Черкаський національний університет імені Богдана Хмельницького
ННІ Інформаційних та освітніх технологій
Кафедра прикладної математики та інформатики

ЗАТВЕРДЖЕНО
Завідувач кафедри
ПМ та інформатики
_____/О.В.Піскун

РОБОЧА ПРОГРАМА НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ ТА БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ»

1. Загальна інформація про курс

Назва курсу, мова викладання	**ТЕХНОЛОГІЇ ЗАХИСТУ ІНФОРМАЦІЇ ТА БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ** Курс викладається українською мовою.
Статус дисципліни	Обов'язкова
Викладач	Дзюба Вікторія Анатоліївна, кандидат технічних наук, викладач кафедри прикладної математики та інформатики
Код класу /	
Корпоративна пошта / E-mail:	viktoriya.dzyuba15@vu.cdu.edu.ua
Затвердження та перегляд робочої навчальної програми	Розглянуто та затверджено на засіданні кафедри прикладної математики та інформатики 28.08.2024, протокол № 1

2. Анотація до курсу

Навчальна дисципліна «Технології захисту інформації та безпека інформаційних систем» є обов'язковим курсом циклу професійної та практичної підготовки фахівця з інформаційних технологій, її вивчення рекомендується планувати у другому семестрі.

Курс охоплює сучасні напрями забезпечення безпеки інформаційних систем, які базуються на технічних, криптографічних та програмних методах і засобах захисту інформації. Крім цього, розглядаються питання захисту інформації в інформаційних системах, організаційно-правове забезпечення захисту інформації.

3. Мета та цілі курсу

Мета курсу - формування компетентностей стосовно розробки технологій захисту інформації, дослідження та практична реалізація механізмів захисту інформаційних систем, які базуються на використанні криптографічних алгоритмів для забезпечення цілісності та конфіденційності інформаційних систем та технологій.

Завданнями вивчення навчальної дисципліни «Технології захисту інформації та безпека інформаційних систем» передбачено:

- отримання знань з основних положень законодавства у галузі захисту інформації, основних міжнародних та національних стандартів з безпеки інформаційних систем та технологій;
- отримання знань в області криптографічного захисту інформації та математичних методів для дослідження поставлених задач;
- отримання знань про сучасні криптографічні алгоритми та криптографічні протоколи;
- розвиток особистості майбутнього спеціаліста в галузі інформаційних технологій, формування компетенцій, що сприяють реалізації в практичній діяльності.

4. Компетентності та очікувані результати навчання

Навчальна дисципліна «Технології захисту інформації та безпека інформаційних систем» забезпечує формування таких компетентностей, передбачених освітньою програмою підготовки магістрів спеціальності: 126 Інформаційні системи та технології.

Загальні компетентності:

ЗК05. Здатність оцінювати та забезпечувати якість виконуваних робіт.

ЗК06. Здатність застосовувати знання у практичних ситуаціях.

Фахові компетентності *(визначені стандартом та освітньою програмою компетентності, формування яких забезпечує ця навчальна дисципліна)***:**

СК04. Здатність розробляти математичні, інформаційні та комп'ютерні моделі об'єктів і процесів інформатизації.

СК06. Здатність управляти інформаційними ризиками на основі концепції інформаційної безпеки.

СК08. Здатність управляти та користуватися сучасними інформаційно-комунікаційними системами та технологіями, у першу чергу,

орієнтованими на роботу у локальній та глобальній мережі.

Згідно з вимогами освітньо-професійної програми, **програмними результатами вивчення** дисципліни «Технології захисту інформації та безпека інформаційних систем» є такі:

РН01. Відшуковувати необхідну інформацію в науковій і технічній літературі, базах даних, інших джерелах, аналізувати та оцінювати цю інформацію.

РН06. Обґрунтовувати вибір технічних та програмних рішень з урахуванням їх взаємодії та потенційного впливу на вирішення організаційних проблем, організовувати їх впровадження та використання.

РН08. Розробляти моделі інформаційних процесів та систем різного класу, використовувати методи моделювання, формалізації, алгоритмізації та реалізації моделей з використанням сучасних комп'ютерних засобів.

РН10. Забезпечувати якісний кіберзахист ІСТ, планувати, організовувати, впроваджувати та контролювати функціонування систем захисту інформації.

5. Обсяг і характеристика курсу

Найменування показників	**Характеристика навчального курсу**	
	денна форма навчання	**заочна форма навчання**
Освітня програма, спеціальність	Веб-орієнтовані інформаційні системи, 126 Інформаційні системи та технології	
Рік навчання	1	
Семестр вивчення	2	
обов'язкова /вибіркова	обов'язкова	
Кількість кредитів ЄКТС	4	
Загальний обсяг годин	120	
Кількість годин навчальних занять	40	
Лекційні заняття	14	
Практичні заняття	0	
Семінарські заняття	0	
Лабораторні заняття	26	
Самостійна та індивідуальна робота	80	
Форма підсумкового контролю	екзамен	

6. Пререквізити курсу

Для вивчення курсу студенти потребують базових знань з дисциплін «Алгебра та геометрія», «Теорія ймовірностей та математична статистика», «Дискретна математика», «Програмне забезпечення та інформаційно-комунікаційні технології».

7. Технічне забезпечення

Вивчення курсу не потребує використання програмного забезпечення, крім загальновживаних офісних програм та онлайн-сервісів.

8. Політика курсу

Письмові роботи. Очікується, що студенти виконають декілька видів письмових робіт (звіти з лабораторних робіт, підготовка презентацій, підсумковий контроль). У випадку якщо студент не отримав протягом семестру необхідну кількість балів для допуску до екзамену, він може виконати передбачені програмою завдання, узгодивши з викладачем терміни виконання.

Академічна доброчесність. Очікується, що роботи студентів будуть їх оригінальними дослідженнями чи міркуваннями. Відсутність посилань на використані джерела, фабрикування джерел, списування, втручання в роботу інших студентів можуть бути кваліфіковані як академічна недоброчесність. Виявлення ознак академічної недоброчесності в письмовій роботі студента є підставою для її не зарахування викладачем, незалежно від масштабів плагіату.

Відвідування занять. Відвідання занять є важливою складовою навчання. Очікується, що всі студенти відвідають усі лекції і лабораторні заняття курсу. Студенти мають інформувати викладача про неможливість відвідати заняття. Допускається 1 пропуск з поважних причин, який не впливатиме на систему оцінювання. У будь-якому випадку студенти зобов'язані дотримуватися усі строків визначених для виконання усі видів письмових робіт, передбачених курсом.

9. Схема курсу

Тема, основні питання / завдання	Розподіл годин за темами та формам и занять (денна/за очна)	Форми та методи проведення	Література. Ресурси в інтернеті	Завдання для самостійної роботи, год	Форма контролю, бали
ЗМІСТОВИЙ МОДУЛЬ 1. БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ					

Лекція 1. Актуальність проблеми забезпечення безпеки в інформаційних системах. 1. Поняття інформаційної безпеки. Основні складові інформаційної безпеки. 2. Поняття несанкціонованого доступу, вразливості комп'ютерних систем, загрози вторгнення, каналу витоку інформації. 3. Цілі, суб'єкти та схеми активних та пасивних вторгнень.	2	Лекція-візуалізація (з використанням презентації).	Основна: 1, 4, 5. Додаткова: 2, 4, 5. Ел. Ресурси: 1-4	Самостійно опрацювати теоретичні питання теми (2 год): 1. Методи та пристрої забезпечення захисту і безпеки. 2. Механізми і політики розмежування прав доступу. 3. Огляд літератури з теми лекції (2 год).	Обговорення, презентації, доповідь на лабораторному занятті (0-5 балів)
Лабораторне заняття 1-2. Актуальність проблеми забезпечення безпеки в інформаційних системах. 1. Інформація, її значення і необхідність захисту в умовах сьогодення. 2. Сучасні задачі технологій захисту інформації. 3. Моделі забезпечення інформаційної безпеки. 4. Захист інформації в розподілених інформаційних системах.	4	Практична робота. Обладнання Комп'ютер/ноутбук з доступом до мережі Інтернет	Основна: 2, 3, 5. Додаткова: 1, 3, 5. Ел. Ресурси: 1-6	1. Розробити схему основних складових інформаційної безпеки (1 год). 2. Виконати порівняльну характеристику підходів до створення систем захисту інформації в комп'ютерних системах (2 год). 3. Побудувати модель забезпечення інформаційної безпеки (2 год).	Завдання 1: 0-1 балів Завдання 2: 0-2 балів Завдання 3: 0-2 балів
Лекція 2. Організаційно правові аспекти захисту інформації. 1. Стандарти та специфікації в галузі інформаційної безпеки. 2. Політика розмежування прав доступу. 3. Засоби безпеки систем управління баз даних.	2	Лекція-інформація (з використанням презентації).	Основна: 1-3, 5. Додаткова: 2, 3, 4. Ел. Ресурси: 1-4.	Самостійно опрацювати актуальні питання за темою лекції (2 год): 1. Перший стандарт у галузі оцінки захищеності комп'ютерних систем. 2. Оціночні стандарти і технічні специфікації. 3. Захист інформації від випадкових загроз. 4. Дискреційне розмежування доступу.	Обговорення, презентації, доповідь на лабораторному занятті (0-3 балів)
Лабораторне заняття 3. Організаційно правові аспекти захисту інформації.	2	Практична робота.	Основна: 1, 2, 5.	1. Підготуватися до обговорення теоретичних питань лекції 2 (2 год).	Завдання 1: 0-1 балів

1. Критерії оцінки безпеки інформаційних технологій. 2. Політика безпеки. Рівень гарантованості безпеки інформаційних систем. 3. Законодавчий, адміністративний і процедурний рівні захисту інформації. 4. Механізми безпеки. Класи безпеки.		Обладнання Комп'ютер/ноутбук з доступом до мережі Інтернет	Додаткова: 3, 4, 5. Ел. Ресурси: 1-6	2. Підготувати презентацію для доповіді відповідно до плану практичного заняття (2 год.).	Завдання 2: 0-2 балів
Лекція 3. Основні програмно-технічні заходи для захисту програмного забезпечення. 1. Основні поняття програмно-технічного рівня інформаційної безпеки. 2. Важливість захисту програмного забезпечення в сучасних умовах. 3. Класифікація методів та засобів захисту програмного забезпечення.	2	Лекція. Обговорення теоретичних питань у форматі дискусії (з використанням презентації).	Основна: 1, 2, 3. Додаткова: 1, 2, 5. Ел. Ресурси: 1-4	Самостійно опрацювати теоретичні питання теми (2 год): 1. Особливості сучасних інформаційних систем, які є важливими з точки зору безпеки. 2. Архітектурна безпека. Сервіси безпеки.	Обговорення, презентації, доповідь на лабораторному занятті (0-5 балів)
Лабораторне заняття 4-5. Основні програмно-технічні заходи для захисту програмного забезпечення. 1. Новітні технології захисту життєвого циклу програмного забезпечення. 2. Програмно-технічні заходи на основі ШІ. 3. Моделі систем доказово достатнього захисту інформації. 4. Матрична модель системи захисту Белла і Ла-Падули.	4	Практична робота. Обладнання Комп'ютер/ноутбук з доступом до мережі Інтернет	Основна: 1, 3, 5. Додаткова: 2, 4, 5. Ел. Ресурси: 1-4	1. Підготуватися до обговорення теоретичних питань лекції 3 (2 год). 2. Скласти класифікацію шкідливих програм із їх загальними характеристиками (2 год). 3. Скласти порівняльну таблицю сучасних технологій захисту програмного забезпечення (2 год). 4. Проходження курсу на платформі Prometheus «Основи інформаційної безпеки» (10 год).	Завдання 1: 0-1 балів Завдання 2: 0-2 балів Завдання 3: 0-2 балів Завдання 4: 0-8 балів
Всього балів за змістовим модулем 1					**21**
Всього годин за змістовим модулем 1	**49**				
Лекцій	**6**				
Практичних занять	**0**				
Лабораторних занять	**10**				

Самостійна робота	**33**				
ЗМІСТОВИЙ МОДУЛЬ 2. КРИПТОГРАФІЧНІ ОСНОВИ ЗАХИСТУ ІНФОРМАЦІЇ					
Лекція 4. Основи криптографії та шифрування даних. 1. Постановка задачі криптографії. 2. Ключ. Шифр. Цілі криптозахисту. 3. Поняття криптографічної стійкості. 4. Шифри моноалфавітної та поліалфавітної заміни. Маршрутні перестановки.	2	Лекція-інформація (з використанням презентації).	Основна: 3, 4, 5. Додаткова: 2, 5. Ел. Ресурси: 1-4.	Самостійно опрацювати питання теми (3 год): 1. Частотний криптоаналіз. 2. Шифр Плейфера. Структура матриці шифру Плейфера. 3. Типи атак на криптосистеми. 4. Ознайомитися із функціоналом програми CrypTool Online.	Обговорення, презентації, доповідь на лабораторному занятті (0-4 балів)
Лабораторне заняття 6. Основи криптографії та шифрування даних. 1. Класичний шифр простої заміни та його криптоаналіз. 2. Біграмний шифр.	2	Практична робота. Обладнання Комп'ютер/ноутбук зі встановленим програмним забезпеченням Python та доступом до мережі Інтернет, текстові повідомлення для шифрування згідно варіанту.	Основна: 1, 2, 5. Додаткова: 2, 4, 5. Ел. Ресурси: 1-4	1. Підготуватися до обговорення теоретичних питань лекції 4 (1 год). 2. Підготувати звіт з лабораторної роботи (2 год.).	Завдання 1: 0-2 балів Завдання 2: 0-2 балів
Лабораторне заняття 7. Класичний шифр поліалфавітної заміни та його криптоаналіз. Криптосистема Хілла. 1. Зашифрування, дешифрування та криптоаналіз повідомлення, зашифрованого шифром Віженера. 2. Побудова та реалізація алгоритму шифрування криптосистемою Хілла.	2	Практична робота. Обладнання Комп'ютер/ноутбук зі встановленим програмним забезпеченням Python та доступом до мережі Інтернет,	Основна: 2, 4, 5. Додаткова: 2, 3, 5. Ел. Ресурси: 1-4	1. Підготуватися до обговорення теоретичних питань лекції 4 (2 год). 2. Підготувати звіт з лабораторної роботи (2 год.).	Завдання 1: 0-2 балів Завдання 2: 0-3 балів

		текстові повідомлення для шифрування згідно варіанту.			
Лекція 5. Основні концепції шифрування. 1. Атаки на систему шифрування. 2. Шифрування з секретним ключем. 3. Шифри підстановки. 4. Одноразові блокноти. Шифрування паролів.	2	Лекція-інформація (з використанням презентації).	Основна: 1, 4, 5. Додаткова: 2, 5. Ел. Ресурси: 1-4.	Самостійно опрацювати питання теми (3 год): 1. Основні конценції задач дешифрування. 2. Шифрування із залученням ШІ 3. Шифр Вернама й проблема практичного використання абсолютно стійкого шифру.	Обговорення, презентації, доповідь на лабораторному занятті (0-5 балів)
Лабораторне заняття 8. Моделювання процесів шифрування за допомогою операції XOR. Алгоритм DES. 1. Шифрування за допомогою операції XOR. 2. Зашифрування повідомлення за допомогою алгоритму DES.	2	Практична робота. Обладнання Комп'ютер/ноутбук зі встановленим програмним забезпеченням Python та доступом до мережі Інтернет, текстові повідомлення для шифрування згідно варіанту.	Основна: 1, 3, 5. Додаткова: 2, 3, 5. Ел. Ресурси: 1-4	1. Підготуватися до обговорення теоретичних питань лекції 5 (2 год). 2. Підготувати звіт з лабораторної роботи (3 год.).	Завдання 1: 0-2 балів Завдання 2: 0-3 балів
Лекція 6. Потокові симетричні шифри. 1. Загальні відомості про потокові шифри. 2. Генератори псевдовипадкових чисел. 3. Симетричний апаратно-орієнтований паралельний потоковий шифр Trivium. 4. Синхронний поточний апаратно-орієнтований шифр Grain.	2	Лекція-візуалізація (з використанням презентації).	Основна: 1, 2, 5. Додаткова: 2, 3, 5. Ел. Ресурси: 1-4.	Самостійно опрацювати актуальні питання за тематикою лекції (3 год): 1. Класифікація задач симетричної криптографії. 2. Лінійні регістри зсуву. 3.Режими блокового шифрування. 4. Стандарт симетричного блокового криптоалгоритму України.	Обговорення, презентації, доповідь на лабораторному занятті (0-6 балів)
Лабораторне заняття 9-10. Дослідження властивостей блокового симетричного шифру AES.	4	Практична робота. Обладнання	Основна: 1, 4, 5. Додаткова:	1. Підготуватися до обговорення теоретичних питань лекції 6 (2 год). 2. Підготувати звіт з лабораторної роботи (3	Завдання 1: 0-2 балів Завдання 2: 0-4

1. Удосконалений стандарт шифрування AES. 2. Шифрування та дешифрування тексту за допомогою алгоритму AES. 3. Алгоритм генерації раундових ключів для шифрування даних. 4. Порівняльний аналіз результатів зашифрування блоків даних у різних режимах за допомогою алгоритму AES у програмі CrypTool.		Комп'ютер/ноутбук зі встановленим програмним забезпеченням Python та доступом до мережі Інтернет, текстові повідомлення для шифрування згідно варіанту.	2, 4, 5. Ел. Ресурси: 1-4	год.).	балів
Лекція 7. Асиметричні криптосистеми. 1. Основні положення криптографії з відкритим ключем. 2. Криптосистема Меркла-Хелмана. Алгоритм рюкзака. 3. Електронний цифровий підпис.	2	Лекція з використанням методів проблемного навчання (з використанням презентації).	Основна: 1-3. Додаткова: 2, 3, 5. Ел. Ресурси: 1-4.	Самостійно опрацювати актуальні питання за тематикою лекції (2 год): 1. Класифікація задач криптографії з відкритим ключем. 2. Криптографічні операції в ОС Windows. 3. Криптографічні провайдери. Сертифікати.	Обговорення, презентації, доповідь на лабораторному занятті (0-7 балів)
Лабораторне заняття 11-12. Криптосистеми з відкритим ключем. Електронний цифровий підпис. 1. Реалізація алгоритму рюкзака. (криптосистема Меркла-Хелмана) 2. Створення та перевірка цифрового підпису повідомлення за допомогою алгоритму RSA. 3. Створення та перевірка цифрового підпису повідомлення за допомогою алгоритму Ель-Гамаля. 4. Система GNU Privacy Guard та оболонка Kleopatra.	4	Практична робота. Обладнання Комп'ютер/ноутбук зі встановленим програмним забезпеченням Python та доступом до мережі Інтернет, текстові повідомлення для шифрування згідно варіанту.	Основна: 1, 4, 5. Додаткова: 2, 4, 5. Ел. Ресурси: 1-4	1. Підготуватися до обговорення теоретичних питань лекції 7 (2 год). 2. Підготувати звіт з лабораторної роботи (6 год.).	Завдання 1: 0-2 балів Завдання 2: 0-5 балів

Лабораторне заняття 13. Хеш-функції. Основи криптографії на еліптичних кривих. 1. Використання криптографічних Хеш-функцій. 2. Стандарт цифрового підпису DSS. 3. Криптосистеми на еліптичних кривих.	2	Практична робота. Обладнання Комп'ютер/ноутбук зі встановленим програмним забезпеченням Python та доступом до мережі Інтернет, текстові повідомлення для шифрування згідно варіанту.	Основна: 1, 4, 5. Додаткова: 2, 4, 5. Ел. Ресурси: 1-4	1. Підготувати звіт з лабораторної роботи (3 год.). 2. Проходження курсу на платформі Дія. Цифрова освіта. «Криптограмотність та блокчейн» (8 год).	Завдання 1: 0-4 балів Завдання 2: 0-8 балів
Всього балів за змістовим модулем 2					**39**
Всього годин за змістовим модулем 2	**71**				
Лекцій	**8**				
Практичних занять	**0**				
Лабораторних занять	**16**				
Самостійна робота	**47**				
Підсумковий контроль: екзамен		Тестування			**40**

10. Система оцінювання та вимоги

Навчальні досягнення студентів оцінюються за 100-бальною шкалою Університету, чотирибальною шкалою (5 «відмінно», 4 «добре», 3 «задовільно», 2 «незадовільно»), і шкалою оцінок ЄКТС. На поточний контроль відводиться 60 балів, на підсумковий контроль (екзамен) – 40 балів.

Оцінювання поточної успішності студентів на окремих навчальних заняттях та за виконання завдань самостійної роботи визначається диференційовано, відповідно до рівня складності завдань, та встановлюється в межах від 0 до 7 балів.

Бали за роботу протягом семестру нараховуються: за підготовку доповідей (у вигляді презентації) та участь в обговореннях, дискусіях під час лабораторних занять (13 балів); здачі звітів лабораторних робіт (31 бал); проходження курсу на платформі Prometheus «Основи інформаційної безпеки» (8 балів); проходження курсу на платформі Дія. Цифрова освіта. «Криптограмотність та блокчейн» (8 балів); проходження підсумкового контролю у вигляді комп'ютерного тесту (40 балів).

Виконання лабораторних робіт, завдань самостійної роботи та індивідуальних завдань є обов'язковим. До їх виконання допускаються всі студенти. Студент, який не виконав поточних завдань, не підготувався до лабораторних занять, отримує 0 балів / не отримує жодного

бала. Поточну заборгованість, пов'язану з непідготовленістю або недостатньою підготовленістю до навчальних занять, студент повинен ліквідувати шляхом виконання у визначений термін завдань, передбачених програмою. За виконані завдання нараховуються від 0 до 7 балів.

Студенти, які за результатами поточного контролю набрали менше 20 балів, вважаються такими, що мають академічну заборгованість, ліквідація якої є обов'язковою. Студенти, які не мають академічної заборгованості за результатами поточного контролю, допускаються до екзамену.

11. Критерії оцінювання успішності навчання

1. Завданням **поточного контролю** є систематична перевірка розуміння та засвоєння програмного матеріалу шляхом усного та письмового опитування, аналіз виконання завдань лабораторної, індивідуальної та самостійної роботи, умінь самостійно опрацьовувати навчальний матеріал, здатності публічно, письмово чи в електронному форматі представляти певний матеріал.
Критеріями оцінювання у ході поточного контролю є:
а) під час поточної аудиторної роботи на лекційних та лабораторних заняттях:
• активна участь у дискусіях та пропонованих формах роботи на лекційних та лабораторних заняттях;
• доповнення та запитання на лекційних та лабораторних заняттях.
б) при усних відповідях:
• повнота розкриття питання;
• логіка викладення, культура мовлення;
• впевненість, емоційність та аргументованість;
• використання основної та додаткової літератури (підручників, навчальних посібників, журналів, інших періодичних видань, інтернет-ресурсів тощо);
• аналітичні міркування, уміння робити порівняння, висновки.
в) при виконанні письмових завдань:
• повнота розкриття питання;
• цілісність, систематичність, логічна послідовність;
• підготовка матеріалу за допомогою комп'ютерної техніки, різних технічних засобів.
г) при виконанні завдань для самостійної та індивідуальної роботи:
• повнота виконання завдання;
• творчість та самостійність виконання.

2. Завданням **підсумкового контролю** (екзамену) є комплексна діагностика результатів навчання, глибини засвоєння студентом програмного матеріалу з навчальної дисципліни, логіки та взаємозв'язків між окремими його змістовими модулями, здатності до творчого використання набутих знань. Екзамен проводиться у формі тестування, яке складається із комбінованих завдань теоретичного та практичного характеру, які охоплюють пройдений матеріал даної дисципліни.

12. Перелік питань для підсумкового контролю

1. Основні напрями захисту інформації та безпеки комп'ютерних систем.
2. Поняття технології захисту інформації. Потенційні загрози та канали витоку інформації у комп'ютерних системах.
3. Організаційно-правові та технічні аспекти захисту інформації. Механізми і політики розмежування прав доступу.
4. Загрози безпеці програмного забезпечення інформаційних систем.
5. Методи ідентифікації та автентифікації користувачів
6. Ідентифікація користувача на основі системи простих паролів.
7. Модифікація системи простих паролів.
8. Реєстраційні та операційні журнали та їх роль у системах захисту інформації.
9. Шифрування на основі одно-абеткових підстановок. Шифр Цезаря.
10. Федеральний стандарт США для симетричних систем шифрування.
11. Асиметричні системи шифрування на основі відкритих та закритих ключів. Алгоритм Ель-Гамаля.
12. Асиметричні системи шифрування на основі відкритих та закритих ключів. Алгоритм RSA.
13. Цифрові підписи та протоколи аутентифікації для симетричних систем шифрування.
14. Протоколи аутентифікації суб'єктів та встановлення комунікації в мережах на основі використання лише закритих ключів.
15. Встановлення справжності суб’єктів у системах на основі використання алгоритму шифрування RSA.
16. Аутентифікація суб'єктів у системах за допомогою відкритих ключів.
17. Підтвердження справжності повідомлень у системах на основі використання цифрових підписів.
18. Управління ключами шифрування у захисті POS-терміналів та банкоматів у режимі реального часу та в режимі онлайн.
19. Узагальнена структура електронної платіжної системи.
20. Вимоги щодо захисту суб’єктів від несанкціонованого доступу відповідно до критеріїв доступності та спостережності.
21. Загальні підходи та методи забезпечення безпеки комп'ютерних систем.

Список рекомендованої літератури / інтернет-ресурси / нормативні документи

Основна

1. Грищук Р.В. Основи кібернетичної безпеки: Монографія / Р.В. Грищук, Ю.Г. Даник; за заг. ред. Ю.Г. Данника. – Житомир: ЖНАЕУ, 2019. – 636 с.

2. Остапов С. Е. Технології захисту інформації / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Чернівці : Видавничий дім "РОДОВІД", 2021. – 428 с.

3. Єсін В. І., Кузнецов О. О., Сорока Л. С. Безпека інформаційних систем і технологій: навчальний посібник [для студентів вищих навчальних закладів, які навчаються за напрямами підготовки «Безпека інформаційних і комунікаційних систем»] – Х. : ХНУ імені В. Н. Каразіна, 2020. – 632 с. ISBN 978-966-623-927-6

4. Остапов С. Е. Технології захисту інформації : навчальний посібник / С. Е. Остапов, С. П. Євсеєв, О. Г. Король. – Х. : Вид. ХНЕУ, 2017. – 476 с.

5. Ukrainian Information Security Research Journal. - Vol. 25 No. 2 (2023): https://jrnl.nau.edu.ua/index.php/ZI/issue/view/925

Додаткова

1. Graham Bartlett, Amjad Inamdar. IKEv2 IPsec Virtual Private Networks: Understanding and Deploying IKEv2, IPsec VPNs, and FlexVPN in Cisco IOS. – Cisco Press, 2019 – 608 с.

2. Menezes A., van Oorschot P., Vanstone S. Handbook of applied cryptography. CRC Press, 2017.

3. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – К.: Видавнича група BHV, 2020. – 608с.

4. Гончарова Л.Л., Возненко А.Д., Стасюк О.І., Коваль Ю.О. Основи захисту інформації в телекомунікаційних та комп'ютерних мережах. – К., 2018. – 435 с.

5. Касянчук, Н. В., Ткачук Л. М. Захист інформації в базах даних. URL: https://conferences.vntu.edu.ua/index.php/all-fm/all-fm-2019/paper/download/ 7001/5715. 2019

Електронні ресурси:

1. Національна бібліотека України ім. В. І. Вернадського. URL: http://www.nbuv.gov.ua
2. Наукова електронна бібліотека періодичних видань НАН України http://dspace.nbuv.gov.ua/
3. Науково-технічна бібліотека ім. Г.І. Денисенка Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» https://www.library.kpi.ua/
4. Харківська державна наукова бібліотека ім. Короленка URL: http://korolenko.kharkov.com

5. ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation criteria for IT security – Part1: Introduction and general model. management [Електронний ресурс]. – Режим доступу до ресурсу: http://www.iso.org/iso/catalogue_detail.htm?csnumber=50341

6. ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. [Електронний ресурс]. – Режим доступу до ресурсу:

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46414