КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

МЕХАНІКО-МАТЕМАТИЧНИЙ ФАКУЛЬТЕТ
Кафедра алгебри та математичної логіки

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної
роботи
Безущак О.О.
«5» вересня 2018 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ
МАТЕМАТИЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ

для здобувачів освітньо-наукового рівня «доктор філософії»

галузь знань	**11 «Математика та статистика»**
спеціальність	**111 «Математика»**
освітній рівень	**третій (освітньо-науковий)**
освітньо-наукова програма	**«Математика»**
вид дисципліни	**вибіркова**

Форма навчання	**денна**
Навчальний рік	**2018/2019**
Рік навчання	2
Кількість кредитів ECTS	4
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**екзамен**

Викладачі: **професор Олійник Андрій Степанович, д.ф.-м.н.**

Пролонговано: на 2019/2020 н.р. (Безущак) «18» вересня 2019 р.
на 20 /20 н.р. ( ) « » 20 р.

КИЇВ – 2018

Розробник: професор кафедри алгебри та математичної логіки **Олійник Андрій Степанович, д.ф.-м.н., доцент**

ЗАТВЕРДЖЕНО
Завідувач кафедри «Алгебри та математичної логіки»

_____Петравчук А.П.
(підпис)

Протокол №1 від «31» 08 2018 р.

Схвалено науково-методичною комісією механіко-математичного факультету

Протокол від "12" 09 2018 року № 1
Голова науково-методичної комісії _____професор, д.ф.-м.н. Курченко О.О.
(підпис)

1. **Мета дисципліни** Розвиток навичок розв'язання комплексних проблем в галузі математики, використання новітніх інформаційних і комунікаційних технологій, здатності до абстрактного мислення, здатності до пошуку, оброблення та аналізу інформації з різних джерел, вміння генерувати нові ідеї, навички роботи в міжнародному науковому просторі, навички формулювання дослідницьких задач з математики, навички формулювання і строгого доведення математичних тверджень, перевірки правильності їх доведень, навички розв'язання задач математичного захисту інформації, навички аналізу загроз інформаційній безпеці, навички побудови відповідної математичної моделі і конструювання адекватних загрозам математично обґрунтованих засобів захисту інформації.

2. Попередні вимоги до опанування або вибору навчальної дисципліни:

1. *Знати*: основні задачі захисту інформації, основні криптографічні примітиви, методи доведення стійкості криптографічних компонент, методи побудови криптосистем з публічним ключем і схем цифрового підпису, протоколи вироблення спільного секрету, розподілу секрету, призначення гомоморфних криптосистем, принцип роботи блокчейну та криптовалют.
2. *Вміти*: проводити критичний аналіз, оцінку і синтез нових ідей і підходів в галузі математичних основ захисту інформації, самостійно застосовувати математичні методи захисту інформації, розробляти та аналізувати криптографічні компоненти.

3. Анотація навчальної дисципіни:

Дисципліна «Математичні основи захисту інформації» належить до вибіркових компонент освітньої програми, блоку дисциплін вільного вибору аспіранта. Вона забезпечує професійний розвиток, спрямована на формування концептуальних та методологічних знань у галузі математики, вміння критично аналізувати, оцінювати і синтезувати нові та комплексні ідеї, аналізувати наукові праці, формулювати методологічну базу власного наукового дослідження, здатність формулювати наукову проблему, робочі гіпотези досліджуваної проблеми. В рамках дисципліни вивчаються основні задачі математичного захисту інформації, криптографічні примітиви для їх розв'язання, способи побудови та аналізу криптографічних компонент, основні криптографічні протоколи.

4. Завдання (навчальні цілі): набуття знань, умінь та навичок (компетентностей) на рівні новітніх досягнень у математиці, відповідно науково-освітньої кваліфікації «Доктор філософії». Зокрема, розвивати: вміння аналізувати сучасні передові концептуальні та методологічні знання; здатність проводити критичний аналіз, оцінку і синтез нових та складних ідей; здатність застосовувати теоретичні та практичні підходи математики; вміння розробляти наукові і інформаційно-освітні ресурси для розв'язання професійних задач, пов'язаних з розвитком та використанням математики; .

5. Результати навчання за дисципліною:

Результат навчання (РН) (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**			
РН 1.1	Знати основні задачі захисту інформації і криптографічні примітиви для їх розв'язання.	*Лекція, практичне заняття*	*Контрольна робота 1 (60% правильних відповідей), екзамен, активна*	*10%*
РН 1.2	Знати основні методи доведення стійкості криптографічних примітивів			*10%*
РН 1.3	Знати основні криптографічні протоколи			*10%*

РН 1.4	Знати призначення і основні властивості блокчейну		*робота на лекції, усні відпові*	*10%*
РН 2.1	Вміти будувати модель загроз і обирати криптографічні компоненти протидії	*Лекція, практичне заняття, самостійна робота*	*Контрольна робота 2 (60% правильних відповідей), екзамен, виконання завдань, винесених на самостійну роботу*	*20%*
РН 2.2	Вміти доводити стійкість криптосистем з публічним ключем та схем цифрового підпису			*20%*
РН 2.3	Вміти використовувати протоколи вироблення спільного секрету та розподілу секрету	*Практичне заняття, самостійна робота*	*Виступ з доповіддю за темою наукового дослідження*	*5%*
РН3.1	Здатність працювати у міжнародному просторі, обґрунтовувати власний погляд на задачу та формулювати робочі гіпотези, спілкуватися з колегами з питань застосування методів та теорій математики, писати наукові роботи			*5%*
РН4.1	Демонстрація авторитетності, інноваційність, високий ступінь самостійності, академічна та професійна доброчесність, послідовна відданість розвитку нових ідей або процесів у передових контекстах професійної та наукової діяльності.			*5%*
РН4.2	Відповідально ставитися до виконуваних робіт, нести відповідальність за їх якість			*5%*

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання

Результати навчання дисципліни **Програмні результати навчання**	**РН 1.1**	**РН 1.2**	**РН 1.3**	**РН 1.4**	**РН 2.1**	**РН 2.2**	**РН 2.3**	**РН 3.1**	**РН 4.1**	**РН 4.2**
(з опису освітньої програми)										
ПРН-З-4. Визначати методологічні принципи та методи наукового дослідження галузі інформаційних технологій в залежності від об'єкту і предмету, використовуючи міждисциплінарні підходи.	+	+	+	+	+	+	+	+	+	+
ПРН-З-5. Використовувати сучасні інформаційні та комунікативні технології при спілкуванні, обміні інформацією, зборі, аналізі, обробці, інтерпретації джерел; здійснювати публікацію джерел	+	+	+	+	+	+	+	+	+	+
ПРН-З-6. Знати, розуміти і застосовувати математичні концепції, методи системного аналізу і математичного моделювання.	+	+	+	+	+	+	+	+	+	+
ПРН-У-1. Аналізувати сучасні передові концептуальні та методологічні знання в галузі науково-дослідницької та/або професійної діяльності і на межі предметних галузей знань	+	+	+	+	+	+	+	+	+	+
ПРН-У-2. Критичний аналіз, оцінка і синтез нових та складних ідей	+	+	+	+	+	+	+	+	+	+

ПРН-У-11. Розробляти наукові і інформаційно-освітні ресурси для розв'язання професійних задач, пов'язаних з розвитком та використанням математики;	+	+	+	+	+	+	+	+	+	+
ПРН-У-12. Розуміти сутність інформації, проводити критичну оцінку кількості і змісту інформації;	+	+	+	+	+	+	+	+	+	+
ПРН-У-14. Прогнозувати розвиток математики	+	+	+	+	+	+	+	+	+	+
ПРН-У-15. Розуміти, аналізувати, цілеспрямовано шукати і вибирати необхідні для рішення професійних наукових задач інформаційно-довідникові та науково-технічні ресурси і джерела знань з урахуванням сучасних досягнень науки і техніки.	+	+	+	+	+	+	+	+	+	+
ПРН-У-19. Здійснювати процедуру встановлення інформаційної цінності джерел шляхом порівняльного аналізу з іншими джерелами	+	+	+	+	+	+	+	+	+	+
ПРН-У-21. Демонструвати здатність діяти соціально відповідально та громадянської свідомо і на основі етичних міркувань (мотивів)	+	+	+	+	+	+	+	+	+	+
ПРН-У-25. Здатність професійно презентувати результати своїх досліджень на міжнародних наукових конференціях, семінарах, практично використовувати іноземну мову (в першу чергу - англійську) у науковій, інноваційній діяльності та педагогічній діяльності.	+	+	+	+	+	+	+	+	+	+
ПРН-У-27. Здатність саморозвиватися і самовдосконалюватися, нести відповідальність за новизну наукових досліджень та прийняття експертних рішень.								+	+	+
ПРН-У-28. Здатність приймати обґрунтовані рішення, мотивувати людей та рухатися до спільної мети.								+	+	+

7. Схема формування оцінки.

7.1. Форми оцінювання здобувачів освітньо-наукового ступеня:

- оцінювання впродовж навчального періоду:

1. Активна робота на лекції, усні відпові: РН1.1, РН1.2, РН1.3, РН1.4– 5 балів/3 бали;

2. Виконання завдань, винесених на самостійну роботу: РН2.1, РН2.2 – 5 балів/3 бали;

3. Контрольна робота 1: РН1.1, РН1.2, РН1.3, РН1.4 – 15 балів/9 балів;

4. Контрольна робота 2: РН2.1, РН2.2 – 15 балів/9 балів;

6. Виступ з доповіддю за темою наукового дослідження: РН2.3, РН3.1, РН4.1, РН4.2, – 20 балів/12 балів;

- підсумкове оцінювання: екзамен.

- *максимальна кількість балів які можуть бути отримані:* 40 балів;

- *результати навчання які будуть оцінюватись:* РН1.1, РН1.2, РН1.3, РН1.4, РН2.1, РН2.2, РН2.3
- *форма проведення і види завдань:* письмова робота.

7.2. Організація оцінювання:

Обов'язковим є виконання завдань, винесених на самостійну роботу, та модульних контрольних робіт за графіком робочої програми.

У частину 1 входять теми 1 - 3, у частину 2 – теми 4 – 6 у частину 3 – теми 7 – 9. Обов'язковим для екзамену є виконання усіх контрольних робіт та доповідь за темою наукового дослідження до вказаної викладачем дати, перед початком екзаменаційної сесії, згідно навчального плану. Переписування чи перескладання тем не практикується.

Терміни проведення форм оцінювання:

1. Контрольна робота: до 5 тижня навчального періоду.

2. Контрольна робота: до 13 тижня навчального періоду.

3. Доповідь за темою наукового дослідження: до 10 тижня навчального періоду.

У випадку відсутності з поважних причин відпрацювання та перездачі контрольні роботи здійснюються у відповідності до „Положення про організацію освітнього процесу".

7.3. Шкала відповідності оцінок

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

При визначені оцінки визначальною є робота в семестрі. Після завершення розгляду тем проводяться письмові контрольні роботи та теоретичне опитування.

8. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ. ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ І ПРАКТИЧНИХ ЗАНЯТЬ

№	Назва лекції	Кількість годин		
		Лекції	Практичні	Самостійна робота
Частина 1. „Основні задачі і поняття захисту інформації. Криптографічні примітиви”				
1	**Тема 1.** Основні задачі захисту інформації: конфіденційність, цілісність, доступність, невідмовність. Загрози інформаційній безпеці. Аналіз загроз. *Самостійна робота:* Проведення аналізу загроз на прикладах задач обробки інформації при роботі над дисертацією.	2		8
2	**Тема 2.** Основні криптографічні примітиви. Складність обчислювальних задач та алгоритмів. Звідність задач. Атаки на криптографічні примітиви. Доведення надійності та стійкості. *Самостійна робота:* Застосування звідності обчислювальних задач до доведення стійкості криптографічних примітивів. Встановлення оцінок складності атак.	2		10
3	**Тема 3.** Розробка і аналіз криптографічних примітивів. Криптографічні стандарти. *Самостійна робота:* Методи аналізу стійкості криптографічних примітивів на прикладі симетричних блочних шифрів.	1	2	10
Контрольна робота 1		1		
Частина 2. „Криптографія з публічним ключем”				
4	**Тема 4.** Синтаксис криптосистем з публічним ключем. Криптосистеми, стійкість яких заснована на складності задачі факторизації. Ймовірносне шифрування. *Самостійна робота:* Доведення стійкості криптосистем з публічним ключем.	2		10
5	**Тема 5.** Основні властивості цифрових підписів. Синтаксис схем цифрового підпису. Побудова схем цифрового підпису. Аналіз надійності. *Самостійна робота:* Застосування схем цифрового підпису для задач ідентифікації.	2	2	10
6	**Тема 6.** Протокол вироблення спільного секрету. Задача дискретного логарифма. Протокол Діффі-Хелмана. *Самостійна робота:* Аналіз атак на схеми вироблення спільного секрету.	2		12

Частина 3. „ Криптографічні протоколи”				
7	**Тема 7.** Протоколи розподілу секрету. Схема Шнора. *Самостійна робота:* Застосування схем розподілу секрету.	2		12
8	**Тема 8.** Гомоморфні криптосистеми та їх застосування. *Самостійна робота:* Побудова гомоморфних криптосистем на основі задач навчання з помилками.	2		12
9	**Тема 9.** Розподілені обчислення. Блокчейн. Криптовалюти. *Самостійна робота:* Застосування розподілених обчислень.	1		12
Контрольна робота 2		1		
ВСЬОГО		18	4	96

Загальний обсяг *120* *годин*, в тому числі:
Лекцій – 1**8** *годин*,
Практичних занять – **4** *години*
Консультації - **2** *години.*
Самостійна робота – ***96*** *години***.**

9. Рекомендовані джерела

Основні:

1. Jean-Philippe Aumasson. Serious Cryptography, 2017.
2. Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. An Introduction to Mathematical Cryptography, 2014.
3. Nigel Smart. Cryptography Made Simple, 2016.

Додаткові:

4. Jonathan Katz, Yehuda Lindell. Introduction to Modern Cryptography, 2015.
5. Johannes A. Buchmann, Evangelos Karatsiolis, Alexander Wiesmaier. Introduction to Public Key Infrastructures, 2013.
6. Alko R. Meijer. Algebra for Cryptologists, 2016.
7. Paul Vigna, Michael J. Casey. The Age of Cryptocurrency: How Bitcoin and Digital Money Are Challenging the Global Economic Order, 2016.