КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ

Кафедра математичної інформатики

«ЗАТВЕРДЖУЮ»
Заступник декана
з навчальної роботи
_____ Олена КАШПУР
«07» травня 2021 р.

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ІНФОРМАЦІЙНА БЕЗПЕКА ТА КРИПТОГРАФІЯ

для студентів

галузь знань	**12 «Інформаційні технології»**
спеціальність	**122 «Комп'ютерні науки»**
освітній рівень	**магістр**
освітня програма	**«Інформатика»**
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	**іспит**

Викладачі: **д.ф.-м.н., проф. Андрій ОЛІЙНИК** (лекції)
к.ф.-м.н., асистент Олексій ФЕДОРУС (лабораторні заняття)

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

на 20 /20 н.р. ( ) « » 20 р.

КИЇВ – 2021

Розробник: Андрій ОЛІЙНИК, д. ф.-м. н., професор кафедри математичної інформатики

ЗАТВЕРДЖЕНО
Завідувач кафедри математичної інформатики
_____ Василь ТЕРЕЩЕНКО
Протокол № 10 від «27» 04 2021 р.

Схвалено гарантом освітньо-наукової програми «Інформатика»
_____ Степан ШКІЛЬНЯК
«6» травня 2021 року

Схвалено науково-методичною комісією факультету комп'ютерних наук та кібернетики
Протокол від «6» травня 2021 року № 10
Голова науково-методичної комісії _____ Людмила ОМЕЛЬЧУК

1. Мета дисципліни: дати знання про вразливості та про захист сучасних інформаційних систем, захист персональних даних та безпеку комп'ютерних мереж; опанувати ключові терміни та поняття в галузі інформаційної безпеки; дати розуміння основ криптографії, знання про її розвиток; дати знання про ключові методи шифрування, що використовуються сьогодні, а також про криптографічні протоколи.

2. Попередні вимоги до опанування або вибору навчальної дисципліни:

1. *Знати*: основні компоненти інформаційних систем; знати основи алгебри, теорії ймовірностей та теорії чисел. Знання технічної англійської мови на рівні В1.
2. *Вміти*: розробляти, аналізувати та застосовувати програмні системи для розв'язання завдань та прикладних задач, використовуючи сучасні методи розробки програм.

3. Анотація навчальної дисципіни :

Навчальна дисципліна «Інформаційна безпека та криптографія» є обов'язковою навчальною дисципліною у складі освітньо-наукової програми підготовки фахівців «Інформатика» за другим (магістерським) рівнем вищої освіти галузі знань 12 «Інформаційні технології» спеціальності 122 «Комп'ютерні науки». Вона забезпечує професійний розвиток студентів магістратури, спрямована на формування теоретичних основ та практичних навичок забезпечення безпеки інформаційних систем, дослідження та використання криптографічних алгоритмів і протоколів для досягнення цілей інформаційної безпеки.

Дана дисципліна є обов'язковою навчальною дисципліною за *програмою "Інформатика"*. Викладається у 1 семестрі (1 курс магістратури) в обсязі – 120 год. (*4 кредити ECTS*), зокрема: лекції – 26 год., лабораторні – 12 год., консультації – 2 год., самостійна робота – 80 год.

У курсі передбачено 2 *змістових частини*, 1 *колоквіум, 6 лабораторних робіт*.

Завершується дисципліна іспитом в 1 семестрі.

4. Завдання (навчальні цілі):

Основними завданнями дисципліни «Інформаційна безпека та криптографія» є набуття знань, умінь та навичок (компетентностей) на рівні новітніх досягнень в галузі інформаційної безпеки відповідно до освітньої кваліфікації магістр комп'ютерних наук. Зокрема, розвивати:

- Здатність до абстрактного мислення, аналізу та синтезу (ЗК1).
- Здатність спілкуватися іноземною мовою (ЗК5).
- Здатність проводити дослідження функціональної та економічної ефективності та надійності інформаційних систем (СК13).
- Здатність проектувати та забезпечувати впровадження серверної інфраструктури корпоративного центру обробки даних компанії (СК17).

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 завдання інформаційної безпеки, загрози та вразливості	*Лекція*	*Колоквіум (60% правильних відповідей), іспит, захист лабораторних робіт 1–5*	*10%*
РН 1.2	Знати основні криптографічні інструменти для досягнення цілей інформаційної безпеки			*10%*
РН 1.3	Знати математичні основи криптографічних алгоритмів			*10%*
РН 1.4	Знати основні криптографічні протоколи			*10%*
РН 2.1	Вміти розробляти і аналізувати засоби інформаційної безпеки	*Лекція, лабораторна робота, самостійна робота*	*Колоквіум (60% правильних відповідей), іспит, захист лабораторних робіт 1–5*	*20%*
РН 2.2	Вміти застосовувати криптографічні засоби для забезпечення інформаційної безпеки			*20%*
РН 2.3	Вміти застосовувати програмні засоби розробки систем	*Лабораторна робота, самостійна робота*	*Захист лабораторних робіт 1–5*	*5%*
РН3.1	Обґрунтовувати власний погляд на задачу, спілкуватися з колегами з питань проектування та розробки програм, складати письмові звіти			*5%*
РН4.1	Демонстрація авторитетності, інноваційності, високого ступеня самостійності, академічної та професійної доброчесності, послідовної відданості розвитку нових ідей або процесів у передових контекстах професійної та наукової діяльності, що стосується теорії та технології програмування			*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**	**РН1.1**	**РН1.2**	**РН1.3**	**РН1.4**	**РН2.1**	**РН2.2**	**РН2.3**	**РН3.1**	**РН4.1**	**РН4.2**
(з опису освітньої програми)										
ПРН 5. Вирішувати складні проблеми, що вимагають систем з великою обчислювальною потужністю для забезпечення масштабованості паралельних алгоритмів і програм.				+	+	+	+	+	+	+
ПРН 8. Аналізувати особливості використання сучасних квантових технологій для забезпечення вирішення проблем, зокрема конфіденційного зв'язку, квантової криптографії, здійснювати дослідження теоретичних та експериментальних аспектів квантової інформатики.	+	+	+	+				+		+
ПРН 15. Володіти методами розробки та впровадження заходів, спрямованих на підвищення ефективності інформаційних систем					+	+	+		+	+

7. Схема формування оцінки.

7.1. Форми оцінювання здобувачів освітньо-наукового ступеня:

- оцінювання впродовж навчального періоду:

1. Колоквіум: РН1.1, РН1.2, РН1.3, РН1.4, РН2.1, РН2.2 – 15 балів / 9 балів;

2. Лабораторні роботи: РН1.3, РН1.4, РН2.1, РН2.2, РН2.3, РН3.1, РН4.1, РН4.2 – 45 балів / 27 балів;

- підсумкове оцінювання: іспит.

- *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;
- *форма проведення і види завдань:* письмова робота.
- *види завдань*: 2 письмових завдання (практичні завдання) та 1 теоретичне питання;
- для отримання загальної позитивної оцінки з дисципліни оцінка за іспит повинна бути не меншою ніж 24 бали;
- студенти не допускаються до іспит, якщо протягом семестру вони набрали менше ніж 36 балів;
- студенти не допускаються до іспиту, якщо протягом семестру вони не виконали та не захистили реферат.

Критерії оцінювання на іспиті

Завдання	**Тема завдання**	**Максимальний відсоток від 40 балів**	**Всього відсотків**
Завдання 1	Теоретичне питання за матеріалами курсу	40%	40%
Завдання 2		По 30%	60%
Завдання 3			
			100%

Для отримання загальної позитивної оцінки з дисципліни оцінка за іспит не може бути меншою 24 балів. Студент не допускається до іспиту, якщо під час семестру набрав менше 24 балів.

Умови лабораторних робіт

Приклад лабораторної роботи:

Створити бібліотеку для заданої симетричної блочної криптосистеми. Провести тестування. Порівняти швидкості шифрування для вказаних режимів потокового шифрування. Підготувати звіт. Надати документацію, вихідний код і результати тестування.

Запитання до колоквіуму

Приклади завдань:

1. Вразливості інформаційних систем.
2. Криптосистеми з секретним ключем.
3. Побудувати модель загроз конфіденційності даних при роботі з електронною поштою.

7.2. Організація оцінювання:

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

Терміни проведення форм оцінювання:

1. Колоквіум: до 8 тижня навчального періоду.

2. Лабораторні роботи 1–5: до 4,6,8,10,12 тижнів навчального періоду відповідно.

У випадку відсутності студента з поважних причин відпрацювання та перескладання лабораторних робіт і колоквіуму здійснюються у відповідності до «Положення про організацію освітнього процесу» від 07.05.2018 року.

7.3. Шкала відповідності оцінок

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

8. СТРУКТУРА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ. ТЕМАТИЧНИЙ ПЛАН ЛЕКЦІЙ

№	Назва лекції	Кількість годин		
		Лекції	Лабора-торні	Самостійна робота
Частина 1. «Основи інформаційної безпеки та симетричної криптографії»				
1	**Тема 1.** Основні завдання інформаційної безпеки. Вразливості і загрози. Основні криптографічні інструменти. *Самостійна робота:* Вивчити причини загроз і вразливостей на прикладах.	2		6
2	**Тема 2.** Атаки на інформаційні системи. Модель загроз. Розробка криптографічних засобів безпеки. *Самостійна робота:* Моделювання загроз на прикладах. Стандартизація криптографічних інструментів.	2		6
3	**Тема 3.** Забезпечення конфіденційності даних. Симетричні блочні шифри. Потокові шифри. *Самостійна робота:* Українські та міжнародні стандарти симетричного шифрування.	4	2	10
4	**Тема 4.** Криптоаналіз симетричних шифрів. Лінійний та диференціальний криптоаналіз. *Самостійна робота:* Ознайомитись з результатами криптоаналізу сучасних симетричних шифрів.	2	2	6
5	**Тема 5.** Забезпечення цілісності даних. Криптографічні хеш функції. *Самостійна робота:* Сучасні українські та міжнародні стандарти криптографічного хешування.	4	2	12
Колоквіум		2		
Всього за частиною 1		16	6	40
Частина 2. «Асиметрична криптографія»				
6	**Тема 6.** Математичні основи асиметричної криптографії. Криптосистеми з публічним ключем. Задача факторизації. *Самостійна робота:* Ймовірнісне шифрування.	2	2	8
7	**Тема 7.** Забезпечення автентичності та невідмовності. Схеми цифрового підпису. *Самостійна робота:* Вразливості схем цифрового підпису.	2		8
8	**Тема 8.** Задача дискретного логарифма. Алгоритми її розв'язування. Схеми цифрового підпису DSA та Шнора. *Самостійна робота:* Український стандарт цифрового підпису.	2	2	8

9	**Тема 9.** Протоколи вироблення спільного секрету. *Самостійна робота:* Вразливості протоколів вироблення спільного секрету.	2	2	8
10	**Тема 10.** Інфраструктура публічних ключів. Сертифікати публічних ключів. Протоколи TLS. *Самостійна робота:* Криптографічна бібліотека OpenSSL.	2		8
Всього за частиною 2		10	6	40
ВСЬОГО / TOTAL		**26**	**12**	**80**
Консультація		2		

Загальний обсяг *120 годин*, в тому числі:
Лекції – **26** *годин*,
Лабораторні – **12** годин**,**
Консультації – **2** *години / hours.*
Самостійна робота – **80** *годин***.**

9. Рекомендовані джерела

Основні / Main:

1. J.-P.Aumasson *Serious cryptography.* No starch press, 2018.
2. C. Paar, J. Pelzl *Understanding cryptography.* Springer, 2010.
3. N.Smart *Cryptography made simple.* Springer, 2016.
4. О.Вербіцький *Вступ до криптології.* ВНТЛ, 1998.

Додаткові:

5. H.Bidgoli (Ed.) Handbook of Information Security, Volume 1. JohnWiley&SonsInc., 2006.
6. H.Bidgoli (Ed.) Handbook of Information Security, Volume 2. JohnWiley&SonsInc., 2006.
7. H.Bidgoli (Ed.) Handbook of Information Security, Volume 3. JohnWiley&SonsInc., 2006.
8. J. Katz, Y. Lindell *Introduction to modern cryptography.* CRC Press, 2015.
9. A. Narayanan, J. Bonneau, Ed. Felten, A. Miller, S. Goldfeder *Bitcoin and cryptocurrency technologies: a comprehensive introduction.* Princeton University Press, 2016.