ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно- інтегрованих технологій, автоматизації, електроінженерії та радіоелектроніки
(повне найменування інституту, назва факультету)

Автоматика та телекомунікації
(повна назва кафедри)

«До захисту допущено»

Завідувач кафедри

_____

_____
(підпис) (ініціали, прізвище)

"___"_____20_ р.

Випускна кваліфікаційна робота

бакалавра
(освітньо-кваліфікаційний рівень)

на тему «Розробка системи захисту даних в телекомунікаційних мережах»

Виконав: студент 4 курсу, групи АКТ-16
(шифр групи)

спеціальності 151 Автоматизація та комп'ютерно-інтегровані технології
(шифр і назва напряму підготовки, спеціальності)

Чистик І.М. _____
(прізвище та ініціали) (підпис)

Керівник доцент каф. АТ, к.ф.-м.н., доцент Лесіна Є.В. _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Рецензент _____ _____
(посада, науковий ступінь, вчене звання, прізвище та ініціали) (підпис)

Засвідчую, що у цій дипломній роботі немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Покровськ – 2020 р.

ДВНЗ «Донецький національний технічний університет»
Факультет комп'ютерно- інтегрованих технологій, автоматизації, електроінженерії та радіоелектроніки
(повне найменування інституту, назва факультету)

Автоматика та телекомунікації
(повна назва кафедри)

Захист відбувся_____
(дата)
з оцінкою _____
секретар ДЕК_____
(підпис)

Випускна кваліфікаційна робота

бакалавра
(освітньо-кваліфікаційний рівень)

на тему «Розробка системи захисту даних в телекомунікаційних мережах»

Виконав студент групи АКТ-16 _____ І.М.Чистик
(підпис, дата) (ініціали, прізвище)

Керівник _____ к.ф.-м.н., доц. Є.В.Лесіна
(підпис, дата) (ініціали, прізвище)

Зав. каф. автоматики та телекомунікацій _____ к.т.н., доц. В.В.Поцепаєв
(підпис, дата) (ініціали, прізвище)

Консультанти
(підпис, дата) (ініціали, прізвище)

_____
(підпис, дата) (ініціали, прізвище)

_____
(підпис, дата) (ініціали, прізвище)

Нормоконтролер _____ Д.О.Жуковська
(підпис, дата) (ініціали, прізвище)

Покровськ – 2020 р.

ДВНЗ «Донецький національний технічний університет»

Факультет комп'ютерно- інтегрованих технологій, автоматизації, електроінженерії та радіоелектроніки
Кафедра автоматика та телекомунікації
Освітній ступінь бакалавр
Спеціальність 151 Автоматизація та комп'ютерно-інтегровані технології
(шифр і назва)

ЗАТВЕРДЖУЮ:
Завідувач кафедри
_____ /_____/
"____" _____20___року

З А В Д А Н Н Я
НА ВИПУСКНУ КВАЛІФІКАЦІЙНУ РОБОТУ СТУДЕНТУ

Чистик Іван Михайлович
(прізвище, ім'я, по батькові)

1. Тема роботи «Розробка системи захисту даних в телекомунікаційних мережах»

керівник роботи: Лесіна Є.В., к.ф.-м.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом від " " року №
2. Строк подання студентом роботи _____
3. Вихідні дані до роботи: Програма реалізації алгоритму шифрування на основі динамічної системи Лоренца
4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно дослідити):
1) Методи захисту даних в телекомунікаційних мережах.
2) Властивості функціонування телекомунікаційних мереж .
3) Критерії надійності криптографічних систем.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):
1) Рисунок 5.8 – Блок схема програми
2) Рисунок 5.9 – Блок схема програми

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
	Затвердження теми дипломної роботи та наукового керівника	17.04.20	
	Огляд стану проблеми, що вирішується у дипломній роботі, та постановка задачі	18.04.20 – 24.04.20	
	Виклад загальних теоретичних основ, які використовуються у дипломній роботі	25.04.20 – 27.04.20	
	Підготовка та оформлення розділів 1-3 дипломної роботи	28.04.20 – 08.05.20	
	Аналітичне та чисельне дослідження атракторів Лоренца та Реслера	09.05.20 – 16.05.20	
	Реалізація алгоритму шифрування даних за допомогою системи Лоренца	17.05.20 – 01.06.20	
	Представлення дипломної роботи науковому керівнику	03.06.20	
	Захист дипломної роботи	16.06.20	

Студент _____ **Чистик І.М.**
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ **Лесіна Є.В.**
(підпис) (прізвище та ініціали)

Лист зауважень

Посада П.І.Б.	Суть зауваження, оцінка та підпис

АНОТАЦІЯ

Чистик Іван Михайлович «Розробка системи захисту даних в телекомунікаційних мережах»/ Випускна кваліфікаційна робота на здобуття освітнього ступеня «бакалавр» за спеціальністю 6.050201 Системна інженерія. – ДВНЗ ДонНТУ, Покровськ, 2020.

Робота містить 91 сторінку, складається з вступу, п’яти розділів, висновку, 14 переліків використаних джерел з найменувань, 16 рисунків.

Мета роботи – розробка програми для шифрування та дешифрування данних, спираючись на принцип роботу генераторів хаосу динамічних систем, наприклад, атрактор Лоренца.

В кваліфікаційній роботі вирішені такі основні задачі:

- досліджено існуючи методи шифрування данних;
- досліджено основні шляхи загроз даним;
- розроблено алгоритм шифрування даних на основі генераторів хаосу;
- розроблено програмний код для шифрування даних на мові С++.

Практичним результатом кваліфікаційної роботи є діюча програма для шифрування та дешифрування даних.

Ключові слова: ШИФРУВАННЯ, АТРАКТОР, АЛГОРИТМ, ЗАХИСТ, ПРОГРАМА, КОНФІДЕНЦІЙНІСТЬ

ЗМІСТ

ВСТУП 8

1 АВТОМАТИЗОВАНІ СИСТЕМИ ОБРОБКИ ІНФОРМАЦІЇ І УПРАВЛІННЯ ЯК ОБ’ЄКТИ БЕЗПЕКИ ІНФОРМАЦІЇ 12

1.1. Предмет безпеки інформації 12

1.1.1. Властивості інформації 12

1.1.2. Види і форми подання інформації 14

1.1.3. Комп'ютерне подання інформації 14

1.1.4. Фізичне представлення інформації та процеси її обробки 18

1.2. Об'єкти інформаційної безпеки 20

1.2.1. Класифікація об'єктів інформаційної безпеки 20

1.2.2. Інформаційні системи з централізованою обробкою інформації 21

1.2.3. Автоматизовані системи управління 27

1.3. Потенційні загрози безпеці інформації в інформаційних системах 29

1.3.1.Випадкові загрози 30

1.3.2. Навмисні загрози 32

2 МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ 40

2.1. Традиційні заходи і методи захисту інформації 40

2.2. Криптографічні методи та засоби захисту інформації 44

2.3. Нетрадиційні методи захисту інформації 48

3 КРИПТОГРАФІЧНЕ ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ 51

3.1. Короткий огляд і класифікація методів шифрування інформації 51
3.2. Адитивні методи 57
3.3. Вибір метода перетворення 58
4 ГЕНЕРАТОРИ ХАОСУ НА ОСНОВІ ДИНАМІЧНИХ СИСТЕМ 65
4.1. Атрактор Лоренца 66
4.2. Атрактор Реслера 70
5 АЛГОРИТМ ШИФРУВАННЯ СИГНАЛІВ 74
5.1. Постановка задачі 74
5.2. Опис алгоритму 75
5.3. Програмна реалізація алгоритму 80
ВИСНОВКИ 89
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 90

ВСТУП

В даний час над проблемою захищеності переданої по мережах інформації працює велика кількість фахівців практично у всіх економічно розвинених країнах світу. Можна сказати, що інформаційна безпека сформувалася в окрему швидко розвивається дисципліну. Однак, незважаючи на зусилля численних організацій, що займаються захистом інформації, забезпечення інформаційної безпеки продовжує залишатися надзвичайно гострою проблемою.

Певні труднощі пов'язані зі змінами в технологіях обробки і передачі інформації. З одного боку, використання інформаційних технологій дає ряд очевидних переваг: підвищення ефективності процесів управління, обробки і передачі даних і т. п. В наш час вже неможливо уявити велику організацію без застосування новітніх інформаційних технологій, починаючи від автоматизації окремих робочих місць і закінчуючи побудовою корпоративних розподілених інформаційних систем.З іншого боку, розвиток мереж, їх ускладнення, взаємна інтеграція, відкритість призводять до появи якісно нових загроз, збільшення числа зловмисників, що мають потенційну можливість впливати на систему.В даний час для забезпечення захисту інформації потрібно не просто розробка приватних механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів, морально - етичних заходів протидії і т.д.). Комплексний характер захисту виникає з комплексних дій зловмисників, які прагнуть будь-якими засобами добути важливу для них інформацію.

Сьогодні можна стверджувати, що народжується нова сучасна технологія — технологія захисту інформації в телекомунікаційних мережах.

Сруктура та обсяг роботи. Робота складається з п’яти розділів, де

спочатку розглядаються системи обробки і передачі інформації, види загроз для даних, способи іх захисту, види методів шифрування, генератори хаосу динамічних систем та опис програми для шифрування данних. Обсяг роботи – 89 сторінок.

Задачею роботи є аналіз захисту даних за домогою методів шифрування.

Об’єктом дослідження є інформація, що передається по телекомунікаційних системах.

Предметом дослідження є інформаційна безпека телекомунікаційних мереж.

Основною **метою роботи** є вивчення методів захисту інформації в телекомунікаційних мережах.

Актуальність теми. Широке застосування комп'ютерних технологій в автоматизованих системах обробки інформації та управління призвело до загострення проблеми захисту інформації, що циркулює в комп'ютерних системах, від несанкціонованого доступу. Захист інформації в комп'ютерних системах має ряд специфічних особливостей, пов'язаних з тим, що інформація не є жорстко пов'язаної з носієм, може легко і швидко копіюватися і передаватися по каналах зв'язку. Відомо дуже велике число загроз інформації, які можуть бути реалізовані як з боку зовнішніх порушників, так і з боку внутрішніх порушників.

В області захисту інформації та комп'ютерної безпеки в цілому найбільш актуальними є три групи проблем :

1. Порушення конфіденційності інформації;

2. Порушення цілісності інформації;

3. Порушення працездатності інформаційно-обчислювальних систем.

Захист інформації перетворюється на найважливішу проблему державної безпеки, коли йдеться про державну, дипломатичну, військову, промислову, медичну, фінансову та іншу довірчу, секретну інформацію. Величезні масиви такої інформації зберігаються в електронних архівах, обробляються в

інформаційних системах і передаються по телекомунікаційних мережах. Основні властивості цієї інформації-конфіденційність і цілісність, повинні підтримуватися законодавчо, юридично, а також організаційними, технічними і програмними методами.

Конфіденційність інформації (від лат. Confidentia-довіра) передбачає введення певних обмежень на коло осіб, що мають доступ до даної інформації. Ступінь конфіденційності виражається деякою встановленою характеристикою (особлива важливість, цілком таємно, таємно, для службового користування, не для друку і т.п.), яка суб'єктивно визначається власником інформації в залежності від змісту відомостей, які не підлягають розголосу, призначені обмеженому колу осіб, є секретом. Природно, встановлена ступінь конфіденційності інформації повинна зберігатися при її обробці в інформаційних системах і при передачі по телекомунікаційних мережах.

Іншою важливою властивістю інформації є її цілісність (integrty). Інформація цілісна, якщо вона в будь-який момент часу правильно (адекватно) відображає свою предметну область. Цілісність інформації в інформаційних системах забезпечується своєчасним введенням в неї достовірної (вірної) інформації, підтвердженням істинності інформації, захистом від спотворень і руйнування (стирання).

Несанкціонований доступ до інформації осіб, не допущених до неї, умисні або ненавмисні помилки операторів, користувачів або програм, невірні зміни інформації внаслідок збоїв обладнання призводять до порушення цих найважливіших властивостей інформації і роблять її непридатною і навіть небезпечною. Її використання може призвести до матеріального та/або морального збитку, тому створення системи захисту інформації, стає актуальним завданням. Під безпекою інформації (information security) розуміють захищеність інформації від небажаного її розголошення (порушення конфіденційності), спотворення (порушення цілісності), втрати або зниження ступеня доступності інформації, а також незаконного її тиражування.

Безпека інформації в інформаційній системі або телекомунікаційній мережі забезпечується здатністю цієї системи зберігати конфіденційність інформації при її введенні, виведенні, передачі, обробці та зберіганні, а також протистояти її руйнуванню, розкраданню або спотворенню. Безпека інформації забезпечується шляхом організації допуску до неї, захисту її від перехоплення, спотворення і введення неправдивої інформації. З цією метою застосовуються фізичні, технічні, апаратні, програмно-апаратні та програмні засоби захисту. Останні займають центральне місце в системі забезпечення безпеки інформації в інформаційних системах і телекомунікаційних мережах.

Завдання забезпечення безпеки :

- захист інформації в каналах зв'язку та базах даних криптографічними методами;
- підтвердження автентичності об'єктів даних і користувачів (аутентифікація сторін, що встановлюють зв'язок);
- виявлення порушень цілісності об'єктів даних;
- забезпечення захисту технічних засобів і приміщень, в яких ведеться обробка конфіденційної інформації, від витоку по побічних каналах і від можливо впроваджених в них електронних пристроїв знімання інформації;
- забезпечення захисту програмних продуктів і засобів обчислювальної техніки від впровадження в них програмних вірусів і закладок;
- захист від несанкціонованих дій по каналу зв'язку від осіб, не допущених до засобів шифрування, але переслідують цілі компрометації секретної інформації та дезорганізації роботи абонентських пунктів;
- організаційно-технічні заходи, спрямовані на забезпечення збереження конфіденційних даних.

1 АВТОМАТИЗОВАНІ СИСТЕМИ ОБРОБКИ ІНФОРМАЦІЇ І УПРАВЛІННЯ ЯК ОБ’ЄКТИ БЕЗПЕКИ ІНФОРМАЦІЇ

1.1. Предмет безпеки інформації

1.1.1. Властивості інформації

Інформація - це результат відображення і обробки в людській свідомості різноманіття навколишнього світу, це відомості про оточуючі людину предмети, явища природи, діяльність інших людей. Відомості, якими обмінюється людина через машину з іншою людиною або з машиною, і є предметом захисту. Однак захисту підлягає не всяка інформація, а тільки та, яка має ціну. Цінним стає та інформація, володіння якої дозволить її існуючому і потенційному власнику одержати який-небудь виграш: моральний, матеріальний, політичний. Оскільки в людському суспільстві завжди існують люди, охочі незаконним шляхом отримати цінну інформацію, у її власника виникає необхідність у її захисті.

Для оцінки потрібно розподілити інформацію на категорії не тільки відповідно до її цінності, але й важливості. Відомий наступний поділ інформації за рівнем важливості:

1) життєво важлива незамінна інформація, наявність якої необхідна для функціонування організації;

2) важлива інформація - інформація, яка може бути замінена або відновлена, але процес відновлення дуже важкий і пов'язаний з великими витратами;

3) корисна інформація - інформація, яку важко відновити, однак організація може ефективно функціонувати і без неї;

4) несуттєва інформація - інформація, яка більше не потрібна

організації, або організація може без неї обійтися.

Існують визначення груп осіб, пов'язаних з обробкою інформації:

- держатель - організація та / або особа - власник інформації;
- джерело - організація та / або особа, яка поставляє інформацію;
- порушник - окрема особа та / або організація, що прагне отримати інформацію.

Наведені категорії важливості заслуговують на увагу і можуть бути застосовані до будь-якої інформації. Це також узгоджується з існуючим принципом розподілу інформації за рівнями таємності.

Рівень секретності - це адміністративна або законодавча міра, відповідна мірі відповідальності особи за витік або втрату конкретної секретної інформації, регламентованої спеціальним документом, з урахуванням державних, військово-стратегічних, комерційних, службових або приватних інтересів.

Конфіденційність - наступний рівень збереження таємниці інформації. Очевидно, що, де є рівень секретності, там є і рівень конфіденційності, але не навпаки.

Практика показала, що захищати необхідно не тільки секретну або конфіденційну інформацію. Несекретна інформація, піддана несанкціонованим змінам (наприклад, модифікації команд управління), може призвести до витоку або втрати пов'язаної з нею секретної інформації.

Сумарна кількість, або статистика несекретной та конфіденційної інформації, в результаті може виявитися секретним, або конфіденційним. Аналогічно зведені дані одного рівня важливості в цілому можуть бути інформацією більш високого рівня таємності або конфіденційності. Для захисту від подібних ситуацій широко застосовується розмежування доступу до інформації за функціональною ознакою. При однаковій мірі важливості інформації, що обробляється в системі обробки, інформація поділяється відповідно до функціональних обов'язків та повноважень

користувачів, що встановлюються адміністрацією організації - власника автоматизованої системи інформації та управління.

1.1.2. Види і форми подання інформації

Відомо, що інформація може бути представлена у вигляді: букв; символів; цифр; слів; тексту; малюнків; схем; формул; графіків; таблиць; планів; креслень; географічних, топографічних, технологічних карт; алгоритмів, відеозаписів, аудіо записів, які, в свою чергу, можуть бути представлені у вигляді: постійної або змінної інформації; команд; повідомлень; довідок; рішень; наказів; розпоряджень; завдань; звітів; відомостей; інструкцій; коментарів; листів і записок; телеграм; чеків; масивів; файлів; WEB-сайтів, порталів; електронних бібліотек, відеотек, фонотек, блогів.

1.1.3. Комп'ютерне подання інформації

Інформація, втілена і зафіксована в деякій матеріальній формі, називається повідомленням. Повідомлення можуть бути безперервними і дискретними (цифровими).

Безперервне повідомлення представляється деякою фізичною величиною (електричною напругою, струмом і т.п.), зміни якої відображають протікання даного процесу. Фізична величина, що передає безперервне повідомлення, може приймати будь-які значення і змінюватися в довільні моменти часу. Таким чином, в безперервному повідомленні кінцевої довжини може міститися велика кількість інформації.

Для дискретних повідомлень характерна наявність фіксованого набору окремих елементів, з яких в дискретні моменти часу формуються різні послідовності елементів. Важливим є не фізична природа елементів, а та обставина, що набір елементів кінцевий і тому будь-яке дискретне

повідомлення кінцевої довжини передає кінцеве число значень деякої величини, а отже, кількість інформації в такому повідомленні звичайне.

При дискретній формі подання інформації окремим її елементам можуть бути привласнені числові (цифрові) значення. У таких випадках говорять про цифрову інформацію, а комп'ютери, машини і системи, що використовують цифрову форму подання інформації, називаються цифровими.

Елементи, з яких складається дискретне повідомлення, називають буквами або символами. Набір цих букв (символів) утворює алфавіт. Тут під літерами, на відміну від звичайного уявлення, розуміються будь-які знаки. Число символів в алфавіті називається об'ємом алфавіту. Обсяг алфавіту визначає кількість інформації, що доставляється одним символом повідомлення. Якщо алфавіт має об'єм A і в будь-якому місці в повідомленні ймовірність появи будь-якого символу однакова, то передану символом кількість інформації можна визначити як кількість біт:

$$I_0 = log_2 A \qquad (1.1)$$

Дискретне повідомлення можна розбити на групи символів і назвати ці групи словами. Довжина слова визначається кількістю символів, які в ньому містяться.

У комп'ютерній техніці широко використовується однорідне подання інформації, при якому в комп'ютерній системі або окремих її частинах всі слова мають певну довжину. Однорідне подання інформації спрощує обмін нею і конструкцію пристроїв комп'ютерної системи.

В алфавіті об'ємом A можна відокремити N різних слів довжини S, де

$$N = A^S. \qquad (1.2)$$

Тоді кількість інформації, що міститься в слові,

$$I_1 = log_2\ N = S\ log_2\ A = SI_0. \quad (1.3)$$

Нерівномірність появи символів, наявність взаємної залежності символів у повідомленні при передачі смислових повідомлень (тексту) є причиною того, що кількість інформації в одному символі зменшується.

Зв'язок між символами повідомлення створює надмірність інформації. У мові надмірність носить природний характер. Однак в обчислювальних системах широко застосовується штучна надмірність при кодуванні повідомлень, яка дозволяє контролювати і усувати помилки при передачі інформації по лініях зв'язку, а також між окремими пристроями цифрової обчислювальної системи.

У цифрових обчислювальних машинах і системах широко вживається двійковий алфавіт, що має лише два символи - 0 і 1. Його застосування спрощує технічну реалізацію пристроїв комп'ютерної техніки. Будь-яке дискретне повідомлення, виражене в деякому алфавіті, перекладається в двійковому алфавіті, якщо довжина двійкового слова відповідає формулі

$$S_2 > S_1\ log_2 \mathrm{A}\,. \quad (1.4)$$

При розвитку технологій цифрового відео та звуку знадобилося ще більше збільшити розрядність оцифровки аналогових сигналів і особливо при отриманні відео та звуку високої якості.

Найбільшого поширення набуло надання інформації за допомогою восьмирозрядного складу, званого байтом.

За допомогою восьмирозрядного складу можна кодувати 256 різних символів (2^8). Кілька байтів утворюють слова.

Комп'ютер робить обробку інформації, що полягає в її запам'ятовуванні, передачі з одних пристроїв на інші, виконанні над інформацією арифметичних і логічних перетворень. Процес обробки інформації автоматизований за допомогою програмного керування.

Програма є алгоритм переробки інформації, записаної у вигляді послідовності команд, які повинні бути виконані машиною для отримання шуканого результату.

Поле - група символів, що мають певне значення і піддаються обробці за одну і ту ж арифметичну або логічну операцію.

Запис являє собою групу полів, що описують ознаки (властивості, характеристики, параметри) деякого об'єкта.

Масив - об'єднання записів, що описує безліч об'єктів (наприклад, екзаменаційна відомість або їх сукупність).

Словами називають групу символів (розрядів) в пам'яті комп'ютера, відповідну деякому полю. Зазвичай термін «машинне слово» відносять до кода певної довжини, який зчитується з оперативної пам'яті або записується в оперативну пам'ять за одне звернення. Машинне слово може являти собою двійкове число з плаваючою або фіксованою комою, команду, кілька складів (байтів). Машинне слово може також містити додаткові розряди (розряд контролю по парності, розряди захисту пам'яті та ін.). Зазвичай машинне слово, зокрема команда, містить ціле число байтів.

Машинна одиниця інформації, відповідна натуральної одиниці - записи, називається фразою (або також записом). Вона може займати кілька машинних слів.

Блоком називають групу фраз (записів), розташованих компактно (без проміжків) на носії зовнішнього накопичувача і записуваних на носій з оперативної пам'яті, а також зчитувальних з носія в накопичувач однією командою. Серед натуральних одиниць інформації немає одиниці, відповідної блоку. Місце в пристрої на магнітному або оптичному носії, в якому зберігається група слів, що складають блок, називається зоною, або сектором.

Інформаційному масиву відповідає машинна одиниця інформації - файл. Файл складається в загальному випадку з декількох блоків.

Томом називається машинна одиниця інформації, відповідна пакету дисків (часто томом називають логічну частину зовнішнього носія, вінчестера, наприклад).

1.1.4. Фізичне представлення інформації та процеси її обробки

Як було показано вище, в обчислювальних системах інформація представляється в двійковому алфавіті. Фізичними аналогами знаків цього алфавіту служать фізичні сигнали, здатні приймати два добре помітних значення, наприклад електричну напругу (потенціал) високого і низького рівня, відсутність і наявність імпульсу струму, протилежні за знаком значення напруженості магнітного поля і т. п.

Неодмінною вимогою до фізичних аналогів двійкового алфавіту є можливість надійного розпізнавання двох різних значень сигналу, які при описі законів функціонування схем позначаються символами 0 (нуль) та 1 (одиниця).

У схемах цифрових пристроїв змінні і відповідні їм сигнали змінюються і сприймаються не безперервно, а лише в дискретні моменти часу.

У цифрових пристроях застосовують три способи фізичного представлення інформації: потенційний, імпульсний і динамічний. Слово може бути представлено послідовним або паралельним способом (кодом). Пристрої послідовної дії працюють повільніше, ніж паралельної. Однак пристрій паралельної дії вимагає більшого обсягу апаратури. У обчислювальній техніці застосовуються обидва способи в залежності від вимог, що пред'являються до конкретного виробу.

Інформація в обчислювальній системі піддається різним процесам: введення, зберігання, обробка і виводу.

Введення інформації в комп'ютерну систему здійснюється з пристроїв введення, що мають велику різноманітність, починаючи з клавіатури,

маніпулятора «миша» і закінчуючи сучасними цифровими фото і відеокамерами, а також з різних дисків, флеш-карт і т. п.

Зберігання інформації проводиться на запам'ятовуючих пристроях: короткочасне - в оперативній пам'яті і в різних регістрах пам'яті, виконаних на напівпровідникових приладах, магнітних і оптичних елементах; довготривале - у зовнішніх запам'ятовуючих пристроях, виконаних на магнітних стрічках (стримерах), дисках і різноманітних лазерних і флеш-технологіях.

Обробка інформації в обчислювальній системі проводиться відповідно до прийнятої системи команд, алгоритмами, обумовленими програмним забезпеченням, і командами, які надходять із зовнішніх пристроїв управління.

Виведення інформації здійснюється на зовнішні пристрої зв'язку та реєстрації інформації без її візуального відображення і пристрої з відображенням: пристрої, що друкують, індикатори, табло та інші пристрої індивідуального і колективного відображення. Вибір методу обробки інформації визначається характером вирішуваних завдань, особливостями використовуваної інформації, а також параметрами технічних засобів автоматизації та можливостями програмного і апаратного забезпечення комп'ютерних систем.

Інформаційні процеси в системах обробки інформації умовно поділяють на три групи:

- інформаційно-довідкове забезпечення посадових осіб органів управління;
- інформаційне забезпечення розрахункових завдань;
- обслуговування інформаційної бази автоматизованої системи управління.

За ступенем стабільності інформацію поділяють на умовно-постійну та змінну. До умовно-постійної інформації відносяться дані, які протягом тривалого часу не змінюються. Щодо використання в процесах управління

вся інформація ділиться на нормативну, довідкову, планову, оперативно-виробничу, звітну і аналітичну.

Інформаційна єдність в автоматизованій системі управління забезпечується наступним шляхом:

- створення системи класифікації та кодування інформації;
- розробки та впровадження уніфікованих систем документації;
- уніфікації принципів побудови нормативів і їх оновлення;
- уніфікації системи показників для забезпечення порівнянності в часі і по різних якісним і кількісним ознаками;
- регламентації потоків інформації по спрямованості, обсягу, періодичності, достовірності і терміновості;
- уніфікації порядку формування та обробки інформації.

1.2. Об'єкти інформаційної безпеки

1.2.1. Класифікація об'єктів інформаційної безпеки

Автоматизовані системи обробки інформації (АСОІ) або автоматизовані системи обробки інформації та управління (АСОІУ), в даний час інтегровані системи (ІС), мають широке застосування. Концепція безпеки інформації, теорія і основні принципи побудови її захисту в них повинні бути єдиними. Такому підходу сприяє також і те, що введення-виведення, зберігання, обробка і передача інформації в усіх видах систем будуються на базі типових методів і засобів. Пошук подібних методів і засобів у забезпеченні безпеки інформації також є основним завданням при проектуванні інформаційної системи.

Об’єкти забезпечення інформаційної безпеки:

- Інформаційні ресурси
- Система створення, розповсюдження і використання інформаційних ресурсів
- Інформаційна структура суспільства (інформаційні телекомунікації, мережі зв’язку, центри аналізу і обробки даних, системи і засоби захисту інформації)
- Засоби масової інформації
- Права людини і держави на отримання, розповсюдження і використання інформації
- Захист інтелектуальної власності та конфіденціальної інформації.

Для детального дослідження і подання зазначених систем з позицій можливого несанкціонованого доступу до інформації та постановки задачі розглянемо елементи їх побудови, починаючи з комп'ютера як основного базового елементу. Нижче розглянуті основні принципи побудови перерахованих вище автоматизованих систем обробки інформації та управління.

1.2.2. Інформаційні системи з централізованою обробкою інформації

Арифметико-логічний пристрій виробляє арифметичні і логічні перетворення над машинними словами, що в нього увійшли, кодами певної довжини, що представляють собою числа або інший вид інформації.

Пам'ять зберігає інформацію, передану з інших пристроїв, у тому числі надходить в комп'ютер ззовні через пристрій введення, і видає в усі інші пристрої інформацію, необхідну для протікання обчислювального процесу. Пам'ять комп'ютера в більшості випадків складається з двох частин: швидкодіючої основної, або оперативної (внутрішньої), пам'яті і

порівняно повільно діючої, але здатної зберігати значно більший обсяг інформації зовнішньої пам'яті. Безпосередньо в обчислювальному процесі бере участь лише оперативна пам'ять, і лише після закінчення окремих етапів обчислень із зовнішньої пам'яті в оперативну пам'ять передається інформація, необхідна для наступного етапу рішення задачі.

Керуючий пристрій (КП) автоматично (без участі людини) управляє обчислювальним процесом, посилаючи всім іншим пристроям сигнали. Зокрема, керуючий пристрій вказує оперативнїй пам'яті, які слова повинні бути передані в арифметично-логічні і в інші пристрої, вмикає арифметико-логічний пристрій для виконання потрібної операції і поміщає отриманий результат в оперативну пам'ять.

Послідовність арифметичних і логічних операцій, які потрібно виконати над вихідними даними і проміжними результатами для отримання розв’язку задачі, називають алгоритмом вирішення задачі чисельним методом. Тому алгоритм можна задати зазначенням, які слід провести операції, в якому порядку і над якими словами. Опис алгоритму у формі, яка сприймається комп'ютером, називається програмою. Програма складається з окремих команд. Команди повинні бути закодовані в цифровому вигляді.[8]

Перед розв’язанням задачі на комп'ютері програма і вихідні дані повинні бути поміщені в її пам'ять. Попередньо ця інформація заноситься на магнітні диски або інші носії. Потім за допомогою пристрою введення програма і вихідні дані зчитуються і переносяться в оперативну пам'ять. Інформація може вводитися в оперативну пам'ять безпосередньо з клавіатури, сенсорного пристрою, сканера або інших пристроїв введення інформації.

Пристрій виведення служить для видачі з комп'ютера результатів обробки інформації, наприклад, шляхом друкування їх на друкованих пристроях або відображення на екрані дисплея.

За допомогою дистанційного пульта управління оператор пускає і

зупиняє комп'ютер, а при необхідності може втручатися в процес виконання завдання.

Засоби програмного забезпечення і апаратні засоби є двома взаємопов'язаними компонентами комп'ютерної техніки.

Система програмного (математичного) забезпечення комп'ютера являє собою комплекс програмних засобів, в якому можна виділити операційну систему, комплект програм технічного обслуговування і прикладних програм.

Оператори не мають прямого доступу до пристроїв комп'ютера. Зв'язок операторів з комп'ютером (точніше, з її апаратними засобами) проводиться за допомогою операційної системи, що забезпечує певний рівень взаємодії людини з комп'ютером. Рівень взаємодії в першу чергу визначається рівнем програмно-апаратного інтерфейсу (інтерфейсної програми).

Комплект програм технічного обслуговування, призначений для зменшення трудомісткості експлуатації комп'ютера, містить програми перевірки працездатності комп'ютера і окремих її пристроїв, визначення (діагностування) місць відмов.

Прикладні програми (додатки) являють собою програми та інтегровані програмні середовища, призначені для вирішення певних завдань (проектних, науково-технічних, планово-економічних та ін.), а також для розширення функцій операційної системи (управління базами даних, реалізації режимів розподіленої обробки даних, режимів реального часу та ін.).

Апаратні засоби комп'ютера і операційна система, його програмне забезпечення в сукупності утворюють одномашину систему обробки даних.

Історично першими і досі поширеними є одномашинні системи обробки даних, побудовані на базі єдиного комп'ютера з традиційною однопроцесорною структурою. Однак продуктивність і надійність існуючого парку комп'ютерів виявляються задовільними не для всього

спектру застосувань. Постановникам завдань, що вирішуються на комп'ютерах, завжди не вистачало оперативної пам'яті, ємності накопичувачів і швидкодії обробки даних. Тому для підвищення надійності і продуктивності кілька комп'ютерів стали пов'язувати між собою, утворюючи багатомашинний комп'ютерний (обчислювальний) комплекс. У двухмашинного обчислювальному комплексі зв'язок найчастіше здійснюється через адаптер, що забезпечує обмін даними між каналами введення-виведення двох комп'ютерів і передачу сигналів переривання.

Кращі умови для взаємодії процесів обробки інформації ті, коли всі процесори мають доступ до всього обсягу даних, що зберігаються в оперативних запам'ятовуючих пристроях, і можуть взаємодіяти з усіма периферійними пристроями комплексу. Комп'ютерний комплекс, що містить кілька процесорів із загальною оперативною пам'яттю і періферійними пристроями, називається багатопроцесорним комплексом.

Процесори, модулі оперативної пам'яті і канали введення-виведення, до яких підключені периферійні пристрої, об'єднуються в єдиний комплекс за допомогою засобів коммунікацій і комутацій, що забезпечують доступ кожного процесора до будь-якого модулю оперативної пам'яті і каналу введення-виведення, а також можливість передачі даних між останніми.

Багатомашинні і багатопроцесорні комп'ютерні комплекси або комплекси обробки інформації розглядаються як базові засоби для створення систем обробки інформациі та обміну різного призначення. Тому до складу компьютерного комплексу прийнято включати тільки апаратні засоби і загальносистемне (базове), але не прикладне програмне забезпечення, пов'язане з конкретною областю застосування комплексу

Система обробки інформації і даних, налаштована на вирішення завдань конкретної області застосування, називається інформаційною системою або системою обробки інформації. Комп'ютерна система включає в себе апаратні засоби і програмне забезпечення, орієнтовані на рішення певної сукупності завдань. У комп'ютерну систему можуть бути включені,

крім комп'ютерних комплексів, і інші апаратні засоби (наприклад, системи отримання та обробки цифрового відео).

Всі останні покоління комп'ютерів самого різного призначення розвиваються в напрямку створення адаптивних комп'ютерних систем, які пристосувалися до вирішуваних завдань. Адаптація комп'ютерної системи до структури реалізованого алгоритму досягається за рахунок зміни конфігурації системи, яка в сучасних компьютерах відбувається на рівні операційної системи, з мінімальним обсягом віддаленої комутації. При цьому з'єднання між процесорами, а також модулями пам'яті і периферійними пристроями встановлюються динамічно відповідно до потреб завдань, оброблюваних системою в поточний момент часу. У зв'язку з цим адаптивні комп'ютерні системи інакше називають системами з динамічною структурою. За рахунок адаптації досягається висока продуктивність в широкому класі задач і забезпечується стійкість системи до відмов.

Для отримання даних з комп'ютера або комп'ютерного комплексу, розташованих на значній відстані від користувача, застосовуються системи телеобробки інформації.

У цих системах користувачі (абоненти) взаємодіють з системою за допомогою терміналів (абонентських пунктів), що підключаються через канали зв'язку до засобів обробки інформаціі. Дані передаються по каналах зв'язку у формі повідомлень - блоків інформації або даних, що несуть в собі, окрім власне інформації або даних, системну інформацію, необхідну для управління процесами передачі та захисту інформації і даних від спотворень. Програмне забезпечення систем телеобробки містить спеціальні засоби, необхідні для управління апаратними засобами, встановлення зв'язку між комп'ютерами та об'єктами, передачі інформації і даних між ними та організації взаємодії користувачів з програмами обробки інформації та даних.

Із зростанням масштабів застосування комп'ютерної техніки в обробці

інформації та обмін нею на відстані виникла необхідність об'єднання зосереджених систем обробки даних в комп'ютерні (інформаційні, обчислювальні) мережі. Доцільність створення комп'ютерних мереж обумовлюється можливістю використання територіально-розосередженими користувачами програмного забезпечення та інформаційних баз, що знаходяться в різних комп'ютерних центрах мережі, а також можливістю організації розподіленої обробки інформації і даних шляхом залучення програмно-апаратних ресурсів декількох комп'ютерних центрів мережі для вирішення особливо складних завдань.

Комп'ютерну мережу можна розглядати як систему з розподіленими по території апаратними, програмними та інформаційними ресурсами. Можлива реалізація на основі комп'ютерних мереж розподіленого (децентралізованого) банку інформації і даних, окремі інформаційні бази якого створюються в місцевих комп'ютерних центрах, наприклад у процесі функціонування автоматизованої системи управління окремих підприємств і об'єднань, а при вирішенні завдань більш високого рівня управління використовуються як єдина база даних та інформації.

Інша можливість - це створення централізованого банку інформації і даних, до якого мають доступ численні, у тому числі що знаходяться на значній відстані, абоненти через свої термінали, абонентські пункти і термінали місцевих систем колективного користування.

Об'єднання в мережу комп'ютерів декількох комп'ютерних центрів сприяє підвищенню надійності функціонування комп'ютерних засобів, так як створюється можливість резервування одних комп'ютерних центрів за рахунок технічних ресурсів інших центрів.

1.2.3. Автоматизовані системи управління

Автоматизовані системи управління в сформованому в даний час розумінні відрізняються від комп'ютерних мереж наявністю коштів, що вирішують завдання управління будь-яким процесом. Наприклад, процесом виробництва будь-яких виробів, процесом управління підприємством, галуззю, народним господарством і т. п.

Розрізняють два типи управління: системи управління технічними пристроями та виробничими процесами та системи адміністративно-організаційного управління.

Автоматизовані системи адміністративно-організаційного управління призначені для комплексної автоматизації всіх або більшості основних функцій органів управління: збору та аналізу інформації, планування та прийняття рішень, доведення рішень до виконавців і контролю виконання. Цим вони відрізняються від автономного використання технічних засобів або автоматизації окремих підсистем управління.

Автоматизовані системи адміністративно-організаційного управління являють собою складні комплекси колективів фахівців, технічних засобів, математичного, програмного, інформаційного та лінгвістичного забезпечення, призначені для збору, переробки й видачі інформації. Зазвичай автоматизовані системи адміністративно-організаційного управління являють собою ряд автоматизованих об'єктів при органах управління різних рівнів, об'єднаних єдиною системою обміну даними - автоматизованою системою зв'язку. Кожен автоматизований об'єкт, у свою чергу, включає інформаційно-обчислювальний комплекс об'єкта, значне число автоматизованих робочих місць адміністративних працівників з пристроями формування запитів, введення та видачі інформації, що забезпечують процес функціонування об'єкта.

Об'єкти автоматизованої системи управління умовно поділяються на

основні та допоміжні. До основних відносяться керуючі об'єкти та об'єкти управління. Керуючий об'єкт є джерелом керуючого впливу, спрямованого на досягнення поставленої мети управління. Об'єкт управління є виконавцем управляючих впливів, одержуваних від керуючого об'єкта.

Допоміжні об'єкти служать для автоматизації обробки і передачі інформації, що циркулює в системі.

Проектування автоматизованих систем обробки даних і інформації - створення комплекту конструкторської та програмної документації, необхідної для виробництва і експлуатації. Мета проектування, призначення проектованої системи, вихідні дані та технічні вимоги встановлюються технічним завданням. У його технічних вимогах задаються: функції системи, склад і характеристики джерел і приймачів даних, а також їх територіальне розміщення; технічні характеристики системи продуктивність, ємність пам'яті, надійність, вартість, масогабаритні та енергетичні; необхідні режими функціонування; умови експлуатації й інші фактори, суттєві для систем того чи іншого призначення.

Стадії проектування автоматизованої системи обробки даних та інформації встановлені ГОСТ 2.103-68:

- технічну пропозицію;
- ескізний проект;
- технічний проект;
- робоча конструкторська документація.

На основі технічного проекту створюється комплект робочої конструкторської документації, за якою готується дослідний зразок системи.

1.3. Потенційні загрози безпеці інформації в інформаційних системах

Дослідження та аналіз численних випадків впливів на інформацію та несанкціонованого доступу до неї показують, що їх можна розділити на випадкові і навмисні. Навмисні загрози часто шляхом їх систематичного застосування можуть бути приведені у виконання через випадкові шляхом довготривалої масованої атаки несанкціонірованними запитами або вірусами.

Наслідки, до яких призводить реалізація загроз:

- руйнування (втрата) інформації;
- модифікація (зміна інформації на помилкову, яка коректна за формою і змістом, але має інший сенс);
- ознайомлення з нею сторонніх осіб.

Ціна зазначених подій може бути самою різною: від невинних непорозумінь до сотень тисяч доларів і більше.

Попередження наведених наслідків в інформаційній системі і є основна мета створення системи безпеки інформації.

Для створення засобів захисту інформації необхідно визначити природу загроз, форми і шляхи їх можливого прояву і здійснення в інформаційній системі [9].

Аналіз негативних наслідків реалізації загроз передбачає обов'язкову ідентифікацію можливих джерел загроз, вразливостей, що сприяють їх прояву і методів реалізації. І тоді ланцюжок виростає в схему, представлену на рис. 1.1.

Загрози класифікуються за можливістю нанесення шкоди суб'єкту відносин при порушенні цілей безпеки. Збиток може бути заподіяно будь-яким суб'єктом (злочин, вина або недбалість), а також стати наслідком, не залежним від суб'єкта проявів. Загроз не так вже й багато. При забезпеченні конфіденційності інформації це може бути розкрадання (копіювання) інформації та засобів її обробки, а також її втрата (ненавмисна втрата, витік).

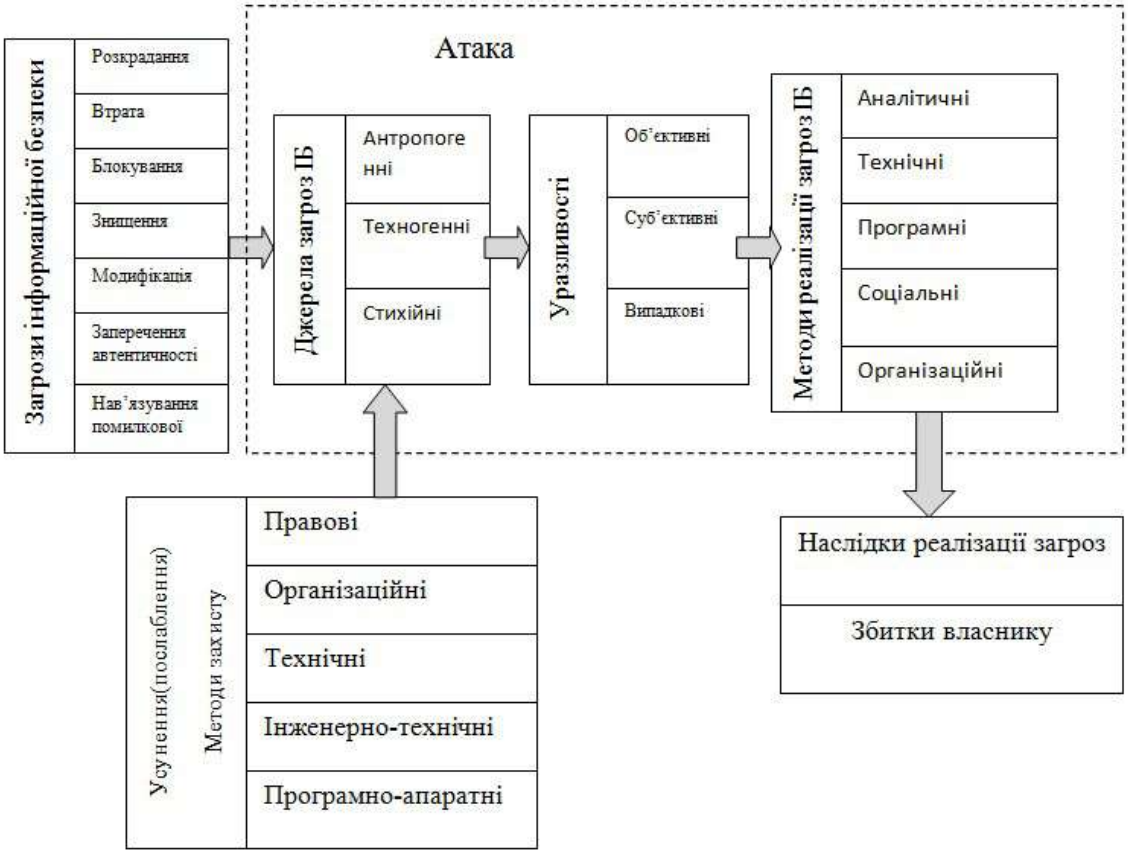

Рисунок 1.1 - Модель реалізації загроз інформаційної безпеки

1.3.1.Випадкові загрози

Інформація в процесі введення, зберігання, обробки, виведення і передачі піддається різним випадковим впливам. В результаті таких впливів на апаратному рівні відбуваються фізичні зміни рівнів сигналів в цифрових кодах, що несуть інформацію.

При цьому спостерігаються в одному або двох, трьох і т. п. розрядах зміни 1 на 0 або 0 на 1, або те й інше разом, але в різних розрядах, наслідком цього в підсумку є зміна значення коду на інше. Далі, якщо застосовувані для цієї мети кошти функціонального контролю здатні виявити ці зміни, проводиться бракування даного коду, а пристрій, блок,

модуль або мікросхема, що беруть участь в обробці, оголошуються несправними. Якщо функціональний контроль відсутній або не здатний виявити несправність на даному етапі обробки, процес обробки триває по хибному шляху, відбувається модифікація інформації. В процесі подальшої обробки в залежності від змісту і призначення помилкової команди можлива або відправка інформації за помилковою адресою, або передача неправдивої інформації адресату, або стирання або запис іншої інформації в оперативному запам'ятовуючому пристрої, виникають небажані події: руйнування (втрата), модифікація і витік інформації.

На програмному рівні в результаті випадкових впливів може відбутися зміна алгоритму обробки інформації на непередбачений, характер якого теж може бути різним: в кращому випадку - зупинка інформаційного або обчислювального процесу, а в гіршому - його модифікація. Модифікації алгоритму або даних можуть пройти непоміченими або привести також до руйнування інформації, а при переплутуванні адреси пристрою - до витоку інформації.

При програмних помилках можуть підключатися програми введення-виведення і передачі їх на заборонені пристрої.

Частота відмов і збоїв апаратури збільшується при виборі і проектуванні системи, слабкої відносно надійності функціонування апаратури. Перешкоди на лініях зв'язку залежать від правильності вибору місця розміщення технічних засобів інформаційної системи щодо один одного і по відношенню до апаратури і агрегатів сусідніх систем.

При розробці складних автоматизованих систем збільшується число схемних, системотехнічних, структурних, алгорітмічних і програмних помилок. На їхню кількість у процесі проектування дуже впливає багато інших факторів: кваліфікація розробників, умови їх роботи, наявність досвіду та ін.

На етапах виготовлення та випробувань на якість вхідної в інформаційну систему апаратури впливають повнота і якість документації,

за якою її виготовляють, технологічна дисципліна та інші фактори.

До загроз випадкового характеру слід також віднести аварійні ситуації, які можуть виникнути на об'єкті розміщення автоматизованої інформаційної системи. До аварійних ситуацій відносяться:

- відмова функціонування інформаційної системи в цілому, наприклад вихід з ладу електроживлення та освітлення;
- стихійні лиха: пожежа, повінь, землетрус, урагани, удари блискавки, обвали і т.п.;
- відмова системи життєзабезпечення на об'єкті експлуатації інформаційної системи.

Імовірність цих подій пов'язана насамперед з правильним вибором місця розміщення інформаційної системи або її елементів, включаючи географічне положення, і організацією протипожежних заходів.

1.3.2. Навмисні загрози

Навмисні загрози пов'язані з різними діями людини, причинами яких може бути досить великий спектр його станів: певне невдоволення своєю життєвою ситуацією, сугубо матеріальний інтерес або просте розвага з самоствердженням своїх здібностей і т. п. Ми не розглядаємо дані причини стану людини.

Наше завдання - попередження, виявлення та блокування можливих дій зловмисника в інформаційній системі. Потенційні загрози з цього боку будуть розглянуті тільки в технічному аспекті.

Для постановки більш конкретної задачі проаналізуємо об'єкт захисту інформації на предмет введення-виведення, зберігання та обробки інформації і можливостей порушника з доступу до інформації за відсутності засобів захисту в даній автоматизованій системі.

В якості об'єкта захисту згідно класифікації вибираємо комп'ютерну

систему, яка може бути елементом комп'ютерної мережі або великий автоматизованої системи управління. Для комп'ютерних систем в цьому випадку характерні наступні штатні канали доступу до інформації:

- термінали (робочі станції, персональні комп'ютери) користувачів;
- термінал (сервер або спеціалізована робоча станція) адміністратора системи;
- термінал (робоча станція) оператора функціонального контролю;
- засоби відображення інформації;
- засоби завантаження програмного забезпечення в комп'ютерний комплекс;
- носії інформації (оперативний пристрій, дистанційний пристрій, пристрій резервування та архівування, паперові носії);
- зовнішні канали зв'язку.

Маючи на увазі, що за відсутності захисту порушник може скористатися як штатними, так і іншими фізичними каналами доступу, назвемо можливі канали несанкціонованого доступу у комп'ютерній системі, через які можливо одержати доступ до апаратури, програмного забезпечення та здійснити розкрадання, руйнування, модифікацію інформації та ознайомлення з нею:

- всі перераховані вище штатні засоби при їх використанні законними користувачами не за призначенням і за межами своїх повноважень;
- всі перераховані вище штатні засоби при їх використанні сторонніми особами;
- технологічні пульти управління;
- внутрішній монтаж апаратури;
- лінії зв'язку між апаратними засобами даної комп'ютерної системи;
- побічне електромагнітне випромінювання інформації з апаратури системи;

- побічні наводки інформації по мережі електроживлення і заземлення апаратури;
- побічні наводки інформації на допоміжних і сторонніх комунікаціях;
- відходи обробки інформації у вигляді паперових, магнітних та лазерних носіїв, кинуті в сміттєву корзину.

Очевидно, що за відсутності законного користувача, контролю і розмежування доступу до термінала кваліфікований порушник легко скористається його функціональними можливостями для несанкціонованого доступу до інформації шляхом введення відповідних запитів або команд [3]. При наявності вільного доступу в приміщення можна візуально спостерігати інформацію на засобах відображення і документування, а на останніх викрасти паперовий носій, зняти зайву копію, а також викрасти інші носії з інформацією: лістинги, магнітні стрічки, диски, флеш-носії і т. п. Особливу небезпеку являє собою безконтрольна завантаження програмного забезпечення в комп'ютер, в якому можуть бути змінені дані, алгоритми або введена програма «троянський кінь» - програма, що виконує додаткові незаконні функції: запис інформації на сторонній носій, передачу в канали зв'язку іншого абонента комп'ютерної мережі, внесення в систему комп'ютерного вірусу і т. п. При відсутності розмежування і контролю доступу до технологічної та оперативної інформації можливий доступ до оперативної інформації з боку терміналу функціонального контролю. Небезпечною є ситуація, коли порушником є користувач комп'ютерної системи, який за своїми функціональними обов'язками має законний доступ до однієї частини інформації, а звертається до іншої за межами своїх повноважень.

З боку законного користувача існує багато способів порушувати роботу інформаційної системи, зловживати нею витягувати, модифікувати або знищувати інформацію. Для цієї мети можуть бути використані привілейовані команди введення-виведення, відсутність контролю

законності запиту та звернень до адреси пам'яті запам'ятовуючих пристроїв і т. п.

При технічному обслуговуванні (профілактиці та ремонті) апаратури можуть бути виявлені залишки інформації на магнітній стрічці або дисках, поверхнях дисків та інших носіях інформації. Стирання інформації звичайними методами при цьому не завжди ефективно. Її залишки можуть бути легко прочитані.

Не має сенсу створення системи контролю і розмежування доступу до інформації на програмному рівні, якщо не контролюється доступ до пульта керування комп'ютера, внутрішнього монтажу апаратури, кабельного з'єднання.

Порушник може стати незаконним користувачем системи в режимі поділу часу, визначивши порядок роботи законного користувача або працюючи слідом за ним по одним і тим же лініях зв'язку. Він може також використовувати метод проб і помилок і реалізувати «дірки» в операційній системі, прочитати паролі. Без знання паролів він може здійснити «селективне» включення в лінію зв'язку між терміналом і головним комп'ютером (сервером); без переривання роботи законного користувача може продовжити її від його імені, анулювавши сигнали відключення законного користувача.

Процеси обробки, передачі та зберігання інформації апаратними засобами автоматизованої системи забезпечуються спрацьовуванням логічних елементів, побудованих на базі напівпровідникових приладів, виконаних найчастіше у вигляді інтегральних схем.

Спрацювання логічних елементів обумовлено високочастотною зміною рівнів напруг і струмів, що призводить до виникнення в ефірі, ланцюгах живлення і заземлені, а також у паралельно розташованих ланцюгах і індуктивностях сторонньої апаратури електромагнітних полів і наведень, що несуть в амплітуді, фазі і частоті своїх коливань ознаки оброблюваної інформації. Використання порушником різних приймачів

може привести до їх прийому і витоку інформації. Зі зменшенням відстані між приймачем порушника і апаратними засобами ймовірність прийому сигналів такого роду збільшується.

Безпосереднє підключення порушником приймальної апаратури і спеціальних датчиків до ланцюгів електроживлення і заземлення, до каналів зв'язку також дозволяє здійснити несанкціоноване ознайомлення з інформацією, а несанкціоноване підключення до каналів зв'язку передавальної апаратури може призвести і до модифікації інформації.

Особливо слід зупинитися на загрозах, яким можуть піддаватися канали та лінії зв'язку комп'ютерної мережі.

Припустимо, що порушник може розташовуватися в деякій точці мережі, через яку повинна проходити вся інформація щойого цікавить. Наприклад, в міжмережевих умовах порушник може прийняти вид шлюзу в деякій проміжній мережі, яка забезпечує єдиний шлях з'єднання між двома процесами.

У цьому випадку, незважаючи на те, що мережа-джерело і мережа-адресат захищені, порушник може впливати на з'єднання, так як воно проходить через шлюз, що з'єднує ці мережі. У загальному випадку передбачається, що порушник може займати позицію, що дозволяє здійснювати пасивне і активне перехоплення.

У разі пасивного перехоплення, порушник тільки стежить за повідомленнями, переданими по з'єднанню, без втручання в їх потік. Спостереження порушника за даними (прикладного рівня) в повідомленні дозволяє розкрити зміст повідомлень. Порушник може також стежити за заголовками повідомлень, навіть якщо дані не зрозумілі йому, з метою визначення місця розміщення і ідентифікаторів процесів, що беруть участь у передачі даних. Порушник може визначити довжини повідомлень і частоту їх передачі для визначення характеру переданих даних.

Порушник може також займатися активним перехопленням, виконуючи безліч дій над повідомленнями, переданими по з'єднанню. Ці

повідомлення можуть бути вибірково змінені, знищені, затримані, переупорядкувати, здубльовані і введені в з'єднання в більш пізній момент часу. Порушник може створювати підроблені повідомлення і вводити їх в з'єднання. Подібні дії можна визначити як зміна потоку і змісту повідомлень.

Крім того, порушник може скидати всі повідомлення або затримувати їх. Подібні дії можна класифікувати як переривання передачі повідомлень.

Сформулюємо п'ять основних категорій загроз безпеки інформації та даних в комп'ютерних мережах:

1) розкриття змісту повідомлень, що передаються;

2) аналіз трафіку, що дозволяє визначити приналежність відправника і одержувача даних до однієї з груп користувачів мережі, пов'язаних спільним завданням;

3) зміна потоку повідомлень, що може призвести до порушення режиму роботи будь-якого об'єкта, керованого з віддаленого комп'ютера;

4) неправомірну відмову в наданні послуг;

5) несанкціоноване встановлення з'єднання.

Дана класифікація не суперечить визначенню терміну «безпека інформації» та поділу потенційних загроз на витік, модифікацію і втрату інформації.

Загрози 1 і 2 можна віднести до витоку інформації, загрози 3 й 5 - до її модифікації, а погрозу 4 - до порушення процесу обміну інформацією

У комп'ютерних мережах порушник може застосовувати такі стратегії:

- отримати несанкціонований доступ до секретної інформації;
- видати себе за іншого користувача, щоб зняти з себе відповідальність або ж використовувати його повноваження з метою формування помилкової інформації, застосування помилкового посвідчення особи, санкціонування хибних обмінів інформацією або ж їх підтвердження;

- відмовитися від факту формування переданої інформації;
- стверджувати про те, що інформація отримана від деякого користувача, хоча насправді вона сформована самим же порушником;
- стверджувати те, що одержувачу в певний момент часу була послана інформація, яка насправді не надсилалася (або надсилалася в інший момент часу);
- відмовитися від факту отримання інформації, яка насправді була отримана, або стверджувати про інший час її отримання;
- незаконно розширити свої повноваження по доступу до інформації та її обробки;
- незаконно змінити повноваження інших користувачів (розширити або обмежити, вивести або ввести інших осіб);
- приховати факт наявності деякою інформацією в іншій інформації (прихована передача однієї в змісті іншої інформації);
- підключитися до лінії зв'язку між іншими користувачі в якості активного ретранслятора;
- вивчити, хто, коли і до якої інформації отримує доступ (навіть якщо сама інформація залишається недоступною);
- заявити про сумнівність протоколу забезпечення інформацією через розкриття деякою інформацією, яка згідно з умовами протоколу, повинна залишатися секретною;
- модифікувати програмне забезпечення шляхом виключення або додавання нових функцій;
- навмисно змінити протокол обміну інформацією з метою його порушення або підриву довіри до нього;
- перешкодити обміну повідомленнями між іншими користувачами шляхом введення перешкод з метою порушення аутентифікації повідомлень.

Аналіз останніх можливих стратегій порушника в комп'ютерних мережах говорить про те, наскільки важливо знати, кого вважати порушником. При цьому в якості порушника розглядається не тільки стороння особа, а й законний користувач. [1]

Аналіз інших загроз свідчить про те, що завдання захисту від них можна умовно розділити на завдання двох рівнів: користувачів і елементів мережі, з якими працюють користувачі мережі.

Висновки до розділу 1

В даному розділі розглядається об’єкт дослідження, системи, завдяки яким передаються дані, а також основні типи загроз, направлені на ці дані. Приведено класифікацію систем передачі даних і основних видів атак

2 МЕТОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ІНФОРМАЦІЇ В ТЕЛЕКОМУНІКАЦІЙНИХ МЕРЕЖАХ

2.1. Традиційні заходи і методи захисту інформації

Для забезпечення безпеки інформації в офісних мережах проводяться різні заходи, що об'єднуються поняттям «система захисту інформації». Система захисту інформації – це сукупність заходів, програмно-технічних засобів, правових і морально-етичних норм, спрямованих на протидію загрозам порушників з метою зведення до мінімуму можливої шкоди користувачам і власникам системи.

Традиційні заходи для протидії витокам інформації поділяються на технічні та організаційні .

До технічних заходів можна віднести захист від несанкціонованого доступу до системи, резервування особливо важливих комп'ютерних підсистем, організацію обчислювальних мереж з можливістю перерозподілу ресурсів у разі порушення працездатності окремих ланок, установку обладнання виявлення і гасіння пожежі, обладнання виявлення води, прийняття конструкційних заходів захисту від розкрадань, саботажу, диверсій, вибухів, установку резервних систем електроживлення, оснащення приміщень замками, установку сигналізації та багато іншого.

До організаційних заходів можна віднести охорону серверів, ретельний підбір персоналу, виключення випадків ведення особливо важливих робіт тільки однією людиною, наявність плану відновлення працездатності сервера після виходу його з ладу, універсальність засобів захисту від всіх користувачів (включаючи вище керівництво).

Несанкціонований доступ до інформації може відбуватися під час профілактики або ремонту комп'ютерів за рахунок прочитання залишкової інформації на носіях, незважаючи на її видалення користувачем звичайними

методами. Інший спосіб-прочитання інформації з носія під час його транспортування без охорони всередині об'єкта або регіону.

Сучасні комп'ютерні засоби побудовані на інтегральних схемах. При роботі таких схем відбуваються високочастотні зміни рівнів напруги і струмів, що призводить до виникнення в ланцюгах живлення, в ефірі, в блізрасположенной апаратурі і т.п. Електромагнітних полів і наведень, які за допомогою спеціальних засобів (умовно назвемо їх "шпигунськими") можна трансформувати в оброблювану інформацію. Зі зменшенням відстані між приймачем порушника і апаратними засобами ймовірність такого роду знімання і розшифровки інформації збільшується.

Несанкціоноване ознайомлення з інформацією можливе також шляхом безпосереднього підключення порушником "шпигунських" засобів до каналів зв'язку та мережевих апаратних засобів.

Традиційними методами захисту інформації від несанкціонованого доступу є ідентифікація та аутентифікація, захист паролями.

Ідентифікація та аутентифікація. У комп'ютерних системах зосереджується інформація, право на користування якою належить певним особам або групам осіб, що діють у порядку особистої ініціативи або відповідно до посадових обов'язків. Щоб забезпечити безпеку інформаційних ресурсів, усунути можливість несанкціонованого доступу, посилити контроль санкціонованого доступу до конфіденційної або до підлягає засекречування інформації, впроваджуються різні системи розпізнавання, встановлення автентичності об'єкта (суб'єкта) і розмежування доступу. В основі побудови таких систем знаходиться принцип допуску і виконання тільки таких звернень до інформації, в яких присутні відповідні ознаки дозволених повноважень.

Ключовими поняттями в цій системі є ідентифікація та аутентифікація. Ідентифікація-це присвоєння будь-якому об'єкту або суб'єкту унікального імені або образу. Аутентифікація – це встановлення автентичності, тобто перевірка, чи є об'єкт (суб'єкт) дійсно тим, за кого він себе видає.

Кінцева мета процедур ідентифікації та аутентифікації об'єкта – суб'єкта) – допуск його до інформації обмеженого користування в разі позитивної перевірки або відмова в допуску в разі негативного результату перевірки.

Об'єктами ідентифікації та аутентифікації можуть бути: люди (користувачі, оператори та ін.); технічні засоби (монітори, робочі станції, абонентські пункти); документи (ручні, роздруківки та ін.); магнітні носії інформації; інформація на екрані монітора та ін.

Встановлення автентичності об'єкта може проводитися апаратним пристроєм, програмою, людиною і т. д.

Захист паролями. Пароль – це сукупність символів, що визначає об'єкт (суб'єкта). При виборі пароля виникають питання про його розмір, стійкості до несанкціонованого підбору, способам його застосування. Природно, чим більше довжина пароля, тим більшу безпеку буде забезпечувати система, бо будуть потрібні великі зусилля для його відгадування. При цьому вибір довжини пароля в значній мірі визначається розвитком технічних засобів, їх елементною базою і швидкодією.

У разі застосування пароля необхідно періодично замінювати його на новий, щоб знизити ймовірність його перехоплення шляхом прямого розкрадання носія, зняття його копії і навіть фізичного примусу людини. Пароль вводиться користувачем на початку взаємодії з комп'ютерною системою, іноді і в кінці сеансу (в особливо відповідальних випадках пароль нормального виходу може відрізнятися від вхідного). Для правомочності користувача може передбачатися введення пароля через певні проміжки часу.

Пароль може використовуватися для ідентифікації та встановлення автентичності терміналу, з якого входить в систему користувач, а також для зворотного встановлення автентичності комп'ютера по відношенню до користувача.

Для ідентифікації користувачів можуть застосовуватися складні в плані технічної реалізації системи, що забезпечують встановлення автентичності

користувача на основі аналізу його індивідуальних параметрів: відбитків пальців, малюнка ліній руки, райдужної оболонки очей, тембру голосу та ін.

Широке поширення знайшли фізичні методи ідентифікації з використанням носіїв кодів паролів. Такими носіями є перепустки в контрольно-пропускних системах; пластикові карти з ім'ям власника, його кодом, підписом; пластикові картки з магнітною смугою; пластикові карти з вбудованою мікросхемою (smart-card); карти оптичної пам'яті та ін.

Засоби захисту інформації за методами реалізації можна розділити на три групи:

- програмний;
- програмно-апаратні;
- апаратний.

Програмними засобами захисту інформації називаються спеціально розроблені програми, які реалізують функції безпеки обчислювальної системи, здійснюють функцію обмеження доступу користувачів по паролях, ключах, багаторівневому доступу і т.д. ці програми можуть бути реалізовані практично в будь-якій операційній системі, зручною для користувача. Як правило, ці програмні засоби забезпечують досить високий ступінь захисту системи і мають помірні ціни [4].

При підключенні такої системи в Глобальну Мережу ймовірність злому захисту збільшується. Отже, цей спосіб захисту прийнятний для локальних замкнутих мереж, які не мають зовнішній вихід.

Програмно-апаратними засобами називаються пристрої, реалізовані на універсальних або спеціалізованих мікропроцесорах, які не потребують модифікацій в схемотехніці при зміні алгоритму функціонування. Ці пристрої також адаптуються в будь-якій операційній системі, мають велику ступінь захисту. Вони обійдуться трохи дорожче (їх ціна залежить від типу операційної системи). При цьому даний тип пристроїв є самим гнучким інструментом, що дозволяє вносити зміни в конфігурацію на вимогу замовника. Програмно-

апаратні засоби забезпечують високий ступінь захисту локальної мережі, підключеної до глобальної.

Апаратними засобами називаються пристрої, в яких функціональні вузли реалізуються на надвеликих інтегральних системах (СБІС) з незмінним алгоритмом функціонування. Цей тип пристроїв адаптується в будь-якій операційній системі, є найдорожчим в розробці, пред'являє високі технологічні вимоги при виробництві. У той же час ці пристрої мають найвищий ступінь захисту, в них неможливо впровадитися і внести конструктивні або програмні зміни. Застосування апаратних засобів утруднено через їх високу вартість і статичності алгоритму. Програмно-апаратні засоби, поступаючись апаратним за швидкістю, дозволяють в той же час легко модифікувати алгоритм функціонування і не володіють недоліками програмних методів. До окремої групи заходів щодо забезпечення збереження інформації та виявлення несанкціонованих запитів відносяться програми виявлення порушень в режимі реального часу.

2.2. Криптографічні методи та засоби захисту інформації

Найбільший інтерес сьогодні викликають наступні напрямки теоретичних і прикладних досліджень: створення та аналіз надійності криптографічних алгоритмів і протоколів; адаптація алгоритмів до різних апаратних і програмних платформ; використання існуючих технологій криптографії в нових прикладних системах; можливість використання технологій криптографії для захисту інтелектуальної власності. Інтерес до досліджень з адаптації алгоритмів до різних апаратних і програмних платформ викликаний створенням кроссплатформних телекомунікаційних систем на базі єдиних стандартів на алгоритми. Один і той же алгоритм повинен ефективно виконуватися на самих різних апаратних і програмних платформах від

мобільного телефону до маршрутизатора, від смарт-карти до настільного комп'ютера.[6]

Існуючі засоби захисту даних в телекомунікаційних мережах можна розділити на дві групи за принципом побудови ключової системи і системи аутентифікації. До першої групи віднесемо засоби, що використовують для побудови ключової системи і системи аутентифікації симетричні криптоалгоритми, до другої - асиметричні.

Проведемо порівняльний аналіз цих систем. Готове до передачі інформаційне повідомлення, спочатку відкрите і незахищене, зашифровується і тим самим перетворюється в шифрограму, тобто в закриті текст або графічне зображення документа. У такому вигляді повідомлення передається по каналу зв'язку, навіть і не захищеному. Санкціонований користувач після отримання повідомлення дешифрує його (тобто розкриває) за допомогою зворотного перетворення криптограми, внаслідок чого виходить вихідний, відкритий вид повідомлення, доступний для сприйняття санкціонованим користувачам.

Методу перетворення в криптографічній системі відповідає використання спеціального алгоритму. Дія такого алгоритму запускається унікальним числом (послідовністю біт), зазвичай званим шифруючим ключем. Для більшості систем схема генератора ключа може являти собою набір інструкцій і команд або вузол апаратури, або комп'ютерну Програму, або все це разом, але в будь-якому випадку процес шифрування (дешифрування) реалізується тільки цим спеціальним ключем. Щоб обмін зашифрованими даними проходив успішно, як відправнику, так і одержувачу, необхідно знати правильну ключову установку і зберігати її в таємниці.

Стійкість будь-якої системи закритого зв'язку визначається ступенем секретності використовуваного в ній ключа. Тим не менш, цей ключ повинен бути відомий іншим користувачам мережі, щоб вони могли вільно обмінюватися зашифрованими повідомленнями. У цьому сенсі криптографічні системи також допомагають вирішити проблему аутентифікації (встановлення автентичності) прийнятої інформації. Зломщик в разі перехоплення

повідомлення буде мати справу тільки з зашифрованим текстом, а істинний одержувач, приймаючи повідомлення, закриті відомим йому і відправнику ключем, буде надійно захищений від можливої дезінформації.

Крім того, існує можливість шифрування інформації і більш простим способом – з використанням генератора псевдовипадкових чисел. Використання генератора псевдовипадкових чисел полягає в генерації гами шифру за допомогою генератора псевдовипадкових чисел при певному ключі і накладення отриманої гами на відкриті дані оборотним способом. Цей метод криптографічного захисту реалізується досить легко і забезпечує досить високу швидкість шифрування, проте недостатньо стійкий до дешифрування.

Для класичної криптографії характерне використання однієї секретної одиниці-ключа, який дозволяє відправнику зашифрувати повідомлення, а одержувачу розшифрувати його. У разі шифрування даних, що зберігаються на магнітних або інших носіях інформації, ключ дозволяє зашифрувати інформацію при записі на носій і розшифрувати при читанні з нього.

З викладеного випливає, що надійна криптографічна система повинна задовольняти ряду певних вимог

- Процедури зашифровування і розшифрування повинні бути "прозорі" для користувача
- Дешифрування закритої інформації має бути максимально утруднено.
- Зміст переданої інформації не повинно позначатися на ефективності криптографічного алгоритму.

Найбільш перспективними системами криптографічного захисту даних сьогодні вважаються асиметричні криптосистеми, звані також системами з відкритим ключем. Їх суть полягає в тому, що ключ, який використовується для зашифровування, відмінний від ключа розшифровування. При цьому ключ зашифровування не секретний і може бути відомий всім користувачам системи. Однак розшифрування за допомогою відомого ключа зашифровування

неможливо. Для розшифровування використовується спеціальний, секретний ключ. Знання відкритого ключа не дозволяє визначити ключ секретний. Таким чином, розшифрувати повідомлення може тільки його одержувач, який володіє цим секретним ключем.Фахівці вважають, що системи з відкритим ключем більше підходять для шифрування переданих даних, ніж для захисту даних, що зберігаються на носіях інформації.

Однією з важливих соціально-етичних проблем, породжених все більш розширюється застосуванням методів криптографічного захисту інформації, є протиріччя між бажанням користувачів захистити свою інформацію і передачу повідомлень і бажанням спеціальних державних служб мати можливість доступу до інформації деяких інших організацій і окремих осіб з метою припинення незаконної діяльності [10].

У розвинених країнах спостерігається широкий спектр думок про підходи до питання про регламентацію використання алгоритмів шифрування. Висловлюються пропозиції від повної заборони широкого застосування криптографічних методів до повної свободи їх використання. Деякі пропозиції відносяться до дозволу використання тільки ослаблених алгоритмів або до встановлення порядку обов'язкової реєстрації ключів шифрування. Надзвичайно важко знайти оптимальне рішення цієї проблеми.

Як оцінити співвідношення втрат законослухняних громадян і організацій від незаконного використання їх інформації та збитків держави від неможливості отримання доступу до зашифрованої інформації окремих груп, що приховують свою незаконну діяльність? Як можна гарантовано не допустити незаконне використання криптоалгоритмів особами, які порушують і інші закони?

Крім того, завжди існують способи прихованого зберігання і передачі інформації. Ці питання ще належить вирішувати соціологам, психологам, юристам і політикам.

Криптографія надає можливість забезпечити безпеку інформації в INTERNET і зараз активно ведуться роботи по впровадженню необхідних

криптографічних механізмів в цю мережу. Не відмова від прогресу в інформатизації, а використання сучасних досягнень криптографії - ось стратегічно правильне рішення. Можливість широкого використання глобальних інформаційних мереж і криптографії є досягненням і ознакою демократичного суспільства.

2.3. Нетрадиційні методи захисту інформації

Потреби сучасної практичної інформатики призвели до виникнення нетрадиційних завдань захисту електронної інформації, однією з яких є аутентифікація електронної інформації в умовах, коли обмінюються інформацією сторони не довіряють один одному. Ця проблема пов'язана зі створенням систем електронного цифрового підпису.

У вітчизняній літературі прижилися три терміни для визначення одного поняття: електронний підпис; електронно-цифровий підпис (ЕЦП); цифровий підпис. Останній варіант є прямим перекладом англійського словосполучення digital signature. Термін "цифровий підпис" більш зручний і точний.

Електронний цифровий підпис-реквізит електронного документа, призначений для захисту даного електронного документа від підробки, отриманий в результаті криптографічного перетворення інформації з використанням закритого ключа електронного цифрового підпису і дозволяє ідентифікувати власника сертифіката ключа підпису, а також встановити відсутність спотворення інформації в електронному документі.

Електронний цифровий підпис являє собою послідовність символів, отримана в результаті криптографічного перетворення електронних даних. ЕЦП додається до блоку даних і дозволяє одержувачу блоку перевірити джерело і цілісність даних і захиститися від підробки. ЕЦП використовується в якості аналога власноручного підпису.

Електронний цифровий підпис в електронному документі рівнозначний власноручному підпису в документі на паперовому носії при одночасному дотриманні наступних умов:

– сертифікат ключа підпису, що відноситься до цього електронного цифрового підпису, не втратив чинність (діє) на момент перевірки або на момент підписання електронного документа за наявності доказів, що визначають момент підписання. Сертифікат ключа підпису - це документ на паперовому носії або електронний документ з електронним цифровим підписом уповноваженої особи засвідчувального центру, які включають у себе відкритий ключ електронного цифрового підпису та які видаються центром учаснику інформаційної системи для підтвердження дійсності електронного цифрового підпису та ідентифікації власника сертифіката ключа підпису;

– підтверджено справжність електронного цифрового підпису в електронному документі. Підтвердження справжності електронного цифрового підпису в електронному документі-позитивний результат перевірки відповідним сертифікованим засобом електронного цифрового підпису з використанням сертифіката ключа підпису приналежності електронного цифрового підпису в електронному документі власнику сертифіката ключа підпису та відсутності спотворень у підписаному цим електронним цифровим підписом електронному документі;

– електронний цифровий підпис використовується відповідно до відомостей, зазначених у сертифікаті ключа підпису.

ЕЦП, як і інші реквізити документа, що виконують засвідчувальну функцію (власноручний підпис, печатка та ін.), є засобом, що забезпечує конфіденційність інформації.

Механізм виконання власноручного (фізичного) підпису безпосередньо обумовлений психофізіологічними характеристиками організму людини, в силу чого цей підпис нерозривно пов'язана з біологічною особистістю підписує. Власноручний підпис дозволяє встановити (ідентифікувати) конкретну людину за ознаками почерку.

ЕЦП, будучи криптографічним засобом, не може розглядатися в якості властивості, властивого безпосередньо власнику ЕЦП як біологічної особистості. Між ЕЦП і людиною, її поставив існує взаємозв'язок не біологічного, а соціального характеру. Виникнення, існування і припинення даного зв'язку обумовлено сукупністю різних правових, організаційних і технічних факторів.

Ототожнення людини за власноручним підписом і підтвердження на цій основі справжності документа, якою він завірений, досягається шляхом проведення судово-почеркознавчої експертизи, вирішальної дану ідентифікаційну задачу.[7]

Визначення справжності ЕЦП свідчить тільки про знання особою, яка її поставила, закритого ключа ЕЦП. Для того щоб встановити, чи дійсно власник сертифіката ключа запевнив документ ЕЦП, треба з'ясувати крім справжності ЕЦП і зазначені вище фактори.

Завдання встановлення факту посвідчення електронного документа ЕЦП власником сертифіката ключа підпису вирішується в результаті процесуальної діяльності з доказування в ході судового розгляду.

Висновки до розділу 2

В даному розділі приведена класифікація методів захисту данних: традиційні(аутентифікація,пароль),криптографічні(шифрування), нетрадиційні(електронний цифровий підпис). Розглянуті основні позитивні і негативні сторони цих методів

3 КРИПТОГРАФІЧНЕ ПЕРЕТВОРЕННЯ ІНФОРМАЦІЇ

3.1. Короткий огляд і класифікація методів шифрування інформації

Захист інформації методом криптографічного перетворення полягає в перетворенні її складових частин (слів, букв, складів, цифр) за допомогою спеціальних алгоритмів, приведенні її до неявного виду. Для ознайомлення з шифрованою інформацією застосовується зворотний процес - декодування (дешифрування). Використання криптографії є одним з найпоширеніших методів, значно підвищують безпеку передачі даних в комп'ютерних мережах, даних, що зберігаються в пристроях пам'яті, і при обміні інформацією між віддаленими об'єктами.

Для перетворення (шифрування) зазвичай використовується деякий алгоритм або пристрій, що реалізує заданий алгоритм, які можуть бути відомі широкому колу осіб. Управління процесом шифрування здійснюється за допомогою періодично змінюваного коду ключа, що забезпечує кожен раз оригінальне представлення інформації при використанні одного і того ж алгоритму або пристрою. Знання ключа дозволяє просто і надійно розшифрувати текст. Однак без знання ключа ця процедура може бути практично нездійсненна навіть при відомому алгоритмі шифрування.

Навіть просте перетворення інформації є досить ефективним засобом, що дає можливість приховати її сенс від більшості некваліфікованих порушників.

Структурна схема шифрування інформації представлена на рис. 1.

Коди і шифри використовувалися протягом багатьох століть задовго до появи комп'ютера. Між кодуванням і шифруванням не існує чіткої відмінності. Зауважимо лише, що останнім часом на практиці слово «кодування» застосовують в цілях цифрового подання інформації при її

обробці на технічних засобах, а «шифрування» - при перетворенні інформації для захисту від несанкціонованого доступу. В даний час деякі методи шифрування добре опрацьовані і є класичними.

Для побудови засобів захисту інформації від несанкціонованого доступу необхідно мати уявлення про деякі традиційних методах шифрування: підстановки, перестановки, комбінованих та ін.

Основні вимоги, пропоновані до методів захисного перетворення:

- вживаний метод повинен бути досить стійким до спроб розкрити вихідний текст, маючи тільки зашифрований текст;
- обсяг ключа не повинен ускладнювати його запам'ятовування і пересилку;
- алгоритм перетворення інформації і ключ, використовувані для шифрування і дешифрування, не повинні бути дуже складними: витрати на захисні перетворення повинні бути прийнятні при заданому рівні збереження інформації;
- помилки в шифруванні не повинні викликати втрату інформації. Через появу помилок передачі шифрованого повідомлення по каналах зв'язку не повинна виключатися можливість надійної розшифровки тексту на приймальному кінці;
- довжина зашифрованого тексту не повинна перевищувати довжину вихідного тексту;
- необхідні тимчасові і вартісні ресурси на шифрування і дешифрування інформації визначаються необхідної ступенем захисту інформації.[11]

Перераховані вимоги характерні в основному для традиційних засобів захисних перетворень. З розвитком пристроїв пам'яті, що дозволяють з більшою щільністю записувати і надійно зберігати тривалий час великі обсяги інформації, обмеження на обсяг ключа може бути значно знижений. Поява і розвиток електронних елементів дозволили розробити недорогі

пристрої, що забезпечують перетворення інформації.

Однак збільшення швидкостей передачі інформації поки ще значно відстає від швидкості її обробки. Ця невідповідність дозволяє значною мірою послабити вимога без шкоди для практично досяжною швидкості передачі. При існуючій надійності апаратури і розвинених методах виявлення та виправлення помилок ця вимога може бути знижене. Крім того, технологія передачі даних, прийнята в комп'ютерних мережах і автоматизованих системах управління, передбачає повторну передачу інформації в разі виявлення помилок передачі повідомлення.

Безліч сучасних методів захисних перетворень можна розділити на чотири великі групи: перестановки, заміни (підстановки), адитивні і комбіновані методи.

Методи перестановки і підстановки зазвичай характеризуються короткою довжиною ключа, а надійність їх захисту визначається складністю алгоритмів перетворення.

Для адитивних методів характерні прості алгоритми перетворення, а їх надійність заснована на збільшенні довжини ключа.

Всі перераховані методи відносяться до так званого симетричного шифрування: один і той же ключ використовується для шифрування і дешифрування.

Крім цього, використовуються методи несиметричного шифрування: один ключ для шифрування (відкритий), другий - для дешифрування (закритий).

Методи перестановки. Суть методів перестановки полягає в тому, що вхідний потік вихідного тексту ділиться на блоки, в кожному з яких виконується перестановка символів.

Перестановки в класичній криптографії зазвичай виходять в результаті запису вихідного тексту і читання шифрованого тексту за різними шляхами геометричної фігури.

Найпростішим прикладом перестановки є запис вихідного тексту по

рядках деякої матриці і читання його за стовпцями цієї матриці. Послідовність заповнення рядків і читання стовпців може бути будь якою і задається ключем. Таким чином, для матриці розмірністю 8х8 (довжина блоку 64 символу) можливо 1,6 х 109 ключів, що дозволяє на сучасних комп'ютерах шляхом перебору розшифрувати заданий текст. Однак для матриці розмірністю 16 х 16 (довжина блоку 256 символів) мається 1,4 х 1026 ключів, і перебір їх за допомогою сучасних засобів вельми скрутний.

Прикладом застосування методу перестановки може бути також восьмиелементна таблиця, яка має сукупність маршрутів, що носять назву маршрутів Гамільтона. Послідовність заповнення таблиці кожен раз відповідає нумерації її елементів. Якщо довжина тексту що шифрується не кратна числу елементів, то при останньому заповненні у вільні елементи заноситься довільний символ. Вибірка з таблиці для кожного заповнення може виконуватися по своєму маршруту, при цьому маршрути можуть використовуватися як послідовно, так і в порядку, що задається ключем.

Для методів перестановки характерні простота алгоритму, можливість програмної реалізації та низький рівень захисту, оскільки при великій довжині вихідного тексту в зашифрованому тексті проявляються статистичні закономірності ключа, що і дозволяє його швидко розкрити. Інший недолік цих методів - легке розкриття, якщо вдається направити в систему для шифрування кілька спеціально підібраних повідомлень. Так, якщо довжина блоку в початковому тексті дорівнює К символів, то для розкриття ключа досить пропустити через шифрувальну систему К-1 блоків вихідного тексту, в яких всі символи, крім одного, однакові.

Існують і інші способи перестановки, які можна реалізувати програмним і апаратним шляхом. Наприклад, реалізований апаратним шляхом блок-перестановки, який для перетворення інформації використовує електричні ланцюги, по яких вона передається паралельним способом (рис. 4). Перетворення тексту полягає в «переплутуванні» порядку розрядів у цифровій кодограми шляхом зміни електричного

монтажу схеми в блоці. Для дешифрування на приймальному пункті встановлюється інший блок, який відновлює порядок ланцюгів.

Методи заміни (підстановки). Методи шифрування заміною (підстановкою) полягають в тому, що символи вихідного тексту (блоку), записані в одному алфавіті, замінюються символами іншого алфавіту відповідно до прийнятого ключем перетворення.

Одним з найпростіших методів є пряма заміна вихідних символів їх еквівалентом з вектора замін. Для чергового символу вихідного тексту відшукується його місце розташування у вихідному алфавіті. Еквівалент з вектора заміни вибирається як віддалений на отриманий зсув від початку алфавіту. При дешифруванні пошук проводиться у векторі замін, а еквівалент вибирається з вихідного алфавіту. Отриманий таким методом текст має порівняно низький рівень захисту, так як вихідний і шифрований тексти мають однакові статистичні характеристики.

Більш стійкою щодо розкриття є схема шифрування, заснована на використанні таблиці Вижинера. Таблиця являє собою квадратну матрицю з числом елементів К, де К - кількість символів в алфавіті. У першому рядку матриці записуються літери в порядку черговості їх в алфавіті, у другій - та ж послідовність літер, але зі зсувом вліво на одну позицію, в третій - із зсувом на дві позиції і т. п. Вивільнені місця справа заповнюються витісненими вліво буквами, записуваними в природній послідовності.

Для шифрування тексту встановлюється ключ, що представляє собою деяке слово або набір букв. Далі з повної матриці вибирається підматриця шифрування, що включає, наприклад, перший рядок і рядок матриці, початковою літерою якої є послідовно букви ключа.

Для шифрування буквених повідомлень необхідно насамперед замінити знаки алфавіту їх цифровими еквівалентами, яким може бути порядковий номер букви в алфавіті.

Для дешифрування використовуються ті ж правила множення матриці

на вектор, тільки в якості основи береться зворотня матриця, а в якості вектора на який множать - відповідну кількість чисел шифрованого тексту. Цифрами вектора-результата будуть цифрові еквіваленти знаків вихідного тексту.

Неважко бачити, що процедури шифрування і дешифрування строго формалізовані, що дозволяє порівняно легко запрограмувати їх для автоматичної реалізації в компютері. Причому важливо, що шифрування і дешифрування здійснюється за однією і тією ж процедурою множення матриці на вектор, для них може використовуватися одна і та ж программа. Недоліком же є те, що для шифрування і дешифрування кожної букви потрібно виконати кілька арифметичних дій, що збільшує час обробки інформації.

Існують і інші методи підстановки. Наведені вище методи підстановки відносяться до моноалфавітної підстановки, які можна представити як числові перетворення букв вихідного тексту, що розглядаються як числа. Кожна буква в тексті множиться на деяке число (зване десятичним коефіцієнтом) і додається до деякого іншого числа (коефіцієнту зсуву):

$$C = (aP + \delta) mod A \qquad (3.1)$$

де a — десятичний коєфіцієнт; δ — коефіцієнт зсуву.

Отримане число зменшується за правилом віднімання модуля A, де A — розмір алфавіту, і зашифрований текст формується з відповідних йому алфавітних еквівалентів.

3.2. Адитивні методи

Як ключ в адитивних методах використовується деяка послідовність літер того ж алфавіта і такої ж довжини, що і в початковому тексті. Шифрування виконується шляхом складання символів вихідного тексту і ключа по модулю, рівному числу букв в алфавіті (так, якщо використовується двійковий алфавіт, то проводиться додавання по модулю два).

Прикладом такого ж методу є гамування - накладання на вихідний текст деякої послідовності кодів, званої гамою. Процес накладення здійснюється наступним чином:

- символи вихідного тексту і гамма представляються в двійковому коді і розташовуються один під іншим;
- кожна пара двійкових знаків замінюється одним двійковим знаком шифрованого тексту відповідно до прийнятого алгоритмом;
- отримана послідовність двійкових знаків тексту який шифрується замінюється символами алфавіту в відповідності з обраним кодом.

Якщо ключ шифрування вибирається випадковим чином, наприклад, формується за допомогою датчика псевдовипадкових чисел, то розкрити інформацію, не знаючи ключа, практично неможливо.

Однак на практиці довжина ключа обмежена можливостями комп'ютерної техніки та апаратури обміну даними, а саме виділяються обсягами пам'яті, часом обробки повідомлення, а також можливостями апаратури підготовки та запису кодів ключів.

3.3. Вибір метода перетворення

Більшість штучних мов (і всі природні мови) мають характерний частотний розподіл букв і інших знаків. Наприклад, Е – буква, яка найчастіше зустрічається в англійській мові, а цифра 2 - найбільш рідкісна. Це зовсім не говорить про те, що не будуть зустрічатися англійські (вихідні) повідомлення, в яких інша буква буде зустрічатися частіше, ніж Е, і рідше, ніж 2. Але для дуже великого числа повідомлень можуть бути встановлені певні характерні частоти. Більшість повідомлень, зашифровані методом перестановки або одноалфавітной підстановки, зберігають характерні частотні розподілення і, таким чином, дають криптоаналітику шлях до розкриття шифру.

Криптоаналітики часто використовують індекс відповідності (ІВ) для визначення того, чи знаходяться вони на правильному шляху. Теоретично очікуване значення ІВ для англійської мови визначається виразом

$$\frac{N-m}{m(N-1)}0{,}066 + 0{,}038\frac{N(m-1)}{m(N-1)}, \qquad (3.2)$$

де N — довжина повідомлення в буквах; m — число алфавітів.

Шифровки, які дають значення ІВ, більші, ніж 0,066 (для англійської мови), самі повідомляють про те, що, ймовірно, використовувалася одноалфавітна підстановка, даючи, таким чином, криптоаналітику чудовий інструмент для того, щоб приступити до розгадки шифру.

Якщо індекс відповідності знаходиться між 0,052 і 0,066, то, ймовірно, був використаний двохалфавітний шифр підстановки, якщо між 0,052 і 0,047 - трехалфавітний, і т. п. Криптоаналітик бере символ що зустрічається найчастіше і допускає, що це пропуск, потім бере наступний найбільш частий символ і припускає, що це «Е» і т. д. За допомогою

компьютера це робиться швидко й акуратно.

Справа ускладнюється, коли криптоаналітик стикається з рівномірним розподілом символів (ІВ = 0,038 для англійскої мови, 1/26 = 0,038, де 26 - число букв в англійському алфавіті), яке виходить при використанні багатоалфавітної пістановки.

Принципове значення для надійності шифрування має довжина коду ключа, відношення його довжини до довжини охопленого ним тексту. Чим більше воно наближається до одиниці, тим надійніше шифрування. При цьому слід мати на увазі, що це відношення поширюється не тільки на дане повідомлення, передане одноразово за призначенням, але й на всі інші повідомлення, закриті цим же кодом ключа. Це пояснюється тим, що ми не знаємо часу підключення порушника до лінії зв'язку і тому заздалегідь припускаємо найбільш небезпечний варіант, коли він підключений постійно. У цьому випадку при багаторазовому повторенні коду ключа по всій довжині тексту існує небезпека його розкриття статистичним методом. Імовірність цієї події залежить не тільки від зазначених вище відносини, а й від обраного методу шифрування.

Пояснимо це на простому прикладі цифрового тексту, закритого цифровим кодом ключа методом гамування.

1. Закрите багатозначне число 1001 1000 1011 1010 1101 1100 отримане щляхом порозрядного складання по модулю 2 числа $X_1X_2X_3X_4X_5X_6$ з однозначним числом К**,** шифрування числа $X_1X_2X_3X_4X_5X_6$ ключом К можна уявити у вигляді системи рівнянь:

$$X_1 \oplus K = 1001;$$
$$X_2 \oplus K = 1000;$$
$$X_3 \oplus K = 1011;$$
$$X_4 \oplus K = 1010;$$
$$X_5 \oplus K = 1101;$$
$$X_6 \oplus K = 1100;$$

2. Виходячи з умови, що Х приймає десяткові значення від 0 до 9, для

пошуку невідомого К визначимо всі відомі значення X_1 і К, сума яких по модулю 2 приводить до результату 1001.

3. Аналогічно визначимо К для чисел 1000, 1011, 1101 і 1100.

4. Аналізуючи отримані значення К для кожного з чисел і виключаючи значення більше 9, визначимо значення, яке присутнє в кожному з десятків результатів.

Це значення буде дорівнювати 1001, в десятковому численні 9. Відповіно, код ключа К = 9, а шукане число: 012345.

Наведений приклад говорить про слабку ефективність метода гамування при малій довжині коду ключа. Інші методи накладення в цьому відношенні також можуть бути слабкі, так як при цьому лише ускладнюється математичне рівняння системи з декількома невідомими і збільшується обсяг обчислень при їх вирішенні, що сучасній математиці і компют’ерній техніці не складає особливих труднощів.

Для підвищення ефективності шифрування застосовуються «довгий» ключ; «подвійний» ключ, де два ключа додавалися по модулю два до вихідного тексту; шифрування псевдовипадковим ключем, де ключ так змінюється з кожним словом, як це забезпечувалося генератором псевдовипадкових чисел.

Цікавим і ефективним способом є застосування рівняння-генератора псевдовипадкових чисел.

Сучасні досягнення математики дозволяють за допомогою рівняння-генератора псевдовипадкових чисел отримати шифр з «нескінченним» ключовим словом, при відносно малій довжині самого ключа. Реалізація цього методу полягає в тому, що в обчислювальну систему закладається спеціальний алгоритм, який при одержанні коду ключа створює за певним законом (рівняння) з кожним тактом нове псевдовипадкове число, ланцюг з яких накладається на текст, що закритий, і таким чином з «короткого» ключа виходить «довгий» і жорстко пов'язаний з ним другий ключ.

Для нас важливо, щоб генератори псевдовипадкових чисел були

відтворюваними, хоча в той же час вони повинні створювати числа, які «здаються випадковими». На основі теорії груп було розроблено декілька типів таких генераторів. В даний час найбільш доступними є конгруєнтні генератори. На основі їх суворого визначення можна зробити математично коректний висновок про те, якими властивостями повинні володіти вихідні сигнали цих генераторів з урахуванням періодичності та випадковості.

Одним з хороших конгруентних генераторів є лінійний конгруентний генератор псевдовипадкових чисел. Цей генератор виробляє послідовність псевдовипадкових чисел T1, T2, T3, ..., Tm, ..., где T_i, — вихідна величина, вибрана в якості породжуючого числа; a і c — константи.

Зазначене рівняння генерує псевдовипадкові числа з певним періодом повторення, що залежать від вибраних значень a і c. Значення m зазвичай встановлюється рівним 2b-1 або 2Ь, де b - довжина слова комп'ютера в бітах.

Ефективним методом шифрування є комбінований метод. Комбінація основних методів шифрування - перестановки і підстановки - дає в результаті складне перетворення, зване похідним шифром. Цей шифр володіє більш сильними криптографічними можливостями, ніж окрема перестановка і підстановка. Цей метод використовується у федеральному стандарті NBS США, званому також стандартом DES, і вітчизняному стандарті ГОСТ 28147-89, введеному в дію з липня 1990

Стандарт DES побудований на комбінованому використанні перестановки, заміни та гамування, причому кожен блок даних що шифруються довжиною 32 біта послідовно піддається 15-кратному перетворенню, а в якості ключа, який служить для генерування послідовності знаків випадкової гами, використовується послідовність в 56 біт. Такий ключ дає 1016 різних комбінацій гами.

Алгоритм DES знайшов широке застосування в багатьох сферах ділового життя з наступних причин:

1) до теперішнього часу ніхто не вказав яку-небудь фундаментальну

слабкість алгоритму;

2) він затверджений в якості національного стандарту. Крім того, уряд встановив програми перевірки і огляду, що гарантують відповідність стандарту. Таким чином, DES став найбільш широко визнаним механізмом криптографічного захисту несекретних даних для масового застосування;

3) різні варіанти його виконання (програмний, мікропрограмний і апаратний) дозволяють задовольнити потреби різноманітних користувачів як за швидкісними показниками, так і економічним. Найбільш широко DES використовується при зберіганні і передачі даних між різними системами обробки інформації; в поштових системах, в електронних системах креслень і при електронному обміні комерційною інформацією за допомогою алгоритму DES можна зашифровувати файли комп'ютера для їх зберігання.

Сам процес криптографічного закриття даних може здійснюватися як програмно, так і апаратно, проте апаратна реалізація володіє в порівнянні з програмною рядом переваг:

– висока продуктивність;

– спрощена організація обробки інформації і т. п.

У багатьох країнах налагоджено промислове виробництво аппаратури для шифрування.

Фахівцями сформована наступна система вимог до алгоритма шифрування:

1) зашифрований текст повинен піддаватися читання тільки при наявності ключа шифрування;

2) число операцій, необхідних для визначення використаного ключа шифрування за фрагментом шифрованого тексту і відповідного йому відкритого тексту, має бути не менше загального числа можливих ключів;

3) знання алгоритму шифрування не повинно впливати на надійність захисту;

4) незначні зміни ключа шифрування повинні призводити до істотної

зміни виду зашифрованого тексту;

5) незначні зміни тексту що шифрується повинні призводити до істотної зміни виду зашифрованого тексту навіть при використанні одного і того ж ключа;

6) структурні елементи алгоритму шифрування повинні бути незмінними;

7) у процесі шифрування повинен здійснюватися постійний контроль даних що шифруються і ключю шифрування;

8) додаткові біти, що вводяться в текст в процесі шифрування, повинні бути повністю та надійно сховані в зашифрованому тексті;

9) довжина шифрованого тексту повинна бути рівною довжині вихідного відкритого тексту;

10) не повинно бути простих і легко встановлюваних залежностей між ключами, які послідовно використовуються в процесі шифрування;

11) будь-який ключ з безлічі можливих повинен забезпечувати надійний захист інформації;

12) алгоритм повинен допускати як програмну, так і апаратну реалізацію; при цьому зміна довжини ключа не повинно вести до погіршення характеристик алгоритму.[12]

Останнім досягненням криптографії стала система з відкритим ключем.

У криптографії з відкритим ключем передбачено два ключі, кожен з яких неможливо обчислити з іншого. Один ключ (відкритий) використовується відправником для шифрування інформації, іншим (закритим) - одержувач розшифровує отриманий шифротекст.

Криптографічні системи з відкритим ключем використовують незворотні або односторонні функції, які володіють такими властивостями: при заданому значень X відносно просто визначити значення $f(x)$ однак якщо $y = f(x)$, то немає простого шляху для визначення X. Іншими словами, надзвичайно важко розрахувати значення зворотної функції

$f^{-1}(y)$.

Дослідження необоротних функцій проводилося в основному за трьома напрямками:

1) дискретне зведення в ступінь;

2) множення простих чисел;

3) комбінаторні завдання, зокрема завдання про укладання ранця.

Діффі і Хеллмана досліджували функцію дискретного піднесення до ступеня, в результаті цього отримали новий алгоритм криптографічного закриття інформації, що дозволяє застосовувати два ключі: відкритий для шифрування, закритий для розшифрування інформації. Система відкритого ключа дозволила вирішити проблему розсилки ключів користувачам при одночасному виконанні вимог по стійкості захисту.

Р. Л. Рівестом, А. Щаміром и Л. Адельманом запропонований метод з ключем загального користування для більш високого ступеня захисту, заснований на застосуванні незворотної функції з потайним ходом, яка визначається як сімейство оборотніх функцій.

Криптографія з відкритим ключем найбільш ефективна при шифруванні переданих даних, а не даних, що зберігаються в пристрої.

На закінчення слід відзначити, що в результаті проведених досліджень з перевірки надійності алгоритму DES Національне агентство з безпеки США з 1 січня припинило підтримку цього стандарту. Бурхливий розвиток криптографії з ключем загального користування дозволяє сподіватися на суттєве спрощення програмно-апаратної реалі¬зації пристроїв шифрування, які базуються на принципах відкритого ключа.

Висновки до розділу 3

В даному розділі розглянуто основні методи шифрування даних, представлено алгоритми роботи деяких із них, виділено особливості їх роботи та позитивні і негативні якості.

4 ГЕНЕРАТОРИ ХАОСУ НА ОСНОВІ ДИНАМІЧНИХ СИСТЕМ

Теорія хаосу – незвичайна і молода наука, що описує поведінку нелінійних динамічних систем. У процесі свого зародження теорія хаосу просто перевернула сучасну науку! Вона розбурхувала уми вчених і змушувала їх все більше і більше занурюватися в дослідження хаосу і його властивостей. На відміну від шуму, який є випадковим процесом, хаос – детермінований. Тобто для хаоса існує закон зміни величин, що входять в рівняння опису хаотичного процесу. Здавалося б, при такому визначенні хаос нічим не відрізняється від будь-яких інших коливань, описуваних у вигляді функції. Але це не так. Хаотичні системи дуже чутливі до початкових умов, і найменші їх зміни можуть привести до колосальних відмінностей. Ці відмінності можуть бути настільки сильними, що неможливо буде сказати, одна або кілька систем піддавалися дослідженню. З науково-популярних джерел найкраще це властивість хаосу описує процес під назвою "Ефект метелика". Багато хто чув про нього, і навіть читали книги і дивилися фільми, в яких використовувався прийом з використанням ефекту метелика. По суті, Ефект метелика відображає головну властивість Хаосу.

Американський вчений Едвард Лоренц, один з першопрохідців в області Хаосу, сказав одного разу: «Метелик, що змахує крилами в Айові, може викликати лавину ефектів, які можуть досягти найвищої точки в дощовий сезон в Індонезії».

Динамічна система – це деяка безліч елементів, для якого задана

функціональна залежність між часовою координатою і положенням у фазовому просторі кожного елемента системи. Простіше кажучи, динамічна система – це така система, у якій стан в просторі змінюється з плином часу.

Багато фізичних процесів в природі описуються системами рівнянь, що представляють собою динамічні системи. Наприклад, це процеси горіння, течії рідини і газів, поведінка магнітних полів і електричних коливань, хімічні реакції, метеорологічні явища, зміна популяцій у рослин і тварин, турбулентності в морських течіях, рух планет і навіть галактик.

Фазовий портрет – це координатна площина, в якій кожна точка відповідає стану динамічної системи в певний момент часу. Іншими словами, це просторова модель системи (може бути двовимірної, тривимірної і навіть чотиривимірної і більше).

Атрактор – деяка множина фазового простору динамічної системи, для якого всі траєкторії з плином часу притягуються до цієї множини. Якщо зовсім простою мовою, то це деяка область, в якій зосереджено поведінку системи в просторі. Багато хаотичні процеси являють собою атрактори, тому що зосереджені в певній області простору.

4.1. Атрактор Лоренца

Атрактор Лоренца – це, мабуть, найвідоміша динамічна система в теорії хаосу. Вже кілька десятків років він привертає велику увагу багатьох дослідників для опису тих чи інших фізичних процесів. Перша згадка атрактора наводиться в 1963 році в роботах Е.Лоренца, який займався моделюванням атмосферних явищ. Атрактор Лоренца – це тривимірна динамічна система нелінійних автономних диференціальних рівнянь першого порядку. Вона має складну топологічну структуру, асимптотично стійка і стійка по Ляпунову. Атрактор Лоренца описується наступною

системою диференціальних рівнянь:

$$\begin{cases} \dot{x} = \sigma - (y - x) \\ \dot{y} = x(r - z) - y \\ \dot{z} = xy - bz \end{cases} \quad (4.1)$$

У формулі точка над параметром означає взяття похідної, яка відображає швидкість зміни величини за часом (фізичний сенс похідної)[13].

При значеннях параметрів σ = 10, r = 28 і b = 8/3 ця проста динамічна система була отримана Е.Лоренцом. Він довго не міг зрозуміти, що відбувається з його обчислювальною машиною, поки нарешті не усвідомив, що система проявляє хаотичні властивості! Вона була отримана в ході експериментів для завдання про моделювання конвекції рідини. Крім того, ця динамічна система описує поведінку наступних фізичних процесів:

– модель одномодового лазера,
– конвекція в замкнутій петлі і плоскому шарі,
– обертання водяного колеса,
– гармонійний осцилятор з інерційною нелінійністю,
– завихрення хмарних мас і т. д.

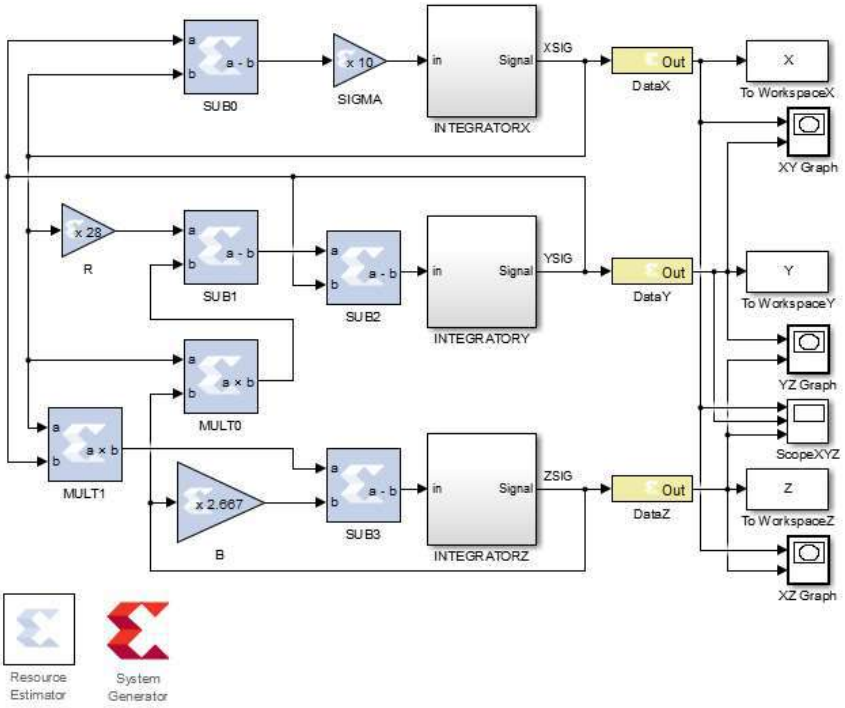

Рисунок 4.1 - система Атрактор Лоренца в середовищі MATLAB

На малюнку використовується ряд наступних позначень:

- вичитачі: SUB 0-3;
- помножувачі на константу: SIGMA, B, R;
- перемножувачі: MULT0-1;
- інтегратори з коміркою завдання початкової умови: INTEGRATOR X, Y, Z;
- вихідні порти OUT: DATA X, Y, Z для сигналів X SIN, Y SIG, SIG;
- Крім того, на схемі представлені допоміжні інструменти аналізу, це:
- збереження результатів обчислення в файл: To Workspace X, Y, Z;
- побудова просторових графіків: Graph XY, YZ, XZ;
- побудова часових графіків: Scope XYZ;
- засоби для оцінки займаних ресурсів кристала і генерації HDL-коду з моделі «Resource Estimator» і «System Generator».

Усередині кожного вузла математичних операцій необхідно вказати розрядність проміжних даних і їх тип. Встановивши в інтеграторах X, Y, Z

в блоці тригера початкове значення системи, наприклад, {10, 0, 0}, можна запустити модель. У тимчасовій розгортці можна спостерігати три наступних сигнали:

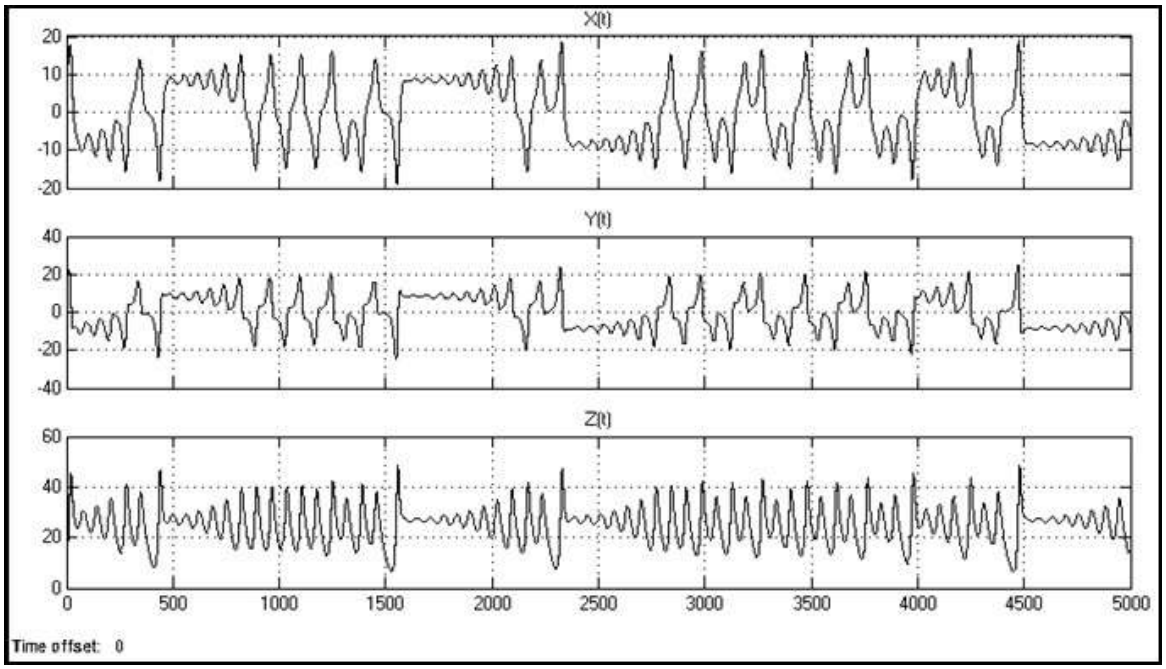

Рисунок 4.2 – Три типи сигналу у тимчасовій розгортці

Навіть якщо час моделювання спрямувати до нескінченності, то реалізація в часі ніколи не повториться. Хаотичні процеси неперіодичні.

У тривимірному просторі атрактор Лоренца виглядає наступним чином:

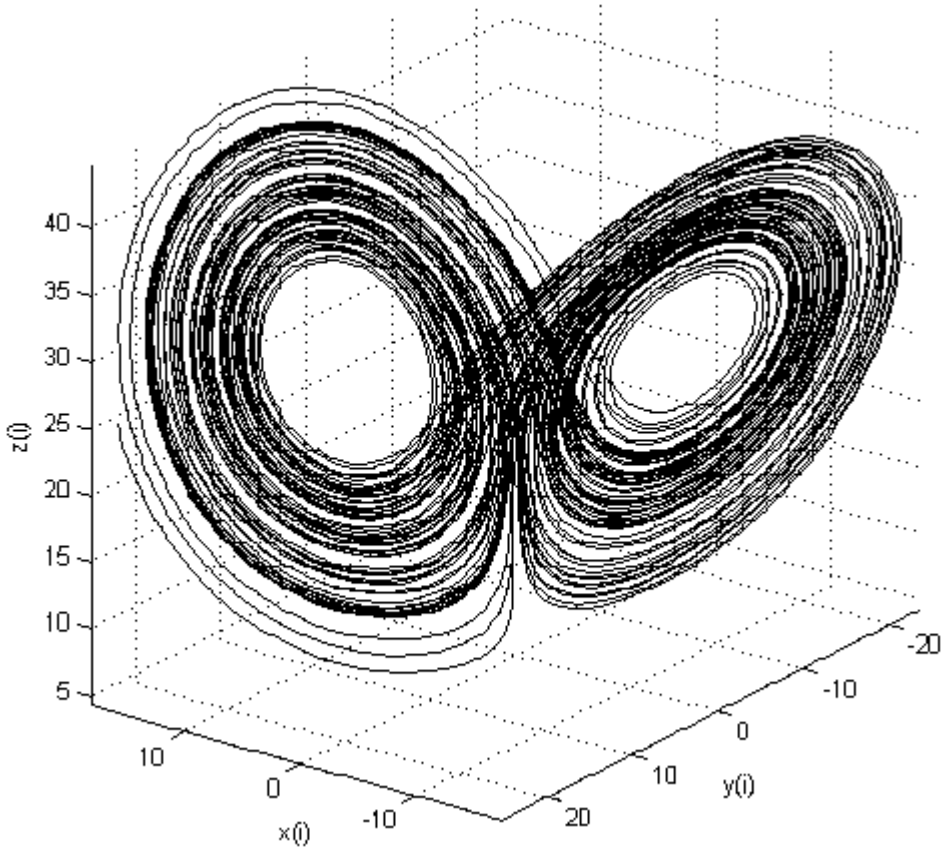

Рисунок 4.3 – Атрактор Лоренца у тривимірному просторі

Видно, що атрактор має дві точки тяжіння, навколо яких відбувається весь процес. При незначній зміні початкових умов процес також буде зосереджений навколо цих точок, але його траєкторії будуть істотно відрізнятися від попереднього варіанту.

4.2. Атрактор Реслера

Для атрактора Ресслера характерна наявність граничної точки прояву хаотичних або періодичних властивостей. При певних параметрах динамічної системи коливання перестають бути періодичними, і виникають хаотичні коливання. Одне з примітних властивостей атрактора Ресслера –

фрактальна структура в фазовій площині, тобто явище самоподібності. Можна помітити, що і інші атрактори, як правило, мають цю властивість[14].

Атрактор Ресслера спостерігається в багатьох системах. Наприклад, він застосовується для опису потоків рідини, а також для опису поведінки різних хімічних реакцій і молекулярних процесів. Система Ресслера описується наступними диференціальними рівняннями:

$$\begin{cases} \dot{x} = -y - z \\ \dot{y} = x + ay \\ \dot{z} = b + z(x - c) \end{cases} \tag{4.2}$$

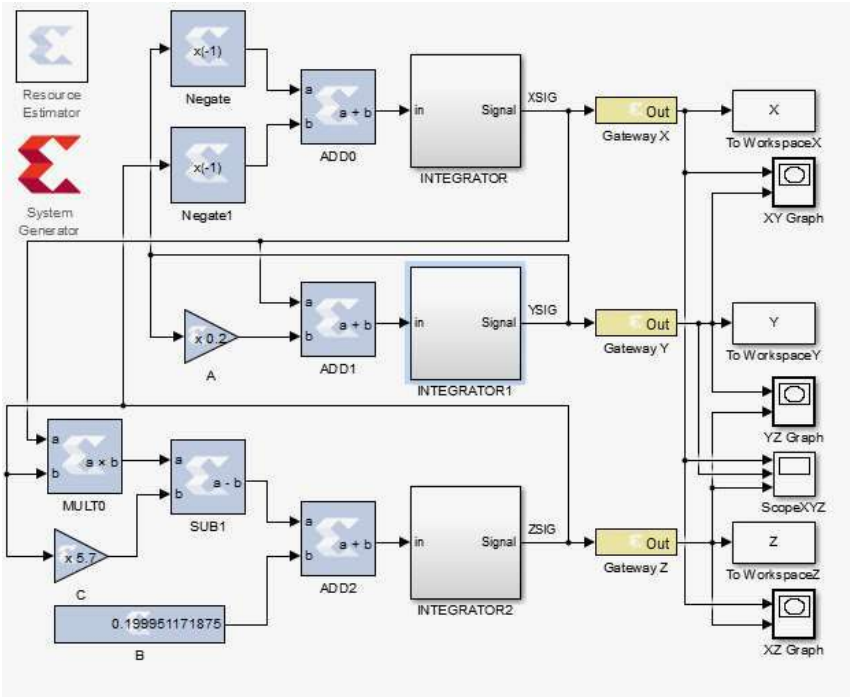

Рисунок 4.4 – система Атрактор Реслера у середовищі MATLAB

Часова реалізація просторових величин:

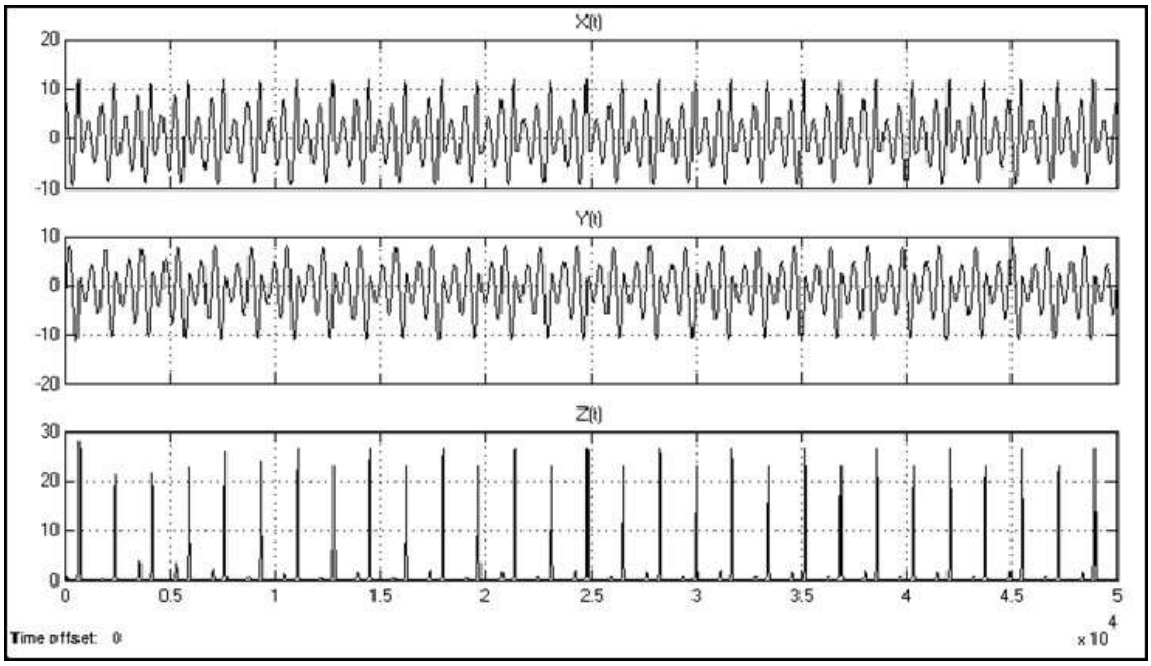

Рисунок 4.5 – Часова реалізація просторових величин

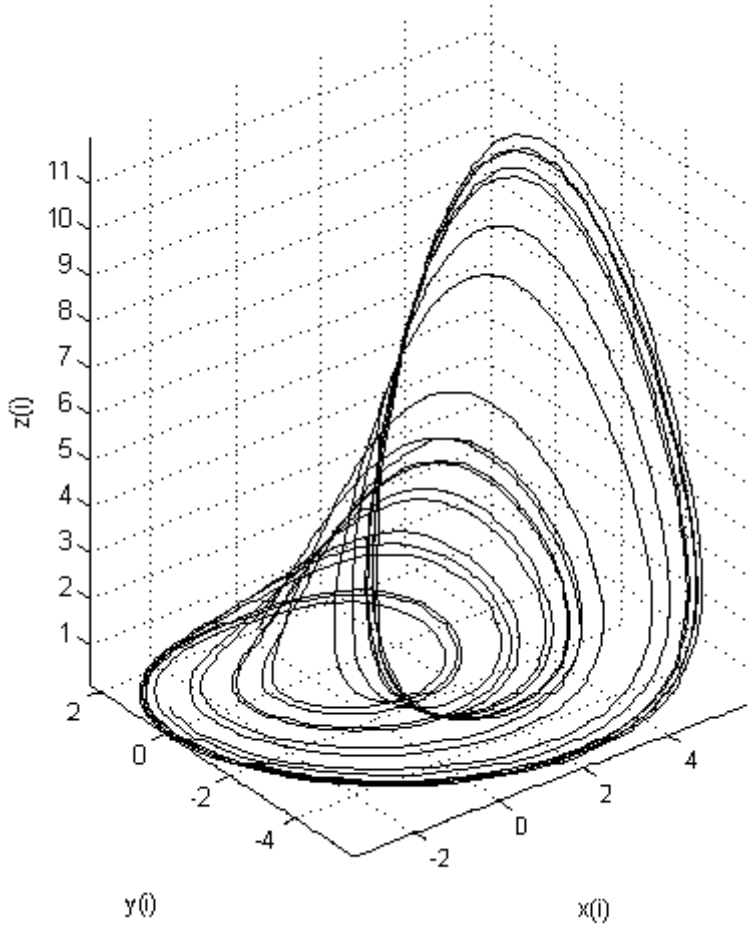

Рисунок 4.6 – Тривимірна модель атрактора Реслера

Перелічені атрактори знаходять застосування в багатьох фізичних процесах в різних областях науки і техніки – від фізики і хімії до механіки і метеорології. Зокрема, генератори Хаосу використовуються для створення довгих послідовностей псевдовипадкових чисел (ПВП). У задачах радіотехніки хаос може застосовуватися для моделювання несучої при створенні надширокосмугових сигналів цифровими методами (на ПЛІС або процесорах).

Висновки до розділу 4

В даному розділі розглянуто тему генераторів хаосу динамічних систем. Також розглядається тема атрактора на прикладі двой найбільш відомих атракторів – Лоренца та Реслера. Побудовані їх системи та проаналізовані особливості роботи.

5 АЛГОРИТМ ШИФРУВАННЯ СИГНАЛІВ

5.1. Постановка задачі

Проблема конфіденційності передачі інформації та більш широка проблема захисту інформації стають все більш актуальними на ринку цивільних застосувань сфери комунікаційних технологій. Прикладами можуть служити захист комерційної інформації в комп'ютерах та інформаційних мережах, безпека електронних платежів, захист від копіювання музичної, відео та іншої інформації, поширюваної по інформаційних мережах, інтернет-телефонія та ін. Типовою вимогою для схем шифрування стає можливість масового застосування та низька собівартість на одиницю "інформаційної" продукції. При вирішенні таких проблем захисту інформації можуть успішно застосовуватися засоби, які засновані на детермінованому хаосі, що породжується нелінійними динамічними системами.

Динамічні системи, що володіють хаотичною поведінкою, в даний час інтенсивно використовуються і застосовуються в різних областях, зокрема для криптографічного захисту інформації. На основі таких систем можуть будуватися генератори псевдовипадкових послідовностей, які надалі використовуються для гамування відкритого тексту. З іншого боку всяка динамічна система, що має структуру вхід-вихід, може використовуватися безпосередньо для перетворення інформації. На основі таких систем створюється шифратор. Входом в систему служить оцифроване повідомлення, а виходом є зашифрований сигнал, спрямований в інформаційні мережі. Необхідною умовою для однозначної дешифрування є існування зворотньої системи.

5.2. Опис алгоритму

Будь-яка інформація, що обробляється різними дискретними обчислювачами, в кінцевому результаті може бути представлена послідовністю бітів (0 або 1). Це подання, власне, і використовується при її перетворенні за допомогою різних динамічних хаотичних систем. Проте в ЕОМ для представлення різних типів даних використовуються більші одиниці – байти (8 біт), машинні слова зазвичай залежно від розрядності машини – від 16 до 64. Найчастіше використовується побайтове подання інформації. Так, кодові таблиці в ЕОМ для подання текстової інформації вказують відповідність між 256 байтами і символами різних алфавітів.

Оперування побайтно представленою інформацією у багатьох випадках спрощує і алгоритми її обробки на ЕОМ. Тому будемо вважати далі одиницею інформації байт, а інформацію, оброблювану в комп'ютерному середовищі, представляти як послідовність різних байтів.

В якості способу шифрування інформації виберемо спосіб її безпосереднього перетворення за допомогою динамічної хаотичної системи, що використовує пряму і зворотну системи.

Алгоритм шифрування, який використовується в даній роботі, заснований на використанні дискретного аналогу динамічної хаотичної системи Лоренца [7].

Кінцевий автомат Лоренца описується системою рівнянь:

$$\begin{cases} x_1(t+1) = x_1(t) + hA_1(x_2(t) - x_1(t)) \\ x_2(t+1) = x_2(t) + h(A_2 x_1(t) - x_2(t) - x_1(t)x_3(t) + Au(t)) \\ x_3(t+1) = x_3(t) + h(x_1(t)x_2(t) - A_3 x_3(t)) \end{cases} \tag{5.1}$$

$$y(t) = x_2(t) + h(A_2 x_1(t) - x_2(t) - x_1(t)x_3(t) + Au(t))$$

Тут адитивна складова – поточний вхідний символ вихідної інформації $u(t)$, $y(t)$ – відповідний символ зашифрованої інформації. Множини

вхідних і вихідних символів, компоненти $x_i(t), i = 1,2,3$ розуміються як елементи кінцевого поля $GF(q)$ або кільця $Z(q)$, а операції додавання і множення є відповідні операції в цьому полі, або кільці.

Для цифрової обробки інформації застосовуються, як правило, поля або кільця характеристики 2, тобто q=2n, n∈N. З огляду на особливості подання інформації в пам'яті комп'ютера, в програмі використовуються поля $GF(2^{8k})$, або кільця $Z(2^{8k})$, k=1,2,3,4. Це пов'язано з тим, що інформаційний файл зберігається в пам'яті комп'ютера як послідовність байтів. Існує кілька типів подання елементів поля Галуа. В програмі використано два з них: цілочисельне представлення і векторне. Неявно при розробці алгоритмів обчислення в полях використовується також поліноміальне подання.

Розшифровка здійснюється зворотнім автоматом Лоренца, що існує для будь-якого $A \in GF(q)$ або $A \in Z(q)$, A $\neq 0$.

Ключем системи шифрування є коефіцієнти системи (5.1), і початковий стан автомата. Перепишемо систему рівнянь Лоренца наступним чином:

$$\begin{cases} \dot{S}_1 = a_{11}S_1 + a_{12}S_2 \\ \dot{S}_2 = a_{21}S_1 + a_{22}S_2 + a_{23}S_1S_3 + a_{24}u \\ \dot{S}_3 = a_{31}S_3 + a_{32}S_1S_2 \end{cases}$$
$$y = \dot{S}_2$$

Коефіцієнти автомата Лоренца $(a_{11}, a_{12}, a_{21}, a_{22}, a_{23}, a_{24}, a_{31}, a_{32})$, а також вхідні стани S_1, S_2, S_3 є ключем системи шифрування. При необхідності ключовим параметром може бути також величина k, яка задає розмір оброблюваного блока інформації (квант інформації) в k байт.

Основні етапи алгоритму шифрування наступні:

1) ініціалізація (настройка) автомата – задаються його коефіцієнти і вхідний стан по ключу шифрування і розмір кванта;
2) обробка чергового кванта інформації відповідно до системи (5.1), яка знаходиться в поточному стані, з видачею зашифрованого кванта і переходом в новий стан. Цей крок повторюється до кінця файлу, що обробляється.

При реалізації перерахунку значень станів S_i автомата обчислення відбуваються в полі $GF(2^p)$ або кільці $Z(2^p)$.

Алгоритм складання простий, так як використовуються тільки поля и кільця характеристики 2. Алгоритм додавання використовує цілочисельне подання елементів поля або кільця. Алгоритм ділення здійснюється по наступній формулі: $\frac{a}{b} = a * b^{-1}$. Обчислення зворотного елементу b-1 здійснюється по наступній формулі: $b^{-1} = 2^p - b + 1$, де b представлено в цілочисельному вигляді. При виконанні цієї операції попередньо відбувається перехід із векторного подання до цілочисельного, а потім назад. Зважаючи на те, що операція взяття зворотного елементу здійснюється в програмі один раз при обчисленні коефіцієнтів оберненого автомата, такий метод обчислення оберненого елементу допустимо.

Система шифрування автоматом Лоренца є симетричною. Це означає, що при розшифровуванні файлу використовується той же ключ, що і при шифруванні. Зворотний автомат Лоренца визначається системою:

$$\begin{cases} S_1^{`} = a_{11}S_1 + a_{12}S_2 \\ S_2^{`} = a_{21}^{back}S_1 + a_{22}^{bsck}S_2 + a_{23}^{back}S_1S_3 + a_{24}^{back}y \\ S_3^{`} = a_{31}S_3 + a_{32}S_1S_2 \end{cases}, \qquad (5.2)$$

$$u = S_2^{`}$$

де $a_{21}^{back} = \frac{-a_{21}}{a_{24}}$, $a_{22}^{back} = \frac{-a_{22}}{a_{24}}$, $a_{23}^{back} = \frac{-a_{23}}{a_{24}}$, $a_{24}^{back} = \frac{1}{a_{24}}$.

Перерахунок коефіцієнтів зворотного автомата відбувається під час настройки системи для розшифрування файлу.

У результаті роботи шифратора виходом буде деяка послідовність, яка повинна мати властивості псевдовипадкової.

Для дослідження ПВП є дві групи тестів.

Графічні тести. Статистичні властивості послідовностей відображаються у вигляді графічних залежностей, з вигляду яких роблять висновки про властивості досліджуваної послідовності.

Оціночні тести. Статистичні властивості послідовностей визначаються числовими характеристиками. На основі оціночних критеріїв робляться висновки про ступінь близькості властивостей аналізованої і істинно випадкової послідовностей. Для оцінки ПВП, що генеруються за допомогою системи Лоренца використовувався пакет статистичних тестів NIST .

Для візуалізації вхідної, а також вихідної двійкової послідовності вона ділиться на 560 рівних частин і потім записується як рядки деякої матриці. Зображення такої матриці будується за наступним правилом: чорним квадратиком відображається елемент, рівний нулю, і відповідно білим квадратиком – елемент, рівний одиниці. Наступні малюнки (рис. 5.1) відповідають послідовності складається з одиниць, послідовності, яка має якийсь періодичний характер, випадкової послідовності.

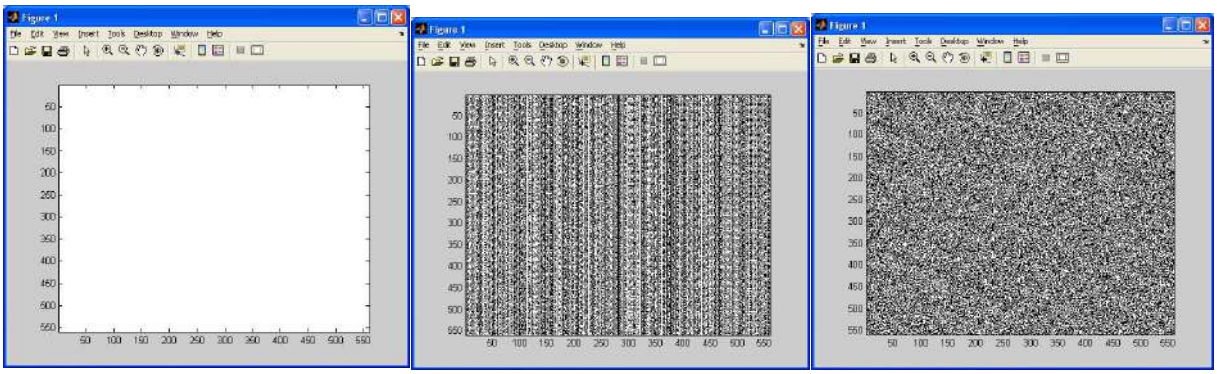

Рисунок 5.1 - Візуалізація послідовностей.

Для шифрування будемо використовувати систему Лоренца (5.1) в кінцевих кільцях $Z(2^p)$ та полях $GF(2^p)$ $8 \le p \le 128$.

Тест 1. Аналіз алгоритмів за допомогою графічної візуалізації. Для даного тесту використовувалися 10 вхідних різних послідовностей довжини 320 000. Кожна послідовність шифрувалася кожним алгоритмом 20 разів з різними, довільно вибраними параметрами. У результаті роботи тестів отримані наступні висновки:

– При шифруванні в кільці $Z(2^8)$ за допомогою системи Лоренца, ні в одному випадку не спостерігається однорідної картинки.
– При яскраво виражених областях у вихідному файлі залишаються їх контури у вихідному файлі.

Приклад 1. Шифрування за допомогою системи Лоренца в кільці $Z(2^8)$.

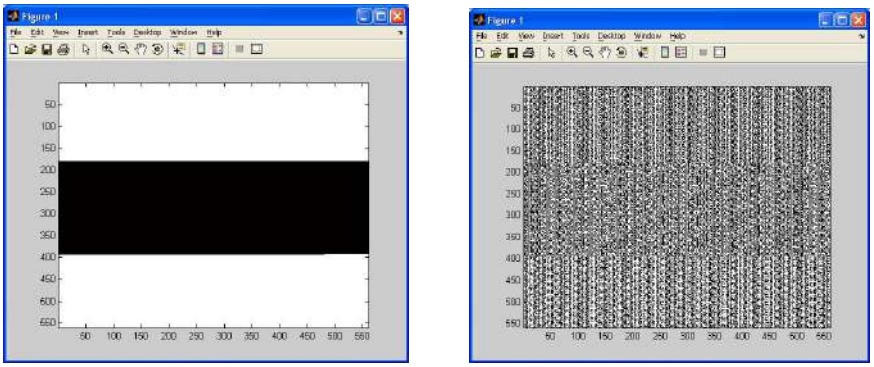

Рисунок 5.2 - Приклад шифрування системи Лоренца в кільці $Z(2^8)$.

– При збільшенні потужності кільця "розмитість" поліпшується.
– При додаванні нелінійності в перше рівняння системи Лоренца картинка трохи поліпшується.
– У полях $GF(2^8)$, $GF(2^{16})$ модифікована система Лоренца має однорідну розмиту картинку.

Тест 2. Використання пакету статистичних тестів NIST для оцінки якості роботи генераторів ПВП. У цьому тесті послідовність з одиниць

довжиною 100000 шифрується 125 разів. Кожен параметр перебирається з кроком $2^p/5$ і беруться всі можливі їх комбінації. Таким чином виходить 125 послідовностей. До них застосовується батарея тестів NIST.

Тести NIST показують, що при шифруванні системою Лоренца в кільці Z_8 виходить незадовільний результат. Зі збільшенням потужності кільця результат поліпшується і час роботи тестів зменшується. При додаванні в систему предиката спостерігається невелике поліпшення результату. Виконанні всіх операцій у полях $GF(2^p)$результати помітно поліпшуються.

Висновки. Будь-яка керована динамічна система, що має структуру вхід-вихід, може використовуватися безпосередньо для перетворення інформації. Ідея використання оборотних систем управління зі складною поведінкою траєкторій лежить в основі завдання синтезу нових ефективних алгоритмів захисту інформації, в першу чергу від несанкціонованого доступу.

Проведені дослідження та їх оцінка дозволяють говорити, що отримані нові результати, що розширюють теоретичну базу сучасної криптології і які є перспективними для створення ефективних криптографічних алгоритмів. У той же час відкритими залишається ряд питань, пов'язаних з впливом динамічних параметрів на стійкість криптоалгоритмів до атак, стійкість до спотворень інформації, появі інваріантних багатовидів.

5.3. Програмна реалізація алгоритму

Реалізацію алгоритму виконано на мові C++ . Основними складовими програми є:

- введення змінних та даних;
- виведення вікна з вхідними даними;
- шифрування данних та виведення вікна з результатом

шифрування;

– дешифрування та виведення на екран результату дешифрування.

В даній реалізації текст, що необхідно зашифрувати, вводиться безпосередньо під час створення даних типу char у коді програми.

Введений текст: «A dynamical system is a concept in mathematics where a fixed rule describes how a point in a geometrical space depends on time. Examples include the mathematical models that describe the swinging of a clock pendulum, the flow of water in a pipe, and the number of fish each springtime in a lake. Состояние динамической системы в любой момент времени описывается множеством вещественных чисел (или векторов), соответствующим определённой точке в пространстве состояний.»

Для представлення операцій, що відбуваються з текстом, буде виводись вікно завдяки команді MessageBox. Під час першого виведення на екран робочого вікна, користувачу буде представлено введений ним текст на двох мовах. Після натискання кнопки Ок, з'явиться нове вікно, у якому буде наведено зашифрований текст відповідно до заданного у програмі алгоритму. Після повторного натискання кнопки Ок, з'явится новее вікно, де буде наведено дешифрований текст, також на двух мовах.

При виконанні побудови рішення (компіляції), викликається консоль, у якій користувачеві будуть показані введені параметри шифрування. Наприклад, в данному випадку були використані такі параметри:

A1=9, A2=99, A3=114; x10=116, x20=47 ,x30=38.

Також обчислюється кількість введених у рядок символів за допомогою команди strlen та виводиться на екран консолі. Завершується робота програми натисканням будь-якої клавіші клавіатури користувача

Результат роботи програми для шифрування та дешифрування тексту:

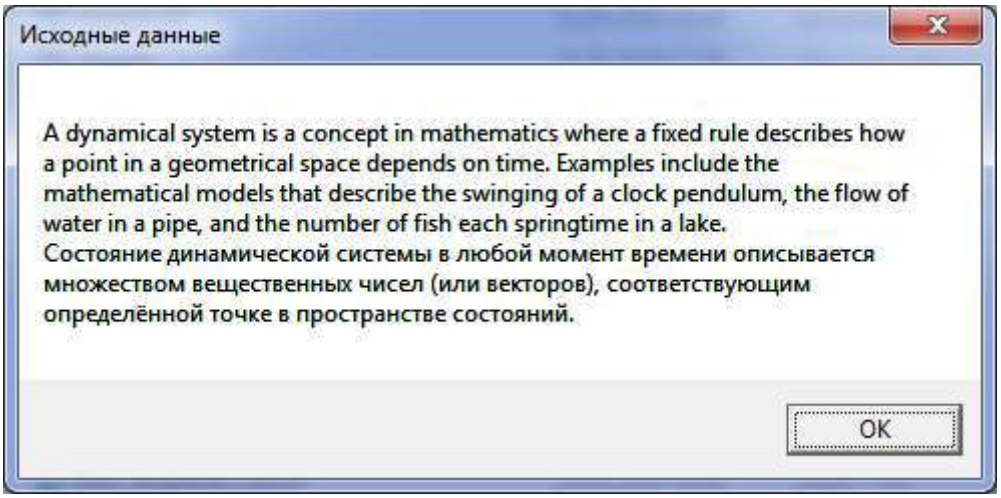

Рисунок 5.3 – Вікно с початковими даними

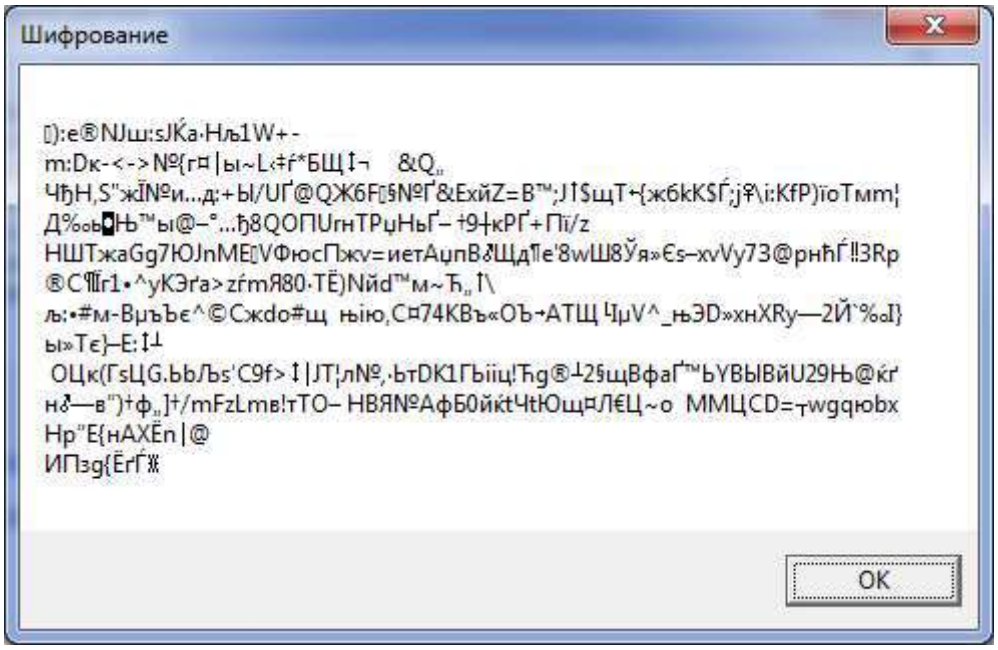

Рисунок 5.4 – Вікно з зашифрованим текстом

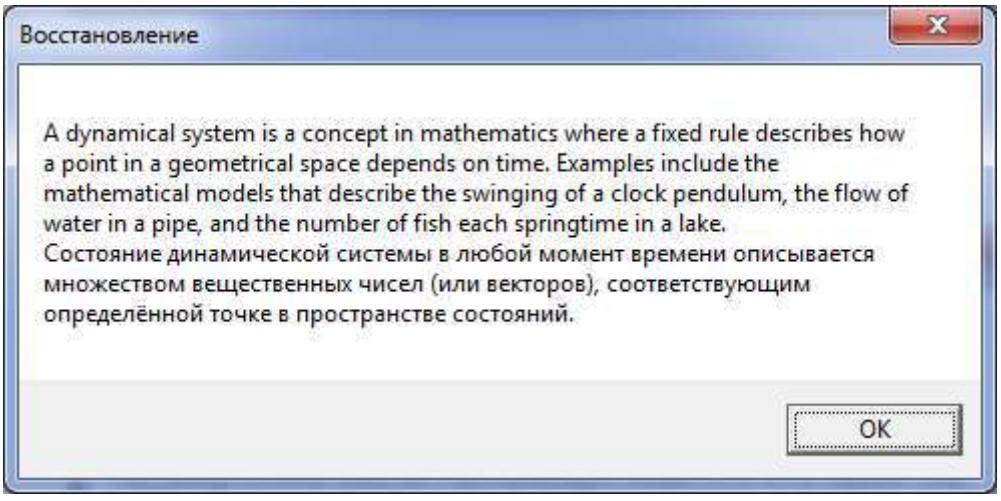

Рисунок 5.5 – Вікно з дешифрованим текстом

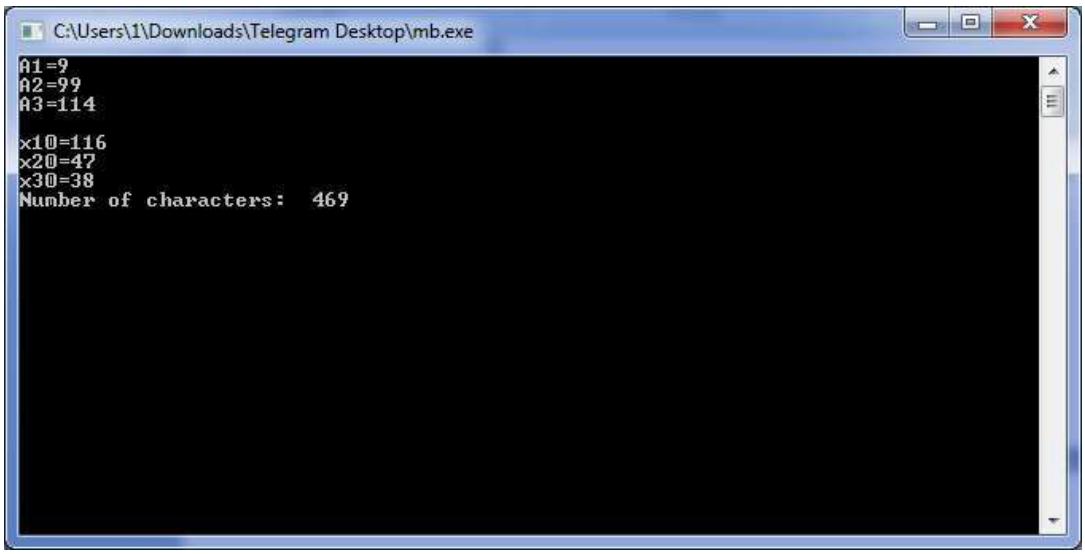

Рисунок 5.6 – Вікно консолі

Лістинг програми для шифрування та дешифрування тексту

```
#include <windows.h>
#include<iostream>
using namespace std;

int mod(int a, int b)
{
    int c;
    c=a%b;
    if (c<0){c=c+b;}
    return c;
}


int main()

//  FreeConsole();

{
    int A1=9,
        A2=99,
        A3=114;

    int x10=116,
        x20=47,
        x30=38;

    int x1,x2,x3;

cout<< "A1="<<A1<<endl<<"A2="<<A2<<endl<<"A3="<<A3<<endl<<endl;
cout<< "x10="<<x10<<endl<<"x20="<<x20<<endl<<"x30="<<x30<<endl;

      char Vs[]="A dynamical system is a concept in mathematics where a fixed rule describes
how a point in a geometrical space depends on time. Examples include the mathematical models
that describe the swinging of a clock pendulum, the flow of water in a pipe, and the number
of fish each springtime in a lake. \nСостояние динамической системы в любой момент времени
```

```
описывается множеством вещественных чисел (или векторов), соответствующим определённой точке
в пространстве состояний.";
      int s=strlen(Vs);
      cout<<"Number of characters:  "<<s<<endl;

MessageBox(0, Vs, "Исходные данные", MB_OK);



//---------------------- шифрование
     for(int i=0; i<=s; i++)
     {
            x1 = x10 + A1 * (x20 - x30);
            x2 = x20 + x10 - A2*x20 - x10 * x30 + Vs[i];
            x3 = x30 + x10 * x20 - A3 * x30;

            x10=mod(x1, 256);
            x20=mod(x2, 256); Vs[i]=x20;
            x30=mod(x3, 256);

        }
//----------------------

MessageBox(0, Vs, "Шифрование", MB_OK);

//---------------------- дешифрование

A1=9;
A2=99;
A3=114;

x10=116;
x20=47;
x30=38;


     for(int i=0; i<=s; i++)
     {
            x1 = x10 + A1 * (x20 - x30);
            x2 = Vs[i] - x20 - x10 + A2*x20 + x10 * x30;
            x3 = x30 + x10 * x20 - A3 * x30;

            x10=mod(x1, 256);
            x20=Vs[i]; Vs[i]=mod(x2, 256);
            x30=mod(x3, 256);

        }
//----------------------

MessageBox(0, Vs, "Восстановление", MB_OK);


    return 0;
}
```

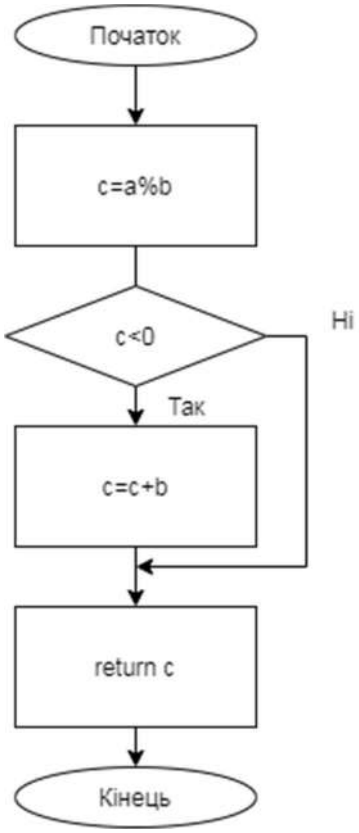

Рисунок 5.7 – Блок схема функції mod

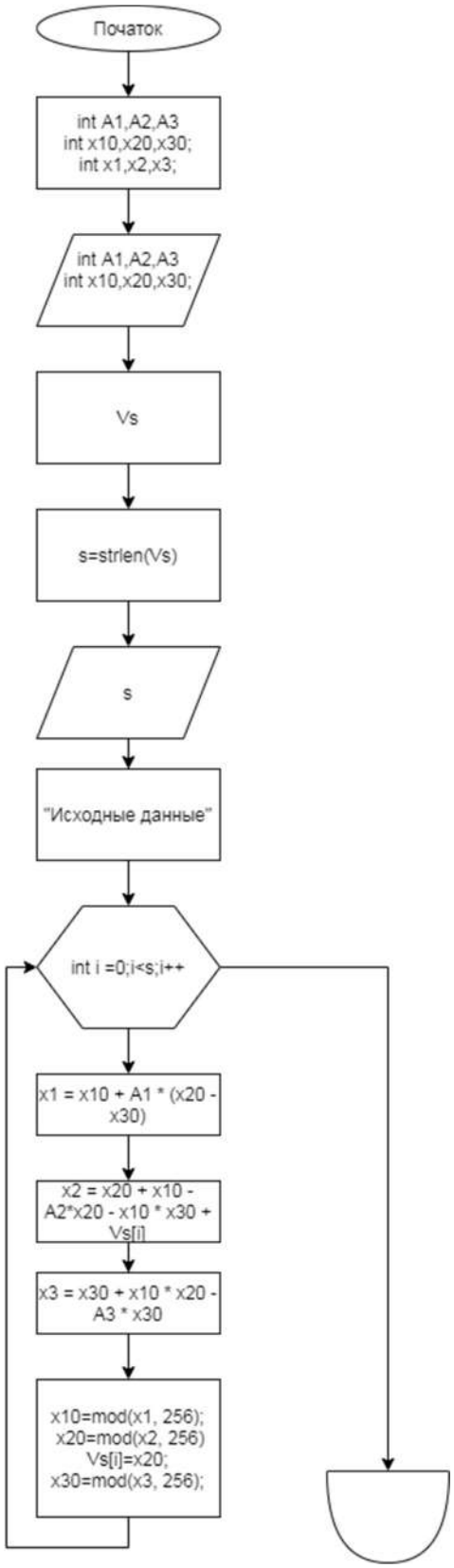

Рисунок 5.8 – Блок схема функції main (ч.1)

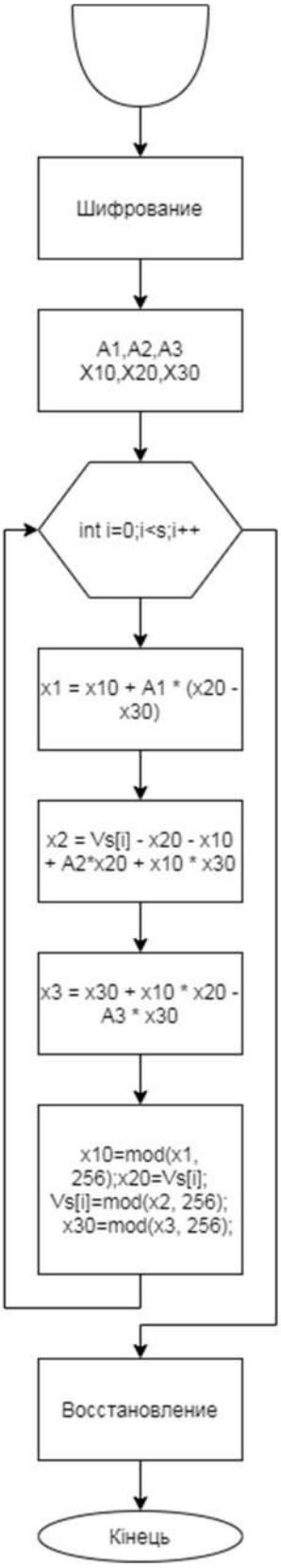

Рисунок 5.9 – Блок схема функції main (ч.2)

Висновки до розділу 5

В даному розділі описується процес шифрування даних, заснований на роботі атрактору Лоренца. На основі роботи атрактора написано програмний код для шифрування та дешифрування введених даних

ВИСНОВКИ

У ході написання дипломного проекту, метою якого був аналіз існуючої проблеми збереження даних в телекомунікаційних мережах та основних методах їх захисту, найбільшу увагу було приділено такому методу захисту інформації, як шифрування за допомогою динамічних систем, тому що на даний момент це один із найбільш ефективних методів, що користується великим попитом.

В даній роботі були розглянуті основні типи загроз, що можуть бути направлені на дані, та способи шифрування, завдяки яким ризик втрати даних знижується.

Обґрунтований вибір тієї чи іншої системи захисту не має сенсу, якщо не наведені критерії ефективності цієї системи. У будь-якому випадку обраний комплекс криптографічних методів повинен поєднувати як зручність, гнучкість і оперативність використання, так і надійний захист від зловмисників циркулюючої в мережі інформації. Тому на даний момент найбільш оптимальні змішані криптосиситеми, в яких текст кодується симетрично, а ключ кодується асиметрично і поміщається разом з кодованим текстом.

Шифрування інформації не є панацеєю. Його слід розглядати тільки як один з методів захисту інформації і застосовувати обов'язково в поєднанні з законодавчими, організаційними та іншими заходами.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Біячуєв, Т.А. Безпека корпоративних мереж / Т. А. Біячуєв. - СПб: СПб ГУ ІТМО, 2004.- 161 с.

2. Волчков, А.Сучасна криптографія / А. Волчков // Відкриті системи.- 2002. - №07-08. - С. 48.

3. Зима, В. безпека глобальних мережевих технологій / В.Зима, А. Молдовян, Н. Молдовян – СПб.: BHV, 2000. - 320 с.

4. Конахович, г. Захист інформації в телекомунікаційних системах / г.Конахович. - М.: МК-Прес,2005.- 356 с.

5. Мельников, В.Захист інформації в комп'ютерних системах / в. Мельников - М.: Фінанси і статистика, Електронінформ, 1997. – 400 с.

6. Молдовян, А.А. Криптографія / А.А. Молдовян, Н. А. Молдовян, Рад Б. Я. – СПб.: Видавництво "Лань", 2001. – 224 с.

7. Семенов, Г. цифровий підпис. Еліптичні криві / г. Семенов / / Відкриті системи.- 2002. - №07-08. - С. 67-68.

8. Устинов, Г. Н. вразливість та інформаційна безпека Телекомунікаційних технологій/ Г.н. Устинов– М.: радіо і зв'язок, 2003.- 342 с.

9. Ярочкин, В. І. Інформаційна безпека. Підручник для вузів / В.І. Ярочкін– м.: академічний Проект, Світ, 2004. - 544 с.

10. Панасенко С. П. Алгоритми шифрування. Спеціальний довідник BHV-Санкт-Петербург, 2009. – 576 с.

11. Водолазський В.Комерційні системи шифрування: основні алгоритми та їх реалізація. Частина 1. // Монітор. - 1992. - N 6-7. - с. 14 – 19.

12. Сяо Д., Керр Д., Меднік С. Захист ЕОМ. - М.: Мир, 1982.

13Атрактор Лоренца.

URL : https://ru.wikipedia.org/wiki/Аттрактор_Лоренца (дата звернення : 31.05.20)

14. Аттрактор Реслера. URL: https://ru.qwe.wiki/wiki/Rössler_attractor(дата звернення: 31.05.20)