ЗАТВЕРДЖЕНО

Вченою радою факультету інформаційно-комп'ютерних технологій
31 серпня 2023 р., протокол № 5

Голова Вченої ради
_____ Тетяна НІКІТЧУК

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ ОК 20 «ІНФОРМАЦІЙНА БЕЗПЕКА ТА ЗАХИСТ ПЗ»

для здобувачів вищої освіти освітнього ступеня «бакалавр»
спеціальності 126 «Інформаційні системи та технології»
освітньо-професійна програма «Системи бізнес-аналітики»
факультет інформаційно-комп'ютерних технологій
кафедра комп'ютерних наук

Схвалено на засіданні
кафедри комп'ютерної інженерії та кібербезпеки
28 серпня 2023 р., протокол № 7

Завідувач кафедри
_____ Андрій ЄФІМЕНКО

Гарант освітньо-професійної програми
_____ Олександра СВІНЦИЦЬКА

Розробник: старший викладач кафедри комп'ютерної інженерії та кібербезпеки Покотило Олександра Андріївна, старший викладач кафедри комп'ютерної інженерії та кібербезпеки Щур Наталія Олександрівна

Житомир
2024 – 2025 н.р.

1. Опис навчальної дисципліни

<table>
<tr><td rowspan="2">Найменування показників</td><td rowspan="2">Галузь знань, спеціальність, освітній ступінь</td><td colspan="2">Характеристика навчальної дисципліни</td></tr>
<tr><td>денна форма навчання</td><td>заочна форма навчання</td></tr>
<tr><td>Кількість кредитів 5</td><td>Галузь знань
12 «Інформаційні технології»</td><td colspan="2">Нормативна
(нормативна, за вибором)</td></tr>
<tr><td>Модулів – 2</td><td rowspan="5">Спеціальність 126 «Інформаційні системи та технології»</td><td colspan="2">Рік підготовки:</td></tr>
<tr><td>Змістових модулів – 2</td><td>2-й</td><td>–</td></tr>
<tr><td rowspan="3">Загальна кількість годин – 150</td><td colspan="2">Семестр</td></tr>
<tr><td>4-й</td><td>–</td></tr>
<tr><td colspan="2">Лекції</td></tr>
<tr><td rowspan="11">Тижневих годин для денної форми навчання:
аудиторних 5
самостійної роботи – 4</td><td rowspan="11">Освітній ступінь «бакалавр»</td><td>32 год.</td><td>–</td></tr>
<tr><td colspan="2">Практичні</td></tr>
<tr><td>–</td><td>–</td></tr>
<tr><td colspan="2">Лабораторні</td></tr>
<tr><td>48 год.</td><td>–</td></tr>
<tr><td colspan="2">Самостійна робота</td></tr>
<tr><td>70 год.</td><td>–</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td colspan="2">Вид контролю: екзамен</td></tr>
</table>

Співвідношення кількості годин аудиторних занять до самостійної та індивідуальної роботи становить:

для денної форми навчання – 43 % аудиторних занять, 57 % самостійної та індивідуальної роботи.

2. Мета та завдання навчальної дисципліни

Метою навчальної дисципліни є вивчення та розуміння сучасних загроз інформаційній безпеці, а також принципів, методів, засобів побудови класичних та сучасних алгоритмів шифрування та методів їх зламу; формування та набуття професійних та предметних компетентностей, практичних знань та вмінь з криптографічного захисту інформаційних ресурсів та криптографічного аналізу.

Завданнями вивчення навчальної дисципліни є:

– забезпечення ґрунтовного оволодіння студентами основними поняттями, методами та алгоритмами захисту інформаційних ресурсів;

– формування у студентів предметних та професійних компетентностей, знань та вмінь з теорії та практики криптографічного захисту даних та криптографічного аналізу.

Зміст навчальної дисципліни направлений на формування наступних **компетентностей**, визначених освітньо-професійною програмою зі спеціальності 126 «Інформаційні системи та технології»:

КЗ 1. Здатність до абстрактного мислення, аналізу та синтезу.

КЗ 2. Здатність застосовувати знання у практичних ситуаціях.

КЗ 3. Здатність до розуміння предметної області та професійної діяльності.

КЗ 4. Здатність спілкуватися іноземною мовою.

КЗ 5. Здатність вчитися і оволодівати сучасними знаннями.

КЗ 6. Здатність до пошуку, оброблення та узагальнення інформації з різних джерел.

КЗ 7. Здатність розробляти та управляти проектами.

КЗ 8. Здатність оцінювати та забезпечувати якість виконуваних робіт.

КЗ 10. Здатність зберігати та примножувати моральні, культурні, наукові цінності і досягнення суспільства на основі розуміння історії та закономірностей розвитку предметної області, її місця у загальній системі знань про природу і суспільство та у розвитку суспільства, техніки і технологій, використовувати різні види та форми рухової активності для активного відпочинку та ведення здорового способу життя.

КС 1. Здатність аналізувати об’єкт проектування або функціонування та його предметну область.

КС 3. Здатність до проектування, розробки, налагодження та вдосконалення системного, комунікаційного та програмно-апаратного забезпечення інформаційних систем та технологій, Інтернету речей (IoT), комп’ютерно-інтегрованих систем та системної мережної структури, управління ними.

КС 4. Здатність проектувати, розробляти та використовувати засоби реалізації інформаційних систем, технологій та інфокомунікацій (методичні, інформаційні, алгоритмічні, технічні, програмні та інші).

КС 5. Здатність оцінювати та враховувати економічні, соціальні, технологічні та екологічні фактори на всіх етапах життєвого циклу інфокомунікаційних систем.

КС 6. Здатність використовувати сучасні інформаційні системи та технології (виробничі, підтримки прийняття рішень, інтелектуального аналізу даних та інші), методики й техніки кібербезпеки під час виконання функціональних завдань та обов'язків.

КС 7. Здатність застосовувати інформаційні технології у ході створення, впровадження та експлуатації системи менеджменту якості та оцінювати витрати на її розроблення та забезпечення.

КС 12. Здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями (у тому числі такими, що базуються на використанні Інтернет).

КС13. Здатність проводити обчислювальні експерименти, порівнювати результати експериментальних даних і отриманих рішень.

Отримані знання з навчальної дисципліни стануть складовими наступних **програмних результатів** навчання за спеціальністю 126 «Інформаційні системи та технології»:

ПР 3. Використовувати базові знання інформатики й сучасних інформаційних систем та технологій, навички програмування, технології безпечної роботи в комп'ютерних мережах, методи створення баз даних та інтернет-ресурсів, технології розроблення алгоритмів і комп'ютерних програм мовами високого рівня із застосуванням об'єктно-орієнтованого програмування для розв'язання задач проектування і використання інформаційних систем та технологій.

ПР 9. Здійснювати системний аналіз архітектури підприємства та його ІТ-інфраструктури, проводити розроблення та вдосконалення її елементної бази і структури.

3. Програма навчальної дисципліни

Змістовий модуль 1. Криптосистеми із закритим ключем

Тема 1. Основні поняття криптології

Загальні відомості про захист інформації в інформаційно-телекомунікаційних системах. Історія розвитку криптології. Цілі, завдання та принципи криптології. Основні поняття та визначення. Класифікація криптографічних систем.

Тема 2. Класичні шифри та їх криптоаналіз

Моноалфавітні шифри простої заміни (підстановки), афінні шифри заміни (підстановки). Шифри перестановки. Поліграмні шифри. Поліалфавітні криптосистеми. Методи криптоаналізу класиних шифрів.

Тема 3. Криптографічна стійкість шифрів

Поняття криптографічної стійкості. Теоретична та практична стійкість шифрів. Розсіювання та перемішування. Типи атак на криптосистеми. Абсолютно стійкий шифр.

Тема 4. Потокові симетричні шифри

Основні властивості алгоритмів потокового симетричного шифрування даних. Класифікація потокових алгоритмів. Генератори псевдовипадкових послідовностей. Потоковий шифри RC4.

Тема 5. Алгоритм блокового симетричного шифрування DES

Основні властивості алгоритмів блокового симетричного шифрування даних. Мережа Фейстеля. Стандарт блокового симетричного шифрування DES. Безпека DES. Модифікації DES.

Тема 6. Режими шифрування блоків. Шифр IDEA

Режими роботи блокових шифрів: режим простої заміни, режим зв’язування блоків, режим зі зворотнім зв’язком по шифротексту, режим зі зворотнім зв’язком по виходу, режим лічильника. Міжнародний стандарт шифрування IDEA. Порівняльний аналіз DES та IDEA.

Тема 7. Удосконалений стандарт шифрування AES

Математична база алгоритму шифрування даних AES: додавання та множення байтів у полі Галуа. Основні операції при зашифруванні та дешифруванні за алгоритмом AES. Формування раундових ключів.

Тема 8. Національний стандарт шифрування ДСТУ 7624:2014 («Калина»)

Етапи шифрування даних за алгоритмом «Калина». Формування допоміжного ключа та раундових (циклових) ключів шифрування. Режими роботи криптографічного алгоритму «Калина». Порівняльний аналіз AES та «Калина».

Змістовий модуль 2. Криптосистеми з відкритим ключем

Тема 9. Основні положення криптографії з відкритим ключем

Ідея криптосистеми з відкритим ключем. Поняття односторонньої функції. Математичні основи асиметричних шифрів. Алгоритм рюкзака (криптосистема Меркла-Хелмана). Порівняльний аналіз симетричних та асиметричних алгоритмів.

Тема 10. Асиметричні криптосистеми

Алгоритм RSA. Проблема розкладання на множники великих чисел. Алгоритм Ель-Гамаля. Алгоритм обміну ключами Діффі-Хелмана. Проблема дискретного логарифмування.

Тема 11. Криптографічні хеш-функції

Поняття хеш-функції та їх основні властивості. Область застосування хеш-функцій. Хеш-функція SHA-256. Хеш-функція «Купина» (ДСТУ 7564:2014). Інші хеш-функції.

Тема 12. Цифровий підпис

Принципи забезпечення автентичності даних з використанням цифрового підпису (ЦП). Процедури підписування та перевірки ЦП. Схеми цифрового підпису RSA та Ель-Гамаля. Стандарт цифрового підпису DSS.

Тема 13. Криптографічні протоколи

Криптографічні протоколи управління ключами. Криптографічні протоколи автентифікації. Механізми розподілення таємниці. Синтез та аналіз криптографічних протоколів.

Тема 14. Основи криптографії на еліптичних кривих

Математичний опис криптографічних еліптичних кривих. Основні операції в групах точок еліптичних кривих. Алгоритм обміну ключами ECDH. Стандарт цифрового підпису ECDSS.

Тема 15. Елементи криптоаналізу сучасних шифрів

Завдання та принципи криптоаналізу. Диференціальний криптоаналіз. Лінійний криптоаналіз. Інші методи криптоаналізу.

Тема 16. Нові напрямки в криптографії

Основи квантового шифрування. Технологія «блокчейн». Програмні засоби криптографічного захисту даних.

4. Структура (тематичний план) навчальної дисципліни

Змістові модулі і теми	Кількість годин			
	денна форма			
	усього	лекції	лабораторні	самостійна робота
Модуль 1				
Змістовий модуль 1. Криптосистеми із закритим ключем				
Тема 1. Основні поняття криптології	8	2	2	4
Тема 2. Класичні шифри та їх крипоаналіз	10	2	4	4
Тема 3. Криптографічна стійкість шифрів	10	2	2	6
Тема 4. Потокові симетричні шифри	8	2	2	4
Тема 5. Алгоритм блокового симетричного шифрування DES	10	2	4	4
Тема 6. Режими шифрування блоків. Шифр IDEA	8	2	2	4
Тема 7. Удосконалений стандарт шифрування AES	10	2	4	4
Тема 8. Національний стандарт шифрування ДСТУ 7624:2014 («Калина»)	10	2	4	4
Разом за змістовий модуль 1	74	16	24	34
Змістовий модуль 2. Криптосистеми з відкритим ключем				
Тема 9. Основні положення криптографії з відкритим ключем	10	2	2	6
Тема 10. Асиметричні криптосистеми	10	2	4	4
Тема 11. Криптографічні хеш-функції	10	2	4	4
Тема 12. Цифровий підпис	10	2	4	4
Тема 13. Криптографічні протоколи	8	2	2	4
Тема 14. Основи криптографії на еліптичних кривих	10	2	4	4
Тема 15. Елементи криптоаналізу сучасних шифрів	10	2	2	6
Тема 16. Нові напрямки в криптографії	8	2	2	4
Разом за змістовий модуль 2	76	16	24	36
ВСЬОГО	150	32	48	70

5. Теми практичних (лабораторних) занять

№ з/п	Назва теми	Кількість годин
		денна форма
1	Класичний шифр простої заміни та його криптоаналіз. Біграмний шифр	6
2	Класичний шифр поліалфавітної заміни та його криптоаналіз. Криптосистема Хілла	6
3	Моделювання процесів шифрування за допомогою шифру одноразового блокноту. Алгоритм DES	6
4	Дослідження властивостей блокового симетричного шифру AES	6
5	Дослідження основних операцій шифру «Калина» у процесі формування допоміжного ключа	6
6	Асиметричні шифри RSA та Ель-Гамаля. Алгоритм обміну ключами Діффі-Хелмана	6
7	Хеш-функції. Цифровий підпис	6
8	Криптографічні перетворення в групах точок еліптичних кривих	6
РАЗОМ		48

6. Завдання для самостійної роботи

Тема 1. Основні поняття криптології

1. Математична модель шифрів, теорія зв’язку в секретних системах Клода Шенона.
2. Законодавча база України в галузі криптографії.

Тема 2. Класичні шифри та їх криптоаналіз

1. Взаємний індекс збігу.
2. Роторні шифрувальні машини та їх криптоаналіз.

Тема 3. Криптографічна стійкість шифрів

1. Модель порушника.
2. Методи та види несанкціонованого доступу.

Тема 4. Потокові симетричні шифри

1. Порівняльний аналіз генераторів псевдовипадкових послідовностей.
2. Потоковий шифр SNOW 2.0.
3. Потоковий шифр Salsa 20.

Тема 5. Алгоритм блокового симетричного шифрування DES

1. Алгоритм шифрування Lucifer.
2. Способи доповнення блоків (padding).

Тема 6. Режими шифрування блоків. Шифр IDEA

1. Режим зв’язування блоків із поширенням (PCBC).
2. Безпека IDEA.

Тема 7. Удосконалений стандарт шифрування AES

1. Алгоритми-фіналісти конкурсу AES: MARS, RC6, Serpent, Twofish.
2. Режими шифрування AES.

Тема 8. Національний стандарт шифрування ДСТУ 7624:2014 («Калина»)

1. Стандарт криптографічного перетворення даних ДСТУ ГОСТ 28147:2009.
2. Порівняльний аналіз ДСТУ ГОСТ 28147:2009 та ДСТУ 7624:2014 («Калина»).

Тема 9. Основні положення криптографії з відкритим ключем

1. Основи модулярної арифметики.
2. Поняття і властивості алгебраїчних груп.
3. Тестування чисел на простоту.

Тема 10. Асиметричні криптосистеми

1. Головоломка Меркла.
2. Криптосистема Рабіна.
3. Джерела ключів асиметричних криптосистем та вимоги до них.

Тема 11. Криптографічні хеш-функції

1. Хеш-функції на основі блокових шифрів. MAC-коди.
2. Порівняльний аналіз хеш-функцій MD2, MD4, MD5 та MD6.

Тема 12. Цифровий підпис

1. Правове регулювання ЦП в Україні та світі.
2. Алгоритм цифрового підпису Шнорра.
3. Сліпий підпис, незаперечний підпис, груповий підпис.

Тема 13. Криптографічні протоколи

1. Вимоги до протоколів автентифікації.
2. Модель загроз порушення автентичності.
3. Модель взаємної недовіри та взаємного захисту.

Тема 14. Основи криптографії на еліптичних кривих

1. Алгоритм обчислення порядку еліптичної кривої.
2. Криптосистема Мессі-Омури над групою точок еліптичної кривої.
3. Аналіз вразливостей криптографічної схеми цифрового підпису ECDSA.

Тема 15. Елементи криптоаналізу шифрів

1. Силові методи криптоаналізу.
2. Криптоаналіз по побічним каналам.

Тема 16. Нові напрямки в криптографії

1. Стеганографія та її застосування.
2. Квантовий криптоаналіз.

7. Індивідуальні завдання

Індивідуальні завдання не передбачено навчальним планом.

8. Методи навчання

За джерелами знань використовуються такі методи навчання: словесні – розповідь, пояснення, лекція, інструктаж; наочні – демонстрація, ілюстрація; практичні – лабораторна робота.

За характером логіки пізнання використовуються такі методи: аналітичний, синтетичний, аналітико-синтетичний, індуктивний, дедуктивний.

За рівнем самостійної розумової діяльності використовуються методи: проблемний, частково-пошуковий, дослідницький.

9. Методи контролю

Поточний контроль – індивідуальне та фронтальне опитування, тестування за темами, захист лабораторних робіт у формі співбесіди, написання модульних контрольних робіт, перевірка самостійної роботи. Самостійна робота оцінюється під час заходів модульного контролю.

Підсумковий контроль – екзамен (підсумкове тестування).

Оцінка за екзамен може виставлятися за результатами роботи студента впродовж усього семестру.

10. Розподіл балів

16 лекцій по 2 год. (32 год.)	8 лабораторних по 6 год. (48 год.)		6 тестів	2 модульні контрольні роботи	Сума
0,5 балів за відвідування	4 бали за звіт	0,5 балів за роботу на парі	2 бали за тест	20 балів	
8 балів	32 бали	8 балів	12 балів	40 балів	100 балів

Шкала оцінювання

За шкалою	Екзамен	Залік	Бали
A	Відмінно	Зараховано	90-100
B	Добре	Зараховано	82-89
C			74-81
D	Задовільно	Зараховано	64-73
E			60-63
FX	Незадовільно	Не зараховано	35-59
F		Не зараховано	0-34

11. Рекомендована література

Основна література

1. Бобало Ю. Я. Інформаційна безпека: навч. посібник / Ю. Я. Бобало, І. В. Горбатий, М. Д. Кіселичник та ін.; за заг. ред. д-ра техн. наук, проф. Ю. Я. Бобала та д-ра техн. наук, доц. І. В. Горбатого. – Львів : Видавництво Львівської політехніки, 2019. – 580 с.
2. Глинчук Л.Я. Криптологія: навч.-метод. посіб. / Л. Я. Глинчук – Луцьк: Вежа-Друк, 2014. – 164 с.
3. Горбенко І. Д. // Прикладна криптологія: Теорія. Практика. Застосування / І. Д. Горбенко, Ю. І. Горбенко. – Харків : Форт, 2013. – 880 с.
4. ДСТУ 7624:2014. Інформаційні технології. Криптографічний захист інформації. Алгоритм симетричного блокового перетворення. – Введ. 01–07–2015. – К. :Мінекономрозвитку України, 2015.
5. Задірака В.К. Комп'ютерні технології криптографічного захисту інформації на спеціальних цифрових носіях: навч. посіб. / В. К. Задірака, А. М. Кудін, В. О. Людвиченко, О. С.Олексюк. – К. -Тернопіль: Підручники і посібники, 2007. – 272 с.
6. Козіна Г.Л. Криптографія від історії до сучасних стандартів: навч.посібник / Г. Л. Козіна. – Запоріжжя : НУ «Запорізька політехніка», 2020. – 192 с.
7. Корченко О. Г. Прикладна криптологія: системи шифрування : підручник / О. Г. Корченко, В. П. Сіденко, Ю. О. Дрейс. – К. : ДУТ, 2014. – 448 с.
8. Alfred J. Menezes. Handbook of Applied Cryptography/ Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. Publisher: CRC Press, 2001. – 780 pages
9. Bruce Schneier. Applied cryptography: protocols, algorithms, and source code in C / 2nd ed. – New York : JohnWiley & Sons, Inc.,1995. – 792 pages.
10. Jean-Philippe Aumasson. Serious Cryptography: A Practical Introduction to Modern Encryption Paperback. Kindle Edition, 2017. – 313 pages.

Допоміжна література

1. Бабенко Т.В. Криптологія у прикладах, тестах і задачах: навч. посібник / Т.В.Бабенко, Г.М.Гулак, С.О.Сушко, Л.Я.Фомичова. – Д.: Національний гірничий університет, 2013. – 318 с.
2. Ємець В. Сучасна криптографія. Основні поняття/ Ємець В., Мельник А., Попович Р. – Л.: БаК, 2003. – 144 с.
3. Маркова І.І. Захист інформації. Криптографічні методи: Підручник для вищих навчальних закладів. / І.І. Маркова, А.І. Рибак, Ю.С. Ямпольський. – Одеса, 2001. – 175 с.

12. Інформаційні ресурси в Інтернеті

1. The CrypTool Portal [Електронний ресурс]. — Режим доступу : http://www.cryptool.org/en
2. CrypTool-Online [Електронний ресурс]. – Режим доступу: https://www.cryptool.org/en/cto/
3. GnuPG [Електронний ресурс]. – Режим доступу: http://www.gnupg.org