КИЇВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ТАРАСА ШЕВЧЕНКА

ФАКУЛЬТЕТ КОМП'ЮТЕРНИХ НАУК ТА КІБЕРНЕТИКИ

КАФЕДРА ІНТЕЛЕКТУАЛЬНИХ ПРОГРАМНИХ СИСТЕМ

«ЗАТВЕРДЖУЮ»

Заступник декана
з навчальної роботи

_____ Кашпур О.Ф.

«____»_____2019 року

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ

ОСНОВИ КРИПТОЛОГІЇ

для студентів

галузь знань	**12 Інформаційні технології**
спеціальність	**121 Інженерія програмного забезпечення**
освітній рівень	**бакалавр**
освітня програма	**Програмна інженерія**
блок вибору	**Програмна інженерія**
вид дисципліни	**вибіркова**

Форма навчання	**денна**
Навчальний рік	**2021/2022**
Семестр	**6**
Кількість кредитів ECTS	**4**
Мова викладання, навчання та оцінювання	**українська**
Форма заключного контролю	**залік**

Викладачі: **к.ф.-м.н., доц. Галкін О.В.** (лекції)

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

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

КИЇВ 2019

Розробник: Галкін Олександр Володимирович, к.ф.-м.н., доц.,
доцент кафедри інтелектуальних програмних систем

ЗАТВЕРДЖЕНО

Завідувач кафедри інтелектуальних програмних систем

_____ О.І. Провотар

Протокол № __ від «___» _____2019 р.

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

Протокол від «____» _____ 2019 року №___

Голова науково-методичної комісії _____ Л.Л. Омельчук

«_____» _____ 2019 року

Затверджено вченою радою факультету комп'ютерних наук та кібернетики

Протокол від «____» _____ 2019 року №___

Голова вченої ради факультету _____ А.В. Анісімов

1. Мета дисципліни – вивчення основних криптографічних алгоритмів, їх особливостей та вразливостей.

2. Попередні вимоги до опанування навчальної дисципліни

1. **Знати**: базові поняття математичного аналізу, лінійної та загальної алгебри, диференціальних рівнянь, теорії алгоритмів, теорії складності обчислень.

2. **Вміти**: програмувати на мові високого рівня.

3. Анотація навчальної дисципліни

Навчальна дисципліна «Основи криптології» є складовою освітньо-професійної програми підготовки фахівців за першим (бакалаврським) рівнем вищої освіти галузі знань 12 Інформаційні технології за спеціальністю 121 Інженерія програмного забезпечення освітньо-професійної програми „Програмна інженерія.

Дисципліна належить до вибіркових дисциплін блоку вибору "Програмна інженерія". Викладається **6** семестрі **3** курсу в **обсязі – 120 год. (4 *кредити ECTS*)**, зокрема: лекції – 42 год., консультації – 2 год., самостійна робота – 76 год. У курсі передбачено 2 частини та 2 контрольні роботи. Завершується дисципліна – **заліком в 6 семестрі.**

В результаті вивчення навчальної дисципліни студент повинен:

знати основні криптографічні алгоритми з симетричним та асиметричним шифруванням, їх переваги та недоліки; основні атаки на криптографічні алгоритми;

вміти створювати програми з використанням криптографічних алгоритмів (симетричних та асиметричних).

Дисципліна є логічним продовженням, доповненням та розширенням дисципліни «Загальна алгебра».

4. Завдання (навчальні цілі). Основними завданнями дисципліни «Основи криптології» є набуття знань, умінь та навичок (компетенцій) на рівні новітніх досягнень в області криптології відповідно до освітньої кваліфікації бакалавр з програмної інженерії.

Зокрема, розвивати:

- Здатність до абстрактного мислення, аналізу та синтезу (ЗК01).
- Здатність застосовувати знання у практичних ситуаціях (ЗК02).
- Здатність спілкуватися державною мовою як усно, так і письмово (ЗК03).
- Здатність вчитися і оволодівати сучасними знаннями (ЗК05).
- Здатність до пошуку, оброблення та аналізу інформації з різних джерел (ЗК06).
- Здатність аналізувати, вибирати і застосовувати методи і засоби для забезпечення інформаційної безпеки (в тому числі кібербезпеки) (СК06).
- Здатність до алгоритмічного та логічного мислення (СК14).
- Здатність застосовувати дискретні структури і сучасні методи дискретної математики під час аналізу, синтезу та проектування інформаційних систем різної природи (СК-15.2).

5. Результати навчання за дисципліною.

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**			
РН1.1	*Знати* основні криптографічні алгоритми з симетричним та асиметричним шифруванням, їх переваги та недоліки	*Лекція, самостійна робота*	*Контрольна робота*	*30%*
РН1.2	*Знати* основні атаки на криптографічні алгоритми	*Лекція, самостійна робота*	*Контрольна робота*	*10%*
РН2.1	*Вміти* створювати програми з використанням криптографічних алгоритмів (симетричних та асиметричних).	*Самостійна робота*	*Захист лабораторної роботи*	*45%*
РН3.1	*Обґрунтовувати* власний погляд на розв'язання задачі, спілкуватися з колегами з питань криптології, проектування та розробки програм, складати письмові звіти	*Самостійна робота*	*Поточне оцінювання, захист лабораторної роботи*	*5%*
РН4.1	*Організовувати* свою самостійну роботу для досягнення результату	*Самостійна робота*	*Поточне оцінювання, захист лабораторної роботи*	*5%*
РН4.2	*Відповідально* ставитися до виконуваних робіт, нести відповідальність за їх якість	*Самостійна робота*	*Захист лабораторної роботи*	*5%*

6. Співвідношення результатів навчання дисципліни із програмними результатами навчання.

Результати навчання дисципліни / **Програмні результати навчання**	**РН1.1**	**РН1.2**	**РН2.1**	**РН3.1**	**РН4.1**	**РН4.2**
ПРН01. Аналізувати, цілеспрямовано шукати і вибирати необхідні для вирішення професійних завдань інформаційно-довідникові ресурси і знання з урахуванням сучасних досягнень науки і техніки.	+	+			+	
ПРН05. Знати і застосовувати відповідні математичні поняття, методи доменного, системного і об'єктно-орієнтованого аналізу та математичного моделювання для розробки програмного забезпечення.	+		+		+	
ПРН21. Знати, аналізувати, вибирати, кваліфіковано застосовувати засоби забезпечення інформаційної безпеки (в тому числі кібербезпеки) і цілісності даних відповідно до розв'язуваних прикладних завдань та створюваних програмних систем.	+	+	+	+	+	+
ПРН25.2. Аналізувати, оцінювати і вибирати інструментальні та обчислювальні засоби, технології, алгоритмічні і програмні рішення для розв'язання завдань інженерії програмного забезпечення.	+	+	+	+		

7. Схема формування оцінки.

7.1. Форми оцінювання студентів.

– семестрове оцінювання (максимальна кількість балів):

1. Контрольна робота 1: РН 1.1 – **20/12 б.**
2. Контрольна робота 2: РН 1.1, РН 1.2 – **20/12 б.**
3. Лабораторні роботи (3): РН 2.1, РН 3.1, РН 4.1-4.2 – **20/12 б. кожна.**

Підсумкове оцінювання (у формі заліку):

- Залікові бали визначаються як сума оцінок/балів за всіма успішно оціненими результатами навчання передбачених даною програмою.
- Оцінки нижче від мінімального порогового рівня не додаються.
- Мінімальний пороговий рівень для сумарної оцінки за всіма компонентами становить 60% від максимально можливої кількості балів.

7.2. Організація оцінювання.

Терміни проведення форм оцінювання:

1. Контрольна робота 1: після лекції №10.
2. Контрольна робота 2: після лекції №21.
3. Лабораторна робота 1 (проект): до 4 тижня семестру.
4. Лабораторна робота 2 (проект): до 9 тижня семестру.
5. Лабораторна робота 3 (проект): до 14 тижня семестру.

Студент має право один раз перескласти контрольну роботу з можливістю отримати не більше 80% балів, призначених за роботу. Термін перескладання визначається викладачем.

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

У разі неякісного або невчасного виконання лабораторної роботи викладач має право не зарахувати завдання або знизити за нього бали.

Студент має право здавати лабораторні роботи після закінчення визначеного для них терміну, але з втратою 10% балів за кожен тиждень, що пройшов від закінчення терміну її здачі.

7.3. Шкала відповідності оцінок

Зараховано / Passed	60-100
Не зараховано / Fail	0-59

8. Структура навчальної дисципліни. Тематичний план лекцій.

№ лекції	Назва лекції	Кількість годин	
		Лекції	С/р
Частина 1. Вступ до дисципліни. Алгоритми з симетричним ключем			
1–3	**Тема 1.** Арифметика залишків, групи, скінченні поля. Базові алгоритми	6	12
4	**Тема 2.** Історичні шифри	2	4
5–6	**Тема 3.** Симетричні шифри	4	6
7	**Тема 4.** Режими роботи симетричних шифрів	2	4
8	**Тема 5.** Розподіл симетричних ключів	2	4
9–10	**Тема 6.** Алгоритми шифрування з відкритим ключем	4	6
Контрольна робота №1			2
		20	38
Частина 2. Алгоритми з відкритим ключем та криптографічні хеш-функції			
11	**Тема 7.** Хеш-функції та шифрування	2	4
12–13	**Тема 8.** Розподіл ключів. Схеми підписів	4	6
14–15	**Тема 9.** Отримання автентичного ключа. Протоколи	4	6
16–17	**Тема 10.** Атаки на схеми з відкритим ключем	4	6
18–19	**Тема 11.** Теоретико-інформаційна стійкість	4	6
20	**Тема 12.** Тести на простоту та факторизація	2	4
21	**Тема 13.** Дискретні логарифми. Реалізація операцій	2	4
Контрольна робота №2			2
		22	38
	ВСЬОГО	**42**	**76**

Загальний обсяг**– *120** год.,* у тому числі:
Лекцій **– *42** год.,*
Консультацій **– *2** год.,*
Самостійна робота **– *76** год.*

Тематика лабораторних проектів

1. Допоміжні алгоритми, що застосовуються в криптології.
2. Алгоритми з симетричним ключем.
3. Алгоритми з відкритим ключем.

Перелік питань для підготовки до заліку

1. Групи та кільця.
2. Функція Ейлера.
3. Мультиплікативні обернені.
4. Китайська теорема про залишки.

5. Розширений алгоритм Евкліда.
6. Шифр зміщення.
7. Шифр заміни.
8. Шифр Віжера.
9. Машина Енігма.
10. Шифр Фейстеля.
11. Шифр DES.
12. Шифр Rijndael.
13. Потокові шифри.
14. Режими роботи DES
15. Протокол Цербер.
16. Протокол Отсей-Ріса.
17. Сімейство MD4.
18. Хеш-функції та блочні шифри.
19. Підпис Шнора.
20. Підпис Ніберга-Рупеля.
21. Цифрові сертифікати та PKI.
22. Інфраструктура PGP.
23. Сертифікати X509.
24. Сертифікати SPKI.
25. Атака Вінера .
26. Атака Хастада.
27. Атака Франкліна-Рейтера.
28. Тест Міллера-Рабіна.
29. Метод Полінга-Хелліана.

9. Рекомендовані джерела

1. Н. Смарт. Криптография. Москва: Техносфера, 2005, 528 с.
2. Б.Я. Рябко, А.Н. Фионов. Основы современной криптографии для специалистов в информационных технологиях. – М.: Научный мир, 2004, 173 с.
3. А.Г. Ростовцев, Е.Б. Маховенко. Теоретическая криптография. – М., 2005, 490 с.