КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

Механіко-математичний факультет
(назва факультету, інституту, центру, коледжу)

Кафедра алгебри та математичної логіки

«ЗАТВЕРДЖУЮ»
Заступник декана/директора
з навчальної роботи
_____ О.М.
«___» _____ 2021 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

Математичні основи захисту інформації

(повна назва навчальної дисципліни)

для студентів

галузь знань 11 математика та статистика
(шифр і назва)

спеціальність 111 математика
(шифр і назва спеціальності)

освітній рівень магістр
(молодший бакалавр, бакалавр, магістр)

освітня програма актуарна та фінансова математика
(назва освітньої програми)

вид дисципліни обов'язкова

Форма навчання	денна
Навчальний рік	2021/2022
Семестр	1
Кількість кредитів ECTS	4
Мова викладання, навчання та оцінювання	українська
Форма заключного контролю	залік

Викладачі: доцент Є. А. Кочубінська

Пролонговано: на 20__/20__ н.р. _____(_____)_ «___»_____20__р.
(підпис, ПІБ, дата)

на 20__/20__ н.р. _____(_____)_ «___»_____20__р.
(підпис, ПІБ, дата)

КИЇВ – 2021

Розробник: Кочубінська Є.А., к.ф.-м. н., доцент кафедри алгебри та математичної логіки

Робоча програма дисципліни «Математичні основи захисту інформації»
затверджена на засіданні кафедри алгебри та математичної логіки

ЗАТВЕДЖЕНО
Зав. кафедри алгебри і комп'ютерної математки
_____ Петравчук А.П.,
(підпис)
Протокол № 1 від 11.08 2020 р.

Схвалено науково-методичною комісією механіко-математичного факультету

Протокол № 1 від «31» серпня 2021 року

Голова науково-методичної комісії _____ (Олійник А.С.)
(підпис) (прізвище та ініціали)
«31» 08 2021 року

1. Мета дисципліни – ознайомлення та оволодіння базовими засадами сучасних методів захисту інформації. Завданням дисципліни є підготовка студентів до самостійного вивчення відповідної науково-технічної літератури та використання набутих знань та навичок у практичній роботі.

2. Попередні вимоги до опанування або вибору навчальної дисципліни

1. *Знати* основні поняття, факти і теореми лінійної алгебри, алгебри і теорії чисел, дискретноъ математика, математичного аналізу.

2. *Вміти* активно використовувати та творчо застосовувати зазначені вище знання в процесі опрацювання матеріалу курсу «Математичні основи захисту інформації».

3. *Володіти елементарними навичками* роботи з групами, скінченними полями, ідеалами, фактор-кільцями, вміти проводити обчислення в скінченних полях.

3. Анотація навчальної дисципліни. В курсі «Математичні основи захисту інформації» висвітлюються базові відомості, поняття, факти сучасних математичних методів захисту інформації. Зокрема, розглядаються: основні задачі сучасної криптографії, поняття складності алгоритму, поняття симетричних та асиметричних криптосистем, задачі факторизації криптосистема RSA, задача дискретного логарифмування та криптосистеми, що на ній базуються, протоколи обміну ключами, поняття цифрового підпису та його різновидів, базові засади криптографії з використанням ідентифікаційних даних, ідея квантових обчислень, швидкі квантові алгоритми базові положення некомутативної криптографії, базові положення гомоморфного шифрування, сучасні симетричні криптосистеми DES та AES.

4. Завдання (навчальні цілі). Досягнення складової *інтегральної компетентності* – здатності розв'язувати складні задачі та практичні проблеми у профільній діяльності, пов'язаній з математичними основами захисту інформації.

Досягнення основних *загальних компетентностей*, зокрема, здатностей: 1) Здатність учитися, здобувати нові знання, уміння, у тому числі в галузях, відмінних від математики (ЗК–1); 2) Здатність використовувати у професійній діяльності знання з галузей математичних, природничих, соціально-гуманітарних та економічних наук (ЗК-2); 3) Здатність вирішувати проблеми у професійній діяльності на основі абстрактного мислення, аналізу, синтезу та прогнозу (ЗК-3); 4) Здатність до пошуку, оброблення й аналізу інформації з різних джерел, необхідної для розв'язування наукових і професійних завдань (ЗК-4); 5) Здатність генерувати нові ідеї (ЗК–5); 6) Здатність спілкуватися державною мовою і усно, і письмово (ЗК-8); 7) Здатність спілкуватися іноземною мовою (ЗК-9); 8) Здатність грамотно будувати комунікацію, виходячи з мети і ситуації спілкування (ЗК-10); 9) Здатність критично оцінювати та переосмислювати власний і чужий досвід, аналізувати свою професійну й соціальну діяльність (ЗК-11).

Досягнення основних *спеціальних компетентностей*: 1) Знання на рівні новітніх досягнень, необхідні для дослідницької та/або інноваційної діяльності у сфері математики та її практичних застосувань (ФК-1); 2) Спроможність розуміти проблеми та виділяти їхні суттєві риси (ФК-4); 3) Спроможність розробляти математичну модель ситуації з реального світу та переносити математичні знання у нематематичні контексти (ФК-5); 4) Здатність доводити знання та власні висновки до фахівців та нефахівців (ФК-6); 5) Здатність до розвитку нових та удосконалення існуючих математичних методів аналізу, моделювання, прогнозування, розв'язування нових проблем у нових галузях знань (ФК-8).

5. Результат навчання за дисципліною. **Табл.1**

Результат навчання (1. знати; 2. вміти; 3. комунікація; 4. автономність та відповідальність)		Форми (та/або методи і технології) викладання і навчання	Методи оцінювання та пороговий критерій оцінювання за необхідності	Відсоток у підсумковій оцінці з дисципліни
Код	**Результат навчання**			
1.	**Студент повинен знати:**	лекційні заняття, самостійна робота	Письмові модульні контрольні роботи, оцінювання роботи під час лекцій, оцінювання виконання завдань для самостійної роботи, опитування під час практичних занять	До 50%
1.1	Знати основні задачі сучасної криптографії. Знати означення хеш-функції. Знати означення цифрового підпису та його різновидів.			5%
1.2	Знати формулювання задачі факторизації та основні методи її розв'язання. Знайти загальну схему криптосистеми RSA та цифрового підпису на основі RSA.			10%
1.3	Знати формулювання задачі дискретного формулювання та основні методи її розв'язання, знати формулювання задачі Діффі-Хелмана. Знати загальні схеми шифрування та обчислення цифрового підпису у скінченній циклічній групи. Знати загальну схему алгоритму шифрування Ель Гамаля, алгоритму Діффі-Хелмана вироблення спільного таємного ключа.			10%
1.4	Знати означення білінійного парного відображення. Знати формулювання білінійної задачі			10%

	Діффі-Хелмана. Знати приклади застосувань. Знати базові ідеї шифрування з використанням ідентицікаційних даних. Знати поняття короткого цифрового підпису.			
1.5	Знати опис алгоритму Шора знаходження дискретного логарифма. Знати формулювання задачі пошуку спряженого елемента.			10%
1.6	Знати означення гомоморфної криптосистеми. Знати приклади застосувань.			5%
2.	**Студент повинен уміти:**	лекційні заняття, самостійна робота, практичні заняття	Письмові модульні контрольні роботи, оцінювання роботи під час лекцій, оцінювання виконання завдань для самостійної роботи	До 35%
2.1	Вміти застосовувати методи Ферма, Полларда до задач факторизації.		перевірка індивідуальних завдань, самостійна аудиторна робота, модульна контрольна робота	10%
2.2	Вміти застосовувати криптографічні примітиви RSA: зашифрування та розшифрування повідомлень, обчислення та перевірка цифрового підпису.		перевірка індивідуальних завдань, самостійна аудиторна робота, модульна контрольна робота	10%
2.3	Вміти обчислювати дискретний логарифм за допомогою методів Шенкса та Полларда.		перевірка індивідуальних завдань, самостійна аудиторна робота, модульна контрольна робота	10%
2.4	Вміти обчислювати спільний таємний ключ за допомогою алгоритму Діффі-Хеллмана в		перевірка індивідуальних завдань, самостійна аудиторна ро-	5%

	різних скінченних циклічних групах.		бота	
3.	**Комунікація**	лекційні заняття, самостійна робота		до 5%
3.1	Здатність грамотно будувати комунікацію, виходячи з мети і ситуації спілкування			
4.	**автономність та відповідальність**	лекційні заняття, самостійна робота	Письмові модульні контрольні роботи, оцінювання роботи під час лекцій, оцінювання виконання завдань для самостійної роботи	до 10%
4.1	продемонструвати розуміння особистої/персональної відповідальності за професійні та/або управлінські рішення, які базуються на використанні математичних методів			

6. Співвідношення результатів навчання дисципліни з програмними результатами

Табл.2

Результати навчання (код) / **Програмні результати навчання**	**1.1**	**1.2**	**1.3**	**1.4**	**1.5**	**1.6**	**2.1**	**2.2**	**2.3**	**2.4**	**3.1**	**4.1**
Знання												
Знати та розуміти фундаментальні і прикладні аспекти наук у сфері математики й актуарної та фінансової математики (ПРН-З-1)	+	+	+	+	+	+	+	+	+	+		
Відтворювати знання фундаментальних розділів математики й актуарної та фінансової математики в обсязі, необхідному для володіння математичним та економічним апаратами відповідної галузі знань і використання математичних та економічних методів у обраній професії (ПРН-З-2)	+	+	+	+	+	+	+	+	+	+		
Володіти основами математичних дисциплін і економічних теорій, зокрема які вивчають моделі природничих і соціальних процесів (ПРН-З-3)	+	+	+	+	+	+	+	+	+	+		
Уміння												
Уміти використовувати фундаментальні математичні закономірності та закономі-	+	+	+	+	+	+	+	+	+	+		

рності актуарної та фінансової математики у професійній діяльності (ПРН-У-1)												
Читати і розуміти фундаментальні розділи математичної та економічної літератури та демонструвати майстерність їх відтворення в аргументованій усній та/або письмовій доповіді (ПРН-У-2)	+	+	+	+	+	+	+	+	+	+		
Доносити професійні знання, власні обґрунтування і висновки до фахівців і широкого загалу (ПРН-У-3)											+	+
Бути наполегливим у досягненні мети під час вирішення математичної проблеми (ПРН-У-8)	+	+	+	+	+	+	+	+	+	+		
Усно й письмово спілкуватися рідною та англійською мовами в науковій, виробничій та соціально-суспільній сферах діяльності із професійних питань; читати спеціальну літературу; знаходити, аналізувати та використовувати інформацію з різних довідкових джерел (ПРН-У-10)	+	+	+	+	+	+	+	+	+	+	+	
Використовувати раціональні способи пошуку та використання науково-технічної інформації, включаючи засоби електронних інформаційних мереж; застосовувати інформаційні ресурси, у тому числі електронні, для пошуку відповідних математичних моделей (ПРН-У-11)	+	+	+	+	+	+	+	+	+	+		

7. Схема формування оцінки

7.1 Форми оцінювання студентів:

рівень досягнення всіх запланованих результатів навчання визначається за результатами написання письмових контрольних робіт, виконання самостійної роботи і за результатами аудиторної роботи. Вклад результатів навчання у підсумкову оцінку, за умови їх опанування на належному рівні і успішної завдань самостійної роботи наступний:

- результати навчання 1.1 – 1.6 [**знання**] до 50 %;
- результат навчання 2.1 – 2.4 [**вміння**] – до 35%;
- результат навчання 3.1 [**комунікація**] – до 5%;
- результат навчання 4.1 [**автономність та відповідальність**] – до 10%.

- **семестрове оцінювання**: контроль здійснюється за таким принципом. У змістовий модуль 1 (ЗМ1) входять теми 1-3, у змістовий модуль 2 (ЗМ2) входять теми 4,5. Протягом семестру після завершення відповідних тем, проводиться письмова модульна контрольна робота. Для визначення рівня досягнення результатів навчання завдання для модульної контрольної роботи перевіряють уміння оперувати набутими знаннями і вміннями, застосовувати їх для розв'язування конкретних математичних задач. Також під час семестру оцінюється самостійна робота студентів та робота в аудиторії.
- **підсумкове оцінювання (у формі іспиту/заліку):** форма іспиту – письмова. Екзаменаційний білет іспиту складається із 8 завдань, 1-4 з яких є теоретичними, 5-8 – задачі. Завдання 1-4 оцінюються в 4 бали кожне, питання 5-8 оцінюються в 6 балів кожне. Всього за іспит можна отримати від 0 до 40 балів. Умовою досягнення

позитивної оцінки за дисципліну є отримання не менш ніж 60 балів, при цьому оцінка за іспит не може бути меншою 24 балів.

- **умови допуску до підсумкового іспиту:** умовою допуску до іспиту є отримання студентом сумарно не менше, аніж *критично-розрахунковий мінімум 36 балів* за семестр. Студенти, які протягом семестру набрали сумарно меншу кількість балів, ніж критично-розрахунковий мінімум 36 балів, для одержання допуску до іспиту обов'язково повинні написати на необхідну порогову кількість балів додаткову контрольну роботу за матеріалом відповідного семестру та доскладають домашні завдання для підвищення балів за виконання самостійної роботи.

У випадку відсутності студента з поважних причин відпрацювання та перездачі модульних контрольних робіт здійснюються у відповідності до „Положення про порядок оцінювання знань студентів при кредитно-модульній системі організації навчального процесу" від 1 жовтня 2010 року.

7.2. Організація оцінювання (*обов'язково зазначається порядок організації передбачених робочою навчальною програмою форм оцінювання із зазначенням орієнтованого графіку оцінювання*):

Оцінювання за формами контролю:

Вид оцінювання	***ЗМ 1***		***ЗМ 2***	
	Міп. – _ балів	*Мах. – __ балів*	*Міп. – _ балів*	*Мах. – __ балів*
Активність на заняттях і виконання позааудиторної самостійної роботи	3	5	9	15
Модульна контрольна робота	24	40		

Орієнтований графік оцінювання:

	Орієнтовний період для здійснення відповідної форма оцінювання
Модульна контрольна робота 1	Листопад
Активність студента на заняттях і виконання ним самостійної роботи	Жовтень- листопад
Добір балів/додаткова контрольна робота/доскладання домашніх завдань	Грудень
Іспит	друга половина грудня

Розрахунок балів, які студент отримує при успішній здачі іспиту:

	Змістовий модуль 1	Змістовий модуль 2	іспит / *залік*	Підсумкова оцінка
Мінімум	**27**	**9**	**24**	**60**
Максимум	**45**	**15**	**40**	**100**

7.3 Шкала відповідності оцінок

Відмінно/ Excellent	90 – 100
Добре/ Good	75 – 89
Задовільно/ Satisfactory	60 – 74

Не задовільно/ Fail	0 – 59
Зараховано/ Passed	60 – 100
Не зараховано/ Fail	0 – 34

8. Структура навчальної дисципліни. Тематичний план лекцій та самостійної роботи

10 семестр

№ теми	Назва теми	Кількість годин			
		Лекції	практичні	самост. робота	Консуль-тації
Змістовий модуль 1 **Базові поняття криптографії**					
1	Проблеми захисту інформації. Основні поняття	4	2	16	
2	Обчислювально складні задачі та криптографія	6	6	16	2
3	Криптографічні протоколи та механізми	2	2	16	
Модульна контрольна робота 1					
Змістовий модуль 2 **Сучасні задачі криптографії**					
4	Використання білінійних парних відображень в криптографії	4	2	16	
5	Комбінаторно-алгебраїчні криптосистеми	6	2	16	2
Модульна контрольна робота 2					
	ВСЬОГО	**22**	14	44	4

Загальний обсяг **120** *год.,* в тому числі:
Лекції – **22** *год.*
Практичні – **14** *год.*
Самостійна робота – **80** *год.*
Консультації – **4** *год.*

9. Рекомендовані джерела

Основна (*Базова):*

1. Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. М., «Гелиос АРВ», 2001.
2. Вербіцький О. В. Вступ до криптології / О. В. Вербіцький. – Львів : ВНТЛ, 1998
3. Коблиц Н. Курс теории чисел и криптографии. М., Научное издательство ТВП, 2001.
4. Koblitz N. Algebraic aspects of cryptography. Algorithms and Computation in Mathematics. 3. Berlin: Springer. ix, 206 p.
5. Hoffstein J., Pipher J., Silverman J. Fn introduction to mathematical cryptography. Springer, 2008.

Додаткова:

1. Лидл Р., Нидеррайтер Г. Конечные поля. В 2-х тт. – М.: Мир, 1988.
2. Китаев А., Шень А., Вялый М. Классические и квантовые вычисления. М., «Мир», 1999.
3. Luther M. Introduction to identity-based encryption. Artech House Information Security and Privacy Series. London: Artech House.
4. Menezes, Alfred J.; van Oorschot, Paul C.; Vanstone, Scott A. Handbook of applied cryptography.) CRC Press Series on Discrete Mathematics and its Applications. Boca Raton, FL: CRC Press. xxviii, 780 p.