Національний технічний університет України
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»

Кафедра обчислювальної техніки

БЕЗПЕКА ПРОГРАМ І ДАНИХ

Робоча програма навчальної дисципліни (Силабус)

Реквізити навчальної дисципліни

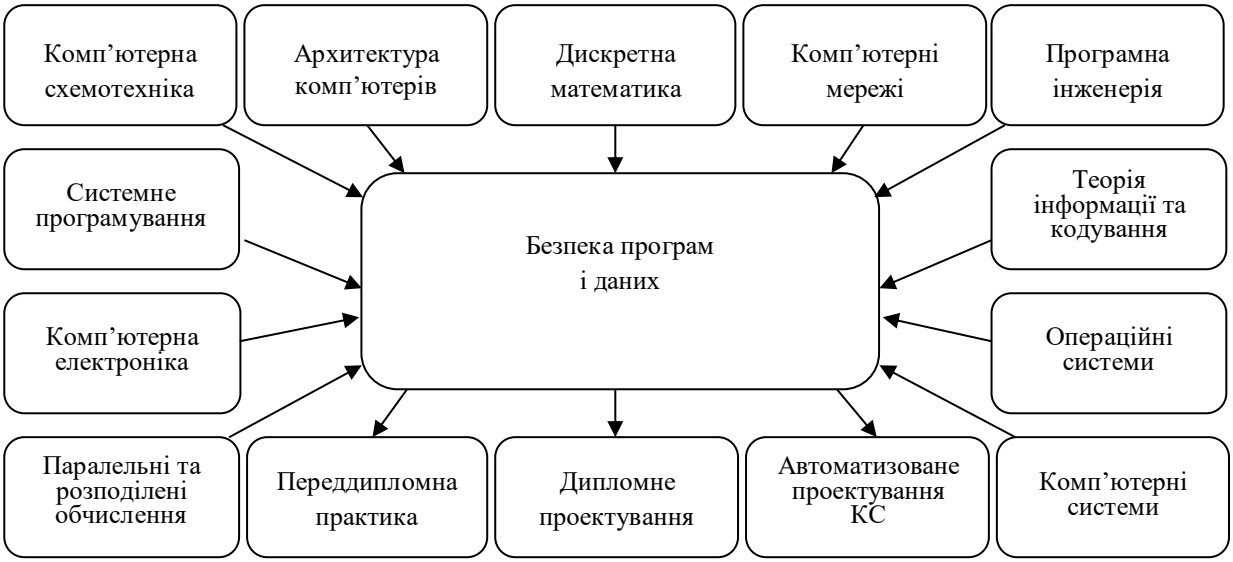
Рівень вищої освіти	*Перший (бакалаврський)*
Галузь знань	*12 Інформаційні технології*
Спеціальність	*121 Інженерія програмного забезпечення*
Освітня програма	*Інженерія програмного забезпечення комп'ютерних систем*
Статус дисципліни	*Вибіркова (цикл професійної підготовки)*
Форма навчання	*очна(денна), заочна*
Рік підготовки, семестр	*3 курс, весняний семестр*
Обсяг дисципліни	*4 кредити*
Семестровий контроль/ контрольні заходи	*Залік*
Розклад занять	*http://rozklad.kpi.ua/Schedules/ScheduleGroupSelection.aspx*
Мова викладання	*Українська*
Інформація про керівника курсу / викладачів	*доцент каф. ОТ, к.т.н., Волокита Артем Миколайович, artem.volokita@kpi.ua*
Розміщення курсу	comsys.kpi.ua bbb.comsys.kpi.ua

Програма навчальної дисципліни

1. Опис навчальної дисципліни, її мета, предмет вивчення та результати навчання

Кредитний модуль «Безпека програм і даних» призначений для вивчення методів та засобів управління доступом до носіїв інформації та баз даних, сучасних стандартів та засобів шифрування для побудови комплексних систем захисту комп'ютерних систем та мереж від вторгнень. Кредитний модуль призначений для вивчення методів проектування та прийомів настроювання програмно-технічних засобів захисту операційних систем, які забезпечують створення високо захищених розподілених комп'ютерних систем.

Місце кредитного модулю в структурно-логічної схемі програми підготовки:



Кредитний модуль пов'язаній з матеріалами, які вивчалися у наступних кредитних модулях:

- дискретна математика (НФ-05)
- програмна інженерія (ЗП-02)
- системне програмування (ЗП-04)
- архітектура комп'ютерів (НП-03)
- паралельні та розподілені обчислення (ЗП-07).
- операційні системи (НП-04)
- комп'ютерні мережі (НП-05)
- комп'ютерні системи (НП-06)

Матеріал даного кредитного модулю буде застосований при вивченні наступних кредитних модулів:

- автоматизоване проектування комп'ютерних систем (ЗП-09)
- переддипломна практика (НП-10),
- дипломне проектування (НП-11).

ІІ. РОЗПОДІЛ НАВЧАЛЬНОГО ЧАСУ

Розподіл навчальних годин по семестрах і видах навчальних занять виконується відповідно до робочих навчальних планів за такою формою:

СЕМЕСТР / КОД КРЕДИТНОГО МОДУЛЯ	*Всього годин*	*Розподіл годин за видами занять*							*Кількість МКР*	*Вид індивідуального завдання*	*Семестрова атестація*
		Лекції	*Практичні заняття*	*Семінарські заняття*	*Лабораторні роботи*	*Комп'ютерний практикум*	*СРС*				
							Всього	*У тому числі на виконання індивідуального*			
7/ЗП-9	72	36	-	–	26	-			1	РГР	Екзамен

ІІІ. МЕТА І ЗАВДАННЯ КРЕДИТНОГО МОДУЛЯ

Метою вивчення кредитного модуля «Захист інформації в комп'ютерних системах» є надбання студентом практичних навичок проектування та програмування при створені комплексних систем чи спеціальних апаратно-програмних підсистем захисту інформації від несанкціонованого доступу на основі:

- вміння формалізувати та використати нормативно-правову базу захисту інформації в автоматизованих системах, методи та засоби управління доступом для розмежування прав користувачів до інформації з обмеженим доступом,
- засвоювання стандартних засобів та алгоритмів шифрування для побудови програмно-технічного забезпечення криптографічного захисту особливо важливої інформації та формування необхідної ключової бази шифрування.
- вміння вирішення аналітичних завдань генерації великий простих чисел, розрахунку ключів та крипостійкості сучасних симетричних й асиметричних систем шифрування та визначення їх базових характеристик.
- придбання прийомів створення й настоювання відповідного програмно-технічного забезпечення для захисту інформаційних ресурсів автоматизованих систем;.

Студент повинен знати:

основні концепції створення доказово достатніх систем захисту інформації, моделі Adept-50, Белла-Лападули та інші, існуючі механізми реалізації моделей захисту, які впроваджуються в різних операційних системах на основі „мандатних списків" та „списків доступу", шляхи реалізації принципів „розширення прав доступу" та „мінімальних привілеїв", стандарти, алгоритми та режими реалізації криптографічного захисту інформації, методи та засоби формування ключів шифрування, протоколи та етапи аутентифікації суб'єктів та повідомлень у відкритих каналах зв'язку, протоколи проведення конференцій та відкритих замовлень, структуру та характеристики електронних платіжних систем та пластикових платіжних карток, вимоги відомих стандартів щодо класифікації та критеріїв захищеності комп'ютерних систем від несанкціонованого доступу до інформації у напрямках конфіденційності, цілісності, доступності, контрольованості.

Студент повинен вміти:

виконати заключні етапи проектування при створенні чи модифікації підсистем захисту інформації від несанкціонованого доступу та попередження вторгнень в комп'ютерні системи, врахувати вимоги до паролів та оцінки базових характеристик систем парольного захисту, написати комплекс програм дискретного управління доступом до інформації на носіях чи сайті, визначити оцінки складності програмної чи апаратної реалізації симетричних та асиметричних алгоритмів криптографічного захисту, алгоритмів DES, 3-DES, SHA, SSL, RSA, El-Gamale та інших, оцінити крипостійкості алгоритмів, застосувати методи та алгоритми формування цифрових підписів та сертифікатів ключів, розробити графічний інтерфейс адміністратора безпеки, виконати налагодження програм захисту інформації, організувати їх розміщення та виконання на робочий станції та в комп'ютерній мережі.

IV. ТЕМАТИЧНИЙ ПЛАН

IV.I. РОЗПОДІЛ НАВЧАЛЬНОГО ЧАСУ ЗА ТЕМАМИ

	Розподіл за семестрами та видами занять						
Назви розділів, тем	*Всього*	*Лекції*	*Практичні заняття*	*Семінарські заняття*	*Лабораторні роботи*	*Комп'ютерний практикум*	*СРС*
Розділ 1. Вступ	**4**	**2**					**2**
Тема 1.1 Проблеми захисту інформації в комп'ютерних системах і мережах (КСМ).		1					1
Тема 1.2 Основні напрямки загроз НСД та канали витоку інформації з КСМ. Цілі, суб'єкти та схеми активних та пасивних вторгнень		1					1
Розділ 2. Комплексний підхід до створення систем захисту інформації в комп'ютерних системах.	**8**	**4**					**4**
Тема 2.1 Нормативно-правова база захисту інформації. Основні напрямки і засоби захисту інформації в КСМ.		1					1
Тема 2.2 Моделі систем доказово достатнього захисту інформації. Концептуальні моделі Adept-50,. Деннінга, Лендвера.		1					1
Тема 2.3 Матрична модель системи захисту Белла і Ла-Падули. Поняття суб'єкта, вектора прав та диспетчера доступу. Розширення прав доступу.		1					1
Тема 2.4. Модель системи моніторингу безпеки КСМ. Поняття фактора загрози та статистичної аномалії.		1					1
Розділ 3. Ідентифікація суб'єктів та управління	**16**	**4**			**8**		**4**

доступом на основі парольної системи.							
Тема 3.1 Ідентифікація користувачів на основі системи паролів. Вимоги до паролів. Схема зберігання паролів в ОС Unix.		1			2		1
Тема 3.2 Аналіз характеристик системи простих паролів. Формула Андерсона.Приклади.		1			2		1
Тема 3.3 Модифікації системи паролів. Підтвердження прав доступу на основі процедури однобічного та двобічного „рукопожаття”.		1			2		1
Тема 3.4 Log-журнали: реєстраційний та операційний. Моніторинг безпеки на основі ведення журналів в ОС Unix та Windows		1			2		1
Розділ 4. Дискретне розмежування доступу суб’єктів к інформації в обмеженій матричній моделі системи захисту.	**4**	**2**					**2**
Тема 4.1 Списки доступу та формування категорій користувачів. Наслідування прав. Замки, ключі та умови доступу в ОС VAX/VMS.		1					1
Тема 4.2 Мандатні списки та реалізація принципу „мінімальних привілей”. Мандатний доступ в ОС Unix.		1					1
Розділ 5. До комп’ютерні підходи щодо криптографічного захисту інформації з обмеженим доступом**.**	**6**	**4**					**2**
Тема 5.1 Шифрування на основі одно та багато алфавітних підстановок. Поняття шифру і таємного ключа. Шифр Цезаря		1					
Тема 5.2 Шифрування на основі перестановок. Задачі		1					1

дешифрування та криптоаналізу							
Тема 5.3 Біграмні шифри. Шифр Віжинера та квадрати Уітстона. Шифрувальні машини		1					
Тема 5.4 Потокові шифри з необмеженою довжиною ключа. Шифрування „гамуванням”.		1					1
Розділ 6. Симетричне шифрування в системах зв’язку з відкритими комунікаціями.	**12**	**4**			**4**		**4**
Тема 6.1 Організація передач даних в секретних системах по Шеннону. Засоби максимізації ентропії.		1					1
Тема 6.2 Шифрування на основі чередування перестановок та підстановок. Система Люціфер.		1					1
Тема 6.3 Федеральний стандарт шифрування Data Encryption Standard. (DES). Загальна схема та функція маскування з ключовими словами.		1			2		1
Тема 6.4 Блок управління ключами в DES. Алгоритм 3-DES та чотири режими реалізації криптографічного захисту на основі DES.		1			2		1
Розділ 7. Асиметричні системи шифрування на основі відкритих та таємних ключів.	**20**	**6**			**8**		**6**
Тема 7.1 Нове направлення в криптографії по Діффі і Хелману. Незворотні функції в шифруванні. Три схеми та задачі криптозахисту.		1			2		2
Тема 7.2 Система RSA. Модулярна арифметика. Алгоритм швидкого дискретного потенціювання. Процесор - акселератор RSA.		1			2		2

Тема 7.3. Проблема генерації великих простих чисел (ВПЧ). Тест Рабіна та мала теорема Ферма. Перевірки на простоту.		2			2		1
Тема 7.4. Схеми та алгоритми розрахунків ключів для системи RSA. Класичний та розширений алгоритми Евкліда. Приклади		2			2		1
Контрольна робота з розділів 2 - 7	**2**	**1**					**1**
Розділ 8. Підвищення крипостійкості в асиметричних системах шифрування.	**6**	**3**					**3**
Тема 8.1 Оцінки криптостійкості алгоритму RSA. Порівняння з схемами DES та 3-DES. Приклади		1					2
Тема 8.2 Система шифрування Ель-Гамаля. Схеми та алгоритми розрахунків ключів для системи Ель-Гамаля. Приклади шифрування та дешифрування		2					1
Розділ 9. Аутентифікація суб'єктів та встановлення „довірчого" зв'язку в розподілених системах та мережах.	**16**	**4**			**6**		**6**
Тема 9.1 Встановлення „довіри" суб'єктів на основі симетричних систем шифрування. Протоколи встановлення зв'язку.		1			2		1
Тема 9.2. Встановлення „довіри" суб'єктів на основі асиметричних систем шифрування. Поняття сертифікату відкритого ключа.		1			2		2
Тема 9.3 Встановлення цілісності повідомлень на основі симетричних та асиметричних систем шифрування. Поняття цифрового підпису.		1			2		1

Тема 9.4 Організація „довірчого” зв’язку в протоколах „відкритих замовлень”. Поняття електронних чеку та квитанції.		1					2
Розділ 10. Системи електронних платежів. Засоби підвищення „довіри” віртуальних відносин.	**8**	**2**					**6**
Тема 10.1 Пластикові картки як база для організації електронних платежів. Банки – емітенти та банки – еквайєри.		1					1
Тема 10.2 Структура системи електронних платежів. POS-термінали. Функції та організація процесінгового центру.		1					1
Тема 10.3 Багато рівнева організація формування та використання ключів шифрування.							2
Тема 10.4 Електронна торгівля на базі технології Е-бізнеса. Протоколи SSL та SET. Ієрархія підписів в довірчих відносинах.							2
РГР з розділів 1-8	26						26
Підготовка до екзамену	12						12
Екзамен	4						4
Всього в семестри:	**144**	**36**	**-**	**-**	**26**		**82**

IV.2 ЛЕКЦІЇ

Розділ 1. Вступ

Лекція 1. Проблеми захисту інформації в комп’ютерних системах і мережах (КСМ). Поняття несанкціонованого доступу (НСД), вразливості КСМ, загрози вторгнення, каналу витоку інформації. Основні напрямки загроз НСД та канали витоку інформації з КСМ. Цілі, суб’єкти та схеми активних та пасивних вторгнень.

[1, с.56-57 ; 2, с. 63-68].

Розділ 2. Комплексний підхід до створення систем захисту інформації в комп'ютерних системах.

Лекція 2. Нормативно-правова база захисту інформації. Поняття інформації з обмеженим доступом та системи захисту. Основні напрямки і засоби захисту інформації в КСМ. Моделі систем доказово достатнього захисту інформації. Концептуальна модель Adept-50. Поняття об'єкта і категорії. Модель Деннінга. Поняття домену безпеки. Модель Лендвера. Поняття периметра відповідальності. [3, с. 31-33 ; 2, с. 53-54, 74-77, 121-122].

Лекція 3. Матрична модель системи захисту Белла і Ла-Падули. Поняття суб'єкта, вектора прав та диспетчера доступу. Розширення прав доступу. Модель системи моніторингу безпеки КСМ. Поняття фактора загрози та статистичної аномалії. Вектор індикації аномалій. [1, с.78-84, 58-62 ; 2, с. 69-73, 90-92, 117-120].

Розділ 3. Ідентифікація суб'єктів та управління доступом на основі парольної системи.

Лекція 4. Ідентифікація користувачів на основі системи паролів. Вимоги до паролів. Схема зберігання паролів в ОС Unix. Аналіз характеристик системи простих паролів. Формула Андерсона. Приклади.. [1, с 65-70. ; 2, с. 104-107].

Лекція 5. Модифікації системи паролів. Підтвердження прав доступу на основі процедури однобічного та двобічного „рукопожаття". Log-журнали: реєстраційний та операційний. Моніторинг безпеки на основі ведення журналів в ОС Unix та Windows.
[1, с. 71-72 ; 2, с. 108-112].

Розділ 4. Дискретне розмежування доступу суб'єктів к інформації в обмеженій матричній моделі системи захисту.

Лекція 6. Списки доступу та формування категорій користувачів. Наслідування прав. Замки, ключі та умови доступу в ОС VAX/VMS. Мандатні списки та реалізація принципу „мінімальних привілей". Мандатний доступ в ОС Unix. [1, с117-123. ; 2, с. 134-138].

Розділ 5. До комп'ютерні підходи щодо криптографічного захисту інформації з обмеженим доступом.

Лекція 7. Шифрування на основі одно та багато алфавітних підстановок. Поняття шифру і таємного ключа. Шифр Цезаря. Шифрування на основі перестановок. Шифр „скитала". Задачі дешифрування та криптоаналізу. [1, с.78-84, 58-62 ; 2, с. 69-73, 90-92, 117-120].

Лекція 8. Біграмні шифри. Шифр Віжинера та квадрати Уітстона. Шифрувальні машини. Потокові шифри з необмеженою довжиною ключа. Шифрування „гамуванням". [3, с. 31-33 ; 2, с. 53-54, 74-77, 121-122].

Розділ 6. Симетричне шифрування в системах зв'язку з відкритими комунікаціями.

Лекція 9. Організація передач даних в секретних системах по Шеннону. Засоби максимізації ентропії. Шифрування на основі чередування перестановок та підстановок. Система Люціфер. [1, с 65-70. ; 2, с. 104-107].

Лекція 10. Федеральний стандарт шифрування Data Encryption Standard. (DES). Загальна схема та функція маскування з ключовими словами. Блок управління ключами в DES. Алгоритм 3-DES та чотири режими реалізації криптографічного захисту на основі DES. [1, с. 71-72 ; 2, с. 108-112].

Розділ 7. Асиметричні системи шифрування на основі відкритих та таємних ключів.

Лекція 11. Нове направлення в криптографії по Діффі і Хелману. Незворотні функції в шифруванні. Три схеми та задачі криптозахисту. Система RSA. Модулярна арифметика.

Алгоритм швидкого дискретного потенцюювання. Процесор - акселератор RSA. [1, с117-123. ; 2, с. 134-138].

Лекція 12. Проблема генерації великих простих чисел (ВПЧ). Тест Рабіна та мала теорема Ферма. Перевірки на простоту. Приклади. [1, с. 71-72 ; 2, с. 108-112].

Лекція 13. Схеми та алгоритми розрахунків ключів для системи RSA. Класичний та розширений алгоритми Евкліда. Приклади. [1, 134-136с.].

Розділ 8. Марковські моделі систем масового обслуговування.

Лекція 14. Оцінки криптостійкості алгоритму RSA. Порівняння з схемами DES та 3-DES. Приклади. [1, с.78-84, 58-62 ; 2, с. 69-73, 90-92, 117-120].

Контрольна робота з розділів 2 - 7.

Лекція 15. Система шифрування Ель-Гамаля. Схеми та алгоритми розрахунків ключів для системи Ель-Гамаля. Приклади шифрування та дешифрування.. [3, с. 31-33 ; 2, с. 53-54, 74-77, 121-122].

Розділ 9. Аутентифікація суб'єктів та встановлення „довірчого" зв'язку в розподілених системах та мережах.

Лекція 16. Встановлення „довіри" суб'єктів на основі симетричних систем шифрування. Поняття майстер – ключа та змінного - ключа. Протоколи встановлення зв'язку. Встановлення „довіри" суб'єктів на основі асиметричних систем шифрування. Поняття сертифікату відкритого ключа. Протоколи встановлення зв'язку. [1, с 65-70. ; 2, с. 104-107].

Лекція 17. Встановлення цілісності повідомлень на основі симетричних та асиметричних систем шифрування. Поняття сигнатури повідомлення та цифрового підпису. Організація „довірчого" зв'язку в протоколах „відкритих замовлень". Поняття електронних чеку та квитанції. [1, с. 71-72 ; 2, с. 108-112].

Розділ 10. Системи електронних платежів. Засоби підвищення „довіри" віртуальних відносин.

Лекція 18. Оцінки криптостійкості алгоритму RSA. Порівняння з схемами DES та 3-DES. Приклади. Структура системи електронних платежів. POS- термінали. Функції та організація процесінгового центру. [1, с.78-84, 58-62 ; 2, с. 69-73, 90-92, 117-120].

IV.5 ЛАБОРАТОРНІ РОБОТИ

Метою проведення циклу лабораторних робіт є придбання студентами необхідних практичних навиків розробки та дослідження макетних зразків підсистем захисту інформації, які являють собою втілення ефективних підходів та алгоритмів створення комплексної системи захисту інформації від несанкціонованого доступу, дослідження характеристик необхідних структур даних, розробки та налагодження окремих компонентів інтерфейсу консолі адміністратора безпеки під ОС Linux, WindowsXP, FreeBSD з застосуванням мов Delfi, Java, C++, Assembler для дослідження механізмів захисту в автоматизованих системах різного призначення.

Лабораторна робота включає:

- постановку вхідної задачі,
- теоретичні відомості з методів та засобів рішення задачі,
- аналіз математичного та алгоритмічного забезпечення,
- обґрунтування вибору програмних засобів дослідження,
- розробку структурної схеми взаємодії підсистем захисту,
- результати виконання покрокової верифікації алгоритмів,
- інтерпретація результатів та висновки,

- листінг програми.
- результати виконання модельних експериментів
- інтерпретація результатів моделювання та висновки,
- листінг програми.

Лабораторна робота 1. Розробка та дослідження програмної підсистеми дискретного управління доступом до окремого носія інформації з складною структурою каталогів.

Лабораторна робота 2. Програмування та дослідження підсистеми ідентифікації користувачів на основі простих паролів з контролем вимог та супроводженням журналів.

Лабораторна робота 3. Програмування та дослідження підсистеми аутентифікації користувачів під час роботи з використанням „питань-відповідей" та таємних функцій.

Лабораторна робота 4. Програмування та дослідження підсистеми моніторингу для виявлення аномалій та небезпечних подій щодо інформації, яка захищається.

Лабораторна робота 5. Розробка програмного макету для дослідження та покрокової веріфікації алгоритму швидкого дискретного потенцюювання та інших операцій з довільною довжиною операндів.

Лабораторна робота 6. Розробка програмного макету для дослідження та покрокової верифікації алгоритмів генерації великих простих чисел з формуванням бази даних ВПЧ**.**

Лабораторна робота 7. Розробка програмного макету для дослідження та покрокової верифікації RSA - підсистеми управління ключами, шифрування та дешифрування повідомлень**.**

Лабораторна робота 8 Розробка програмного макету для дослідження та покрокової верифікації DES - підсистеми формування сигнатур, шифрування та дешифрування повідомлень.

IV.6 ІНДИВІДУАЛЬНІ ЗАВДАННЯ

Індивідуальні завдання передбачають виконання розрахунково-графічної роботи (РГР) в 8-му семестрі.

Тематика РГР пов'язана з поглибленим вивченням методів організації захисту інформації на основі контрольованого доступу та криптографічного супроводження інформаційних технологій, що оперують з конфеденційними даними. Створення пакета програм для ідентифікації та аутентифікації користувачів, а також для формування ключової інформації базується на сучасних мовах програмування та відповідних бібліотеках.

Розрахунково-графічна робота по дисципліні «Захист інформації в комп'ютерних системах» пов'язана з теоретичним обґрунтуванням та розробленням програмно-технічного забезпечення для тестування окремих схем та алгоритмів підвищення рівня захисту інформації на носіях та процедур передачі даних з обмеженим доступом у відкритих каналах зв'язку з проведенням дослідження їх впливу на продуктивність комп'ютерних систем та стійкість щодо зовнішніх вторгнень.

Необхідно також реалізувати алгоритми роботи підсистем захисту для кожного режиму шифрування, визначити можливості та проблеми генерації та накопичення необхідної ключової інформації та дослідити механізми підвищення довіри до отриманої інформації на основі цифрових підписів та сигнатур повідомлень. Розробити структурну схему системи управління доступом у вибраної операційної системи, модифікувати підсистему парольного захисту та включити додатні елементи моніторингу безпеки.. Згідно завданню розробити програмний макет системи комплексного захисту інформації від несанкціонованого доступу, застосовуючи необхідні бази даних та журнали, засоби генерації та обробки ключів та шифрів:

- засоби операційних систем щодо управління безпекою з метою реалізації дискретного управління доступом в матричний моделі захисту,
- засоби оперування з цілими числами довільної довжини,

- засоби генерації псевдо випадкових та великих простих чисел для створення бази перевірки та розрахунків ключів шифрування,
- засоби візуального програмування для створення необхідних інтерфейсів,
- засоби створення та обробки списків відповідних мов програмування.

В розрахунково-графічній роботі необхідно виконати відповідно індивідуального завдання розробку комплексної підсистеми захисту інформації від несанкціонованих втручань, її використання, модифікації та знищення, розрахувати час та ймовірність безпечного використання паролів та ключів в залежності від їх довжини, виконати дослідження часових характеристик складності формування та передач ключової та шифрованої інформації, побудувати та використати списки: заборонених комбінацій паролів, небезпечних дій користувачів та їх програм, простих чисел до 100 000, таблиць підстановок та перестановок для алгоритмів симетричного шифрування.

Примирний перелік завдань для розрахунково-графічної роботи:

- підсистема дискретного управління доступом к інформації на відокремленому носії під Linux,
- підсистема дискретного управління доступом к інформації на відокремленому носії під MS DOS,
- підсистема дискретного управління доступом к інформації на відокремленому носії під Widows,
- підсистема ідентифікації користувачів на основі паролів, що перевіряються,
- підсистема аутентифікації користувачів на основі таємних відповідей та функцій,
- підсистема моніторингу безпеки на основі аналізу небезпечних подій,
- підсистема шифрування та покрокового виконання алгоритмів RSA, El-Gamale чи DES,
- обчислення ключів шифрування для систем шифрування RSA, El-Gamale чи DES,
- формування цифрових підписів та сигнатур повідомлень на основі RSA, El-Gamale чи DES,
- швидке дискретне потенціювання цілих чисел з довільною довжиною,
- обчислення спеціального виду великих простих чисел довільної довжини,
- перевірки чисел на простоту на основі теореми Ферма та інших тестів.

Розділи, теми і окремі питання програми, які пропонуються для самостійного вивчення, для поглибленого вивчення магістрантами або бакалаврами, які планують магістерську підготовку:

- засоби захисту інформації на пластикових платіжних картках,
- засоби управління доступом до Internet - сайтів,
- засоби формування та використання ключової інформації в банківських технологіях та електронних платіжних системах,
- протоколи підвищення довіри до суб’єктів та повідомлень в Е-бізнесі.

-

IV.7 КОНТРОЛЬНІ РОБОТИ

Контрольна робота 1. Теми : 3.2, 4.2., 7.2, 7.3, 7.4, 8.1..
Мета роботи: перевірити результати вивчення прийомів аналізу характеристик підсистем парольного та криптографічного захисту, розрахунків великих простих чисел, визначення таємних та відкритих ключів шифрування.

V. МЕТОДИЧНІ ВКАЗІВКИ

Навчальна робоча програма дисципліни для заочної форми навчання повинна включати контрольні роботи, яки компенсують обмеженість часу лабораторних робіт.

VI. НАВЧАЛЬНО-МЕТОДИЧНІ МАТЕРІЛИ

СПИСОК ОСНОВНОЇ ЛІТЕРАТУРИ

1. Столлингс В. Криптография и защита сетей. М: С-Пб: Изд. Дом «Вильямс», 2001. – 672 с.
2. Романец Ю.В., Тимофеев П.А., Шаньгин В.Ф.. Защита информации в компьютерных системах и сетях. Учебник. М: Радио и связь., 1999. - 328 с.
3. Широчин В.П. Архитектоника мышления и нейроинтеллект. – К: Юниор, 2004. - 560 с.
4. Широчин В.П., Мухин В.Е., Кулик А.В. Вопросы проектирования средств защиты информации в компьютерных системах и сетях. К: ВЕК. 2000. - 112 с.

СПИСОК ДОДАТКОВОЇ ЛІТЕРАТУРИ

1. Вербіцький О.В. Вступ до криптології. – Львів, НТЛ, 1998. – 248 с.
2. Щербаков А.Ю. Компьютерная безопасность: теория и практика. – М: «Молгачева», 2001. – 352 с.
3. Норткарт С., Новак Д. Обнаружение нарушений безопасности в сетях. Третье издание. – М:-К: «Вильямс», 2003. – 447 с.
4. Норткарт С., Купер М., Фирноу М., Фредерик К. Анализ типовых нарушений безопасности в сетях. – М:-К: «Вильямс», 2001. – 460 с.
5. Олифер В.Г., Олифер Н.А. Сетевые операционные системы. – С-Пб: Питер, 2001. – 544 с.
6. Манн С., Митчелл Э., Крелл М. Безопасность Linux. Руководство администратора. М: ИД Вильямс, 2003. – 624 с.
7. Брагг Р. Система безопасности Windows 2000. М: ИД Вильямс. 2001. – 592 с.
8. Коул Э. Руководство по защите от хакеров. –М:-К: «Вильямс», - 2002. – 633 с.
9. Хоффман Л.Дж. Современные методы защиты информации. М: Сов. радио. 1980. 264 с.
10. Мафтик С. Механизмы защиты в сетях ЭВМ. М: Мир, 1993.216 с.
11. Гундарь К.Ю., Гундарь А.Ю., Янишевский Д.А. Защита информации в компьютерных системах. К: Корнейчук, 2000, 152 с.
12. Бондаренко М, Скрипник Л., Горбенко И., Потий А. Перспективы применения международного стандарта ISO/IEC 15408 в Украине. Сб. Правове, нормативне та метрологічне забезпечення систем захисту информації в Україні, вып.3, 2001. с. 7- 26.
13. Шорошев В. Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах. Сб. Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, вып.3, 2001. с. 86-90.
14. Луцький Г.М., Широчин В.П., Пустоваров В.І., Жабин В.І. та інші. "Концепція та концептуальні підходи, нормативно-правова база захисту інформації в комп'ютерних системах" (Звіт з НДР) Депонір. в УкрІНТЕІ, No держреєстрації 0194UO38973, 1994., 7.5 п.л.
15. Національний стандарт ТЗІ України НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в компютерних системах від несанкціонованного доступу. Чинний з 01.07.1999 р.
16. Національний стандарт ТЗІ України НД ТЗІ 2.5-005-99 Класифікація автоматизованих систем і стандартні функціональні профілі захищенності оброблювальної інформації від несанкціоновіанного доступу. Чинний з 01.07.1999 р.
17. Weissman C. Security Controls in the ADEPT-50 Time Sharing System. // Proceedings AFIPS, FJCC. – 1969. – v. 35. – pp. 119-133.
18. Hartson R., Hsiao D. Full protection specification in the semantic model for database protection languages. // Proceedings Annual Conference ACM. – Houston, New York. – 1976. – pp. 90-95.
19. Harrison M. A.. Russo W. L. Protection in Operating Systems. // Communications of the ACM. – 1976. – v. 19, № 8. – pp. 461-471.

20. Spier M. J. A Model Implementation for protective domains. // International Journal on Computer Information Science. – 1973. – v. 2, № 3. – pp. 201-229.
21. Bell D. E., LaPadula L. J. Secure computer systems: mathematical foundations and model. // M74-244, The MITRE Corp., Bedford, Mass.- May 1973.
22. Bell D. E. Secure computer systems: a refinement of the mathematical model. // Springfield, The MITRE Corp. – 1974. – Report № 2574, pp. 75
23. Graham R. M., Denning P. J. Protection – Principles and Practice. // Proceedings AFIPS. – 1972. – v.40, pp. 417-429.
24. Denning D. E. A Lattice Model of Secure Information Flow. // Communications of the ACM. – 1976. – v. 19, № 5. – pp. 236-243
25. Landwehr C., Heitmeyer C., McLean J. A security model for military message systems. // ACM Trans. on Computer Systems. – 1984. – V. 2, № 3. – pp. 198-222.

Таблиця відповідності рейтингових балів оцінкам за університетською шкалою:

Значення рейтингу з кредитного модуля **R**	***Традиційна залікова оцінка***
100-95	**відмінно**
94-85	**дуже добре**
84-75	**добре**
74-65	**задовільно**
64-60	**достатньо**
Менше 60	**незадовільно**
Не виконані умови допуску	**не допущено**

Робочу програму навчальної дисципліни (силабус):

Складено к.т.н., доцент, Волокита Артем Миколайович.

Ухвалено кафедрою обчислювальної техніки (протокол No_10_від 25.05.2022).

Погоджено Методичною комісією факультету (протокол No10 від 9.06.2022).