уміння працювати в командах	Самостійна робота	ПО, іспит	5

6 Співвідношення результатів навчання дисципліни з програмними результатами навчання

Результати навчання дисципліни **Програмні результати навчання**	**РН.1**	**РН.2**	**РН.3**	**РН.3.1**	**РН.4**
(з опису освітньої програми)					
ПР03. Вміти визначати ймовірнісні розподіли стохастичних показників та факторів, що впливають на характеристики досліджуваних процесів, досліджувати властивості та знаходити характеристики багатовимірних випадкових векторів та використовувати їх для розв'язання прикладних задач, формалізувати стохастичні показники та фактори у вигляді випадкових величин, векторів, процесів.	+	+			
ПР15. Розуміти українську та іноземну мови на рівні, достатньому для обробки фахових інформаційнолітературних джерел, професійного усного і письмового спілкування, написання текстів за фаховою тематикою.	+	+	+	+	+
ПРСАС 1. Проводити статистичне оцінювання невизначених параметрів розподілів стохастичних факторів досліджуваних процесів, формалізувати стохастичні фактори у вигляді випадкових величин, векторів, процесів.	+	+			

7 Схема формування оцінки

7.1 Форми оцінювання студентів:

- семестрове оцінювання:

1. Контрольна робота 1 (РН.1, РН.2): 20/12 балів
2. Контрольна робота 2 (РН.1, РН.2): 20/12 балів
3. Поточне оцінювання (РН.1, РН.2 РН..3, РН.3.1, РН.4): 20/12 балів

- підсумкове оцінювання (у формі іспиту):

- максимальна кількість балів які можуть бути отримані студентом: 40;
- результати навчання, які оцінюються: РН.1, РН.2, РН.3, РН.3.1, РН.4.
- форма проведення: письмова - види завдань: теоретичні питання (40%), задачі (60%).

Студент допускається до екзамену, якщо в семестрі набрав не менше ніж 36 балів. Для отримання загальної позитивної оцінки з дисципліни оцінка за екзамен має бути не менше 24 балів.

7.2. Організація оцінювання.

Терміни проведення форм оцінювання:

1. Контрольна робота 1: після лекції №5.
2. Контрольна робота 2: після лекції №10.

За відсутності студента з поважних причин перездача іспит здійснюється відповідно до «Положення про порядок оцінювання знань студентів при кредитно-модульній системі організації навчального процесу» від 1 жовтня 2010 року.

7.3. Шкала відповідності оцінок

Відмінно / Excellent	90-100
Добре / Good	75-89
Задовільно / Satisfactory	60-74
Незадовільно / Fail	0-59

СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ

№ п/п	Назва лекції	Кількість годин		
		лекції	семінари	С/Р
	Частина 1 **Односторонні функції. Основні схеми асиметричної криптографії**			
1	Поняття односторонньої (важкооборотної) функції Одностороння функція дискретного піднесення до степеня. Оцінки складності обчислення і обернення. Схема Діффі і Хеллмана розподілу ключів по відкритим каналам.	2		1
2	Визначення односторонніх функцій з секретом. Одностороння функція з секретом RSA. Побудова криптосистеми RSA. Алгоритми зашифрування і розшифрування. Обгрунтування коректності та стійкості.	2		2
3	Цілі і задачі цифрового підпису. Цифровий підпис в схемі RSA (без використання хеш-функції). Побудова системи цифрового підпису, алгоримів формування та перевірки цифрового підпису.	2		*2*
4	Система Мессі-Омури передачі шифрованого повідомлення. Система шифрування Ель-Гамаля. Побудова криптосистем, обгрунтування коректності і стійкості. Цифровий підпис Ель-Гамаля (без хеш-функції).	2		2
5	Базові поняття теорії складності алгоритмів. Визначення односторонньої функції в рамках теорії складності. Обмеження на застосування криптографічних алгоритмів асиметричної криптографії.	1		2
	Контрольна робота 1	1		1

	Частина 2 **Хеш-функції. Одностороння функція Рабіна. Асиметричні криптографічні протоколи**			
6	Визначення хеш-функцій в криптографії. Характеристики відомих хеш-функцій. Цифрові підписи RSA і Ель-Гамаля з хеш-функцією. Атаки на цифровий підпис з побудовою колізій.	2		1
7	Алгоритми обчислення квадратних коренів по простому модулю і модулю *n*, рівному добутку двох нерівних простих чисел $p \neq q$. Одностороння функція з секретом Рабіна. Системи шифрування і цифрового підпису Рабіна.	2		1
8	Протоколи доведення без розголошення. Протоколи розподілу секретів. Протоколи генерування випадкових біт. Сліпий цифровий підпис на основі RSA. Протоколи електронної готівки.	2		2
9	Ідентифікація та автентифікація. Принципи автентифікації. Криптографічні протоколи автентифікації.	2		2
10	Криптосистеми на еліптичних кривих. Алгоритми Діффі-Хеллмана та Ель-Гамаля на на еліптичних кривих. Основні принципи побудови квантових криптографічних систем. Квантовий протокол BB84.	1		2
	Контрольна робота	1		2
	ВСЬОГО	**20**		**40**

Загальний обсяг **60** *год.*[1], в тому числі:
Лекцій **–20** *год.*
Самостійна робота – **40** *год.*

Перелік питань для підготовки до контрольних робіт

1. Проблема розподілу ключів та інші труднощі, що виникли в симетричній криптографії у 2-ій половині XX століття. Поняття односторонньої (важкооборотної) функції. Приклади обчислювально односторонніх функцій в симетричній криптографії. Визначення односторонніх функцій. Одностороння функція дискретного піднесення до степеня. Оцінки складності обчислення і обернення.
2. Схема Діффі і Хеллмана розподілу ключів по відкритим каналам. Вибір параметрів, побудова алгоритму, обгрунтування стійкості. Атака «противник посередині».
3. Визначення односторонніх функцій з секретом. Одностороння функція з секретом RSA. Властивості, оцінки складності обчислення. Обернена функція для функції RSA, оцінки складності обчислення при відомому і невідомому секреті. Концепція криптосистем з відкритим ключем.
4. Побудова криптосистеми RSA. Алгоритми зашифрування і розшифрування. Обгрунтування коректності та стійкості RSA. Обчислення оберненої функції при відомому секреті. Сертифікація відкритих ключів.

1

5. Цілі і задачі цифрового підпису. Цифровий підпис в схемі RSA (без використання хеш-функції). Побудова системи цифрового підпису, алгоримів формування та перевірки цифрового підпису. Обгрунтування коректності та стійкості цифрового підпису RSA.
6. Безпечне збереження паролів з використанням односторонньої функції. Система Мессі-Омури передачі шифрованого повідомлення. Система шифрування Ель-Гамаля. Побудова криптосистем, обгрунтування коректності і стійкості.
7. Цифровий підпис Ель-Гамаля (без хеш-функції). Побудова системи цифрового підпису, алгоритмів формування і перевірки цифрового підпису. Обгрунтування коректності і стійкості. Атака на цифровий підпис Ель-Гамаля при повторі разового ключа. Центри сертифікації ключів.
8. Поняття алгоритму. Визначення часової і ємнісної складності алгоритмів. Визначення полиномиальної, експоненційної і субекспотенціальной складності. Класи P і NP, NP-повні задачі. Проблема співвідношення класів P і NP, значення для криптографії її можливих рішень. Визначення односторонньої функції в рамках теорії складності. Обмеження на застосування криптографічних алгоритмів асиметричної криптографії.
9. Недоліки цифрового підпису без хеш-функцій. Мультиплікативна та інші атаки на цифровий підпис RSA без хеш-функцій.
10. Області застосування хеш-функцій. Визначення хеш-функцій в криптографії. Слабкі і сильні односторонні хеш-функції. Цифрові підписи RSA і Ель-Гамаля з хеш-функцією.
11. Атаки на цифровий підпис за допомогою побудови колізій. Імовірнісні моделі пошуку колізій. Оцінки ймовірностей колізій і трудомісткості атак. Загальні схеми побудови хеш-функцій. Характеристики відомих хеш-функцій.
12. Алгоритми обчислення квадратних коренів по простому модулю і модулю n, рівному добутку двох нерівних простих чисел $p \neq q$. Поліноміальне зведення задачі факторизації числа $n=pq$, $p \neq q$ прості числа, і задачі знаходження квадратних коренів по модулю n (при невідомих p і q).
13. Одностороння функція з секретом Рабіна. Властивості, алгоритми обернення при відомому секреті, оцінки складності. Обгрунтування стійкості. Системи шифрування Рабіна. Атаки на різні системи шифрування Рабіна з вибраним шифротекстом.
14. Цифровий підпис Рабіна. Побудова системи, алгоритмів формування і перевірки цифрового підпису. Обгрунтування коректності, оцінки складності.
15. Протоколи доведення без розголошення на основі односторонньої функції Рабіна. Атаки на протоколи. Протоколи генерування випадкових біт (схема Блюма-Мікалі).
16. Протоколи розподілу секретів.
17. Сліпий цифровий підпис на основі RSA. Протоколи електронної готівки. Невидимий цифровий підпис.
18. Ідентифікація та автентифікація. Сфери, процедури використання. Принципи автентифікації. Криптографічні протоколи парольної автентифікації. Автентифікація на основі асиметричних та симетричних алгоритмів шифрування. Автентифікації з протоколом доведення без розголошення.
19. Квантова криптографія. Основні принципи побудови квантових криптографічних систем. Квантовий протокол BB84, труднощі у реалізації і використанні. Про квантовий комп'ютер і стійкість криптографічних алгоритмів в постквантовій моделі обчислень.

20. Криптосистеми на еліптичних кривих Задача дискретного логарифму в термінах ЕК. . Алгоритм Діффі-Хеллмана на ЕК. Побудова алгоритму шифрування Ель-Гамаля на еліптичних кривих. Алгоритм представлення повідомлення (блоку ВТ) як точки ЕК.

9. Рекомендовані джерела

1. Бессалов А.В., Телиженко А.Б. Криптосистемы на эллиптических кривых : Учеб. Пособие. – К.: ІВЦ „Видавництво „Політехніка”", 2004. – 224с.
2. Богуш В.М., Кривуца В.Г., Кудін А.М. Інформаційна безпека. Термінологічний навчальний довідник. – К.: 2004. – 508м с.
3. Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. - М.: МЦНМО, 2003. – 328с.
4. Вербіцький О.В. Вступ до криптології. – Львів: Науково-технічна література, 1998. – 248с.
5. Диффи У., Хеллман М. Защищенность и имитостойкость. // ТИИЭР. – 1979. – Т.67, №3. – С.71-109.
6. Задірака В.К., Олексюк О.С. Комп”ютерна криптологія. – К.: 2002. – 504 с.
7. Кузнецов Г.В., Фомичев В.В., Сушко С.О. Фомичова Л.Я. Математичні основи криптографії. – Дніпропетровськ: Національний гірничій університет, 2004. – Ч.1. – 391 с.
8. Кузьминов Т.В. Криптографические методы защиты информации. - Новосибирск: Наука. Сиб. предприятие РАН, 1998. – 194с.
9. Мао, Венбо. Современная криптография: теория и практика.: Пер. с англ. – М.: Издательский дом «Вильямс», 2005. – 768с.
10. Месси Дж.Л. Введение в современную криптологию. // ТИИЭР. – 1988. – Т.76, №5. – С.24-42.
11. Симмонс Г.Дж. Обзор методов аутентификации информации. // ТИИЭР. – 1988. – Т.76, №5. – С.105-125.
12. Тилборг Ван Х.К.А. Основы криптологии. Профессиональное руководство и интерактивный учебник. - М.: Мир, 2006. – 471с.
13. Чмора А.Л. Современная прикладная криптография. - М.: Гелиос АРВ, 2001. – 256с.
14. Шнайер Б. Прикладная криптографія: протоколы, алгоритмы и исходные коды на языке С, 2 юбил. изд.. – СпБ : ООО «Альфа книга», 2017. - 1040 с.
15. Ященко В.В. (ред.) Введение в криптографию – М.: МЦНМО: «ЧеРо», 1999. – 272с.
16. Menezes A., P. van Oorschot, S.Vanstone. Handbook of Applied Cryptography. – CRC Press, 1997. – 780 p.