Вінницький національний технічний університет
Факультет інфокомунікацій, радіоелектроніки та наносистем
Кафедра телекомунікаційних систем та телебачення

Пояснювальна записка

до магістерської кваліфікаційної роботи
за освітньо-кваліфікаційним рівнем «магістр»
на тему:
ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БЕЗПРОВІДНИХ МЕРЕЖ WiMAX
08-34.МКР.012.00.000 ПЗ

Виконав: студент 2-го курсу,
групи ТТК-18м
спеціальності 172 – Телекомунікації та радіотехніка
_____ Чуба В.В.

Керівник: к.т.н., доцент каф. ТКСТБ
_____ Городецька О.С.

«____» _____ 2019 р.

Рецензент: к.т.н., доцент каф. БМІ
_____ Тимчик С.В.

«____» _____ 2019 р.

Вінниця ВНТУ - 2019 рік

Вінницький національний технічний університет
Факультет інфокомунікацій, радіоелектроніки та наносистем
Кафедра телекомунікаційних систем та телебачення
Освітньо-кваліфікаційний рівень магістр
Галузь знань 17– Електроніка та телекомунікації
(шифр і назва)
Спеціальність 172 – Телекомунікації та радіотехніка
(шифр і назва)
Освітня програма Технології та засоби телекомунікацій

ЗАТВЕРДЖУЮ
Завідувач кафедри ТКСТБ
к.т.н., професор Г.Г. Бортник

"___" _____2019 року

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

Чуба Валерію Валерійовичу.
(прізвище, ім'я, по батькові)

1. Тема роботи Підвищення інформаційної безпеки в безпровідних мережах WiMAX
керівник роботи Городецька Оксана Степанівна, канд. техн. наук, доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "02" 10 2019 року № 254

2. Строк подання студентом роботи 02 грудня 2019 року

3. Вихідні дані до роботи 1. Режим роботи алгоритму шифрування – RC5; 2. Швидкість шифрування інформаційного повідомлення – 10,92 кбіт/с; 3. Швидкість шифрування базового алгоритму – 2728,211 кбіт/с; 4. Тип алгоритму шифрування основного файлу – симетричні алгоритми 3DES або AES; 5. Тип криптографічного обчислювального блоку – ATSAM3U4C; 6. Тип ідентифікуючого пристрою блоку шифрування - STM32F103RE; 7. Тип ядра криптографічного блоку – Cortex-M3; 8. Тактова частота ЦП – 96 МГц; 9. ПЗП ЦП – 256 Кбайт; 10. ОЗП ЦП – 52 Кбайт; 11. Тип зовнішнього інтерфейсу – USB 400 Мбіт/с.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1. Методи захисту інформації в сучасних бездротових мережах; 2. Розробка методів аутентифікації і розмежування доступу; 3. Розробка методів захисту інформації при зберіганні та передаванні в безпровідних мережах. 4. Розробка безпечної мобільної операційної системи та підсистеми захисту програмного забезпечення.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
1. Структура системи захисту від загроз порушення конфіденційності; 2. Блок-схема процесу аутентифікації локальних користувачів; 3. Структурна схема служби доступу до файлової системи; 4. Алгоритм заперечного шифрування; 5. Блок-схема алгоритму базового заперечного шифрування; 6. Алгоритм використання заперечного шифрування для зберігання резервних серій ключової інформації; 7. Алгоритм шифрування файлу в файловій системі EFS; 8. Структурна схема служби передачі даних; 9. Структурная схема блоку криптографічного сховища інформації; 10. Структурна схема пристрою

ідентифікації; 11. Архітектура віртуального програмного середовища; 12. Алгоритм роботи завантажувача операційної системи; 13. Алгоритм роботи безпечного завантажувача фірми Atmel; 14. Алгоритм перевірки автентичності пакета оновлення ПЗ.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Спеціальна частина	Городецька О.С., доцент кафедри ТКСТБ		
Економічна частина	Адлер О.О., к.т.н., доцент		
Охорона праці та безпека в надзвичайних ситуаціях	Березюк О.В. к.т.н., доцент		

7. Дата видачі завдання 02 вересня 2019 року

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської кваліфікаційної роботи	Строк виконання етапів роботи	Примітка
1.	Розробка технічного завдання	06.09.2019р.	
2.	Методи захисту інформації в сучасних бездротових мережах	13.09.2019р.	
3.	Розробка методів аутентифікації і розмежування доступу	04.10.2019р.	
4.	Розробка методів захисту інформації при зберіганні та передаванні в безпровідних мережах	25.10.2019р.	
5.	Розробка безпечної мобільної операційної системи та підсистеми захисту програмного забезпечення	08.11.2019р.	
6.	Аналіз економічної ефективності розробки	15.11.2019р.	
7.	Охорона праці та безпека в надзвичайних ситуаціях	22.11.2019р.	
8.	Оформлення пояснювальної записки та графічної частини	29.11.2019р.	
9.	Нормоконтроль МКР	02.12.2019р.	
10.	Попередній захист МКР, рецензування МКР	06.12. 2019р.	
11.	Захист МКР ЕК	09.12. 2019р.	

Студент _____ Чуба В.В.
(підпис)

Керівник роботи _____ Городецька О.С.
(підпис)

РЕФЕРАТ

УДК 621.391

Чуба В. В. Підвищення інформаційної безпеки в безпровідних мереж WiMAX. Магістерська кваліфікаційна робота зі спеціальності «Телекомунікації та радіотехніка» – Вінниця: ВНТУ, 2019. – 139 с. На українській мові.

Рисунків 32, таблиць 15, бібліографія 63.

У роботі запропоновані альтернативні методики захисту конфіденційності та забезпечення доступності інформації, переданої в бездротових мережах. Дана методика заснована на застосуванні додатку динамічної маршрутизації «маршрутизації сервіс» і дозволяє вирішувати задачу захисту інформації без застосування алгоритмів шифрування.

Розглянуто існуючі методи захисту інформації в бездротових мережах, описані їхні переваги і недоліки. Показано, що більшість існуючих методів є вузькоспеціалізованими при протидії загрозам інформації, а також не застосовні в силу різних обмежень для захисту деяких видів інформації. Це зумовлює необхідність розробки і реалізації спеціалізованих методів захисту інформації, переданої в бездротових мережах, спрямованих на вирішення поставлених завдань.

В результаті виконання роботи досліджений алгоритм динамічної маршрутизації трафіку. На основі даного алгоритму реалізований «маршрутизації сервіс» передачі даних через розподілені мережі. Вироблені основні компоненти, необхідні для функціонування системи. Дано оцінки вірогідності мережевих атак на передану інформацію в разі застосування «маршрутизації сервісу».

ABSTRACT

UDC 621.391

Chuba V.V. Improving information security in WiMAX wireless networks. Master's qualification work in the specialty "Telecommunications and Radio Engineering" - Vinnitsa: VNTU, 2019. - 139 p. In Ukrainian language.

Figures 32, tables 15, bibliography 63.

The paper proposes alternative methods of protecting the privacy and availability of information transmitted over wireless networks. This technique is based on the application of dynamic routing application "routing service" and allows you to solve the problem of information security without the use of encryption algorithms. Existing methods of information security in wireless networks are considered, their advantages and disadvantages are described.

Most existing methods have been shown to be highly specialized in counteracting information threats, and are not applicable due to various restrictions on the protection of certain types of information.

This necessitates the development and implementation of specialized methods for protecting information transmitted over wireless networks, aimed at solving problems.

As a result of the work, the algorithm of dynamic traffic routing is investigated. Based on this algorithm, a "routing service" of data transmission over distributed networks is implemented. The basic components necessary for the functioning of the system are made. The probability of network attacks on the information transmitted in the case of "service routing" is estimated.

ЗМІСТ

ВСТУП

Актуальність роботи. Розвиток інформаційних технологій ставить перед собою завдання підвищення надійності функціонування мереж. Для вирішення таких задач необхідні дослідження існуючих мережевих протоколів, мережевих архітектур, розробка способів підвищення безпеки при передачі інформаційних ресурсів через мережу.

Вибір бездротових технологій дозволяє отримати переваги в швидкості, мобільності. Поява нового класу широкосмугових бездротових мереж з комірчастою структурою (меш-мережі) дозволило досягти значного збільшення зони інформаційного покриття. Основною перевагою даного класу мереж є наявність спеціальних приладів - меш-порталів, що дозволяють інтегрувати в меш-мережа інші бездротові мережі (WiMAX, Wi-Fi, GSM) і Інтернет, а значить, і надати користувачеві всілякі сервіси цих мереж.

До недоліків меш-технології можна віднести той факт, що протоколи маршрутизації меш-мережі досить специфічні, а їх розробка – складна задача з безліччю критеріїв і параметрів. При цьому існуючі протоколи вимагають значних доопрацювань в питаннях підвищення безпеки і надійності передачі інформації.

Інформаційно-комунікаційні технології (ІКТ) є вагомим засобом розвитку Національної програми інформатизації. Серед основних напрямів реалізації концепції технічного захисту інформації в Україні – створення методології синтезу систем багаторівневого захисту інформації, адекватних загрозам її безпеки, зокрема в інформаційно-комунікаційних технологіях. У контексті забезпечення функціональної та інформаційної безпеки ІКТ в межах міжнародного і національного інформаційно-комунікаційного простору актуальним є створення комплексної системи захисту даних у безпровідних комунікаціях і цифрових системах зв’язку, спрямованої на забезпечення безпеки інформації від витоку технічними каналами, несанкціонованих дій та спеціального впливу.

З вищесказаного випливає висновок про необхідність розробки нових способів захисту інформації при передачі в розподілених бездротових мережах в умовах впливу навмисних атак. У зв'язку з цим тема роботи є актуальною і практично важливою.

Аналіз останніх досліджень. Мережеві атаки, збої і відмови мережевого обладнання – основні фактори, що впливають на безпеку передачі інформації в розподілених бездротових мережах. Проблемою забезпечення безпеки передачі інформації в розподілених бездротових мережах займалися I. Akyildiz, W.Wang, X.Wang, T. Dorges, N. BenSalem. Під забезпеченням безпеки

передачі інформації в комп'ютерній мережі розуміється захист її конфіденційності, цілісності та доступності [1-14].

Серед методів забезпечення доступності інформації в бездротових мережах дослідниками виділяється комбінування різних методів контролю, дублювання, резервування. Цілісність і конфіденційність інформації в бездротових мережах забезпечується методами побудови віртуальних каналів, заснованих на застосуванні криптографічних інструментів.

Загальним недоліком даних методів - зниження продуктивності мережі, пов'язане з вимогами до додаткової обробки інформації. Зазначений недолік є критичним для передачі цифрової відеоінформації. Крім того, вдосконалення методів криптоанализа все більш знижує надійність існуючих криптоалгоритмів

Мета і завдання роботи. Метою цієї роботи є дослідження методики захисту інформації в розподілених бездротових мережах, в умовах впливу навмисних атак та розробка алгоритму кодування для зебезпечення передачі інформації в мережах з радіодоступом.

Для досягнення зазначеної мети, треба було вирішення наступних запитань:

- дослідження алгоритмів динамічної маршрутизації трафіку в розподілених мережах.
- дослідження методів захисту інформації в розподілених бездротових мережах.
- аналіз алгоритму динамічної маршрутизації інформації при передачі в розподілених бездротових мережах в умовах впливу навмисних атак.
- аналіз алгоритму генерації потоку мережевих атак.
- аналіз прототипу маршрутизациї сервісу для експериментальної перевірки запропонованої методики захисту.
- аналіз протоколу WEP
- дослідження функцій кодування для забезпечення гармоійного вихідного повідомлення
- аналіз розробленої системи кодування на відповідність значень правилам псквдовипадковості.
- визначення ключових послідовностей кодуючої функції для забезпечення псевдовипадкового характеру.

Об’єкт дослідження є процеси захисного перетворення переданої по відкритих каналах інформації на основі вимог обчислювальної нерозрізненості по шифротексту від імовірнісного захисного перетворення.

Предмет дослідження є метод аутентифікації користувачів на основі використання одноразових паролів, що генеруються за допомогою алгебраїчного алгоритму псевдовипадкового захисного перетворення.

Наукова новизна одержаних результатів:

1. Розроблено метод аутентифікації користувачів, що відрізняється використанням одноразових паролів, що генеруються за допомогою алгебраїчного алгоритму псевдовероятностного захисного перетворення.

2. Розроблено метод захисного перетворення передається по відкритих каналах інформації, що відрізняється виконанням вимоги обчислювальної нерозрізненості по шифртексту від імовірнісного захисного перетворення.

3. Розроблено метод захисту програмного забезпечення від дизассемблирования, що відрізняється введенням помилкових гілок коду за допомогою псевдовероятностного захисного перетворення машинного коду.

4. Розроблено новий метод зберігання ключів шифрування, що відрізняється виконанням псевдовероятностного захисного перетворення ключів.

Практичне значення. Практичне значення роботи полягає в тому, що застосування універсальної операційної системи в мобільних пристроях телекомунікаційних та інформаційних систем, в тому числі в системах захисту інформації, дозволить уніфікувати підходи до забезпечення безпеки при розробці таких систем. Даний підхід спростить розробку і виробництво мобільних пристроїв. Область застосування розробленої ОС включає розробку захищених аутентифікуючих пристроїв (токенів, ідентифікаторів), систем охорони, пристроїв захисту програмного забезпечення, персональних пристроїв зберігання даних (захищених файлових сховищ), апаратних засобів для виконання захисних перетворень даних.

Апробація роботи та її основні результати роботи проводилися на Всеукраїнській науково-практичній інтернет-конференції Молодь в науці: дослідження, проблеми, перспективи (МН-2020) у 2019 році.

1 МЕТОДИ ЗАХИСТУ ІНФОРМАЦІЇ В СУЧАСНИХ БЕЗПРОВІДНИХ МЕРЕЖАХ

1.1 Технології захисту даних

Криптографічні технології захисту інформації в розподілених мережах застосовуються для вирішення завдань захисту конфіденційності переданої інформації, підтвердження цілісності та автентичності даних, аутентифікації абонентів при встановленні з'єднання. Розглянемо деякі алгоритми шифрування даних.

Алгоритм DES - блоковий симетричний алгоритм, один з найбільш поширених, що використовуються в системах захисту комерційної інформації.

Алгоритм DES побудований відповідно до методології мережі Фейстеля. У ньому здійснюється шифрування 64-бітових блоків даних за допомогою64-бітового ключа, в якому вагомими є 56-біт (8-біт перевірочні для контролю на парність). Процес шифрування полягає в початковій перестановці бітів 64-бітового блоку, шістнадцяти раундах шифрування і в кінцевої перестановці бітів на рис. 1.1.

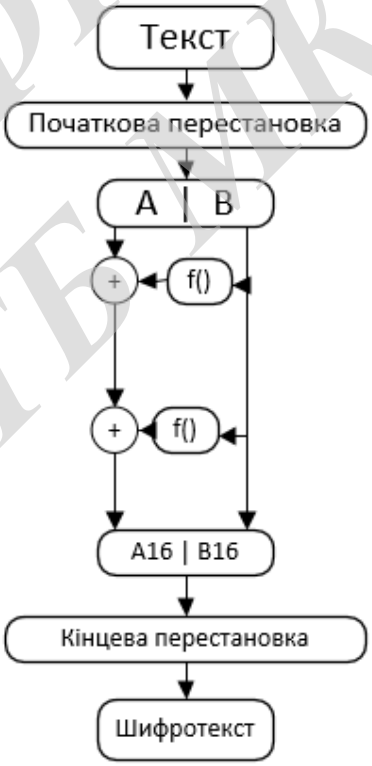


Рисунок 1.1 – Спрощена схема шифрування алгоритму DES

Сучасна мікропроцесорна техніка дозволяє вже сьогодні за досить прийнятний час зламувати симетричні блокові шифри здовжиною ключа 40 біт. Для такого взламування використовується «метод грубої сили». «Метод грубої сили» передбачає перебір всіх можливих варіантів ключа шифрування до знаходження шуканого ключа. Нехай розмір ключа шифрування в бітах рівний b. Відповідно, існує 2 варіантів ключа. В результаті застосування подібної атаки ключ шифрування обов'язково буде знайдений, причому в середньому пошук потребує
2^{b-1} тестовихоперацій. В даний час на ринок надійшли FPGA і ASIC чіпи, які володіють можливістю перебирати відповідно від 30 до 200 мільйонів значень в секунду.

Алгоритм шифрування даних, який визначається ГОСТ 28147-89, являє собою 64-бітовий блочний алгоритм з 256-бітовим ключем. Даний алгоритм шифрує інформацію блоками по 64-біта, які розбиваються на два субблока по 32 біта (N1 і N2). Субблок N1 певним чином обробляється, після чого його значення складається зі значення субблока N2, потім субблоки міняються місцями. Таке перетворення виконується 16 або 32 раундів в залежності від роботи алгоритму. В кожному раунді виконуються наступні операції: накладення ключа (на субблок), таблична заміна і побітовий циклічний зсув вліво. У відкритій літературі досить мало робіт, присвячених криптоанализу алгоритма Д 28147-89. Це особливо помітно в порівнянні з величезним числом робіт, присвячених криптоанализу стандарту шифрування DES. Алгоритм ДСТУ 28147-89 вважається дуже стійким - в даний час для його розкриття НЕ запропоновано більш ефективних методів, ніж згаданий вище метод «грубої сили».

Алгоритм AES, на відміну від алгоритму ДСТУ 28147-89, являє кожен блок даних, що обробляються у вигляді двомірного байтового масиву розміром 4x4, 4x6 або 4x8 в залежності від встановленої довжини блоку. Далі на відповідних етапах виробляються перетворення або над незалежними стовпцями, або над незалежними рядками, або над окремими байтами. Алгоритм AES складається з 10 або 14 раундів і виконує 4 перетворення: табличну заміну кожного байта масиву (ByteSub), зрушення рядків масиву (ShiftRow), операції над незалежними стовпцями масиву (MixColumns), додавання ключа (AddRoundKey). Незважаючи на достатню стійкість алгоритму AES, за останні роки криптоаналітики вельми серйозно просунулися в розкриті даного алгоритму. Наприклад, запропонована теоретична атака вже на 10 раундів алгоритму AES-192.

Вітчизняні стандарти цифрового підпису - ДСТУ Р 34.10-94 і ДСТУ Р 34.10-2001. Криптографічна стійкість даних схем цифрового підписи

грунтується на складності рішення задачі дискретного логарифмування в групі точок еліптичної кривої, а також стійкості використовуваної хеш-функції.

Іншим способом захисту інформації, що передається по каналах зв'язку, є створення так званих захищених віртуальних мереж VPN (Virtual Private Network). В основі концепції побудови віртуальних мереж VPN лежить ідея побудови віртуальних захищених тунелів міжвузлами мережі для забезпечення конфіденційності і цілісності інформації, переданої через відкриті мережі. Економічна ефективність від впровадження VPN-технологій стимулює підприємства до їх активного впровадження, в цьому випадку компанія може відмовитися від оренди виділених каналів зв'язку для створення власної мережі. Тунель VPN представляє собою з'єднання, проведене через відкриту мережу, по якій передаються криптографічно захищені пакети повідомлень. Захист інформації в процесі її передачі по тунелю VPN заснований на виконанні наступних функцій: аутентифікація взаємодіючих сторін, шифрування переданих даних, перевірка справжності та цілісності доставленої інформації.

Принцип тунелювання полягає в тому, щоб перетворити передані дані разом зі службовими полями в новий «пакет». При цьому пакет протоколу нижчого рівня поміщається в поле даних пакета протоколу більш високого або такого ж рівня. Варто зазначити, що тунелювання саме по собі не захищає даних від несанкціонованого доступу або спотворення, але завдяки тунелюваню з'являється можливість повногокриптографічного захисту вихідних пакетів. Щоб забезпечити конфіденційність даних, відправник шифрує вихідні пакети, упаковує їх у зовнішній пакет з новим IP- заголовком і відправляє по мережі. В якості протоколів тунелювання можуть бути використані протоколи канального рівня PPTP і L2TP, а також протокол мережевого рівня IPSec. Протоколи SSL і TLS застосовуються в якості протоколу захищеного каналу на сеансовому рівні моделі OSI. Тунелі VPN можуть створюватися для різних типів кінцевих користувачів - або це локальна мережа LAN з шлюзом безпеки, або окремі комп'ютери віддалених і мобільних користувачів. Для створення віртуальної приватноїмережі великого підприємства потрібні VPN-шлюзи, VPN-сервери і VPN-клієнти.

За способом технічної реалізації розрізняють наступні групи VPN: VPN на основі маршрутизаторів; VPN на основі міжмережевих екранів; VPN на основі програмних рішень; VPN на основі спеціалізованих апаратних засобів.

Основна перевага VPN в порівнянні з виділеними лініями: віртуальні приватні мережі не менш надійні в плані захисту інформації, проте в 5-10, а іноді і в 20 разів дешевше. Головний недолік – падіння продуктивності мережі, пов'язаний з криптографічною обробкою трафіку, що проходить через VPN-

пристрій. Виникаючі затримки можна розділити на три основних типи: затримки при встановленні захищеного з'єднання між VPN-пристроями; затримки, пов'язаної з шифруванням і розшифруванням захисних даних, а також з перетвореннями, необхідними для контролю їх цілісності; затримки, пов'язаної з додаванням нового заголовку до переданих пакетів. Чим більший обсяг переданих даних, тим більші вносяться затримки. Таке падіння продуктивності мережі не критично для більшості додатків і сервісів, але, наприклад, згубно для передачі потокового відео і звуку. До того ж з розвитком інформаційних технологій потреба в швидкісний передачі трафіку великого обсягу все зростає, відповідно зростають і вимоги, як до самих каналах зв'язку, так і до засобів їх захисту.

На закінчення розглянемо технології забезпечення безпеки в бездротових мережах.

1.2 Технологія безпеки WEP

IEEE 802.16 визначає кілька служб для забезпечення безпеки середовища. Служби безпеки забезпечуються в значній мірі WEP протоколом, щоб захистити дані канального рівня в бездротової пе¬редаче між точками доступу і клієнтами. Тобто WEP не забезпечує безперервний захист, а тільки для бездротової частини підключення [12].

У стандарті IEEE визначені три основних служби безпеки для WLAN:

1. Ідентифікація - служба, що забезпечує ідентичність спілкуються станцій клієнта, тобто керування доступом до мережі за допомогою відмови в доступі станціям, які не можуть підтверджувати справжність

2. Конфіденційність - служба забезпечення секретності, «еквівалентної звичайної мережі» з метою запобігання "пасивних атак" (перегляду даних не були ідентифіковані клієнтами).

3. Цілісність - служба, що забезпечує гарантію, що повідомлення не змінені в процесі передачі між клієнтами і точкою доступу (ак-активне напад).

1.2.1 Принципи побудови системи захисту

Для забезпечення конфіденційності переданих в мережах повідомлення можуть бути використані різні перетворення. Найбільш широке поширення через простоту технічної реалізації в даний час отримало перетворення, засноване на складання по модулю два однакових знаків вихідного повідомлення і послідовності, сформований так званим генератором випадкових чисел. При цьому можливі деякі модифікації цього перетворення

шляхом введення зворотного зв'язку по перетвореному або вихідного повідомлення .

Зауважимо, що якщо перетворене повідомлення формується з вихідного шляхом додавання за модулем два однойменних знаків вихідного повідомлення і послідовності, сформованої генератором випадкових чисел, то воно є вразливим для тих вторгнень, метою яких є цілеспрямована зміна вихідного повідомлення. Дійсно, якщо вихідне повідомлення частково відомо зловмисникові, то модифікація знаків повідомлення реалізується досить просто шляхом інвертування знаків перетвореного повідомлення в тих місцях, де потрібно інверсія знаків іс¬ходного повідомлення .

Якщо перетворене повідомлення формується з вихідного з використанням зворотного зв'язку по перетвореному повідомленням або вихідного повідомлення, то зловмисник не в змозі визначити вихідне повідомлення, яке буде отримано з перетвореного повідомлення на приймальній стороні при навмисному зміні хоча б одного знака перетвореного повідомлення. Це обумовлено тим, що такі перетворення характеризуються поширенням помилки за повідомленням. В цьому випадку цілеспрямована модифікація повідомлення для зловмисника представляє значні труднощі.

Оскільки у всіх цих випадках використовується деякий генератор випадкових чисел, то при правильному його побудові та виборі ключа перетворення представляється можливим забезпечити лише потрібну конфіденційність повідомлень.

Тому розглянуті перетворення в принципі не дозволяють забезпечити одночасно конфіденційність і цілісність переданих повідомлень. Цілісність повідомлення означає, що це повідомлення справді і не піддавалося несанкціонованої або випадкової модифікації в про¬цессе передачі в мережі зв'язку.

Підтвердження справжності в більшості практичних випадків здійснюється наступним чином. За допомогою деякого перетворення з повідомлення формується так званий електронний код підпису, який додається до цього повідомлення. Для перевірки цілісності повідомлення на приймальній стороні використовується той же перетворення, що і на отримуючій стороні. При цьому якщо сформований на приймальній стороні електронний підпису збігається з електронним кодом підписи, доданим до повідомлення, то повідомлення вважається справжнім. Таким чином, для забезпечення конфіденційності і цілісності, переданих в ВС повідомлень, необхідно використовувати систему, що складається з пристрою перетворення повідомлень, пристрої формування, а, при необхідності, і перевірки електронного коду підпису, а також пристрої комутації.

функціонує наступним чином.

Оригінал тексту $X\,(i)$ перед видачею в мережу зв'язку надходить в пристрій перетворення повідомлень, де формується повідомлення $Y\,(i)$ за допомогою деякого перетворення.

Далі, перетворене повідомлення $Y\,(t)$ надходить в пристрій формірова¬нія електронного коду підпису.

У цьому пристрої здійснюється формування електронного коду підпису До з повідомлення $Y\,(t)$ за допомогою іншого перетворення. Після цього повідомлення $Y\,(t)$ і код До надходять в пристрій комутації, де формується повідомлення $< Y\,(t), K >$, яке і видається в мережу зв'язку. Для виразності покладається, що довжина перетвореного повідомлення $Y\,(t\,)$ становить L знаків, а електронного коду підпису - т знаків.

На приймальній стороні при отриманні повідомлення $< Y\,(t), \text{К} >$створюється виділення з нього перетвореного повідомлення $Y\,(t)$ і електронного коду підпису K, які видаються в пристрій формування елек тронного кода підпису. У цьому пристрої з повідомлення $Y\,(t)$ за допомогою точно такого ж перетворення, яке використовувалося на передавальній стороні для формування електронного коду підпису K, здійснюється формування коду $K\,*$ і його порівняння з кодом К. Якщо виконується умова $K\,* = K$, то приймається рішення про те, що в процесі передачі повідомлення $Y\,(t)$ піддалося модифікації, і здійснюється зворотне перетворення цього повідомлення з метою отримання вихідного повідомлення.

1.2.2 Модифікований генератор псевдовипадкових послідовностей

Розглянемо методи генерування послідовності випадкових чисел U_n, рівномірно розподілених між нулем і одиницею на інтервалі [0,1]. Так як процесор може представляти дійсні числа тільки з певною точністю, ми будемо генерувати ціле число X_n між нулем і деяким числом m дріб:

$$U_n = X_n/m$$

буде, отже, лежати між нулем і одиницею. Зазвичай m вибирають рівним розміру слова в процесорі. Тому X_n можна розглядати як ціле число, що займає все комп'ютерне слово, з точкою, яка відділяє цілу частину числа від дробової, що стоїть в правому кінці слова, а U_n- як основа того ж слова з розділяє точкою, що стоїть в лівому наприкінці слова.

В даний час найбільш поширеними генераторами випадкових чисел є лінійні генератори, в яких використовується наступна схема, запропонована Д. Г. Лехмером.

Виберемо чотири числа:

m - модуль, $0 < m$;

a– помножувач;$0 < a < m$; (1.1)

c– прирощуваня;$0 < c < m$;

X_0– початкове значення$0 < X_0 < m$.

Потім отримаємо бажану послідовність випадкових чисел(X_n), вважаючи:

$$X_{n+1} = (aX_n + c) mod\ m,\ \ n \geq 0 \quad (1.2)$$

Ця послідовність називається лінійною послідовністю. Послідовність не може бути "випадковою" при деяких наборах чисел m, a, с іX_0.

Конгруентністю послідовність завжди утворює петлі, тобто обов'язково існує цикл, що повторюється нескінченне число разів. Це можливість є загальним для всіх послідовностей виду $X_{n+1} = f(X_n)$, деfутворює саме в собі. Повторювані цикли називаються періодами.

Розглянемо випадок, коли с = 0, так як генеруючі числа матимуть менший період, ніж прис $\neq 0$. Обмеження с = 0 зменшує довжину періоду послідовності, хоча при цьому все ще можливо зробити період достатньо довгим. В оригінальному методі, запропонованому Д. Г. Лехмером, с вибиралося рівним нулю, хоча він і допускав випадок, коли $c \neq 0$, як один з можливих. Той факт, що умова $c \neq 0$може призводити до появи більш довгих періодів, був встановлений В. Е. Томсоном і незалежно від нього А. Ротенбергом. Лінійну конгруентну послідовність при с = 0 називають мультиплікативний конгурентним методом, а при $c \neq 0$- змішаним конгурентним методом.

Можна відразу відкинути випадок, коли а = 1, при якому послідовність$f(X_n)$

представлена у вигляді $X_n = (X_0 + nc) mod\ m$і поводиться явно не як випадкова послідовність. Випадок, коли а = 0, навіть гірше попереднього. Отже, для практичних цілей припускаємо, що

$$a >= 0 b > 1 \quad (1.3)$$

Узагальнимо формулу

$$X_{n+k} = \left(a^k X_n + \frac{(a^k-1)c}{b}\right) modmk >= 0, n >= 0 \qquad (1.4)$$

де $(n + k)$-й член виражається безпосередньо через n-й. Розглянемо випадок, коли n = 0, підпослідовність, що містить кожен k-й член послідовноності $\{X_n\}$, є також лінійної конгруентної послідовністю, множник якої дорівнює $a^k \, mod \, m$і збільшення рівне $\left(\frac{(a^k-1)c}{b}\right) modm$ Важливим наслідком з (2.14) є те, що загальна послідовність, визначена за допомогою a, c і Xo, може бути дуже просто виражена в термінах спеціального випадку, коли $c = 1$і $X_0 = 0$. Нехай

$$Y_0, Y_{n+1} = (aY_n + 1) modm \qquad (1.5)$$

Значить, післядовність, визначена в (2.12), буде має вигляд:

$$X_n = (AY_n + X_0) modmA = (X_0 b + c) modm \qquad (1.6)$$

Розглянемо вибір модуля. Першим завданням, є знаходження оптимальних значень параметрів, що визначають лінійну конгурентну послідовність. Спочатку з'ясуємо, як правильно вибрати число m. Потрібно щоб m було досить великим, так як період не може мати більше m елементів. Інший фактор, який впливає на вибір m, - швидкість генерування: потрібно підібрати значення m

Як приклад розглянемо даний процесор. Можна обчислити у modm, вставляючи у в регістри AiXi виконуючи поділ на m. Якщо yimпозитивні, то у modm з'явиться в регістрі X. Але поділ порівняно повільно протікає операція, і цей недолік можна компенсувати, якщо вибрати значення m таким як довжина слова процесора.

Нехай w буде довжиною комп'ютерного слова, а саме – 2^e на e - розрядній двійковій обчислювальній машині. Результат операції підсумовування зазвичай дається по модулю w (але не на машинах, що використовують процедуру одиничного доповнення); множення по модулю w також дуже просте, оскільки зачіпаються тільки молодші розряди. Результат з'являється в регістрі A. Деяка техніка може використовувати представлення обчислення по модулю w + 1. Зазвичай, як правило, потрібно, щоб c = O, коли m = w + 1; тоді ми просто повинні обчислити (aX) mod (w + 1).

Розглянемо чому використовується т = w ± 1, коли вибір m = w очевидно більш зручний. Причина в тому, що, коли m = w, цифри правій частині X_n

набагато менш випадкові, ніж цифри лівій частині. Якщо d є дільником m і якщо

$$Y_n = X_n mod d, \tag{1.7}$$

можна легко показати, що

$$Y_{n+1} = (aY_n + c) mod d \tag{1.8}$$

(Нехай $X_{n+1} = aX_n + c - qm$, де q - деяке ціле число. Якщо обидві частини рівності взяти по модулю d, можна втратити qm, коли d-множник m). Для ілюстрації важливості вираження (1.8) припустимо, що є двійковий комп'ютер. Якщо $m = w = 2^6$, молодші чотири розряду X_nєчислами$Y_n = X_n mad\ 2^4$. Суть виразе (1.8) полягає в тому, що молодші чотири розряди (X_n) формують послідовність з періодом 16 або менше. Аналогічно п'ять молодших розрядів є періодичними з періодом не більше 32 і найменший значущий розряд X_n є або постійним, або строго періодичним.

Подібна ситуація не виникає, коли m = w ± 1; в такому випадку молодші розряди X_n поводяться так само випадково, як і старші. Наприклад, при w = 235 і m - 235 - 1 числа послідовності будуть не дуже випадкові, якщо розглянути тільки їх залишки по модулю 31, 71, 127 або 122921, але молодші розряди, які представляють числа послідовності, взяті по mod 2, будуть досить випадкові.

Альтернатива полягає в тому, щоб в якості m взяти найбільше просте число, менше, ніж w.

У більшості випадків використані молодші розряди несуттєві і вибір m = w є задовільним.

Розглянемо вибір множника для створення періоду максимальної довжини. Довгий період необхідний для будь-якої послідовності, що використовується в якості джерела випадкових чисел. Безумовно, ми очікуємо, що в періоді міститься значно більше чисел, ніж потрібно для одноразового використання. Тому тут увагу буде зосереджена на довжині періоду. Довжина періоду - це тільки одна з вимог до лінійних послідовносей, які використовуються, як випадкові последовності. Наприклад, коли a = c = 1, послідовність прийме простою вигляд: $X_{n+1} = (X_n + 1) mod m$. Очевидно, що ця послідовність має період довжиною m, але не дивлячись на це в неї немає нічого випадкового. Так як можливі стільки m різних значень, довжина періоду, безсумнівно, не може бути більше m. Чи можна досягти максимальної довжини періоду –m ? Як показано вище

це завжди можливо, хоча вибір a = c = 1 не забезпечує бажаної властивості послідовності. Досліджуємо всі можливі значення a, c і X_0, які дають період довжиною m. Виявляється, що такі значення параметрів можуть бути охарактеризовані дуже просто; коли m є твором різних простих чисел, тільки значення a = 1 забезпечує повний період, але коли m ділиться на просте число в великій мірі, то існує значна свобода у виборі a. Наступна теорема дозволяє визначити, можливо, чи можливе досягнення періоду максимальної довжини.

Лінійна послідовність, певна числами m, a, сі X_0, має період довжиною m тоді і тільки тоді, коли:

1) числа сіm взаємно прості;

2) b = a - 1 кратно p для кожного простого p, що є дільником m;

3) b кратно 4, якщо m кратно 4.

Нехай число m допускає розкладання на прості множники у вигляді

$$m = p_1^{e1} \dots p_t^{et} \tag{1.9}$$

Довжина періоду A лінійної послідовності, визначеній параметрами (X_0, a, c, m), є найменшим спільним кратним довжин періодів лінійних послідовностей.

Розглянемо спеціальний випадок використання виключно мультиплексованих генераторів, коли c = 0. Не дивлячись на те, що процес генерування випадкових чисел є трохи більш швидким в даному випадку, як показано вище максимальний період не може бути досягнутий. Дійсно, це абсолютно очевидно, так як послідовність задовольняє співвідношенню $X_{n+1} = aX_n mod m$і значення X_n= 0 може з'явитися, тільки якщо послідовність зявляється в нуль. Взагалі, якщо d - будь-який дільник m і якщо X_nкратно d, всі наступні елементи мультиплікативної послідовності будуть кратні d. Так що коли c = 0, необхідно, щоб $X_n$imбули взаємно, простими числами для всіх n, що і обмежує довжину періоду максимум до f(m)- числа цілих взаємно простих чисел cm, що лежать між 0 im.

1.3 Захист інформації на основі динамічної маршрутизаціїї трафіка

Пропонується здійснити розподілення передачі по декількох фізичних каналах окремих частин переданих даних таким чином, щоб складність відновлення вихідних даних без будь-якої їх частини була максимальною або мінімальної залежно від поставленого завдання. При подальшому пересиланю частин даних передбачається використовувати проміжні передавачі F "i e [1, п] зображенні на рис. 1.6.

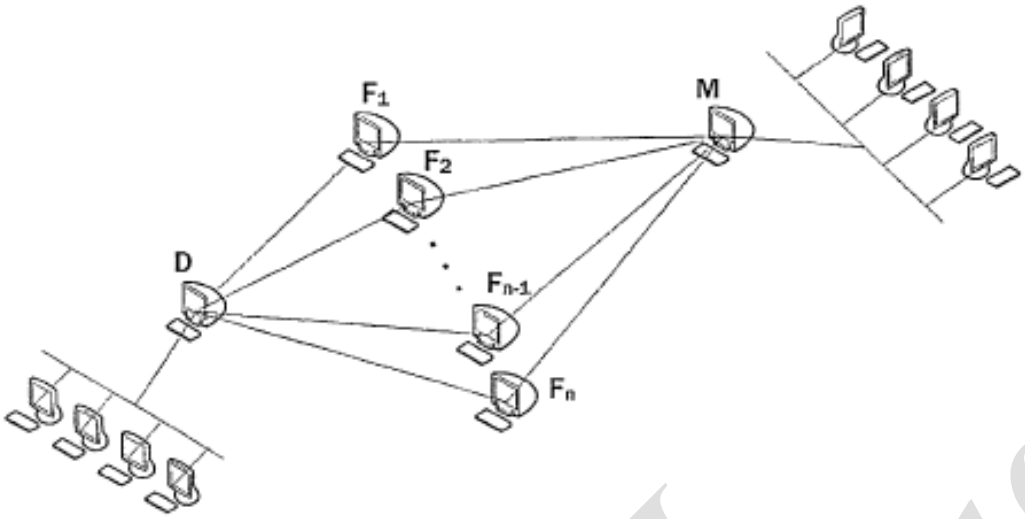


Рисунок 1.6 – Система мультиплексування трафіку

Позначимо прийняту термінологію:

Оригінал тексту - повідомлення, передане по мережі за допомогою запропонованого в роботі методу, реалізованого в даній системі.

Демультиплексор (D) - модуль, що відповідає за розподіл постуаючих на нього даних вихідного повідомлення на проекції і їх відправку. Так само на демультиплексор можуть бути покладені функції визначення стану мережі на основі станів певних компонентів системи, таких як буфери передачі і певні службові сигнали підтвердження.

Мультиплексор (M) - модуль, що виконуючий функції зворотні демультіплекору. Даний модуль збирає проекції фрагменти даних, передані по різним каналам в один потік, утворюючи вихідне повідомлення. Якідемультиплексор, мультиплексор здатний детектувати певні події в мережі по стану входних до нього потоків.

Передавач - модуль, що відповідає за транзит даних. На передавачі так само реалізована певна логіка, необхідна для правильного функціонування алгоритмів мультиплексора і демультиплексор.

Демультиплексор, мультиплексор і передавач є основними компонентами системи.

Фізичний пристрій - комп'ютер, на якому виконується програмний додаток мультиплексора, передавача, демультиплексор або кілька програм одночасно.

Логічний канал зв'язку між пристроями - логічне з'єднання протоколу TCP або UDP .

Фізичний канал - окрема, виділена ділянка передачі IP-даних, що представляє собою деяке фізичне середовище передачі. В одному фізичному каналі може бути утворено безліч логічних каналів, різних TCP або UDP з'єднань.

Зона передчі даних - сукупність логічних компонентів системи, є закінченою, самостійно функціональною одиницею. Зона здійснює рознесення, передачу та збір даних. Кожна зона містить мультиплексор, демультиплексор і, декілька передавачів.

Гілка передачі даних - послідовність логічних пристроїв з'єднаних за схемою: демультиплексор - передавач (і) - мультиплексор.

Основне призначення компонентів демультиплексор і мультиплексор - поділ і збір даних. Також ці компоненти передають і приймають розділені дані.

Найбільш очевидний варіант реалізації системи в мережі IP – на сеансовому рівні моделі OSI. Таким чином, для її коректного функціонування необхідне використання проміжних компонентів - передавачів. Вони виступають в якості вузлових точок, між якими встановлюються логічні з'єднання.

Після обробки даних на рівні додатків стека TCP або UDP пакети передаються мережному рівню IP. У заголовку отриманого IP пакета в поле відправник вбудоване IP адреса демультиплексора, а в поле одержувач IP адрес передавача. Завдяки такій реалізації відбувається приховування «Глобальних адресів», адреса кінцевого пункту призначення і адреса пристрою, спочатку відправивша дані. Таким чином, при перехопленні і аналізі пакета на ділянці передавач - мультиплексор, адрес демультиплексора визначити неможливо. Це наглядно представлено в заголовках IP пакета при його проходженні від демультиплексора до мультиплексора. Ніде в заголовках не зустрічається пара $IP_{джерело}$= $IP_{демультиплексора}$ и $IP_{визначення}$ =$IP_{мультиплексора}$

У випадку, якби мультиплексор і демультиплексор працювали один з одним напряму, то, перехопивши окремий пакет, можна було б визначити адреси демультиплексора і мультиплексора, що неприпустимо. Так само в цьому випадку неможливо було б зробити розділення каналів, оскільки роздільні логічні потоки передавалися б по одному фізичному шляху.

Пропоноване рішення має на увазі підвищення стійкості інформації при несанкціонованому доступі до середовища передачі на основі наявних фізичних засобів. Характерною особливістю системи є те, що вона, є повністю прив'язаною до властивостей середовища передачі і топології мережевої структури, покладаючись на наявність структурної надмірності, яка особливо властива для мережі Internet.

1.3.1 Маршрутизований сервіс

Пропонується вдосконалити систему «демультиплексор - передавачі - мультиплексор», розробивши інструмент, що дозволяє передавачам виконувати автоматичну «інтелектуальну» маршрутизацію. Реалізація даного підходу полягає в установці на передавачі програми «маршрутизований сервіс», коригуючого роботу протоколів маршрутизації для маркованої інформації.

Система мультиплексування трафіку вразлива перед класом активнихмережевих атак, описаних в першому розділі. Розглянемо ще раз одну з активнихмережевих атак - атаку, засновану на сніффінге яка зображена на рис. 1.7.

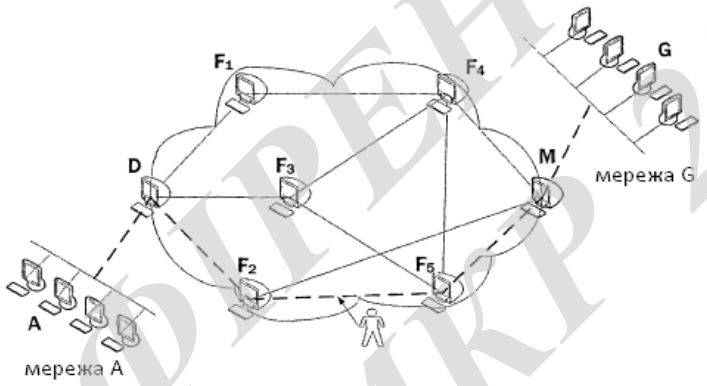


Рисунок 1.7 – Робота протоколів маршрутизації між A і Gв момент Δt можливий варіант атаки на проміжку B-F

Порушник, володіючи знаннями, що деяка організація регулярно передає дані з A в G, може досить точно визначити маршрут від A доG в момент часу Δt і здійснити перехоплення на якомусь з ділянок слідування трафіку. F_1, F_2, F_3, F_4, F_5 - передавачі системи мультиплексування трафіку, в разі її використання в розподіленій мережі, або в загальному випадку деякі вузлові сервера, необхідні дляпросторового уявлення маршруту слідування трафіку. Виробляючи посилку пакетів, порушник в момент часу Δt визначив маршрут прямування трафіку (показано пунктиром) і справив атаку на підконтрольному маршрутизаторі, розташованому на ділянці F_2F_5.

Розроблено програму «маршрутизований сервіс» (S_M), що дозволяє підвищити безпеку передачі інформації в розподілених бездротових мережах в умовах впливу активних атак. S_M – клієнт сервернапрограма, що дозволяє користувачеві передавати дані специфічним маршрутом.

Наведемо опис компонентівS_M.

$$S_M = \{S_{MS}, S_{MC}\}.$$

S_{MC}- клієнтська частина S_M, яка встановлюється на комп'ютерах користувачів і надає діалог для ініціалізації процессу передачі інформації за допомогою маршрутизованого сервісу

S_{MS}- серверна частина S_M, яка встановлюється на довіреному сервері і виконує динамічну маршрутизацію інформації, що надходить нацей сервер.

$S_{MS} = \{F_S, F_S^{\text{дост}}, \text{M}, f\}$.

$F_S = \{F_{S1}, F_{S2}, \dots F_{SF}\}$- безлічдовіренихсерверівмережі. Під довіреною сервером розумієтьс багатофункціональний сервер розподіленої бездротової мережі, до якого порушник не має доступу.

$F = |F_S|$- кількість довірених серверів мережі. В рамках термінології системи мультиплексування трафіку в ролі довіреної сервера може виступати і передавач при виконанні вищенаведених умов.

$F_S^{\text{дост}} = \{F_{S1}^{\text{дост}}, F_{S2}^{\text{дост}}, \dots, F_{SF}^{\text{дост}}\}$ - описує кількість доступних довірених серверів в початковий момент часу t_0, а потім через інтервали часу, рівні τ. $F_{Si}^{\text{дост}}$- кількість доступних довірених серверів для $F_{Si}, i \in [1; F]$.

$M = \{M_1, M_2, \dots, M_F\}$- безліч матриць маршрутизації. Матриця маршрутизації M_I формується на сервері F_{SI} в початковий момент часу t_0, а потім переформовувалися через інтервали $i \in [1; F]$. Кожна матриця $M, \in F_{SI}$містить елементи m_{kj}, що характеризують доступність довірених серверів відносно один одного з $F_{SI}, k \in [1, F], j \in [1, F]$.

$F_{SI}^{\text{дост}}$ обчислюється за допомогою елементів матриці M_I наступнимчином:

$$F_{SI}^{\text{дост}} = \sum_{j=1}^{F} m_{ij} \,. \qquad (1.10)$$

f - параметр, що визначає кількість використовуваних довірених серверів на всьому маршруті від відправника до одержувача протягом одного сеансу (розмір «кластера сеансу передачі»).

На довірених серверах з безлічі F_S встановлюється серверна частина сервісу - S_{MS}, що виконує автоматичну «інтелектуальну» маршрутизацію трафіку.

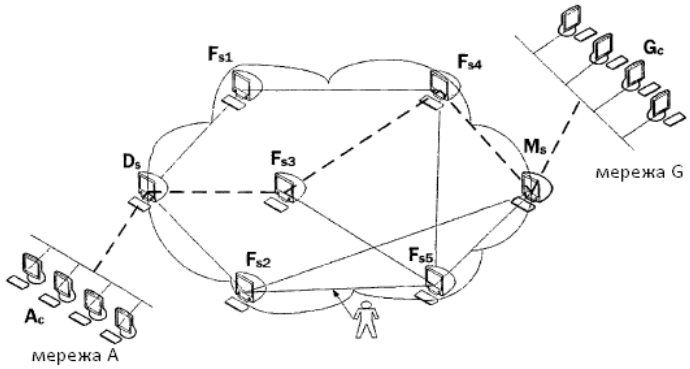


Рисунок 1.8 – Зміна маршруту трафіку за рахунок використання маршрутизації сервісу S_Mна передавачах$F_i, i \in [1,5]$

Показано, що використання S_M дозволило уникнути проходження трафіком підконтрольної порушниками ділянки зображеної на рис. 1.8. Дане рішення S_M(підсумковий маршрут) є імовірнісним з ймовірністю прийняттяp_j, $0 < p_j \leq, j \in [1, k]$. Де k- кількість різних маршрутів від D_S доM_S на графі з вершинами D_S, F_{S1}, F_{S2}, $F_{S3}F_{S4}$, F_{S5}, M_S і ребрами, які визначаютьсяпоточною топологією мережі . Розрахунок значень p_j буде розглянуто далі.

На відміну від модулів S_{MS}, які запускаються тільки в тих випадках,коли користувачеві необхідно здійснити передачу даних, модулі S_{MS}працюють постійно. Крім забезпечення процесу передачі, $S_{MS} \in F_{SI}$ черезінтервал τобчислює коефіцієнти m_{ir}таблиці маршрутизації$M_i \in F_{Si}, i \in [1, n], r \in [1, n]$.

Елементи m_{ir} визначаються наступним чином: $m_{ir} = 0$, якщо $i = r$ або F_{Si}недоступний з F_{Si} (сервер F_{Sr} фізично вийшов з ладу, втрачено зв'язок з F_{Sr}); $m_{ir} = 1$, якщо F_{Sr} доступний з F_{Si}.

Таблиця 1.1 –Маршрутизація для довірених серверів S_M

	D_S	F_{S1}	F_{S2}	F_{S3}	F_{S4}	F_{S5}	M_S
D_S	0	1	1	1	0	0	0
F_{S1}	1	0	0	0	1	0	0
F_{S2}	1	0	0	0	0	1	1
F_{S3}	1	0	0	0	1	1	0
F_{S4}	0	1	0	1	0	1	1
F_{S5}	0	0	1	1	1	0	1
M_S	0	0	1	0	1	1	0

1.3.2 Методика захисту інформації в бездротовій розподіленій мережі

Після опису системи в цілому проводиться розбиття її на великі фрагменти. Цей процес називається функціональної декомпозицією, а діаграми, які описують кожен фрагмент і взаємодія фрагментів, називаються діаграмами декомпозиції. Визначення контексту - побудова найбільш абстрактного рівня опису системи в цілому. Тому в рамках цієї діаграми під суб'єктом розуміється вся розроблена методика захисту інформації в цілому.

В якості входу - тобто об'єктів, які використовуються і перетворюютьсяфункціональним блоком для отримання результату, виступають об'єкти:

- дані;
- пакети даних і пакети інструкцій;
- бази даних;
- таблиці маршрутизації.

Характеристика цих об'єктів.

В якості виходу - тобто результату роботи системи виступають об'єкти:

- дані;
- пакети даних і пакети інструкцій;
- бази даних довірених серверів;
- таблиці маршрутизації;
- графи маршрутів;
- оцінки реалізації атак.

В якості СУБД для цієї бази була обрана СУБД MySQL 5.0. Ця СУБД має ряд корисних переваг для дослідника (Безкоштовність, невеликий розмір, мультиплатформеність, функціональність, а також зручність доступу, маніпуляції і представлення даних). для СУБД MySQL написано безліч клієнтських програм, за допомогою яких можна дуже швидко і наглядно провести обробку даних без написання програми.

В якості керування - тобто інформації, яка використовується в процесі виконання роботи, виступають об'єкти:

- топологія мережі;
- протоколи маршрутизації;
- розроблений алгоритм динамічної маршрутизації;
- розроблений алгоритм генерації потоку атак;
- контрольовані ділянки;
- таблиці маршрутизації;
- бази даних довірених серверів.

Механізми - ресурси, які виконують роботу.

- адміністратори;
- учасники;
- обладнання, канали зв'язку;
- довірені сервера;
- додаток «маршрутизації сервіс».

Після опису методики в цілому проводиться розбиття її на великі фрагменти. Цей процес називається функціональної декомпозицією, а діаграми, які описують кожен фрагмент і взаємодія фрагментів, називаються діаграмами декомпозиції. після декомпозиції контекстної діаграми проводиться декомпозиція кожного великогофрагмента системи на більш дрібні і так далі, до досягнення потрібного рівня подробиці опису.

1.3.3 Алгоритм динамічної маршрутизації трафіку

Розроблений алгоритм динамічної маршрутизації інформації врозподілених бездротових мережах який знаходиться в додатку Г, описується наступними етапами.

Крок 1. Обчислення елементів множин M і$F_S^{\text{дост}}$ docm в початковий момент часу $t0$.

Крок 2. Ініціалізація передачі. Під час отримання запиту S_{MC} наініціалізацію сеансу передачі даних виконати наступні дії:

2.1 запросити значення параметра f;

2.2 створити пакет інструкцій, що містить ip-адреса відправника, ip-адреса одержувача, значення f і розділ «довірені сервера»;

2.3 використовуючи операцію рандомізації, отримати псевдовипадкове число k;

2.4 провірити доступність F_{Sk}, якщо сервер недоступний - повернутися до п.2.3;

2.5 сформувати пакет даних і промаркувати його як пакет S_M;

2.6 відправити пакет даних і пакет інструкцій на довірений сервер F_{Sk},Якщо потрібно подальша передача даних - повернутися до п.2.5;

2.7 завершіть роботу S_{MC} ;

Крок 3. Динамічна маршрутизація на довіреному сервері F_{Si}:

3.1 переформіровать матрицю маршрутизації в разі, якщо різниця поточного часу і часу останньої зміни M_i більшеt. При отриманні пакетів S_M- перейти до п.3.2;

3.2. відкрити отриманий пакет інструкцій, в розділ «довірені сервера» додати ip-адреса F_{Si};

3.3. якщо кількість записів в розділі «довірені сервера» одно f ,відправити пакети даних, що відносяться до даного пакету інструкцій, на ip-адреса одержувача і повернутися на п.3.1;

3.4 використовуючи операцію рандомізації, отримати псевдовипадкове числоk;

3.5 провіритидоступність F_{Sk}, якщо сервер недоступний - повернутися до п.3.4;

3.6.провірити наявність інформації про F_{Sk},в розділі «довірені сервера»; якщо F_{Sk},присутній в даному розділі - повернутися до п.1.4; .

1.4 Аналіз методів захисту інформаціййної безпеки

1.4.1. Принципи організації захищеної перевірки цілісності

Для вирішення завдань забезпечення цілісності спостережливості і справжніності інформації застосовуються криптографічні контрольні суми. Методи формування криптографічних контрольних сум можна поділулити на два класи: на базі симетричних криптографічних перетворень (коди аутентифікації повідомлень (КАС)) і використовують несиметрчні перетворення (цифрові підписи) із застосуванням секретних ключів. Такі функції можуть застосовуватися як безпосередньо в якості криптографічної контрольної суми, так і в інших перетвореннях. Наприклад, для формування цифрового підпису необхідна ефективна функція відображення повідомлення в образ невеличкий фіксованою довжини (хеш-значення, хеш - код або просто хеш). Ці функції називають функціями хешуванням або хеш-функціями .

Розглянемо класифікацію функцій хешування.

Функцією хешування (в широкому сенсі) називається функція I, яка задовольнить мінімум двом вимогам.

1. Стиснення - функція h відображає вхідний повідомлення x дальності кінцевої довжини в хеш - значення y = h (x) невеликий фіксованіванною довжини, при цьому вхідний повідомлення будемо називати прообразом.

2. Простота обчислення - для заданої функції h і повідомлення x, h (x) обчислюється не вище ніж з поліноміальною складністю.

Функції хешування, що використовуються в криптографії, повинні заловільняти додатковим вимогам, які будуть розглянуті далі .

Всі існуючі функції хешування можна розділити на два великі класи : безключового хеш-функції, що залежать тільки від повідомлення, і хеш-функції з секретним ключем, що залежать як від повідомлення, так і від секретного ключа .

Підкласом безключового хеш-функцій є коди виявлення змін (modification detection codes, MDC-коди). У криптографії приміються специфічні підкласи MDC-кодів, які є однонаправлені-ними і біс колізійними хеш-функціями, які отримали широке розширення в системах цифрового підпису.

Функції вироблення кодів аутентифікації повідомлень (КАП) є підкласом ключових хеш-функцій і мають додатковим властивістю обчислювальної стійкості .

За використовуваним внутрішніх перетворень функції хешування можна розділити на:

- функції, які використовують бітові логічні перетворення. Ці функції застосовують до вхідного повідомленням побітові нелінійні операції "і", "або", "не", "виключає або" (XOR), різні зрушення і, як правило, є багато цикловими;

- функції, які використовують симетричні блокові кодери. Використовюється в основному для реалізації функцій вироблення КАС;

- функції, що використовують перетворення в групах, полях і кільцях з цілочисельним або поліноміальних базисом;

- функції, які використовують матричні перетворення.

Вимоги до застосовуваних в криптографії хеш-функцій

Аналіз умов застосування функцій хешування і практичного їх використання дозволив сформулювати вимоги, що пред'являються до премінених в криптографії бесьключевой хеш-функцій. Вони складаються в наступному:

1. Стійкість до обчислення прообразу - неможливість знаходження невідомого прообразу для будь-яких використовуються стандартні хеш - значень, тобто для заданої хеш-функції і обчислювально неможливо знайти невідомий прообраз x при попередньо заданому хеш - значення y = h (x) для будь-якого значення y. Під терміном "обчислювально неможливо" тут і далі будемо розуміти, що алгоритм, який виконує дане перетворення, володіє не менш ніж експоненційної складністю.

2. Стійкість до обчислення другого прообразу - неможливість надходження будь-якого іншого прообразу, який давав би таке ж хеш - значення, як і заданий, тобто для заданої хеш-функції h і прообразу x обчислювально неможливо знайти другий прообраз X'ФX , для якого виконувалося б умова h (x) = h {x ').

3. Стійкість до колізій - неможливість знаходження двох праобразів для яких вироблялося б однакове значення, тобто для заданої хеш-функції h обчислювально неможливо знайти два прообрази, для яких виконувалося б умова h (x) = h (x ').

Вимога стійкості до колізій є більш жорстким, ніж потреба стійкості до обчислення другого прообразу, так як передбачає довільний вибір двох прообразів.

Односпрямованої хеш-функцією називається функція h, задовольнив ряющий вимогам стиснення, простоти обчислення, стійкості до обчислення прообразу і стійкості до обчислення другого прообразу.

Бесколлізіонной хеш-функцією називається функція h, задовільняюча вимогам стиснення, простоти обчислення, стійкості до обчислення другого прообразу і стійкості до колізій.

На практиці зазвичай використовуються хеш-функції, які є одночасно бесколлізіоннимі і односпрямованим.

Однонаправлені хеш-функції можуть застосовуватися для вирішення других завдань, наприклад, вироблення ключів і псевдовипадкових чисел. Для використання в таких завданнях хеш-функція повинна відповідати таким вимогам

1. Відсутність кореляції - вхідні і вихідні біти не повинні корелювати, тобто зміна будь-якого вхідного біта призводить до великих непередбачуваних змін вихідних біт.

2. Стійкість до близьких колізій - для заданої однонаправленої функції h обчислювально неможливо знайти два прообрази , для яких хеш - значення h (x) і h (x') відрізнялися б на малу кількість біт.

3. Стійкість до часткової односпрямованість - обчислювально неможливо відновити будь-яку частину вхідного повідомлення так само, як і всі повідомлення. Більш того, по будь-якої відомої частини вхідного повідомлення обчислювально неможливо відновити частину (відновлення невідомих біт вимагає не менше ніж 2м операцій).

4. Можливість роботи в режимі розтягування - можливість обчислення хеш-функції при довжині вхідного повідомлення менше ніж довжина хеш - значення.

Вимога до застосовуваним в криптографії хеш-функцій з секретним ключем, наступне:

обчислювальна стійкість - неможливість знаходження хеш-значення для заданого повідомлення без відомого секретного ключа, тобто для заданий ключовий хеш-функції h і однієї або більше коректних пар прообразів і хеш -

значень і невідомому секретному ключі до обчислювально неможливо знайти іншу коректну пару.

Вимога обчислювальної стійкості передбачає виконання потреби стійкості ключа (по одній або більше коректних пар прообразів і хеш-значення обчислювально неможливо відновити секретний ключ к), однак, вимога стійкості ключа не передбачає виконання вимоги обчислювальної стійкості .

Функція хешування з секретним ключем h є функцією розробки КАП, якщо виконуються вимоги стиснення, обчислювальної простоти (при відомому сеансовому ключі) і обчислювальної стійкості.

Слід розрізняти функції вироблення КАП і односпрямовані хеш-функції з секретним ключем, що є частиною повідомлення, так як вони мають різні властивості. У функціях вироблення КАП секретний ключ застосовується до кожного блоку повідомлення, а в односпрямованих хеш-функціях ключ використовується префіксним (на початку повідомлення), постфіксним (в кінці повідомлення) або комбінованим методом, що знижує стійкості функції [14].

1.4.2 Критерії оцінки кудуючої послідовності

Для оцінки одержуючих псевдовипадкових послідовностей (ОСП) скористаємося статистичними критеріями оцінки [15].

Статистичними показниками розкиду результатів є середньо-квадратичне відхилення S і відносний показник розкиду результатів - коефіцієнт варіації

$$\bar{X}\frac{1}{n}\sum X_i \tag{1.11}$$

$$\sqrt{\frac{\sum(X-\overline{X})^2}{n-1}} \tag{1.12}$$

$$V = \frac{S}{X} * 100\% \tag{1.13}$$

де X- результат окремого визначення

$\bar{X}$ - середнє арифметичне всіх визначень

n - число визначень

S- середньоквадратичне відхилення

V- коефіцієнт варіації

Чим менше коефіцієнт варіації, тим вище відтворюваність результатів.

Статистичним критерієм правильності є середня арифметчна величина (X) і ступінь її відхилення від належного (номінального) значення.

Для статистичної оцінки правильності результатів рекомендується використовувати наступні критерії:

1) Відсоткове відхилення від заданої величини, що розраховується як відношення різниці величин (заданої і істинної) до заданої величині, показане в відсотках. У разі, якщо відсоткове відхилення від заданої ввеличини менше 3S, правильність результатів знаходиться в допустимих межах. Тут S - середньоквадратичне відхилення, що розраховується за формулою (1.12).

Крім того, порівняння досліджень можна проводити за наявністю стастатистичних зв'язки між ними. Для цього використовують кореляційний метод.

2) Кореляція вказує на ступінь зв'язку двох рядів чисел, тобтовивчається залежність між результатами двох методів.

Коефіцієнт кореляції розраховують за формулами:

$$r = \frac{\sum(X-\bar{X})\,(Y-\bar{Y})}{\sqrt{\sum(X-\bar{X})^2(Y-\bar{Y})^2}}, \tag{1.14}$$

або

$$r = \frac{n\sum XY-\sum X\sum Y}{\sqrt{n\sum X^2-(\sum X)^2}\sqrt{n\sum Y^2-(\sum Y)^2}}, \tag{1.15}$$

де X, Y- результати порівнюваних методів.

Про тісний кореляції можна говорити тільки в тому випадку, коли r маєзначення не нижче 0,9. Коефіцієнт кореляції нижче 0,7 вказує на слабкий зв'язок.

3) Критерій «хі-квадрат» є основним статистичним критерієм оцінки псевдовипадкових послідовностей. Розглянемо застосування методу. Нехай кожне спостереження може належати одній з категорій. Проводимо n незалежних спостережень. Нехай p_s - можливість того, що кожне спостереження відноситься до s, і нехай Ys – число спостережень, які дійсно відносяться до категорії s. Утворюємо статистику:

$$W = \sum_{s=1}^{k} \frac{(Y_s-np_s)^2}{np_s}, \tag{1.16}$$

або

$$W = \frac{1}{n}\sum_{s=1}^{k} \frac{(Y_s)^2}{P_S} - n, \tag{1.17}$$

Емпіричне правило говорить, що потрібно взяти на стільки великим, щоб всі значення n_{ps} були більше або дорівнюють п'яти.

Завершальний описχ^2критерію виглядає наступним чином:

Беремо досить велике число n незалежних спостережень. Визначається число спостереженьяке відноситься до кожної з k категорій і величину W відповідно до (1.16) і (1.17). Потім W порівнюється з табличним значенням при $u = k - 1$.Якщо Wменьше 1% точки або більше 99% точки, то ці числа відкидаються як недостатньо випадкові. Якщо W лежить між 1% і 5% точками або між 95% і 99% точками, то ці числа вважаються «подозрілими». В інших випадках приймаємо числа задовільно випадковими по χ^2критерію. Перевірка по χ^2критерію часто проводиться не менше 2-х разів з різними даними, і якщо, принаймні, 1 результат є підозрілим, то числа вважаються недостатньо випадковими.

1.4.3 Аналіз кодуючої функції

Зробимо аналіз можливих значень т, для цього досліджуємо пове¬деніе функції генерування ПСП залежно від даного коефіцієнта, для чого зафіксуємо ктах і Ко, відзначимо також що задана функція не залежить від довжини генеруємо послідовності L. Відзначимо також, що з огляду на нормування генератора щодо 0,5 $Kmax$ коефіцієнт m знаходиться около 2.

З огляду на, що послідовність повинна бути близька до випадкової, очевидно повинна виконуватися умова того що ймовірність появи 0 -і ймовірність появи 1 -повинні прагнути до величини 0,5. Очевидно, що в нашому випадку Ро і Р відповідають частотам появи відповідного знака в ПСП, таким чином

$$P(0) = \frac{n_0}{n}, P(1) = \frac{n_0}{n}, n = n_0 + n_1, \quad (1.18)$$

Задамо $K_{max} = 10^6, K_0 = 100{,}1 = 1000$ і будемо змінювати m. Побудуємо залежість поведінки $K(i)$і подивимося поведінку функції. Результат представимо в табл 1.2. і у вигляді графічної залежності зображено на рис 1.2

Таблиця 1.2 – Залежність P_0іP_1відm

m	*P\{m)*	*Рфп)*	*m*	*P\{m)*	*P_0(m)*
1	0	1	1,75	0,51	0,49
1,05	0,61	0,39	1,80	0,51	0,49
1,10	0,66	0,34	1,85	0,52	0,48
1,15	0,64	0,36	1,90	0,51	0,49
1,20	0,6	0,4	1,95	0,49	0,51
1,25	0,61	0,39	1,995	0,49	0,51
1,30	0,65	0,35	1,999	0,49	0,51
1,35	0,68	0,32	1,9995	0,51	0,49
1,40	0,72	0,28	1,99999	0,49	0,51
1,45	0,57	0,43	1,999995	0,49	0,51
1,50	0,54	0,46	2	0,5	0,5
1,55	0,53	0,47	2,0009	0,48	0,52
1,60	0,49	0,51	2,00095	0,13	0,87
1,70	0,51	0,49	2,001	0,01	0,99

Як бачимо з побудованої залежності при $m \to 1, m \to 2{,}01$ послідовність створюється на проміжку $1 < m < 1{,}6$ функція поводиться не достатньо випадково, тобто відхилення від математичного очікування 0,5 носить занадто значний характер. Таким чином, очевидно, що$m = \sqrt{1.62}$, отже, довжина даного діапазону: $Lm = 0{,}401$

Ми визначили діапазон для ключового поля m. Для визначення розміру даного ключового поля досить знати розрядність процесора, на якому будується даний пристрій, і визначити кількість регістрів відводимо для зберігання даного ключа.

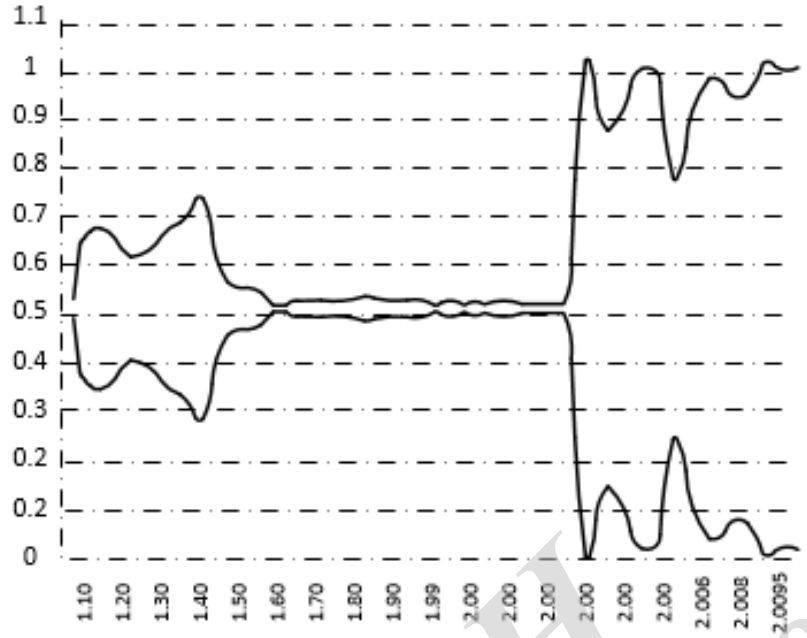


Рисунок 1.9 – Залежність $P_m(m)$і$P_0(m)$

Таким чином, з огляду на, що при зберіганні числа у форматі з плаваючою точкою на зберігання дробової частини відводиться 20 біт, отримаємо:

$$N_m = 2^{20} * L_m * R, \tag{1.19}$$

Де, Lm - діапазон можливих значень ключового поля $m.R$ - кількість регістрів виділених для зберігання ключа m.

1.5 Аналізметоду маршрутизації трафіку

1.5.1 Можливості взлому

Для оцінки ефективності розроблених методів захисту був обраний наступний підхід. Пропонується розбити всі типові мережеві атаки, яким може піддатися розроблена система на два класи: атаки на трафік між «суміжними» серверами і атаки безпосередньо на довірені сервера F_{si} Поняття «суміжності» визначається динамічно для кожного сеансу передачі, наприклад, «суміжними» є сервера F_{St}і F_{St+1}, обрані на i та i+1 етапі передачі, $t \in [1, n], i \in [1, f]$. У першому розділі були розглянуті основні види активних мережевих атак. Так, наприклад, атака «людина посередині» буде ставитися до першого класу, а DDoS-атака відповідно до другого класу.

1.5.2 Оцінка ймовірності реалізації загрози першого класу

Для оцінки ймовірності реалізації загроз першого класу уявімо, що порушник отримав несанкціонований доступ до єдиного фізичного каналу зі всіх каналів задіяних в системі і не має доступу до інших каналах. Тобто, він має можливість аналізу, блокування і модифікації всієї інформації, що передається по цьому каналу.

Обчислимо оцінку успішної атаки першого класуR_{A1}, коли порушник контролює ділянку між довіреними серверами F_{Sj} і F_{Sj-1}При невідомому просторовому розташуванні F_S вважаємо атаку успішною, якщо при роботі сервісу S_M сервера F_{Sj} і F_{Sj+1} були обрані на i та $i\ +\ 1$ етапі передачі, j є $[1, F]$, і є $[1, f]$

$$F_{A1} = \begin{cases} \frac{2}{F_{S0}^{\text{дост}}\left(F_{S0}^{\text{дост}}\right)} f = 2 \\ \frac{2}{F_{S0}^{\text{дост}}\left(F_{S0}^{\text{дост}}\right)} \sum_{i=1}^{f-2} \left[\left(\frac{2}{F_{S0}^{\text{дост}}-1} \cdot \frac{1}{F_{SO}^{\text{дост}}-1-i} \right) \cdot \left(\prod_{j=1}^{\prime} \frac{F_{S0}^{\text{дост}}-j-1}{F_{S0}^{\text{дост}}-j+1} \right) \right], f > 2 \end{cases} \quad (1.20)$$

Перша дужка визначає ймовірність вибору довірених серверів, між якими знаходиться контрольована ділянка на поточному етапі передачі, друга дужка - ймовірність того, що до поточного етапу передачі дані сервера ще не були жодного разу обрані.

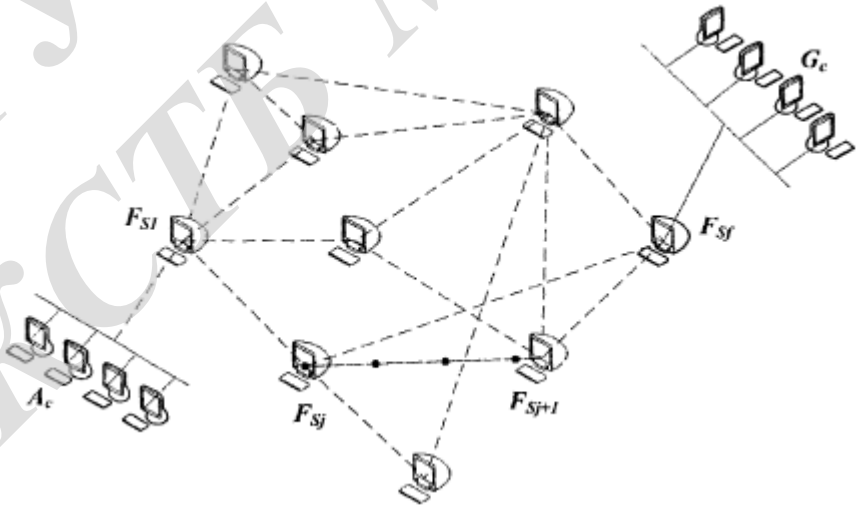


Рисунок 1.10 - Можливе подання бездротової розподіленої мережі з контрольованим порушником ділянкою $F_{Sj}F_{Sj+1}$.

Формула легко поширюється на випадок -подконтрольних порушнику ділянок між довіреними серверами.

Спробуємо обчислити порядок величини. Так, наприклад, при великих F, F_{Si}^{docm} і досить малому f, причому $F \gg f$ і $Fs\text{docm}F$ дана оцінка представляється у вигляді:

$$R_{A1} = O\left(\frac{1}{F^2}\right) \tag{1.21}$$

Наведене вище допущення описується так: всього довірених серверів - багато, недоступних серверів в певний момент часу - мало, використовуваних серверів для одного сеансу передачі від відправника до одержувача - мало.

1.5.3 Оцінка ймовірності реалізації загрози другого класу

Другий, більш широкий, клас атак представляється у вигляді ординарного потоку подій, тобто послідовності подій, що входять одна за одною у випадкові проміжки часу.

Позначимо, q - кількість успішно атакованих серверів в одиницю часу (інтенсивність). Тоді оцінка реалізації атак на -довірених серверів за час t описується розподілом Пуассона.

Розподіл Пуассона виникає в теорії потоків подій. Доведено, що для найпростішого потоку з постійною інтенсивністю q число подій, що відбулися за час t, має розподіл Пуассона з параметром$\lambda = q \cdot t$. Отже, ймовірність того, що за час t не відбудеться жодної події, дорівнює $(\text{e} - q * t)$, тобто функція розподілу довжини проміжку між подіями є експоненціальною.

Випадкова величина у має розподіл Пуассона, якщо:

$$P(y = y_0)\frac{\lambda^y e^{\lambda}}{y!}, y = 0,1,2, \ldots \tag{1.22}$$

де λ - параметр розподілу Пуассона, $P(\text{y} = \text{yo}) = 0$ для всіх інших у (при $y = 0$ позначено $0! = 1$).

Порахуємо ймовірність того, що за час t буде успішно атаковано m-довірених серверів (з -доступних):

$$R_{A2}(m,t) = \frac{\lambda^m}{m!}e^{-\lambda} = \frac{(q \cdot t)^m}{m!}e^{-(q-t)} \tag{1.23}$$

Значення q можливо оцінити за допомогою спеціальних Систем Виявлення Вторгнень (СВВ-сенсорів). СВВ-сенсори, вони займаються аналізом використання ввірених їм ресурсів і, в разі виявлення будь-яких підозрілих або просто нетипових подій, здатні робити деякі самостійні дії по виявленню, ідентифікації і усунення їх причин. Сенсори реєструють різні види мережевих атак на спостережувані сервера. Уявімо q як суму інтенсивностей кінцевого числа різних видів успішних атак, наприклад, таких як, спуфинг, «людина посередині», флуд, DDos. Таким чином,

$$R_{A2}(m,t) = \frac{\lambda^m}{m!} e^{-\lambda} = \frac{(q \cdot t)^m}{m!} e^{-(q-t)} \quad (1.24)$$

де p_i- ймовірність успіху атаки і-го виду, h_i- кількість атак і-го виду,$i \in [1,k]$.

1.5.4 Алгоритм генерації потоку атак

Для даного алгоритму задаються наступні параметри.

$F_S = \{ F_{S1} F_{S2}, \dots, F_{Sj}, \dots, F_{SF})$ - безліч довірених серверів мережі.

$F =_{|F_S|}$ - кількість довірених серверів мережі.

t_a- час дії одного виду атаки на довірений сервер.

u_1 - період затримки атаки.

u_2- період блокування довіреної сервера.

k- число видів атак.

i, j, t- допоміжні змінні.

Вводяться такі функції і процедури.

ТекЧас () - функція, яка повертає поточний час в форматі «dd.mm.yyyyhh24: mi: ss».

ГенВип (x) - функція, що генерує псевдовипадкове ціле число за допомогою операції рандомізації, що належить інтервалу [1; x], x> = 1;

Розблок (F_j)- процедура, яка переводить сервер F_jрежим «доступний».

$A_i(F_j)$ - функція розподілу дискретної випадкової величини «результат атаки на сервер F_j» з ймовірністю прийняти значення 1 (атака успішна) дорівнює p_Iі ймовірністю прийняти значення 0 (атака невдача) дорівнює 1 - p.

Пауза (t) - процедура, яка реалізує Ожина на час t;

СкладСерв (F_j)- функція, яка повертає статус сервера F_j (доступний - 0; блокований - 1);

Блок (F_j, x) - функція, яка переводить сервер F_J в режим «блокований» і повертає поточний час в форматі «dd.mm.yyyyhh24: mi: ss» змінну x.

Блок-схема моделює вплив потоку атак на довірені сервера у додатку Е

З допомогою операції рандомізації вибираються один з довірених серверів мережі і мережева атака одного з видів. Проводиться експеримент $A_t(F_{Sj})$- «атака на серверF_{Sj}», який визначається дискретною випадковою величиною з розподілом «ймовірність прийняти значення 1 (успіх) дорівнюєpi , ймовірність прийняти значення 0 (невдача) дорівнює$1 - p_t$, $i \in [1, k]$. У разі успіху, сервер блокується і стає недоступним на час u_2.

Відносно уразливості до основних видів атак довірений сервер нічим не відрізняється від звичайного сервера розподіленої мережі, до якого порушник спочатку не має доступу. Для успішної атаки на довірений сервер порушника може скористатися наступними уразливими: недокументовані помилки в операційній системі сервера, помилки в допоміжних програмах, помилки адміністрування сервера. Різні види вразливостей призводять до можливості реалізації різного роду погроз: втрати конфіденційності, атакам типу «відмова в обслуговуванні», виконання на сервері неавторизованого коду і тд. Чим більше вразливостей, тим простіше провести атаку на сервер. Відповідно, можна ввести деякий коефіцієнт уразливості серверів$\varphi_j \in F_j, j \in [1, n], 0 < \varphi_j \leq 1$.

Тоді ймовірність реалізації атаки -го виду на сервер F з коефіцієнтом уразливості φз оцінки можна представити у вигляді:

$$p_t = \varphi \cdot p_{0l} \tag{1.25}$$

де p_{0i}- ймовірність успіху атаки і-го виду, що залежить тільки від ступеня підготовленості порушника і використовуваних ним коштів.

Довірені сервера мережі, які є об'єктами системи «маршрутизації сервіс» S_M, знаходяться в зонах відповідальності різних адміністраторів, наприклад, фізично в різних містах або країнах. Звичайно, кожен адміністратор намагається налаштувати сервери найкращим чином. Але на ділі на ф впливають не врахованіспочатку фактори: завдання керівництва - запустити на сервері додаткові служби або відкрити додаткові порти, професійні навички нового адміністратора та ін. Наведені аргументи підтверджують факт, що можна розглядати як самостійну змінну в формулах.

Оцінці значень POI і щ можна присвятити окреме дослідження, яке було б корисно автору даної роботи.

Головна перевага системи «маршрутизації сервіс», яке варто відзначити, підбиваючи підсумок дослідження активних атак другого класу на довірені сервера, - стійкість системи до блокування порушником одного або декількох довірених серверів. Завдяки розробленому алгоритму динамічної маршрутизації система не очікує відновлення працездатності недоступних довірених серверів, а динамічно перебудовує маршрут прямування трафіку. Слід також скасувати, що весь маршрут не відомий спочатку, ніхто не знає він і при попаданні даних на перший довірений сервер. Кожен з довірених серверів «самостійно» вибирає наступний сервер для передачі даних.

1.6 Реалізація програмного комплексу

Для програмної реалізації описаної системи були обрані технології Visual Basic Script і Windows Manadgement Instrumentarium. Мова VBScript - зручний засіб для автоматизації дій з обробки даних, управління системою, взаємодії з офісними додатками, роботи з базами даних і мережевими службами в системах сімейства Windows. VBS-сценарій є об'єктно-орієнтованою мовою програмування, тобто основною концепцією є поняття об'єктів і класів. Відзначимо гідності VBS-сценаріїв, які зіграли головну роль при виборі даної мови програмування для реалізації прототипу системи: сценарії не вимагають компіляції та їх код будь-який момент можна відредагувати; VBS-сценарії практично не обмежені у функціональності і можуть використовувати різні системні бібліотеки та об'єкти інших додатків

Інструментарій управління Windows (WMI) є відкритою системою інтерфейсів доступу до будь-яких параметрах операційної системи, пристроїв і додатків, які функціонують в ній. Він дозволяє представити дані операційної системи у вигляді об'єктів і їх властивостей і методів. Для звернення до ресурсів WMI найбільш використовуваним мовою програмування є VBScript.

Пропонована в роботі схема програмного комплексу «маршрутизації сервіс» містить чотири основні блоки. Кожен блок виконує певне функціональне призначення.

1. Блок RD - з потоку IP-пакетів виділяє пакети з маркером SM- Передає ці пакети блоку SD;

2. Блок SD - база даних, містить відомості про пакети SM, оброблених довіреною сервером FSl, / е [l; F]. У разі необхідності буферизирует пакети даних.

3. Блок AD - аналізує пакети даних і інструкцій, прийняті від блоку SD, додає інформацію про поточний довіреному сервері F_{Si},$i \in [1; F]$в пакет інструкцій. Передає блоку MD команди на передачу даних і трасування

довірених серверів, формує таблицю маршрутизації$M, \in F, i \in [1; F]$. Отримує від SD інформацію про нові довіренихсерверах, що з'явилися в мережі.

4. Блок MD - відправляє черговий пакет на один з обраних довіренихсерверів або в пункт призначення.

2 РОЗРОБКА МЕТОДІВ АУТЕНТИФІКАЦІЇ І РОЗМЕЖУВАННЯ ДОСТУПУ

Дана глава присвячена розробці методів аутентифікації. У розділі будуть представлені розроблені алгоритми посиленою аутентифікації користувачів, описані механізми розмежування доступу в розробленій операційній системі. Також будуть описані принципи побудови систем розмежування доступу.

2.1 Моделі розмежування доступу

Підсистема розмежування доступу до ресурсів є однією з основних частин будь-якої багатокористувацької системи. Навіть при самому зневажливе ставлення до безпеки даних в системі, розробник операційної системи обмежує доступ користувачів до ресурсів ядра операційної системи.

Недоторканність ресурсів ядра відіграє чималу роль в стабільності роботи операційної системи. З вищесказаного випливає, що навіть при відсутності в системі будь-яких засобів забезпечення безпеки даних, операційна система все одно має в своєму складі хоча б мінімальну підсистему розмежування доступу користувачів до даних.

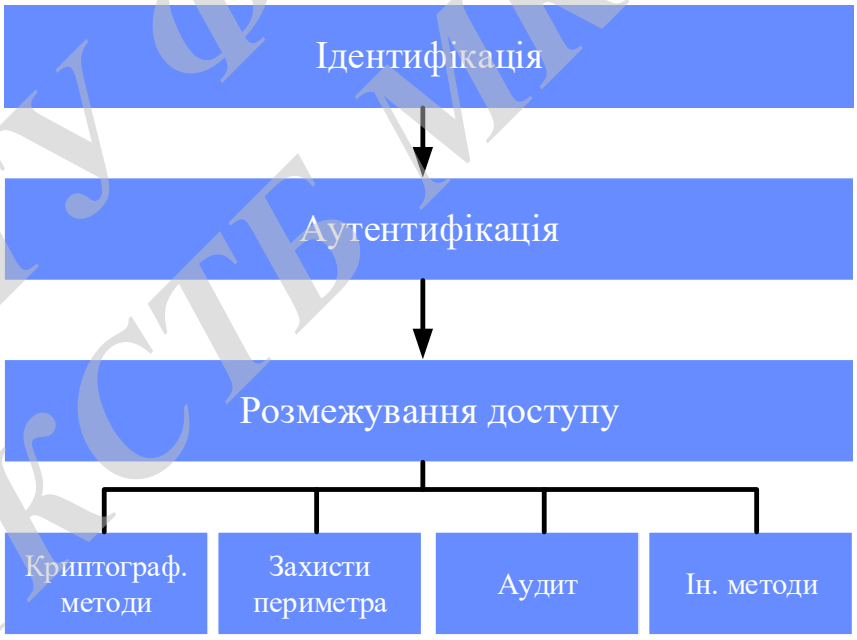


Рисунок 2.1 - Структура системи захисту від загроз порушення конфіденційності

Для ефективної роботи будь-якої системи захисту інформації необхідно чітко визначити суб'єкти і об'єкти доступу. Об'єкт доступу — одиниця

інформаційного ресурсу АС, доступ до якої регламентується правилами розмежування доступу. [7]. Суб'єкт доступу ─ особа або процес, дія якого регламентується правилами розмежування доступу [7]. Об'єктами доступу операційної системи є: файлові об'єкти, процеси, об'єкти пам'яті, периферія. Всі об'єкти розмежування доступу в операційній системі мають свій унікальний ідентифікатор (для об'єкта оперативної пам'яті - унікальна адреса, для периферії - унікальний дескриптор, і т.д.). Щоб сформувати чіткі правила розмежування доступу до об'єктів, необхідно однозначно визначити суб'єкти доступу. На рисунку 2.1 зображено структура системи захисту від загроз порушення конфіденційності. Процес визначення суб'єкта доступу починається з ідентифікації і перевірки автентичності. В ході процесу ідентифікації буде визначено суб'єкта доступу. В операційній системі буде створений унікальний ідентифікатор користувача.

Якщо користувачами операційної системи стає більш ніж один суб'єкт, виникає необхідність в прозорому, універсальному механізмі розмежування доступу до ресурсів системи.

Модель систем дискреційного розмежування доступу. Дана модель характеризується розмежуванням доступу між пойменованими суб'єктами і об'єктами. Кожен суб'єкт, який має певне право, може делегувати його іншому суб'єкту. Доступ суб'єкта до об'єкта визначається кінцевим безліччю можливих операцій. Для кожної трійки об'єкт-суб'єкт-операція в системі строго визначено правило. Дана система може бути реалізована у вигляді матриці доступу. Стовпці і рядки цієї матриці описують відповідно безліч суб'єктів і об'єктів. В осередках даної матриці вказується тип дозволеної операції. Щонайменше, є два підходи до побудови дискреційного управління доступом: кожен об'єкт системи має прив'язаного до нього суб'єкта, званого власником. Саме власник встановлює права доступу до об'єкта; система має одного виділеного суб'єкта адміністратора, який має право встановлювати права володіння для всіх інших суб'єктів системи.

Мандатний управління доступом. Для реалізації цього принципу кожному суб'єкту і об'єкту повинні зіставлятися спеціальні мітки (мандати). Кожен об'єкт має рівень конфіденційності, а кожен суб'єкт має відповідно рівень доступу. У мандатної системі розмежування доступу має бути реалізовано два основних правила: «немає запису вниз» суб'єкту заборонено писати в об'єкт, якщо рівень доступу суб'єкта вище рівня конфіденційності об'єкта; «немає читання вгору» суб'єкту заборонено читати об'єкт, якщо рівень доступу суб'єкта нижче рівня конфіденційності об'єкта.

Рольове розмежування. Основною ідеєю управління доступом на основі ролей є ідея про зв'язуванні дозволів доступу до ролей, котрі призначаються

кожному користувачеві. Дана модель розмежування доступу, дуже зрозуміла людині. В інших сферах діяльності людини часто зустрічаються ролі (працівник-начальник, студент-викладач і т.д.). Кожна роль має свій строго певний набір прав доступу до об'єктів. Як правило, даний підхід застосовується в системах захисту СУБД, а окремі елементи реалізуються в мережевих операційних системах.

2.2 Контроль і управління доступом

У розробленій операційній системі контроль і управління доступом представлений двома підсистемами: підсистемою аутентифікації і системою контролю доступу до файлової системи. Застосування концепції «все є файл» дозволило значно уніфікувати підходи розмежування доступу до файлових об'єктів, оперативної пам'яті і апаратним пристроям.

Підсистема аутентифікації в розробленій операційній системі грає одну з важливих ролей. У підсистемі аутентифікації ОС реалізований цілий ряд функцій:

1. аутентифікація локальних користувачів;
2. аутентифікація віддалених користувачів.

Підсистема аутентифікації є набором бібліотек, які використовуються для проведення процедур аутентифікації. Прототипом структури підсистеми аутентифікації послужила застосовується в операційних системах сімейства Linux архітектура PAM (Pluggable Authentication Modules - модулі аутентифікації).

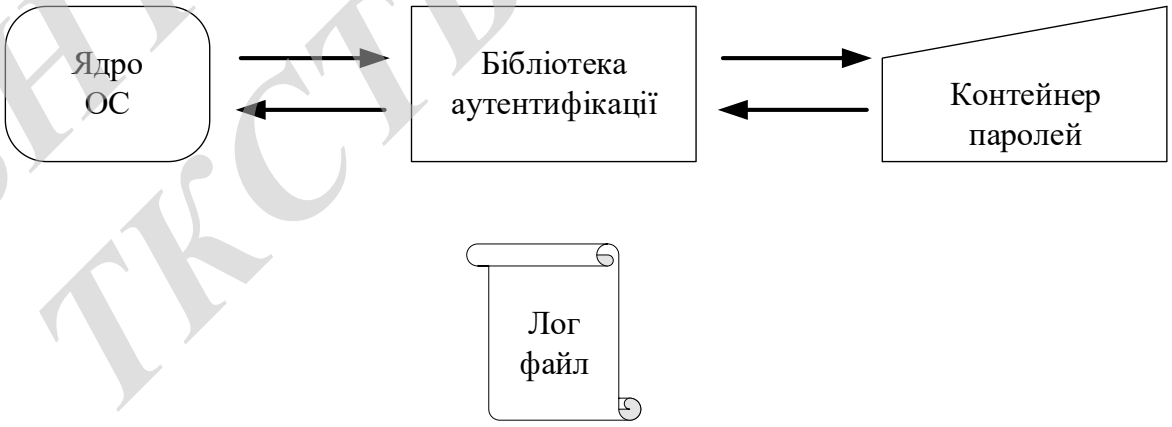


Рисунок 2.2 - Підсистема аутентифікації користувачів

Підсистема аутентифікації локальних користувачів (рисунок 14) забезпечує класичну аутентифікацію користувачів з використання

багаторазових паролів. Є можливість налаштування параметрів пральний політики: довжини пароля; алфавіту пароля; умов блокування користувачів.

Будь-які операцій аутентифікації і зміни аутентифікаційних даних користувачів пишуться в системний журнал. Для захисту користувачів від примушує атаки в операційній системі був розроблений алгоритм аутентифікації користувачів із захистом від примушує атаки.

Далі запропонований алгоритм захисту користувачів від примушує атаки в процесі аутентифікації в ОС. Для захисту користувача від примушує атаки в ОС генерується додатковий набір аутентифікаційних даних. При цьому для захисту користувачів було вибрано досить просте і ефективне рішення.

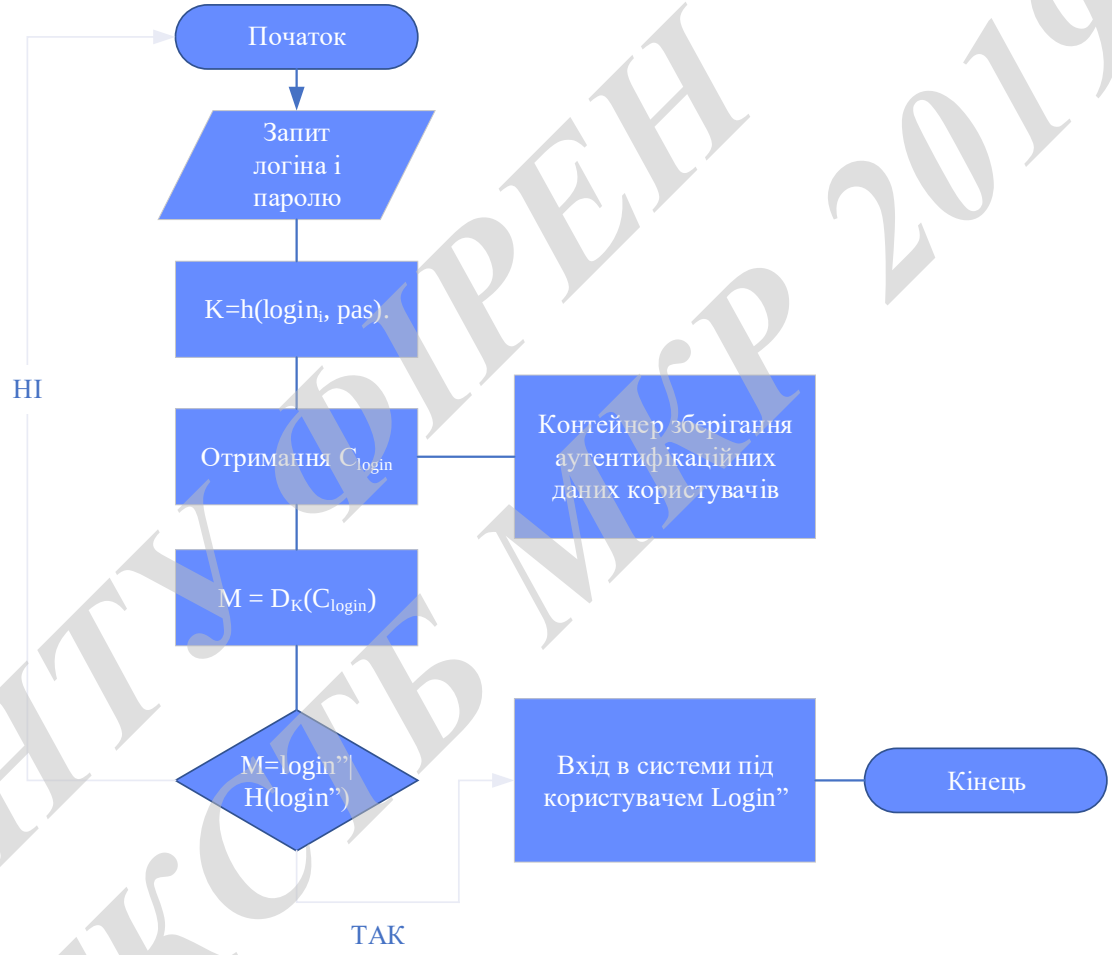


Рисунок 2.3 - Блок-схема процесу аутентифікації локальних користувачів

Для цього вибирається ім'я два імені користувача зі схожою назвою (наприклад, user1 і userl). Один користувач має необхідні права в системі. Другий користувач має мінімальні права. У разі введення резервного пароля (при примушує атаці) буде виконаний вхід обмеженим користувачем.

Алгоритм аутентифікації користувачів із захистом від примушує атаки зображений на блок-схемі (рисунок 2.3).

Процес аутентифікації полягає в наступному:

1. запросити у користувача логін і пароль;

2. обчислити ключ шифрування як хеш-значення логіна і пароля;

3. витягти зі сховища шифртекст, відповідно до логіном користувача;

4. розшифрувати повідомлення ключем, отриманим на кроці 2;

5. якщо повідомлення складається з login "(можливо відмінного від введеного) і хеш-значення отриманого login" (для перевірки результату), то вхід в систему під користувачем login ", інакше перехід до кроку 1.

При введенні резервного пароля буде розшифровано значення резервного логіна і користувач зайде під користувачем з усіченими правами. Метод захисту: метод парольної аутентифікації з захистом від примушує атаки. Відмінні риси: захист від примушує атаки, можливість застосування в будь-яких призначених для користувача ОС (орієнтованість на архітектуру PAM).

У розробленій операційній системі передбачена можливість віддаленого доступу. На додаток до стандартних багаторазовим паролів в ОС передбачена аутентифікація з використанням одноразових паролів.

Найбільш популярний протокол аутентифікації на одноразових паролів S / KEY описаний в стандарті інтернету RFC1760. Даний протокол заснований на хеш-функції MD4. У розробленій операційній системі застосований протокол одноразових паролів, додатково посилений заперечує шифруванням, запропонованим в [68], що дозволяє протидіяти змушує атаці. Алгоритм працює за клієнт-серверної схемою.

Далі проводиться операції "виключне АБО" значень P і S. Обчислення тимчасових паролів проводяться за такими формулами:

$$K_N = h(PxorS), \text{для } N = 1,$$

$$K_N = h(K_{N-1}), \text{ для } N > 1 .$$

Так генеруються 2 списки з N паролів, при цьому для кожного списку вектор ініціалізації також повинен бути унікальний.

Для створення файлу криптографічних значень для N одноразових паролів вибираються 2N випадкових значень. Додатково вибирається випадкове значення першого криптографічного значення C.

$$M_N = h(ID)|R_{1N}, \bar{M}_N = h(ID)|R_{2N};$$

$$K = R_{1(N-1)};$$

$$C_N = \left[{M_N}^{K_{11}} K p_2 (p_2^{-1} mod p_1) + {\bar{M}_N}^{K_{21}} K p_1 (p_1^{-1} mod p_2)\right] mod p_1 p_2.$$

Для отримання останнього криптографічного значення C використовується наступні формули:

$$M_1 = h(ID)|R_{12}, \bar{M}_1 = h(ID)|R_{22};$$

$$K = K_0;$$

$$C_1 = \left[{M_1}^{K_{1N}} K p_2 (p_2^{-1} mod p_1) + {\bar{M}_1}^{K_{2N}} K p_1 (p_1^{-1} mod p_2)\right] mod p_1 p_2.$$

На стороні клієнта зберігаються:

1. Перелік з 2N паролів;

2. парольний фраза і 2 вектора ініціалізації (якщо необхідна генерація паролів).

Використання одноразових паролів починається з останнього пароля (). На стороні сервера зберігаються:

1. файл криптографічних значень (містить N криптографічних значень);

2. номер поточного пароля користувача;

3. значення простих чисел;

4. тимчасовий загальний ключ.

Для дешифрування перевірочного повідомлення необхідно обчислити наступні значення.

$$M = (CK^{-1})^{K_{1N}^{-1}} \; mod \; p_1$$

$$\bar{M} = (CK^{-1})^{K_{2N}^{-1}} \; mod \; p_2$$

У первісному стані тимчасовий ключ, а номер поточного пароля - 1. Для перевірки одноразового пароля сервер робить дешифрування криптографічного значення за такою формулою.

$$M_1 = (C_1 K^{-1})^{K_{1N}^{-1}} \; mod \; p_1$$

Варто зауважити, так як сервер не має відомостей, який серії користувач надав пароль (або), серверу необхідно спробувати дешифрувати значення, використовуючи і просте число.

$$M_1 \neq (C_1 K^{-1})^{K_{1N}^{-1}} \, mod \, p_2$$

В даному випадку сервер не зможе дешифрувати перевірочне повідомлення. Для перевірки правильності перевірочного повідомлення сервер порівнює перші 256 біт перевірочного повідомлення з обчисленим значенням В разі вдалої аутентифікації в якості тимчасового загального ключа приймається розшифроване значення (таким чином, проводиться зав'язка послідовності паролів).

У разі якщо користувач передасть сервера пароль, перевірка справжності пройде успішно. Однак в якості тимчасового загального ключа буде прийняте невірне значення (а точніше значення) і наступний пароль (або) буде визнаний неправильним.

Аналіз ефективності застосування в мобільній ОС. Метод захисту: Спосіб застосування отрицаемого шифрування в системах аутентифікації на одноразових паролів.

Відмінні риси: захист користувача від примушує атаки, можливість реалізації у вигляді генераторів паролів і пральних карток (заздалегідь згенерованих).

2.3 Сервіс контролю доступу до файлової системи

У роботах [7 - 9] представлені системи контрольованого розмежування доступу до файлів. Ієрархічна структура файлової системи є ідеальним об'єктом застосування моделей розмежування доступу.

Для забезпечення контролю доступу до ресурсів в операційній системі передбачено кілька різних механізмів. Одним з таких механізмів є спеціалізований сервіс доступу до файлової системи. Дана системна служба надає користувачам можливості доступу до файлової системи. Звичайно, використовуючи функції динамічної бібліотеки, прикладне програмне забезпечення також може одержати високошвидкісний доступ до файлів. Однак для здійснення процесу запису в файл процесу необхідно зарезервувати достатньо великий обсяг оперативної пам'яті (близько 2 кілобайт). Для процесів, які не можуть дозволити собі таке марнотратство (в умовах мобільної системи це більшість процесів) і існує служба доступу до файлової

системи. Дана служба має схожу будову з сервісом криптопровайдера, який був розглянутий раніше. На рисунку 2.4 зображено структурну схему служби доступу до файлової системи.

Служба доступу до файлової системи складається з двох основних блоків: ядра служби, яке виконує запити прикладних процесів (в ядро входить чергу запитів на виконання операції); таблиці доступу.

Ядро служби забезпечує чергове виконання завдань процесів на операції доступу до файлової системи. Черговість виконання операцій може бути заснована на пріоритетах процесів в операційній системі. В якості критерію черговості, в залежності від налаштувань операційної системи, можуть бути використані і інші регулярні змінні.

Таблиця доступу являє собою матрицю, в якій відбивається взаємозв'язок номера процесу операційної, об'єкта доступу (посилання на файл), методу доступу (запис, читання, і т.д.) і час останнього доступу. Дана таблиця заповнюється ядром сервісу в міру звернення прикладних процесів до новим файловим об'єктам (функція fopen).

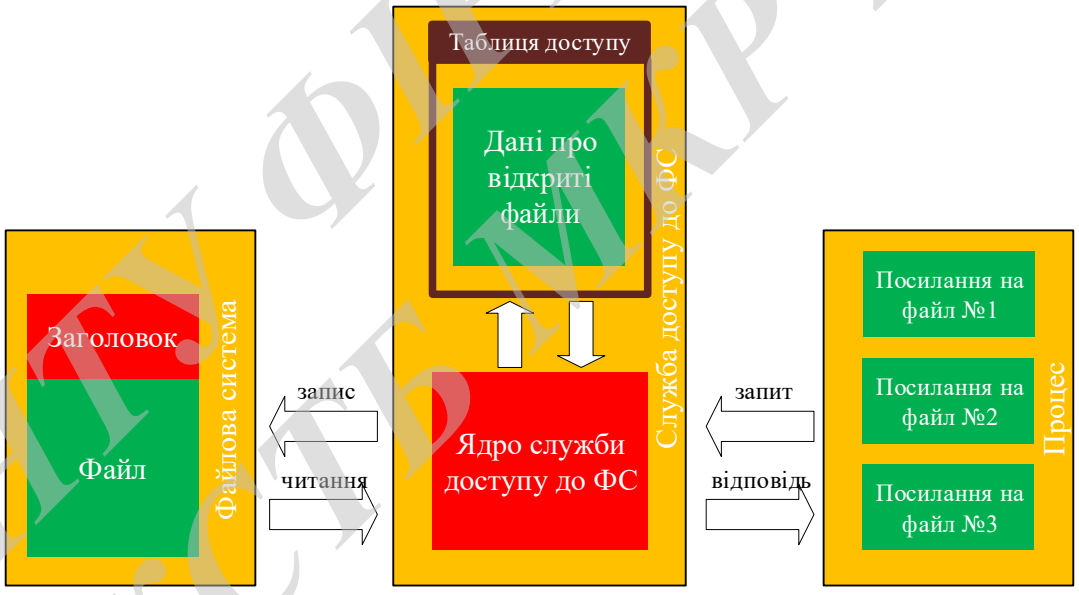


Рисунок 2.4 - Структурна схема служби доступу до файлової системи

Сервіс контролю доступу до ФС забезпечує:

- оптимізацію зайнятої оперативної пам'яті (в процесі аналізу "Кинутих файлів");

- аналіз наслідків аварійного завершення роботи операційної системи (в залежності від настройки ОС таблиця доступу може писатися в незалежну пам'ять і при аварії таблиця залишиться неушкодженою);

- забезпечення безпеки (аудит процесів доступу до файлів, робота сенсорів системи виявлення вторгнення).

До додаткових функцій сервісу доступу до файлової системи відноситься:

- забезпечення доступу до криптографічних функцій для виконання операцій над захищеними файлами;

- уніфікація доступу до файлової системи.

Метод захисту: сервіс контролю доступу до файлової системи. Відмінні риси: ефективний розподіл ресурсів, прозорі правила розмежування доступу (діскреціонное розмежування), виконує роль СЗІ від НСД мобільної ОС (так як в системі застосовується принцип "все є файл"), уніфікація методів доступу до ФС.

2.4 Висновки до розділу 2

У цьому розділі була розглянута підсистема розмежування доступу, яка є найбільш важливою в складі операційної системи. Було розглянуто таке поняття як користувач системи (як особливий вид суб'єкта доступу). Далі була описана універсальна модель розмежування доступу, яка включає в себе процеси ідентифікації, аутентифікації і ін.

Було проаналізовано ефективність алгоритмів аутентифікації, що застосовуються в операційних системах. З метою підвищення ефективності функціонування підсистеми були розроблені: алгоритм аутентифікації користувачів системи, спосіб аутентифікації на одноразових паролів, які забезпечують захист від атак з примусом.

В цьому розділі вирішені наступні завдання дослідження: розробка методу аутентифікації користувачів, стійкого до принуждающим атакам.

3 РОЗРОБКА МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ ПРИ ЗБЕРІГАННІ ТА ПЕРЕДАВАННІ В БЕЗПРОВІДНИХ МЕРЕЖАХ

Даний розділ присвячений розробці методів захисту інформації, що зберігається і переданої інформації, стійких до атак з примусом користувача розкрити ключ захисного перетворення. До завдань даного розділу також входить виділення і аналіз ефективності методів захисного перетворення інформації, що застосовуються в операційних системах. Будуть описані розроблені методи захисного перетворення інформації.

3.1 Методи захисного перетворення інформації в ОС

В сучасних операційних система криптографічні методи захисту інформації використовуються повсюдно. Існує велика кількість реалізованих алгоритмів [74]. Для простого і уніфікованого доступу до криптографічних функцій в операційній системі реалізується спеціалізований модуль. В даному модулі (модуль іноді називають криптопровайдером) реалізуються різні криптографічні функції. Решта підсистеми операційної системи можуть використовувати криптопровайдер на свій розсуд. В рамках криптопровайдера класично реалізуються наступні криптографічні алгоритми.

Алгоритми симетричного шифрування. Алгоритми шифрування даної категорії відрізняються високою продуктивністю. Ця властивість робить симетричне шифрування вкрай ефективним при обробці великої кількості даних (наприклад, при прозорому шифруванні на магнітному диску).

Симетричне шифрування має незаперечний недолік ─ один ключ для шифрування і розшифрування. На перший погляд очевидним рішенням даної проблеми є застосування двохключового (асиметричних) алгоритмів шифрування. Однак асиметричне шифрування має порівняно низьку продуктивність і при цьому воно має досить високу обчислювальну складність. Саме з цієї причини асиметричне шифрування вкрай рідко реалізується в крітопровайдерах.

Для компенсації недоліків симетричного шифрування в криптопровайдера найчастіше використовують алгоритми обміну ключовою інформацією. Такі алгоритми також іноді називають алгоритмами створення спільного ключа обміну. До таких алгоритмів відноситься протокол Ді ФФІ-Хеллмана (протокол описаний в [75]). Даний протокол дозволяє створити однаковий ключ обміну у двох абонентів. Загальний ключ обміну обчислюється з відкритого ключа віддаленого абонента і власного закритого ключа. Після генерації загального ключа шифрування з'являється можливість

для обміну з використанням швидкісних симетричних шифрів. Вищевказана схема (застосування протоколу генерації загального ключа спільно з симетричним шифруванням) найчастіше застосовується в сучасних засобах криптографічного захисту інформації. Прикладом вдалого комбінування асиметричних і симетричних протоколів може служити протокол "безпечного перехідника" SSL (secure socket slayer) [76]. Даний протокол застосовується в web-браузерах, і комбінує в собі комбінацію протоколів RSA і DES або RSA і потрійний DES.

Зберігання ключової інформації. Безпечне зберігання ключів в операційній системі є важливою завдань підсистеми захисту ОС. В процесі експлуатації криптографічних протоколів іноді доводиться проводити процедуру зміни (оновлення ключової інформації). Необхідність зміни ключів може бути викликана різними причинами: закінчився термін дії ключової інформації; ключова інформація скомпрометована.

Нерідко для забезпечення безперервності захищеної взаємодії між учасниками інформаційного обміну застосовується резервування ключової інформації. Для цього на етапі розподілу ключів формуються кілька комплектів ключів. Сторони домовляються про номер (серії) застосовуваного ключа. В даній схемі важливо захистити резервні ключ (наприклад, зашифрувавши резервні ключі додатковим ключем). Варто помітити, що отримання резервної ключової інформації і серії активного ключа може бути метою зловмисника.

Алгоритми хешифрування. Алгоритми хешіфрованія є алгоритм перетворення інформації, які дозволяють виявити будь-які зміни в вихідному файлі. Вимоги до хеш-функції:

- неможливість фабрикації (високу складність підбору повідомлення із заданим значенням хеш);

- неможливість модифікації (незначні зміни в вихідному файлі повинні призводити до значної зміни значення хеш);

- односпрямованість (хибність обчислення вихідного повідомлення по заданому значенню хеш);

- стійкість до колізій (складність знаходження пари повідомлень з одним значенням хеш);

- стійкість до знаходження другого прообразу (складність знаходження другого повідомлення з тим же значенням хеш за наявною парі повідомлення - хеш).

Алгоритми електронного підпису. Алгоритми електронного підпису є криптографічні алгоритми, що дозволяють забезпечити механізми перевірки

автентичності та автентичності повідомлень. В основі алгоритмів електронного підпису лежить асиметричне шифрування.

Алгоритми генерації випадкових чисел. Алгоритми генерації випадкових чисел з певними параметрами є важливою частиною системи криптографічного захисту інформації. Найменша передбачуваність в алгоритмі генерації ключової інформації може стати передумовою до атаки на ключову систему. У деяких криптографічних алгоритмах (наприклад, в алгоритмах асиметричного шифрування) необхідно згенерувати випадкове число великого розміру, яке відповідає властивостям простоти. В [77] виділяються наступні основні підходи до генерації випадкових чисел:

- програмна генерація, яка передбачає обчислення чергового псевдослучайного числа як функції поточного часу, послідовності символів, введених користувачем, особливостей його клавіатурного почерку;

- програмна генерація, заснована на моделюванні якісного генератора псевдовипадкових кодів з рівномірним законом розподілу;

- апаратна генерація з використанням фізичних величин (шум радіо ефіру, фізичні характеристики напівпровідників в нестандартних режимах). Заперечується шифрування. Під поняттям отрицаемого шифрування розуміється спосіб криптографічного перетворення, в якому зашифровуються спільно два або більше різних повідомлень на двох чи більше різних ключах, і обгрунтовується принципова можливість реалізувати таких перетворень [68]. Для знаходження пар ЯЗАТИСЯ-КЛЮЧ для функції шифрування F, таких щоб вони мали ідентичну криптограму C, необхідно вирішити наступну систему рівнянь.

$$\begin{cases} F(K_1, C) = M \\ F(K_2, C) = \bar{M} \end{cases},$$

де ключі шифрування; повідомлення; функція шифрування; криптограма.

У концепції заперечується шифрування розглядається мета забезпечення досить високої стійкості до принуждающим атакам. У моделі таких атак передбачається, що атакуючий має деякий ресурс впливу на відправника, одержувача або зберігача криптограми, що примушує останнього уявити ключ розшифрування криптограми. Стійкість до атак з примусом забезпечується тим, що, по крайней мере, одне з зашифрованих повідомлень не є секретним і атакуючому надається ключ, за яким розшифрування криптограми призводить до розкриття цього повідомлення.

При цьому процедура розшифрування виконується таким чином, що у атакуючого немає обґрунтованих доводів, які він міг би привести на користь

твердження, що з криптограмою пов'язані ще якісь інші повідомлення. [68] Аналіз ефективності застосування в мобільній ОС. Метод захисту: спосіб заперечується шифрування "підбір пари ПОВІДОМЛЕННЯ-КЛЮЧ". Рівень ефективності: середній.

Переваги: захист від примушує атаки, не відрізнятись від застосовуваного алгоритму шифрування.

Недоліки: вкрай низька продуктивність алгоритму. Метод захисту: Спосіб зберігання резервних серій ключів. Рівень ефективності: середній. Переваги: відсутня необхідність використання протоколів розподілу ключів. Недоліки: необхідність вирішувати питання зберігання ключової інформації.

3.2 Криптографічна підсистема

Для того щоб в операційній системі була можливість повсюдно застосовувати криптографічні алгоритми, в ОС було необхідно реалізувати функціональну і гнучку криптографічний підсистему. Ця підсистема надає користувачам (підпрограм, рубрик та розділів сайту) цілий комплекс криптографічних алгоритмів.

Криптографічний підсистема ОС представляє комплекс з двох механізмів. Колективна бібліотека криптографічних функцій. Даний механізм застосовується в низькорівневих додатках ОС (додатки рівня ядра). Виконання криптографічних функцій проводиться з процесу, що викликав функцію, що визначає мінімальні затримки отримання відповіді. Кількість пам'яті, яка необхідна для виконання функції, має бути попередньо зарезервовано процесом "батьком". Так як мобільні системи мають обмежену кількість оперативної пам'яті, використовувати бібліотеку повсюдно не представляється можливим.

Для вирішення вищезазначеної проблеми в операційній системі передбачений спеціалізований сервіс (криптопровайдер), який здійснює криптографічні перетворення по "замовленням" інших процесів. Такий механізм має ряд позитивних особливостей: економія ресурсів операційної системи (наприклад, оперативної пам'яті); уніфікація алгоритму захисту ключової інформації; уніфікація алгоритму доступу до криптографічних операцій.

Так як операційній системі необхідно задовольнити запити на криптографічні перетворення безлічі процесів, в криптопровайдера необхідно передбачити: механізм послідовного виконання завдань (черга завдань); механізм розмежування доступу (для захисту ключової інформації різних процесів); протокол взаємодії криптопровайдера з процесом.

На рисунку 3.1 представлений процес шифрування блоку даних. Як уже згадувалося, криптопровайдер є самостійний процес, який по черзі виконує завдання інших процесів.

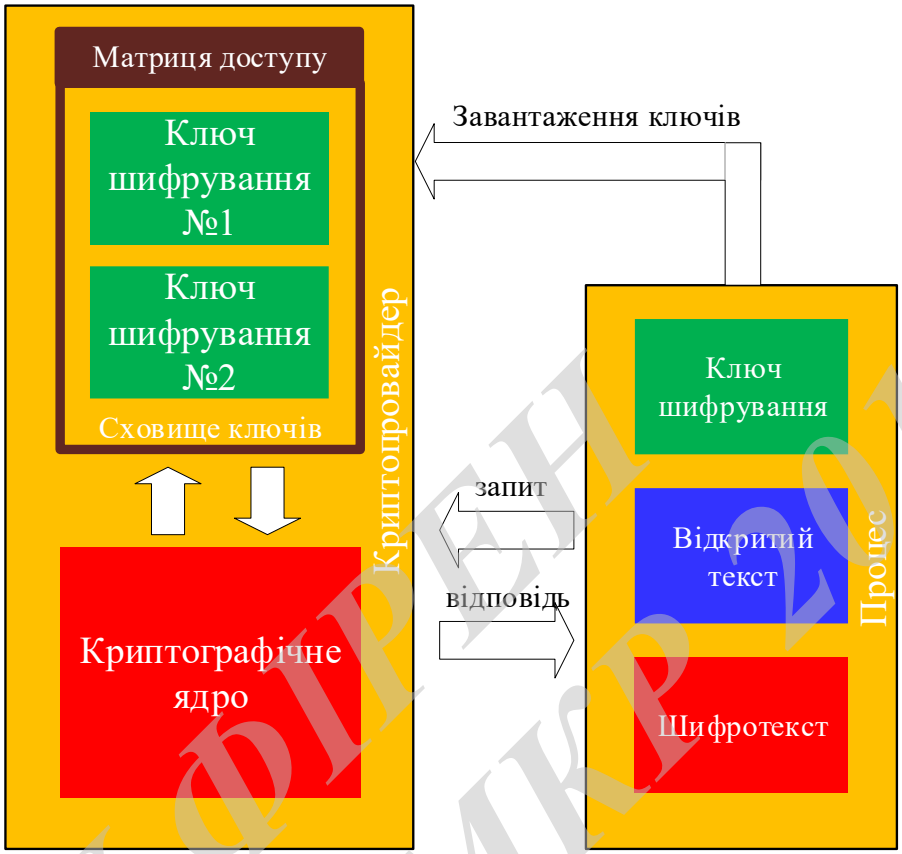


Рисунок 3.1 - Процес взаємодії криптопровайдера із прикладними процесами

Для захисту ключової інформації користувачів криптопровайдер має в своєму складі спеціалізоване сховище ключів. сховище ключів розташовується в виділеної для криптопровайдера пам'яті (постійної або оперативної). Якщо на апаратній платформі передбачений механізм контролю пам'яті, то він обов'язково повинен бути використаний для захисту вищевказаних ділянок пам'яті. У мікроконтролерах архітектури ARM фірми STMictolectronics дана технологія називається MPU (від англ. Memory Protect Unit). Також в сховище ключів додатково реалізований механізм дискреційного розмежування доступу (суб'єктом доступу є ідентифікатор процесу в системі).

Протокол взаємодії процесів з криптопровайдером складається декількох груп операцій:

- операції з ключової інформації (генерація ключа, запис ключа в файл, читання ключа з файлу);

- операції шифрування даних (шифрування блоку даних, розшифрування блоку даних, шифрування файлу, розшифрування файлу);

- операції хешування (розрахувати хеш блоку даних, розрахувати хеш файлу);

- операції електронного підпису (виробити підпис файлу, перевірити підпис файлу).

При необхідності зашифрувати файл, процес виконує по черзі запити на виконання операції:

1. генерація ключа шифрування;

2. запис ключа шифрування в ключовий файл (для можливості подальшого розшифрування файлу);

3. завантаження ключа шифрування з ключового файлу;

4. шифрування файлу.

Також варто зауважити, що операції роботи з ключами (запис ключа в файл, читання ключа з файлу) можуть оперувати сховищами різного типу. Залежно від критичності збережені на різних пристроях зберігання ключів (смарт-карти, пристрої Touch memory).

У підсистемі криптографічного захисту реалізовані наступні криптографічні алгоритми. Симетричне шифрування - ГОСТ 28147-89 [78]. Алгоритм обміну ключами - протокол Діффі-Хеллмана (англ. Diffie-Hellman, DH). Алгоритм електронного підпису - ГОСТ Р 31.10-2001, ГОСТ Р 31.10-94 [79] [80]. Алгоритм гешування ─ ГОСТ Р 34.11-2012.

Заперечне шифрування. В операційній системі реалізований алгоритм отрицаемого шифрування, описаний в [81]. В даному випадку в основі алгоритму ЗОШ лежить алгоритм симетричного шифрування ГОСТ 28147-89. Також застосовується алгоритм отрицаемого шифрування, запропонований в роботі [68]. Більш докладно опис вищевказаних алгоритмів буде наведено далі.

Аналіз ефективності застосування в мобільній ОС Метод захисту: метод застосування криптопровайдерів в низькопродуктивних системах.

Відмінні риси: метод адаптований для зниження споживання обчислювальних ресурсів, наявність виконання в режимі черзі, можливість багатокористувального застосування.

3.2.1 Алгоритм алгебраїчного алгоритму псевдоймовірного захисного перетворення

У роботах представлені практично застосовні алгоритми шифрування [68] [81] [12]. В операційній системі були застосовані кілька алгоритмів заперечного шифрування. Перший алгоритм ЗОШ описаний в роботі [68]. Погляньмо на цей алгоритм більш докладно, який є рішенням системи рівнянь

$$\begin{cases} C \equiv C_1 \bmod p_1 \\ C \equiv C_2 \bmod p_2 \end{cases},$$

систему можна представити у вигляді

$$\begin{cases} C \equiv M^{K_1} K_2 \bmod p_1 \\ C \equiv \overline{M}^{K_3} K_4 \bmod p_2 \end{cases}.$$

Відповідно до китайської теореми про залишки рішення обчислюється по наступною формулою:

$$C = \left[M^{K_1} K_2 p_2 \left(p_2^{-1} \bmod p_1 \right) + \overline{M}^{K_3} K_4 p_1 \left(p_1^{-1} \bmod p_2 \right) \right] \bmod p_1 p_2 .$$

При змушує атаці необхідно надати атакуючому одне з повідомлень. Нехай в якості "помилкового" повідомлення виступає M. Тоді атакуючому надається в якості ключа шифрування трійка значень K3, K4, p2. Розшифрування виконується за формулою

$$\overline{M} = \left(C K_4^{-1} \right)^{K_3^{-1}} \bmod p_2 .$$

В останній формулі зворотні значення для подключей K3 і K4 обчислюються за модулями p2 - 1 і p2, відповідно. За потреби розшифрування "істинного" секретного повідомлення M виконується обчислення по тій же формулі, але з використанням ключа, що представляє собою трійку значень (K1, K2, p1):

$$M = \left(C K_2^{-1} \right)^{K_1^{-1}} \bmod p_1 .$$

Вищевказаний протокол застосовується в протоколі аутентифікації по одноразовим паролів. Більш детально даний протокол буде описаний в роботі далі. Аналіз ефективності застосування в мобільній ОС Метод захисту: спосіб алгебраїчного алгоритму псевдовероятностного захисного перетворення. Відмінні риси: має властивості нерозрізненості від імовірнісного шифрування і однаковості процедури розшифрування криптограми по всьому простору ключів [68].

3.2.2 Алгоритм захисного перетворення з використанням складних операцій

В роботі [12] описаний загальний спосіб побудови алгоритмів заперечного шифрування з використанням будь-яких складних операцій (в тому числі блочних шифрів). У найпростішому випадку алгоритм шифрування може бути реалізований підбором таких двох пар ПОВІДОМЛЕННЯ-КЛЮЧ, щоб при проведенні однакових криптографічних перетворень було отримано однаковий шифртекст. Даний алгоритм ЗОШ може бути реалізований на базі блокового алгоритму шифрування з необхідною довжиною блоку (малюнок 18). Погляньмо на цей алгоритм більш докладно. Для знаходження пар ПОВІДОМЛЕННЯ-КЛЮЧ необхідно вирішити систему рівнянь.

$$\begin{cases} E_{K1}(C)\ mod\ 2^n = M \\ E_{K2}(C)\ mod\ 2^n = \bar{M} \end{cases}$$

Запропонований алгоритм ЗОШ легко програмно реалізуємо. Для шифрування двох повідомлень М1 і М2 необхідно виконати наступні дії:

1. згенерувати ключ К1 і зробити шифрування повідомлення М1;
2. згенерувати ключ К2 і розшифрувати шифртекст, який був отриманий на кроці 1;
3. порівняти отримане на кроці 2 з вихідним повідомленням М2;
4. якщо умова вірна - закінчити, інакше перейти до кроку 2. Шифроване повідомлення повинні мати однакову довжину (рівну довжині блоку шифрування).

$$|M| = |\bar{M}| = n$$

Такий спосіб ЗОШ, звичайно, не відрізняється особливою ефективністю. Для шифрування необхідно виконати добірок.

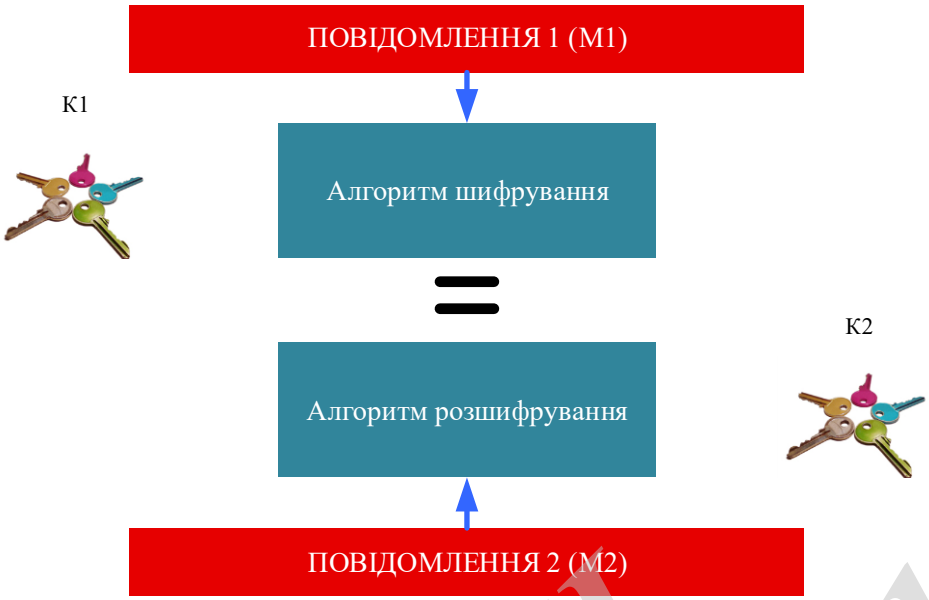


Рисунок 3.2 - Алгоритм заперечного шифрування

Існують і інші більш ефективні алгоритми заперечного шифрування.

3.2.3 Алгоритм захисного перетворення на базі блокового шифрування

В ході дослідження були розроблені ефективний алгоритм отрицаемого шифрування. В [81] було запропоновано алгоритм швидкого отрицаемого шифрування з використанням блокових алгоритмів шифрування. На рисунку 3.3 зображена блок-схема вищевикладеного алгоритму. Далі буде розглянуто даний алгоритм.

Повідомлення, яке необхідно зашифрувати, ділиться на частини (наприклад, посимвольно).

$$M = \{t_1, t_2, \dots, t_{1n}\}$$
$$\bar{M} = \{m_1, m_2, \dots, m_{1n}\}$$

До символу з ПОВІДОМЛЕННЯ 1 приєднується ВИПАДКОВЕ ЗНАЧЕННЯ 1, далі проводиться шифрування з використанням ключа К1 і розшифрування шифртекста з використанням ключа К2. Якщо отриманий потрібний символ ПОВІДОМЛЕННЯ 2, то дана криптограма зберігається.

Основна задача алгоритму підібрати таке ВИПАДКОВЕ ЗНАЧЕННЯ 1, щоб виконалося це умова.

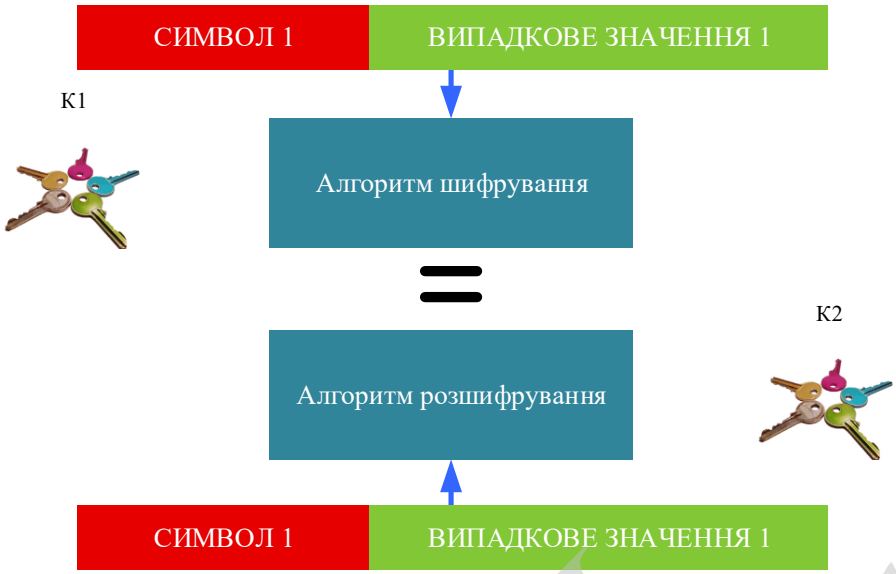


Рисунок 3.3 - Алгоритм отрицаемого шифрування

Для обчислення шуканого значення шифртекста для кожного символу повідомлення необхідно вирішити систему рівнянь.

$$\begin{cases} E_{K1}(t_i, r) = C_i \\ E_{K2}(m_i, \bar{r}) = C_i \end{cases}$$

Ефективність алгоритму залежить від значення обраних параметрів. Розглянемо процедуру шифрування (рисунок 3.4) пари повідомлень T і M:

Нижче показана блок-схема вищевказаної процедури шифрування.

Так як запропонований алгоритм в своїй основі має алгоритм блочного шифрування (наприклад, алгоритм ГОСТ28147-89 в режимі простої заміни), процедура розшифрування алгоритму дуже проста. Для розшифрування блоку шифртекста застосовується процедура розшифрування згідно специфікації застосовуваного алгоритму блочного шифрування (в нашому прикладі, процедура розшифрування ГОСТ28147-89).

В роботі [8] були описані критерії ефективності функціонування запропонованого алгоритму. Згідно з працею, швидкість алгоритму отрицаемого шифрування може бути оцінена при використанні такої формули.

$$\lambda'_{\text{ОШ}} \approx (2^{-u-1}u/n)\lambda_{\text{БШ}},$$

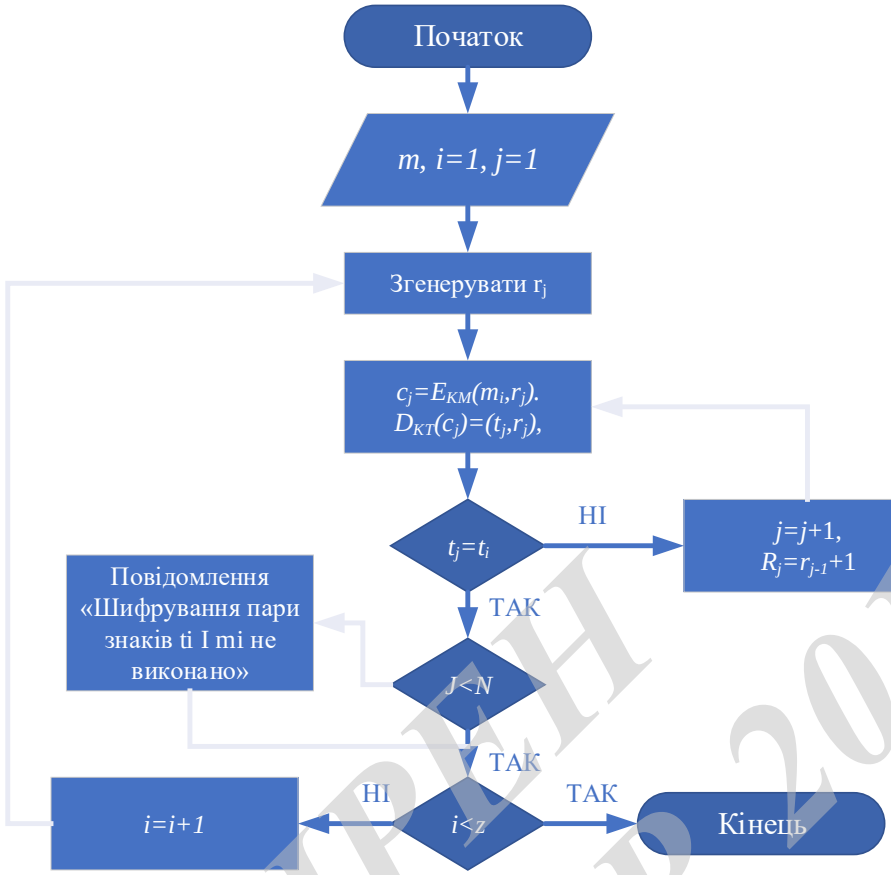


Рисунок 3.4 - Блок-схема алгоритму розробленого способу ЗОШ

Швидкість заперечного шифрування залежить від середнього числа обираних значень rj при шифруванні однієї пари знаків ti і mi (кроки 3-7 алгоритму ЗОШ). Значення залежить від ймовірності виконання на кроці 6 умови tj = ti. Значення можна обчислити за такою формулою.

$$\eta \approx [\Pr(t_j = t_i)]^{-1} = 2^u,$$

З формули (1) випливає, що ефективність представленого алгоритму ЗОШ залежить в основному від 2 параметрів: швидкості базового алгоритму шифрування; відношення розміру блоку даних до блоку випадкових значень.

Також в ході дослідження були експериментально перевірені дані твердження. Була підготовлена програма, яка реалізує запропонований алгоритм ЗОШ (з можливістю налаштування параметрів ЗОШ).

Експериментальне середнє числа обираних значень rjтакже порівнянно з теоретичним значенням.

Як уже згадувалося, швидкість отрицаемого шифрування в основному залежить від швидкості алгоритму шифрування блоку. Також відчутний вплив на швидкість виконання раунду отрицаемого шифрування надає розмір блоків

даних (значення u). Наприклад, ймовірність збігу 4 біт (крок 6 алгоритму) в 16 разів вище ймовірності збігу 8 біт. Але, на жаль, зменшення розміру блоків даних неминуче призводить до збільшення відношення розміру криптограми до розміру шифрованих повідомлень. В даному випадку зашифроване повідомлення буде більше вихідних даних.

$$|t_i| + |m_i| < |C_i|$$

У разі примушує атаки пропонується затверджувати, що в даному випадку застосовувалося розподіл усіх шифрування. З цієї причини блок шифртекста більше шифрованих даних. Зловмисник не зможе довести зворотного.

На рисунку 3.5 зображено графік відношення кількості вибірок значень rjк номеру шифруемого блоку (ЗОШ ГОСТ28147, u = 4, k = 60).

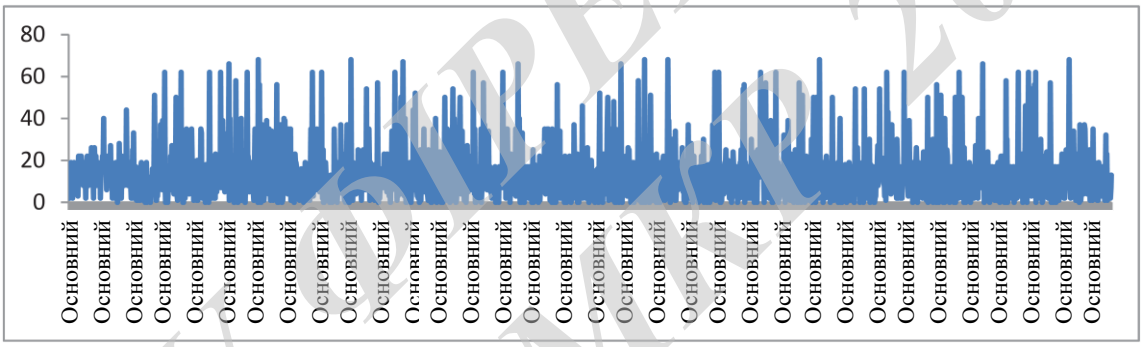


Рисунок 3.5 - Графік залежності числа пробних вибірок значення rj від номера поточної пари шіфруемих символів при використанні блокового шифру ГОСТ28147 і параметрів u = 4, n = 64

З графіка видно, що більшість значень лежить в межах 20 вибірок на блок. Середнє число обираних значень при підборі значень rj близько до теоретичним значенням.

Представлені в даному розділі алгоритми ЗОШ мають практичну значимість і можуть застосовуватися в різних підсистемах захисту операційних систем. Використовуючи сучасні обчислювальні потужності і дотримуючись вищевказані правила вибору параметрів отрицаемого шифрування (з базовим алгоритмом шифрування ГОСТ 28147-89), можна досягти швидкостей до 6 Мбіт / сек. Застосування швидкісних шифрів [8] може значно збільшити дане значення.

Аналіз ефективності застосування в мобільній ОС Метод захисту: спосіб заперечується шифрування. Відмінні риси: має властивості нерозрізненості від

імовірнісного шифрування, застосовується блокове шифрування, має високі швидкісні характеристики.

3.2.4 Застосування методів захисного перетворення, стійких до атак з примусом, в ОС

Висока продуктивність запропонованого в попередньому розділі алгоритму ЗОШ дозволяє застосовувати алгоритми отрицаемого шифрування на практиці самими різними способами. В ході роботи було запропоновано кілька практичних застосувань алгоритмів отрицаемого шифрування [83] - [85], частина з яких реалізована в розробленій операційній системі. Далі представлені напрямки практичного застосування алгоритмів, що заперечується шифрування.

При зберіганні важливих даних в криптоконтейнера. Зберігання важливої інформації є найбільш очевидне застосування отрицаемого шифрування. Так як швидкість шифрування не дозволяє шифрувати значні обсяги даних, на початковому етапі пропонується використовувати заперечується шифрування для приховування невеликих повідомлень (наприклад, криптографічних ключів). У даній роботі запропоновано спосіб застосування ЗОШ для зберігання ключової інформації (розділ 3.3)

У різних алгоритмах аутентифікації. Алгоритми, що заперечується шифрування також можна використовувати при реалізації підсистем аутентифікації. В даному випадку заперечується шифрування використовується для маскування робочої області легітимного користувача.

Наприклад, при завантаженні системи в разі примушує атаки завантажиться не профіль користувача, а гостьовий. Так як ідея заперечується шифрування має на увазі неможливість ідентифікувати в шифртексту наявність додаткових повідомлень, навіть сама наявність облікового запису користувача в операційній системі може успішно ховатися від зловмисника. У даній роботі запропоновано алгоритм аутентифікації, що володіє захистом від примушує атаки.

У протоколах одноразових паролів. Розроблено алгоритми одноразових паролів, в яких в разі примушує атаки блокуються наступні дії користувача (наприклад, зловмисник змусив користувача увійти в систему електронних платежів, але подальші операції проводити вже неможливо). У даній роботі запропоновано протокол одноразових паролів, що володіє захистом від примушує атаки.

В алгоритмах захисту програмного забезпечення від налагодження (аналізу). Оскільки при шифруванні обох повідомлень в алгоритмах

негативного шифрування проводяться одні і ті ж криптографічні перетворення, зловмисник не може передбачити подальшу поведінку програми, просто аналізуючи код програми. Наприклад, зашифрованими можуть бути адреси наступної команди, а в якості ключа може служити деякий змінюваний параметр. Далі в роботі запропоновано метод застосування ЗОШ для захисту програмного забезпечення від аналізу.

Згідно [12] незаперечною позитивною особливістю алгоритмів отрицаемого шифрування є можливість застосування в них блокових алгоритмів шифрування (в тому числі вітчизняних алгоритмів). Дана можливість дозволяє застосовувати заперечується шифрування на базі вже готових програмних продуктів, які реалізують блокові алгоритми. Це дозволить значно зменшити час впровадження отрицаемого шифрування.

Ідентифікатор апаратної платформи застосовується для захисту операційної системи від запуску на НЕ довіреному обладнанні. Залежно від можливостей апаратної платформи розмір ідентифікатора може бути різний. У контролерах фірми STMElectronics існує запрограмований унікальний апаратний ідентифікатор розміром 48 біт. У разі якщо апаратна платформа не має унікального ідентифікатора, в якості ідентифікатора може бути використано будь-яка не перезаписуваний значення (наприклад, серійний номер мікросхеми).

Кожен екземпляр операційної системи повинен мати унікальний ідентифікаційний номер. Даний ідентифікатор використовується в підсистемі безпечного оновлення операційної системи.

Груповий ідентифікатор також використовується в процесах оновлення операційної системи. Груповий ідентифікатор застосовується в разі необхідності провести оновлення операційних систем певного класу пристроїв. У 64 бітах даного ідентифікатора передбачені розділи для опису типу апаратної платформи, номера операційної системи і номера зборки. Також є кілька байт резерву.

Наступним важливим питанням є організація ключової інфраструктури. В операційній системі передбачено сховище ключів. Це спеціально виділений простір в незалежній пам'яті, в якому можуть бути збережені як для користувача, так і вбудовані (встановлені) ключі операційні системи. Як уже згадувалося, в операційній системі активно використовується як симетричне шифрування, так і асиметричне шифрування. Симетричне шифрування використовується тоді, коли необхідно обробити велику кількість даних. Ключі для симетричного шифрування формуються на основі алгоритму відкритого розподілу ключів Діффі-Хеллмана [86]. З цієї причини в

операційній системі відсутні системні ключові контейнери симетричного шифрування. У таблиці 4 відображені основні типи ключів (асиметричні).

Варто зазначити, що кожна категорія ключів з таблиці містить відкритий і закритий ключ. Особливістю використання асиметричного шифрування є необхідність застосовувати процеси контролю автентичності відкритої частини ключа.

3.3 Спосіб застосування методів захисного перетворення, стійких до атак з примусом, для зберігання ключів

У розробленій операційній пропонується застосовувати заперечне шифрування для приховування наявності резервних серій ключової інформації. На рисунку 3.6 представлений алгоритм зберігання набору резервних серій ключової інформації.

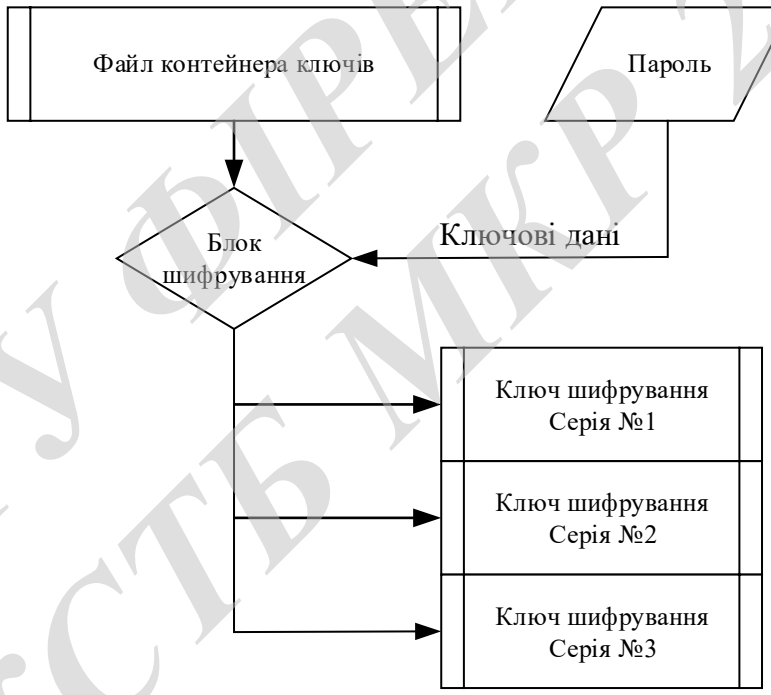


Рисунок 3.6 - Використання заперечного шифрування для зберігання резервних серій ключової інформації

Контейнер ключів являє собою файл, який містить в собі значення шифртекста C. Для обчислення даного значення для n серій ключів необхідно знайти рішення системи рівнянь

$$\begin{cases} E_{K1}(C)\ mod\ 2^r = M_1 \\ \dots \\ E_{Kn}(C)\ mod\ 2^r = M_n \end{cases}$$

де ключі шифрування ключів (пароль фіксованої довжини); захищаються серії ключів; функція шифрування; криптограма; r-розрядність криптограми.

Інформація про наявність резервних серій ключової інформації може мати значну цінність для зловмисника. В якості алгоритму шифрування застосовується ГОСТ 28147-89. Так як довжина файлу шифртекста не залежить від кількості зашифрованих серій ключової інформації, у зловмисника відсутня можливість довести, що існують кілька серій ключів.

Додатковою позитивною особливістю даного способу зберігання ключової інформації є можливість поєднати процес генерації ключової інформації і вироблення файлу - контейнера ключів.

В даному випадку обчислення зводиться до знаходження n значень ключів шифрування ключів за формулою

$$E_{Kn}(C)\ mod\ 2^r = M_n.$$

Варто зазначити, що даний метод може застосовуватися тільки з урахуванням вимог цільових алгоритмів шифрування для ключової інформації. Аналіз ефективності застосування в мобільній ОС. Метод захисту: Спосіб застосування отрицаємого шифрування для зберігання ключів. Відмінні риси: приховування факту наявності резервних серій ключової інформації, можливість інтеграції з процесом генерації ключової інформації (при обліку знижень вимог до ключів).

3.4 Захищена файлова система

Наявність в операційній системі підсистеми захисту збережених файлів значно підвищує загальний рівень захищеності операційної системи. Важливість забезпечення безпеки інформації, що зберігається розглянута в роботах [7, 8]. Які б досконалі засоби управління доступом не застосовувалися в операційній системі, дані кошти діють тільки на суб'єкти, що існують в рамках моделі ОС. Зловмисник може просто витягти жорсткий диск з ПК і зробити аналіз збережених данних.Для захисту від даного виду загроз використовують захищені файлові системи.

Однією з найбільш популярних реалізацій захищеної файлової системи є Encrypted File System (EFS) розробки компанії Microsoft. Дана файлова система має досить простий і як наслідок "прозорий" для розуміння алгоритм роботи.

Висока продуктивність EFS обумовлена застосуванням різних типів алгоритмів шифрування. Як відомо симетричне шифрування має високі швидкісні характеристики. Для шифрування основного обсягу файлу (тіла файлу) в EFS застосовується симетричні алгоритми 3DES або AES.

Застосування симетричного шифрування неминуче призведе до необхідності вирішувати проблеми управління ключової інформації в операційній системі:

- зберігання ключової інформації для кожного файлу (застосовувати один ключ для шифрування всіх файлів недоцільно);
- неможливість спільного використання одного файлу.

Для вирішення даних проблем в EFS для шифрування кличів шифрування файлів використовується асиметричне шифрування. Застосування асиметричного шифрування забезпечує: безпечне зберігання ключа шифрування файлу; інтеграцію з корпоративної інфраструктурою відкритих ключів (PKI).

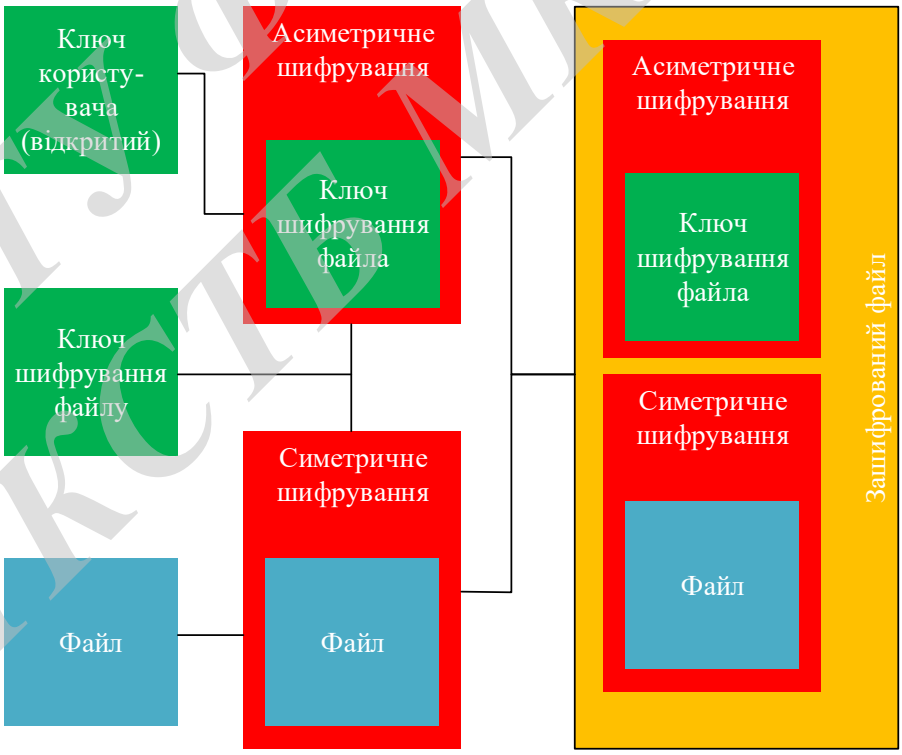


Рисунок 3.7 - Алгоритм шифрування файлу в файловій системі EFS

На рисунку 3.7 зображено блок схема алгоритму шифрування файлу в файловій системі EFS. Процес шифрування файлу складається з наступних кроків: генерація ключа шифрування файлу (для кожного файлу власний); шифрування тіла файлу ключем шифрування файлу (симетричний алгоритм шифрування); шифрування ключа шифрування файлу персональним відкритим ключем користувача; скріплення зашифрованого ключа шифрування файлу до зашифрованого тілу файлу.

Вищевказані операції виконуються в EFS, прозоро для користувача. Продуктивність сучасних процесорів дозволяє зробити процес шифрування файлу непомітним для користувача (процесори фірми Intel наразі мають власний криптографічний співпроцесор).

Для розшифрування файлу необхідно виконати ряд наступних кроків:

- відкріплення зашифрованого ключа шифрування файлу від тіла фала;
- розшифрування ключа шифрування файлу з використанням персонального закритого ключа користувача;
- розшифрувати тіло файлу з використанням отриманого ключа шифрування файлу.

EFS є приклад простої і ефективної захищеної файлової системи.

Аналіз ефективності застосування в мобільній ОС.

Метод захисту: файлова система EFS.

Рівень ефективності: високий.

Переваги: висока продуктивність файлової системи, висока захищеність даних.

Недоліки: відсутня можливість перевірки автентичності даних, вразливість ключовий підсистеми (зберігання ключів проводиться на тому ж жорсткому диску).

Варто згадати, що на території РФ передбачена сертифікація засобів криптографічного захисту інформації відповідно до [8].

Потреба в безпечному і прозорому зберіганні даних обумовлює безсумнівну необхідність реалізації в операційній системі захищеної файлової системи. Термін віртуальна пам'ять зазвичай асоціюється з можливістю адресувати простір пам'яті, набагато більше, ніж ємність первинної (реальної, фізичної) пам'яті конкретної обчислювальної машини. [9].

У структурі розробленої операційної системи представлена захищена віртуальна файлова система. В операційній системі використовується відома концепція "все є файл". Тобто всі можливі об'єкти файлової системи, доступ до яких може бути необхідний процесам, проектуються на файлову систему.

До таких об'єктів можуть належати: запущені процеси; сховища даних різного типу (флеш-пам'ять, незалежна пам'ять і ін.); інтерфейси взаємодії із зовнішнім середовищем (інтерфейси RS-232, RS-485, TWI).

Структура віртуальної файлової системи розроблена на основі аналізу існуючих файлових систем.

Зважаючи на той факт, що дана файловий є віртуальною, а значить «високорівневою», перед файлової системою не ставилися такі спеціалізовані завдання файлових систем як: журналирования (для організації можливості «відкату» змін), реалізації середовищ завантаження (завантажувальні сектора), реалізація різного виду засоби резервування даних.

Всі вищевказані функції реалізуються на низькому (по відношенню до віртуальної файлової системи) рівні - в конкретної файлової системи низького рівня (FAT32, NTFS і т.д.) До однієї з основних завдань, які вирішує віртуальна захищена файлова система, відноситься уніфікація доступу до файлів на різних носіях (флеш-пам'ять, незалежна пам'ять і т.д.). Не секрет, що в різних пристроях зберігання даних використовуються різні методи запису або читання інформації. В незалежну пам'ять деяких виробників можлива тільки послідовний запис (блок за блоком). Флеш-пам'ять (на прикладі файлової системи FAT32) дозволяє проводити операції запису-читання мінімальними блоками даних (мінімум 512 байт). У концепції віртуальної файлової системи запис на вищевказані пристрої зберігання даних може відрізнятися лише за двома параметрами:

- максимально-можливий розмір файлу (залежить від обсягу доступних блоків даних пристрою зберігання),

- швидкості запису (швидкість в незалежну пам'ять багато менше записи даних на сучасні флеш-накопітілі).

Захист даних, що зберігаються закладалася як в рівній мірі важлива для існування файлової системи, як і реалізація об'єктів файлової системи (Файлів і каталогів). З цієї причини на етапі проектування до віртуальної файлової системи висувалися такі вимоги:

- забезпечення безпеки інформації, що зберігається шляхом її криптографічного перетворення,

- можливість реалізації різних методів розмежування доступу до ресурсів файлової системи (наявність у об'єктів файлової системи міток доступу, матриць доступу і т.д.)

Файлова система складається з файлових двох типів файлових об'єктів: власне, файлів і каталогів. В контексті віртуальної файлової системи файл являє собою посилання.

Структура каталогів файлової системи представляє дерево каталогів, яке починається з кореневого каталогу. Кореневої каталог являє собою спеціальний динамічний каталог. У процесі запуску операційної системи формується і структура кореневого каталогу. Залежно від фактичного розташування даних (внутрішня пам'ять, зовнішній пристрій зберігання) в тіло кореневого каталогу записуються значення адрес дочірніх каталогів, розмір стандартного кластера і кількість доступних для запису кластерів.

Механізми захисту, які застосовуються для запобігання несанкціонованих дій з файлами, залежать від інформації, що зберігається і, звичайно, від місця фізичного зберігання (внутрішня пам'ять, зовнішній пристрій зберігання). Для захисту файлів на зовнішніх і відчужуваних носіях застосовуються функції прозорого шифрування, підпису даних. На рисунку 3.8 показана структура файлу, що зберігається на зовнішньому носії.

```
1  ##################################################
2  [header]
3  name= 1.txt
4  flag= 29ff
5  metka= 0000
6  ovner= 0000
7  group= 0000
8  offset= 0116
9  sign_h= AAAAAAAAAAAAAAAAAAAAAA
10 sign_m= BBBBBBBBBBBBBBBBBBBBBB
11 key_m= CCCCCCCCCCCCCCCCCCCCCC
12 ##################################################
13 12345testtesttesttest
```

Рисунок 3.8 - Структура захищеного файлу

Структура захищеного файлу складається з додаткового заголовка файлу і тіла файлу, в якому зберігається вихідний файл цілком (в зашифрованому вигляді).

Концепція "все є файл" дозволяє уніфікувати доступ процесів до абсолютно будь-яким периферійних пристроїв. На рисунку 3.9 представлений процес передачі даних по інтерфейсу USB.

Процес передачі даних через інтерфейс складається з наступних етапів:

- процес №1, використовуючи стандартні функції доступу до файлової системи, проводить запис в файл даних які необхідно передати;

- ядро операційної системи використовує драйвер послідовного інтерфейсу USB (в даному випадку Virtual COM - віртуальний інтерфейс RS232);

- апаратний інтерфейс USB передає дані на ПК;

- драйвер послідовного інтерфейсу USB на ПК (також Virtual COM);

- процес №2 підключається до віртуального COM-порту, і отримує передані дані.

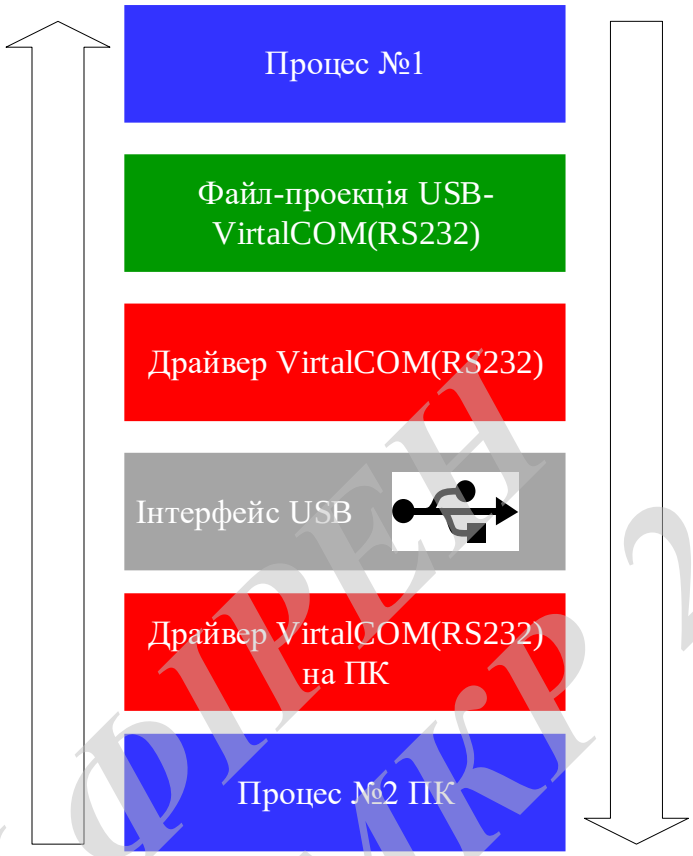


Рисунок 3.9 - Взаємодія процесу з інтерфейсом USB

З одного боку, процес передачі даних не виглядає простим. Однак для процесу №1 передача даних це звичайна операція запису в файл. Цей факт дозволяє зробити операційну систему уніфікованої і абстрагувати прикладне програмне забезпечення від необхідності взаємодіяти з апаратною платформою.

Аналіз ефективності застосування в мобільній ОС. Метод захисту: захищена файлова система.

Відмінні риси: інтеграція в ФС електронного підпису, можливість застосування різних моделей розмежування доступу (мандатної, дискреційної), наявність файлових об'єктів різних типів (метод, файл, каталог) реалізація методу "все є файл".

3.5 Захист даних при передаванні в безпровідних мережах

Захист переданих по мережі даних здійснюється за допомогою системної служби - служби передачі даних. Дана служба являє собою спеціалізований процес рівня ядра. Служба передачі даних, як і вже розглянуті служби криптопровайдера і доступу до файлової системи, обслуговує прикладні процеси в порядку черги. Як і криптопровайдер, служба передачі даних має в своєму складі сховище ключів, в яке завантажуються ключі шифрування даних різних процесів. При необхідності передачі даних в зашифрованому вигляді процес попередньо завантажує ключі в сховище. На рисунку 3.10 зображено структурну схему служби передачі даних.

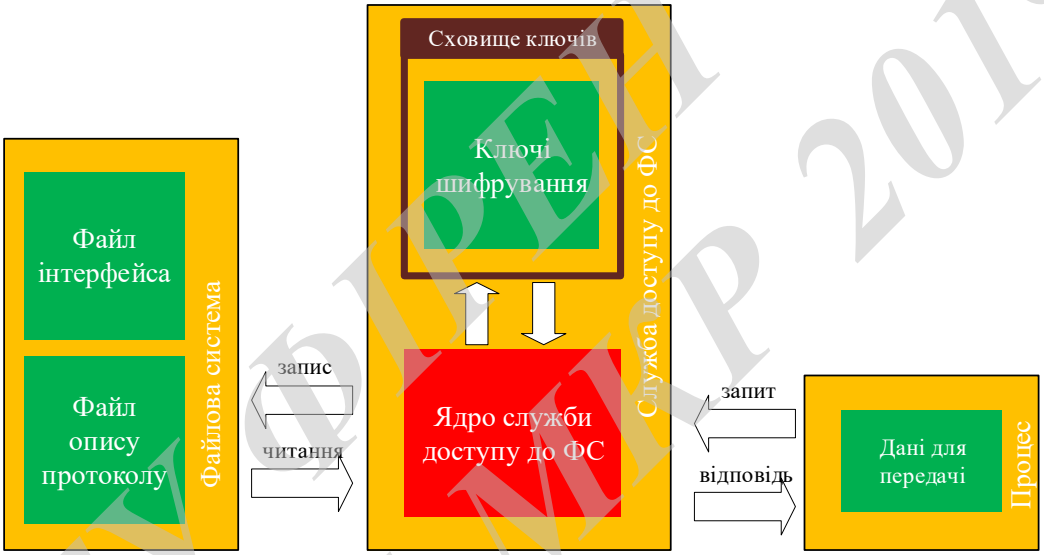


Рисунок 3.10 - Структурна схема служби передачі даних

Особливістю служби передачі даних передачі є наявність можливості модифікації прикладних протоколів взаємодії при необхідності. Всі підтримувані протоколи передачі даних представляють собою спеціалізовані файли опису, розташовані в зумовлених каталогах:

- для загальносистемних протоколів (такий як віддалений інтерпретатор командного рядка): шлях до файлів опису «/ lib / net / proto /»;

- для прикладних процесів (шлях оголошується попередньо, до використання виклику функцій протоколу): шлях до файлів опису є відносним, наприклад, «/ mnt / 0 / proc1 / lib / proto /».

Файл опису протоколу передач даних являє собою файл певної структури, який містить всі необхідні для обміну. До таких параметрів належать: системне ім'я протоколу, напрям взаємодії (симплекс, дуплекс, полудуплекс), формат переданого пакета, опис викликаються процедур.

Створити свій власний протокол виробнику прикладного програмного забезпечення не складе труднощів. Найскладнішою частиною файлу опису є опис викликаються процедур. В даному блоці файлу опису можна використовувати посилання на виконувані файли з необхідними параметрами. В основі служби передачі даних лежить механізм інкапсуляції (аналогічно моделі взаємодії відкритих систем [9]), що дозволяє ізолювати розробника від необхідності взаємодії з апаратними інтерфейсами.

Аналіз ефективності застосування в мобільній ОС

Метод захисту: підсистема передачі даних. Відмінні риси: підтримка настройки протоколів передачі, інтеграція сервісу передачі даних з криптографічним захистом даних.

3.6 Висновки до розділу 3

Розділ присвячений методам захисту інформації, що передається та зберігається. Криптографічний захист є однією з найбільш простих для реалізації. Тому криптографічні алгоритми часто застосовуються в різних підсистемах операційних систем. У цьому розділі були описані розроблені ефективні алгоритми захисного перетворення даних. Описано методи практичного застосування даних перетворень методів захисного перетворення, стійких до атак з примусом в ОС.

Далі була описана підсистема захисту переданих даних і захищена файлова система. В цьому розділі вирішені наступні завдання дослідження:

- розробка методу захисту інформації, що зберігається стійкий до атак з примусом користувача розкрити ключ захисного перетворення;
- розробка методу захисного перетворення передається по відкритих каналах інформації, стійкий до атак з примусом користувача розкрити ключ захисного перетворення.

4 РОЗРОБКА БЕЗПЕЧНОЇ МОБІЛЬНОЇ ОПЕРАЦІЙНОЇ СИСТЕМИ ТА ПІДСИСТЕМИ ЗАХИСТУ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Дана глава присвячена опису розробленої моделі захищеної операційної системи для мобільних систем. Будуть запропоновані вдосконалені методи захисту інформації. Для запропонованих методів захисту будуть виділені відмінні риси, які дозволяють ефективно застосовувати дані методи в мобільних операційних системах. Буде описана архітектура підсистеми захисту програмного забезпечення розробленої мобільної операційної системи.

4.1 Апаратна платформа пристроїв безпровідної мережі WiMAX

Для виконання налагодження і випробувань розробленої операційної системи були використані налагоджувальні апаратні платформи (макетні стенди). Стенди імітують деякі поширені класи засобів захисту інформації, в тому числі:

- криптографічне сховище інформації,
- персональний ідентифікуючий пристрій для інтерфейсу USB (USB-токен).

Для адаптації роботи операційної системи на різних апаратних платформах для дослідження навмисно були обрані контролери різних виробників, в тому числі:

- високопродуктивний ATSAM3U4C фірми Atmel [3];
- енергоефективний STM32F103RE фірми STMicroelectronics [4];
- надкомпактний LPC1111FHN33 фірми NXP [5].

Як можна бачити з таблиці кожна з макетних плат має свої позитивні сторони. Криптографічне сховище інформації являє собою пристрій, до якого підключається сховище інформації (SDHC карта пам'яті), який підключається до персонального комп'ютера за допомогою інтерфейсу USB. Структурна схема стенду зображенана рисунку 4.1. Стенд має досить великі обчислювальні можливості. В склад схеми входять два високопродуктивних 32-х розрядних мікроконтролера архітектури ARM. Перший - центральний мікроконтролер ATSAM3U4C має продуктивність практично 100 мільйонів операцій в секунду. Даний контролер призначений для забезпечення потокового шифрування даних на диску. Також особливість даного контролера є вбудований контроллер високошвидкісної шини USB 2.0 (Режим High Speed) 400 Мбіт / сек., Що забезпечить комфортну роботу з пристроєм зберігання. Другий контролер - LPC1111FHN33 має меншу продуктивність (50

мільйонів операцій в секунду). даний контролер застосовується для організації призначеного для користувача інтерфейсу, зберігання ключів користувача. Обидва контролера з'єднані швидкісним інтерфейсом SPI (швидкість 25 Мбіт / сек.).

Стенд з двома обчислювальними платформами також був використаний для випробування механізму "чорний ящик", запропонованого в [9]. даний механізм дозволяє використовувати менш стійкі криптографічні алгоритми без шкоди загальної захищеності криптографічного системи.

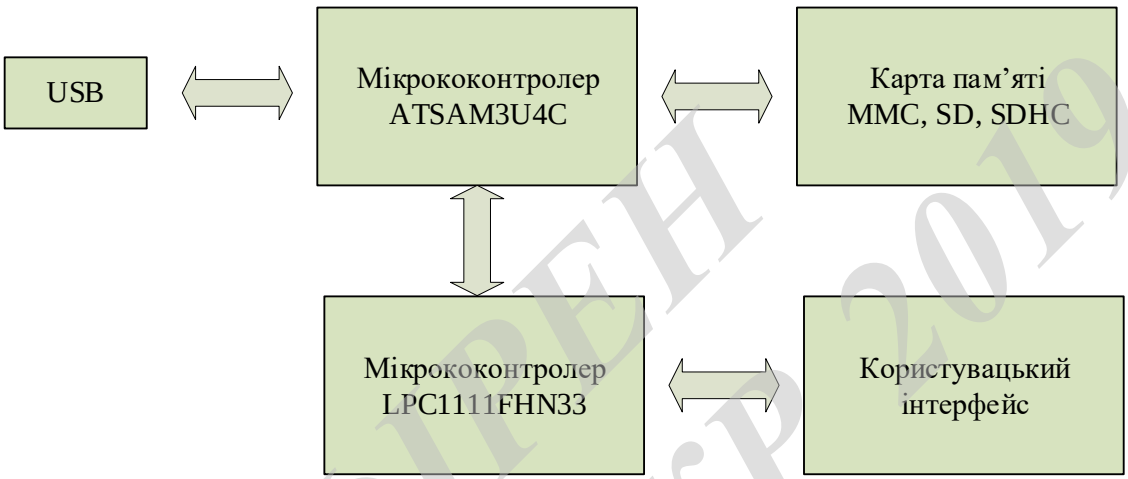


Рисунок 4.1 - Структурная схема стенду криптографічного сховища інформації

На рисунку 4.2 представлена структурна схема другого стенду, розробленого для відкладання операційної системи на базі класичного персонального ідентифікаційного пристрою. Пристрої даного класу призначені для організації систем посиленою (багатофакторної) аутентифікації, зберігання ключових контейнерів і ін. Пристрій має відрізняться компактністю, енергоефективністю (а також енергонезалежністю) і наявністю достатнього кількість постійної пам'яті.

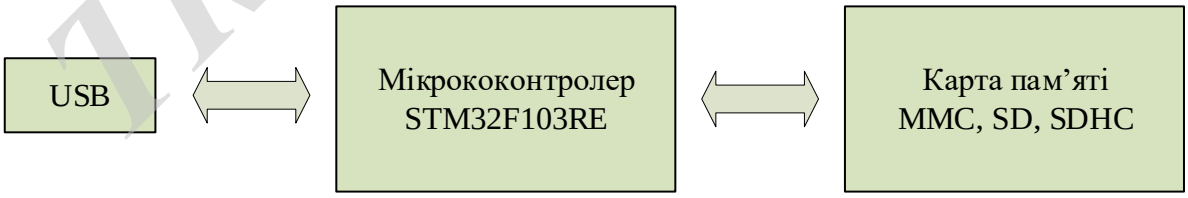


Рисунок 4.2 - Структурна схема пристрою ідентифікації

Обчислювальна платформа стенду представлена мікро контролером STM32F103RE. Даний контролер має високу продуктивність (72 мільйона операцій в секунду). Також в контролер інтегровані годинник реального часу.

Енергоефективність контролера обумовлена наявністю декількох планів електропостачання ядра (висока продуктивність, робота від батарей). Різні режими роботи необхідні для виконання операцій резервування важливих операцій при відлученні пристрою від постійного електроживлення.

4.2 Ядро операційної системи

Найбільш поширені архітектури ядра операційної систем були розглянуті в першому розділі. Розроблена операційна мобільна операційна система організована по класичній архітектурі типу «Мікроядро». Вибір архітектури даного типу був зроблений за наступними причин:

- необхідністю реалізації в системі режиму «аварійного завершення »(так як система буде експлуатуватися в несприятливих умовах мобільних пристроїв);

- теоретично досить низька продуктивність апаратної платформи (мобільні системи мають порівняно невелику продуктивність);

- багатоцільовий характер застосування операційної системи (різних видів пристроїв потрібен різний набір сервісних додатків).

У розробленій операційній системі реалізовано микроядро, яке, в залежності від умов експлуатації, може перебувати в одному з трьох режимів роботи.

Нормальний режим функціонування. Нормальний (штатний) режим роботи ядра реалізує всі необхідні служби (набір служб різниться в залежності від застосування операційної системи). Операційна система виділяє прикладним програмам всю необхідну пам'ять. Процесорний час в рівній мірі ділиться між процесами. Апаратна платформа знаходиться в продуктивному режимі (у разі якщо апаратна платформа підтримує управління електроживленням).

Передаварійним режим функціонування. В даний режим переходить ядро при виникненні події небезпечного функціонування операційної системи (наприклад, при відключенні постійного електроживлення апаратної платформи). Завдання даного стану ядра:

- по можливості завершити (закрити або зберегти стан) прикладні процеси для запобігання втрати призначених для користувача даних;

- записати дані оперативної пам'яті (критичні області - наприклад, криптографічні контейнери) в незалежну пам'ять;

- завершити всі існуючі операції запису на диск, щоб запобігти пошкодженню структури сховища даних.

В ході забезпечення вищезазначених завдань ядро виділяє під свою роботу більшість процесорного часу.

Енергозберігаючий режим. В апаратних платформах, в яких реалізована можливість роботи від автономного джерела живлення, може застосовуватися енергозберігаючий режим роботи ядра.

Вибір конкретного режиму роботи проводиться операційною системою в автоматичному режимі. Вибір режиму роботи грунтується на правилах, які описані в динамічних настройках операційної системи. Файл конфігурації ядра операційної системи розташований за адресою «/Etc/kernel.conf». Всі необхідні параметри представлені у вигляді текстових значень.

Для настройки того чи іншого параметра досить змінити значення в файлі. Залежно від типу параметра в якості значення може бути число, логічне значення або текстове поле. Стосовно до представленого наприклад, у файлі конфігурації можуть бути встановлені наступні параметри:

- частота тактирования ядра (CFG_CPU_FREQ); даний параметр впливає на час роботи системних обробників подій;

- частота спрацьовування події перемикання контексту потоку (CFG_SYSTICK_FREQ); даний параметр має важливе значення, так як він визначає мінімальний час виконання процесу (по закінченню цього часу управління буде передано іншому процесу).

- максимальна кількість прикладних процесів (CFG_CPU_FREQ); кількість запущених процесів встановлюється в залежності від кількості оперативної пам'яті;

- адреса розташування і розмір стека, який використовується для зберігання значень змінних виконуваних процесів.

Концепція динамічної конфігурації з одного боку дозволить операційній системі бути досить гнучкою для реалізації завдань самого різного характеру. З іншого боку, динамічні параметри зумовлює появу деякої кількості вразливостей. Для захисту ядра операційної системи від атаки, заснованої на виклик помилок шляхом модифікації конфігураційних файлів, в операційній системі використовується механізм електронного підпису. Детально цей механізм буде розглянуто пізніше.

Аналіз ефективності застосування в мобільній ОС

Метод захисту: адаптоване ядро. Відмінні риси: адаптованість до експлуатації в мобільному режимі, захист критичних даних від втрати, можливість конфігурації ядра для роботи в різних умовах, підтримка різних архітектур.

4.3 Підсистема віртуального програмного середовища

Віртуалізація є перспективним напрямком в розробці операційних систем. У роботах [7 - 9] розглянуті перспективні методи застосування віртуальних середовищ в автоматизованих системах.

Підсистема віртуальної програмного середовища призначена для захисту ресурсів операційної системи від алгоритмічних атак через яке виконує програмне забезпечення (рисунок 4.3).

В операційній системі передбачена система віртуальних команд. Для зручності розробників програмного забезпечення віртуальні команди мають схожий синтаксис з мовою ASSEMBLER. Дане рішення дозволяє використовувати при компіляції синтаксичні аналізатори різних мов програмування високого рівня (C, Basic, Pascal і т.д.).

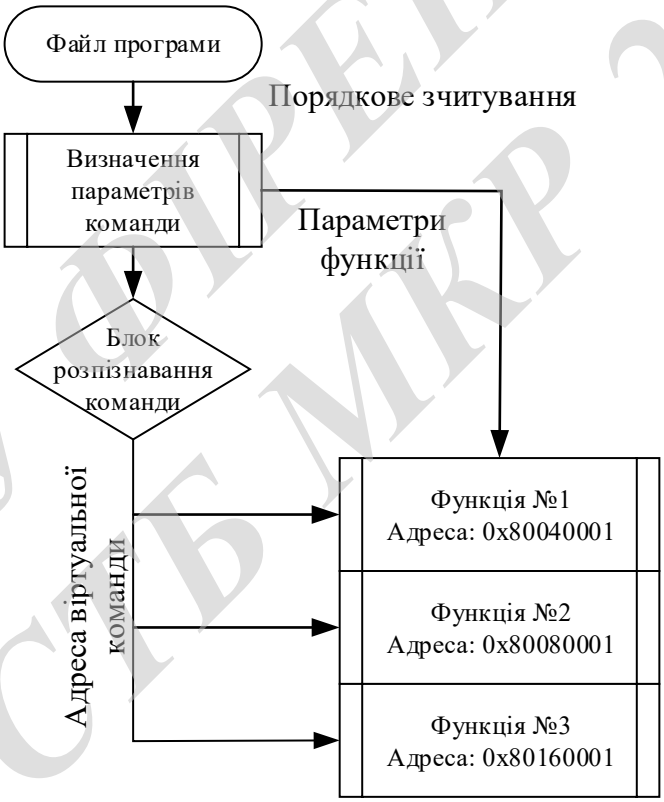


Рисунок 4.3 - Архітектура віртуального програмного середовища

Після написання програми проводиться компіляція програми. Для цього застосовується спеціальний додаток - компілятор. Компілятор виконується на апаратній платформі. Дане рішення дозволяє випробувати розроблене додаток на цільовій платформі і уникнути помилок, які можуть бути обумовлені помилкою програміста і особливостями застосовуваної апаратної платформи.

На вхід компілятора надходить файл тексту програми. Який перетворюється в машинний код програми

Модулі рівня ядра мають можливість прямого використання основного стека (загального) операційної системи. До основних завдань підсистеми управління пам'яттю відноситься: виділення областей пам'яті процесам; звільнення пам'яті (після завершення виконання процесу); оптимізація пам'яті.

У мобільних системах доступна оперативна пам'ять операційної системи є досить обмеженим ресурсом. Оптимізацію (дефрагментацію) пам'яті необхідно виконувати постійно в процесі роботи операційної системи.

Як уже згадувалося, в операційній системі застосовується принцип «все є файл». Кожне системне пристрій, порт введення-виведення має своє відображення в файлової системі. З точки зору пам'яті кожне таке відображення є посилання на функцію ядра, файл і т.д. Кожен об'єкт, розміщений в пам'яті, має власне іменування (адреса). В операційній системі застосовуються класичні типи адресації, описані раніше.

Абсолютна адресація (пряма вказівка на адресу в пам'яті мікроконтролера) застосовується тільки в ядрі ОС і деяких системних службах. Дане рішення було прийнято з метою забезпечення безпеки. Абсолютна адресація може дати зловмисникові інформацію про апаратній платформі, яка може бути використана, наприклад, для атаки переповнення пам'яті. Можливі й інші атаки.

В операційній системі передбачені механізми системи виявлення вторгнення. Зокрема, виконується контроль використання оперативної пам'яті і контролю доступу до файлових об'єктів. Так як для запуску користувальницьких додатків застосовується віртуальна машина, основним видом адресації є відносна адресація. Користувача додаток немає необхідності отримувати дані ззовні свого простору пам'яті. Всі оголошені змінні розміщуються в заздалегідь визначеному місці. Адресація пам'яті програми є відносною по відношенню до стартового адресою початку стека, який виділений з додатком перед його запуском. Віртуальна машина стежить, щоб додаток ні в якому разі не потрапило за межі свого адресного просторі.

При спробі отримати доступ поза виділеного адресного простору додаток буде завершено з помилкою. Крім цього всі спроби доступу можуть проводитися тільки з використанням функцій доступу віртуальної машини, в яких застосовуються тільки відносні адреси. Реєстрова адресація також застосовується в операційній системі.

Аналіз ефективності застосування в мобільній ОС. Метод захисту: підсистема віртуального виконання команд. Відмінні риси: застосування мови ASSEMBLER спрощує "портирование" існуючих додатків в мобільну ОС,

інтеграція віртуального середовища з підсистемою захисту пам'яті, інтеграція віртуального середовища з системою виявлення вторгнень.

4.4 Програмний захист мобільних пристроїв

Методи захисту від аналізу (налагодження) додатків доцільно розділити за методом аналізу (налагодження) додатків: методи протидії статичному аналізу (дізассемблерірованіе), методи протидії активному аналізу (налагодження), методи протидії емуляції.

Так як статичний аналіз заснований на дослідженні низкоуровнего (машинного) коду програми, все методи протидії статичному аналізу засновані на приховуванні основного коду програми. Серед методів протидії статичному аналізу можна виділити (згідно [6]):

— шифрування тіла додатки (ключових блоків) — можна запустити програму розшифровується і проводиться запуск основної програми;

— заплутування коду (пакування) — перемішування коду, створення великої кількості додаткових посилань;

— алгоритмічна захист — впровадження в код програми (на етапі її розробки) спеціалізованої логіки, націленої на захист додатки від аналізу; прикладом може бути маскування передачі управління (використання непрямої передачі управління).

Аналіз ефективності застосування в мобільній ОС. Метод захисту: шифрування тіла додатки. Рівень ефективності: високий. Позитивні сторони: висока ефективність методу (ефективність залежить від застосовуваного алгоритму шифрування). Негативні сторони: залежність області застосування від продуктивності процесора, схильність атакам на криптографічний алгоритм (наприклад, атака на ключову систему). Метод захисту: заплутування коду. Рівень ефективності: середній. Позитивні сторони: простота реалізації, наявність універсальних засобів (пакувальники).

Негативні сторони: частини заплутаного коду все одно зв'язні і можуть бути проаналізовані. Не варто недооцінювати і інші методи захисту. Наприклад, при грамотному застосуванні алгоритмічної захисту можна досягти досить непоганих результатів.

Протидіяти методу активного аналізу (налагодження) додатки теоретично також не так складно. Згідно [6] виділяють наступні методи.

Контроль часу. Суть методу полягає у вимірюванні часу виконання ключових блоків коду. Так як при налагодженні (аналізі) додатки виконання команд відбувається по команді людини ("покроковий" режим налагодження), час виконання таких команд зна чительно більше. Час виконання команд може

бути виміряна як запитом системного часу, так і за кількістю тактів, виконаних процесором.

Контроль контрольних сум. В даному випадку програма підраховує контрольні суми ключових блоків (наприклад, при старті додатка). Так як при аналізі додатка отладчики нерідко встановлюють так звані контрольні точки (точки зупину) в коді програми, контрольні суми ключових блоків програми будуть змінені.

Алгоритмічна захист. У разі захисту від активного аналізу додатки також є багато різних спеціальних прийомів програмування. Прикладом буде служити застосування в додатку переривання (int 01h і int 03h). Вищевказані переривання використовуються програмами-отладчиками для реалізації "покрокового" режиму виконання програми. Якщо в захищуваному додатку навмисно використовувати дані переривання, то це створить проблеми зловмисникові.

Як уже згадувалося емуляція (як метод аналізу програм) зазвичай ефективніше застосовувати спільно іншими методами аналізу. Як для захисту від аналізу активного застосування, так і для виявлення факту емуляції (підробки оточення) застосовують метод контролю зовнішнього середовища. Для цього захищається додаток може контролювати, наприклад, такі параметри: кількість оперативної пам'яті, контрольні суми системних бібліотек і інші параметри системи.

Аналіз ефективності застосування в мобільній ОС. Метод захисту: контроль часу. Рівень ефективності: низький.

Позитивні сторони: .

Негативні сторони: дані виміру часу виконання залежать від зовнішнього середовища і можуть бути сфальсифіковані.

Метод захисту: контроль контрольних сум.

Рівень ефективності: середній.

Позитивні сторони: □.

Негативні сторони: для ефективного застосування засобу підрахунку контрольних сум повинні бути захищені.

Метод захисту: алгоритмічна захист.

Рівень ефективності: низький.

Позитивні сторони: простота застосування.

Негативні сторони: метод прямо не перешкоджає аналізу, а лише заважає роботі програм отладчиков (уповільнює роботу отладчиков).

4.5 Спосіб захисту програмного забезпечення від несанкціонованого доступу

В даному підрозділі запропоновані ефективні методи захисту програмного забезпечення від аналізу. У розробленій операційній системі реалізовані функціональні можливості захисту програмного забезпечення.

У попередньому розділі описані класичні алгоритми захисту прикладного програмного забезпечення від налагодження (статичного аналізу, налагодження, емуляції).

Методи захисту програми від статичної налагодження можуть бути додатково посилені за допомогою застосування отрицаемого шифрування. Найбільш часто респонденти користуються послугами в додатку структурою є «умова». "Умова" використовується як самостійно, так і в більш складних структурах, таких як «цикл».

Для захисту від статичного аналізу (дизассемблирования) доцільно в ключових блоках програми замість структури «умова» використовувати заперечується шифрування. Замість ключа використовувати вхідні дані «умови».

На виході необхідно реалізувати помилкові гілки коду (наприклад, в зашифрованому повідомленні може міститися адреса наступного блоку програми). Така структура (далі блок шифрування) буде застосована і в інших методах захисту від налагодження, які будуть описані далі. На вхід блоку шифрування буде подаватися параметр (ключ). На виході блоку буде отримано адреса наступної команди (відкритий текст). На рисунку 4.4 зображено блок-схему функції, яка в якості конструкції типу «умова» використовує блок шифрування. Як можна бачити результату виконання «якщо» можна реалізувати будь-яку кількість гілок коду істинних або помилкових. При цьому для зловмисника подальше виконання кожної з гілок коду буде рівноймовірно.

Застосування отрицаемого шифрування в якості конструкції типу «Умова» дозволить значно ускладнити (особливо при багаторазовому застосуванні) статичний аналіз додатки (дизасемблювання).

При захисті від статичного аналізу також застосовується і шифрування тіла або найбільш критичних блоків програми. Для шифрування тіла програми або критичних блоків оригінальну програму можна застосування отрицаемого шифрування.

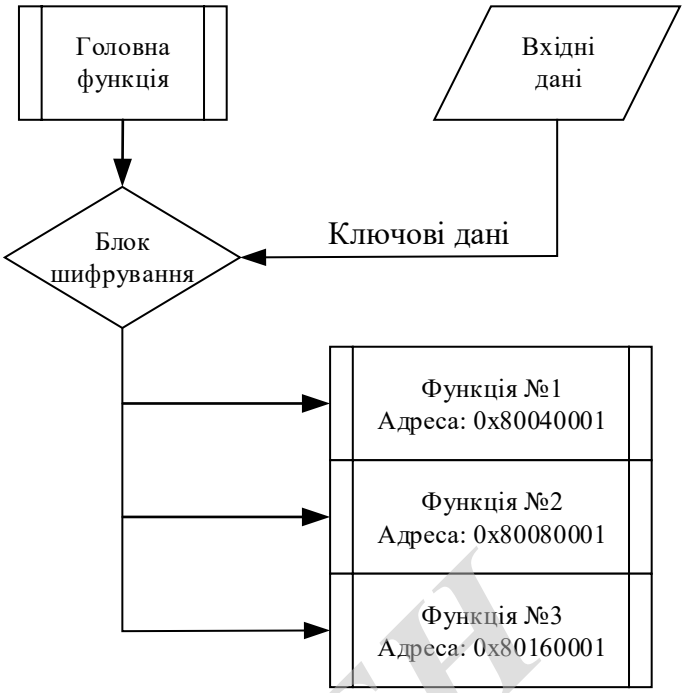


Рисунок 4.4 - Використання заперечного шифрування в якості конструкції типу «if»

В даному випадку в якості ключа може бути використовувати цілий ряд зовнішніх параметрів (контроль зовнішнього середовища) таких як стан операційної системи. На виході так само, як і в попередньому випадку, необхідно реалізувати помилкові гілки коду.

Для захисту програми від активного аналізу засобами налагодження також може застосовуватися заперечується шифрування.

Метод захисту від активної налагодження "контроль часу" додатково ускладнюється введенням в алгоритм методу отрицаемого шифрування.

Перша стратегія застосування отрицаемого шифрування для контролю часу - контроль часу виконання.

На вході блоку шифрування: різниця в часі (наприклад, може бути передано кількість тактів процесора, яке пройшло за період часу).

На виході блоку шифрування: адреса наступного блоку основної програми (або помилкової гілки алгоритму).

Друга стратегія застосування отрицаемого шифрування для контролю часу - контроль моменту часу виконання.

На вході блоку шифрування: нині.

На виході блоку шифрування: адреса наступного блоку основної програми (або помилкової гілки алгоритму). Така стратегія може також бути застосована також в пробних версіях програмних продуктів (наприклад, для роботи програми на протязі конкретного місяця).

Стратегій застосування отрицаемого шифрування для контролю зовнішнього середовища можна розробити досить багато (стратегія залежить від вхідних даних - кількості оперативної пам'яті, наявність бібліотек і т.д.). Перспективною виглядає наступна стратегія, яка призначена для контролю адреси flash-пам'яті мікроконтролера, звідки запущений екземпляр програми.

На вході блоку шифрування: адреса першої команди тестованого блоку (в мікроконтролерах архітектури ARM - значення лічильника команд).
На виході блоку шифрування: адреса наступного блоку основної програми (або помилкової гілки алгоритму).

Використовуючи даний метод, екземпляр програми може визначити, що він запущений поза захищеного блоку пам'яті, і активізувати захисні дії.
Застосування шифрування тіла програми може бути використано і для захисту від активної налагодження програми.

На вході блоку шифрування: деякий умова (в залежності від використовуваної стратегії) в якості ключа, блок зашифрованого коду. На виході блоку шифрування: блок розшифрованого коду програми (або помилковий блок програми).

При впровадженні системи захисту від налагодження слід приймати що: програмний продукт в будь-якій своїй частині може бути підданий аналізу; зовнішнє середовище (оперативна пам'ять, зовнішні бібліотеки, засоби операційної системи) постійно знаходиться під наглядом; зловмисник може мати великі можливості і мати всі необхідні знання для аналізу програми.

У кожен момент часу на вході блоку шифрування може бути навмисно направлено (зловмисником в ході аналізу додатки) певне значення. Використання для таких цілей програм отладчиков може розглядатися як "примус" програми до виконання деяких дій. У такому випадку застосування отрицаемого шифрування допоможе більш ефективно застосовувати класичні методи захисту програми від налагодження.
Аналіз ефективності застосування в мобільній ОС.
Метод захисту: Способи застосування отрицаемого шифрування в методах захисту додатків від аналізу.
Відмінні риси: підвищена захищеність методу захисту від аналізу за рахунок протидії прямого аналізу коду функції захисту (результат не передбачуваний для зловмисника).

4.6 Підсистема резервування даних

Забезпечення доступності оперативних даних операційної системи є важливою проблемою розробників операційної системи. Організація резервування в різних системах розглянуті в роботах [12, 13]. У зв'язку з особливими умовами експлуатації мобільні операційні системи повинні включати в себе різні додаткові механізми резервування даних. В процесі роботи операційної системи в будь-який момент може статися «нештатна ситуація». В операційній системі передбачений захист від:

1. раптове відключення живлення апаратної платформи виконання (наприклад, внаслідок дій користувача);
2. переривання процесу передачі даних (втрата або спотворення пакетів);
3. витяг відчужуваного носія інформації (наприклад, карти пам'яті MMC);
4. спотворення файлової системи внаслідок впливу статичної електрики (флеш-пам'ять схильна до стирання від впливу статичної електрики).

Варто сказати, що оскільки резервування є введення додаткової надмірності, а мобільна операційна система має обмежені ресурси, доцільно проводити резервування тільки тих даних, які дійсно мають критично великий вплив на операційну систему.

Система резервування даних постійної пам'яті розробленої операційної системи реалізована на базі віртуальної файлової системи. для
зберігання особливо критичних файлів використовується спеціальне файловий простір, яке фізично розташовується в незалежній пам'яті.
Захист даних оперативної пам'яті (особливо оперативних даних ядра ОС) здійснюється застосуванням механізмів захисту апаратної платформи (незалежна пам'ять).
Аналіз ефективності застосування в мобільній ОС
Метод захисту: підсистема резервування даних.
Відмінні риси: інтеграція з апаратними механізмами захисту.

4.7 Безпечне завантаження операційної системи безпровідної системи

У зв'язку із збільшеними можливостями сучасної електроніки велика кількість впроваджуваних систем, побутової техніки, мережевого обладнання, а також засобів захисту інформації та іншої продукції, яка має в своїй основі обчислювальні операції, розроблено на базі операційних систем.

Більшість виробників застосовують операційні системи в своїх продуктах в зв'язку з тим, що це дозволяє не витрачати час розробників на

написання драйверів для уніфікованої периферії. В операційних системах застосовуються різні методи захисту даних користувачів, а також авторських прав виробників на програмні рішення. Застосування уніфікованого апаратного забезпечення спільно з операційними системами, які використовують засоби захисту, породжують ще одну складну задачу - довірену завантаження операційної системи. Багато виробників операційних систем приділяють величезну увагу захисту операційної системи в процесі її завантаження. Прикладом може служити розробка корпорації Microsoft, описана в роботі [14]. Завантажувач операційної системи Microsoft Windows забезпечує перевірку автентичності ядра операційної системи і коректність апаратної платформи. У роботах [15, 16] також глибоко розглянуто процес довіреної завантаження операційної системи.

Завантаження операційної системи являє собою процес виходу програмних модулів операційної системи в штатний режим роботи після включення. В процес завантаження в залежності від архітектури ОС може включатися: передача управління ядру операційної системи; виконання процедур ініціалізації ядра операційної системи; запуск сервісів операційної системи; запуск прикладного програмного забезпечення.

Передача управління операційній системі є першим і невід'ємним етапом завантаження будь-якої ОС. Розглянемо процес завантаження на прикладі ядра CORTEX-M3. Згідно [9] пам'ять ядра CORTEX-M3 складається з декількох функціональних блоків пам'яті. До таких блокам відносяться оперативна пам'ять, постійний запам'ятовуючий пристрій (флеш-пам'ять). Процедури операційної системи розташовані в флеш-пам'яті контролера (простір пам'яті 0x8000000-0x0801FFFF). Принцип роботи ядра CORTEX-M3 полягає в тому, що ядро контролера виконує команду, розташовану в пам'яті за адресою, який заданий в спеціалізованому регістрі ядра контролера (лічильнику команд). Виконання команди може відбуватися практично з будь-якого дозволеного місця пам'яті (наприклад, з оперативної пам'яті).

Процес передачі управління операційній системі полягає в запису адреси першої процедури ядра ОС в регістр лічильника команд мікроконтролера. Захищеної операційній системі необхідно мати інформацію про місце її запуску. Також важлива інформація про те, чи є операційна система єдиним (саморозміщувані) користувачем апаратних ресурсів.

Підсистеми захисту операційних систем самі представляють собою звичайне додаток (процедури). Так само, як і інші додатки, підсистеми захисту можуть бути схильні до налагодженні. Для захисту оперативних даних процесів нерідко використовується апаратне розмежування доступу до пам'яті. Наприклад, в контролерах архітектури ARM фірми STMicroelectronics

мають спеціалізований модуль управління пам'яттю (MPU - Memory Protect Unit, модуль захисту пам'яті). Але навіть цей модуль не допоможе, якщо контролер знаходиться в режимі налагодження. Для мінімізації ймовірності вищеописаних загроз ядро операційної системи і повинно мати повне управління над апаратної платформою.

Деякі апаратні платформи (наприклад, контролери ARM фірми Atmel) надають можливості контролю завантаження з використанням загрузчиков. Завантажувач є програмою, призначену для безпечної передачі управління операційної системи (Рисунок 4.5).

Рисунок 4.5 - Розташування завантажувача в пам'ять

Завантажувач розташований в просторі стартовою завантаження процесора (Зазвичай цю адресу дорівнює 0). Додатково цей завантажувач захищений апаратно. Перезаписати завантажувач можна тільки спільно зі стиранням основний пам'яті.

Другою важливою проблемою завантаження операційної системи є питання автентичності модулів операційної системи. При використанні уніфікованих контролерів не завжди є можливість обмежити застосування засобів налагодження в процесі виконання операційної системи.

Теоретично будь-який модуль операційної системи може бути змінений зловмисником. Для захисту важливих частин операційної системи застосовують засоби контролю цілісності і електронного підпису, які також можуть бути інтегровані в програму-завантажувач.

Аналіз ефективності застосування в мобільній ОС.

Метод захисту: контроль цілісності і електронного підпису модулів в процесі завантаження ОС.

Рівень ефективності: високий.

Позитивні сторони: висока ефективність методів електронного підпису.

Негативні сторони: проблема автентичності ключа перевірки підпису (ключ також зберігається на пристрої та може бути підмінений зловмисником).

У розробленій операційній системі реалізована підсистема довіреної завантаження. В операційній системі є спеціалізований модуль завантаження.

Завантажувач вирішує цілий ряд проблем, пов'язаних можливістю завантаження неаутентичного програмного продукту в системі: перевірка автентичності найважливіших модулів операційної системи до її завантаження; розшифрування ядра операційної системи; безпечне оновлення ядра операційної системи; самоконтроль апаратних засобів.

На рисунку 4.6 зображено алгоритм роботи завантажувача розробленої операційної системи.

Для захисту найважливішого модуля операційної системи (ядра) застосовується шифрування тіла програми. Перед початком завантаження ядра операційної системи завантажувач виробляє розшифрування тіла ядра операційної системи. Як ключ використовуються наступні параметри:

- унікальний ідентифікатор контролера (мається у найбільш популярних виробників контролерів архітектури ARM, наприклад, фірм STMElectronics, Atmel);
- хеш найважливіших областей постійної пам'яті;
- персональний ключ пристрою.

Використовуючи вищевказані дані, виконується формування ключа шифрування. Відсутність явного зберігання ключа в пам'яті контролера дозволяє виключити атаки, засновані на аналізі постійної пам'яті контролера.

Аналіз ефективності застосування в мобільній ОС

Метод захисту: застосування ресурсів апаратної платформи при формуванні ключа шифрування.

Відмінні риси: відсутня необхідність зберігання результуючого ключа шифрування, прихильність ключа шифрування до конкретної апаратної платформи.

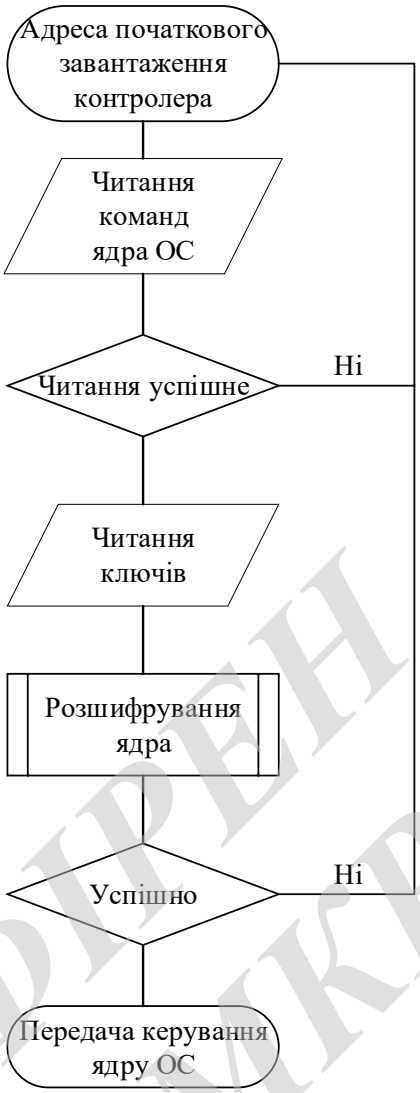


Рисунок 4.6 - Алгоритм роботи завантажувача

4.8 Безпечне оновлення операційної системи абонентського пристрою

Операційна система є вкрай складним програмним продуктом і містить в своєму складі велику кількість процедур. І, як все створене людиною, може містити помилки. Тому виробники операційних систем постійно вдосконалюють свої продукти. У роботах [17, 18] розглядаються основні принципи побудови загрузчиков, що забезпечують оновлення модулів програмного забезпечення. Крім забезпечення заміни програмних модулів додатково необхідно забезпечити безпеку процесу оновлення операційної системи.

На рисунку 4.7 (оригінальне зображення з документа [19]) зображений алгоритм роботи безпечного завантажувача фірми Atmel для контролерів архітектури ARM власного виробництва.

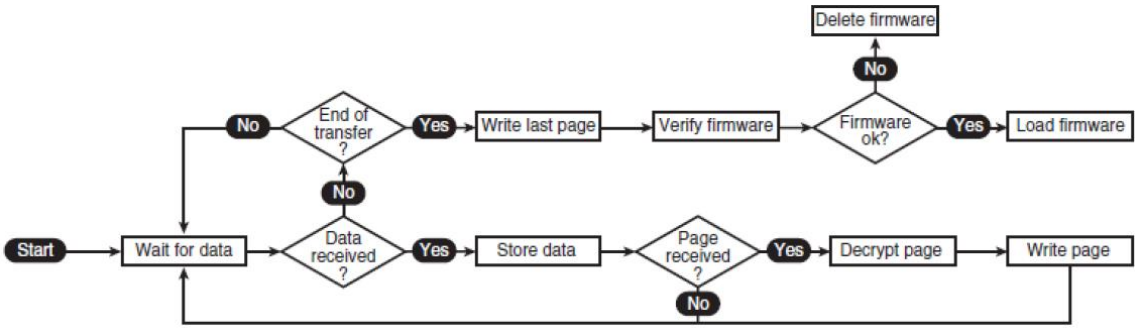


Рисунок 4.7 - Алгоритм роботи безпечного завантажувача фірми Atmel

В даному засобі завантаження передбачені різні засоби передачі даних (USB, USART). Процес передачі образу операційної системи контролюється по блоках. При отриманні чергового блоку даних проводиться перевірка коректності передачі. Після передачі останнього блоку даних проводиться перевірка отриманого образу. На останньому етапі проводиться оновлення операційної системи з образу.

Аналіз ефективності застосування в мобільній ОС.

Метод захисту: Алгоритм безпечного оновлення.

Рівень ефективності: середній.

Переваги: захист поновлення при передачі по мережі.

Недоліки: необхідність перезавантаження для оновлення програмних модулів, відсутня перевірка справжності оновлень.

Наявність підсистеми поновлення є важливою конкурентною характеристикою операційної системи. Ця підсистема не обов'язково повинна мати можливість «поновлення через інтернет». Основним її завданням є забезпечення можливості безпечного оновлення програмного забезпечення. Ця функція може бути реалізована і найпростішим шляхом «перепрошивки» мікроконтролера.

Розроблена операційна система має в своєму складі засоби безпечного забезпечення програмного забезпечення. Підсистема поновлення включає в себе:

- безпечний завантажувач операційної системи з функцією оновлення (для поновлення ядра операційної системи);

- прикладний сервіс поновлення (для оновлення модулів операційної системи і користувальницьких додатків).

В завантажувач операційної системи, який був описаний в попередньому розділі, вбудовані функції безпечного оновлення. Для здійснення оновлення ядра операційної системи завантажувачу необхідно перейти зі стандартного режиму «завантаження» в режим оновлення. В даному режимі завантажувач

не виконуватиме свою пряму задачу - завантаження операційної системи. В даному режимі завантажувач приймає на себе управління апаратними засобами контролера, а конкретно ініціює підключення до інтерфейсу USB. З точки зору комп'ютера підключення пристрою ніяк не відрізняється від стандартного режиму роботи пристрою.

Використовуючи інтерфейс USB, завантажувачу
передається пакет оновлень. Далі проводиться перевірка справжності пакета оновлення та оновлення. Процес перевірки передачі пакета в контролер побудований за класичною схемою, яка була описана в третьому розділі. Більш важливим є процес перевірки автентичності пакета поновлення.

Блок-схема алгоритму перевірки автентичності пакета поновлення зображена на рисунку 4.8.

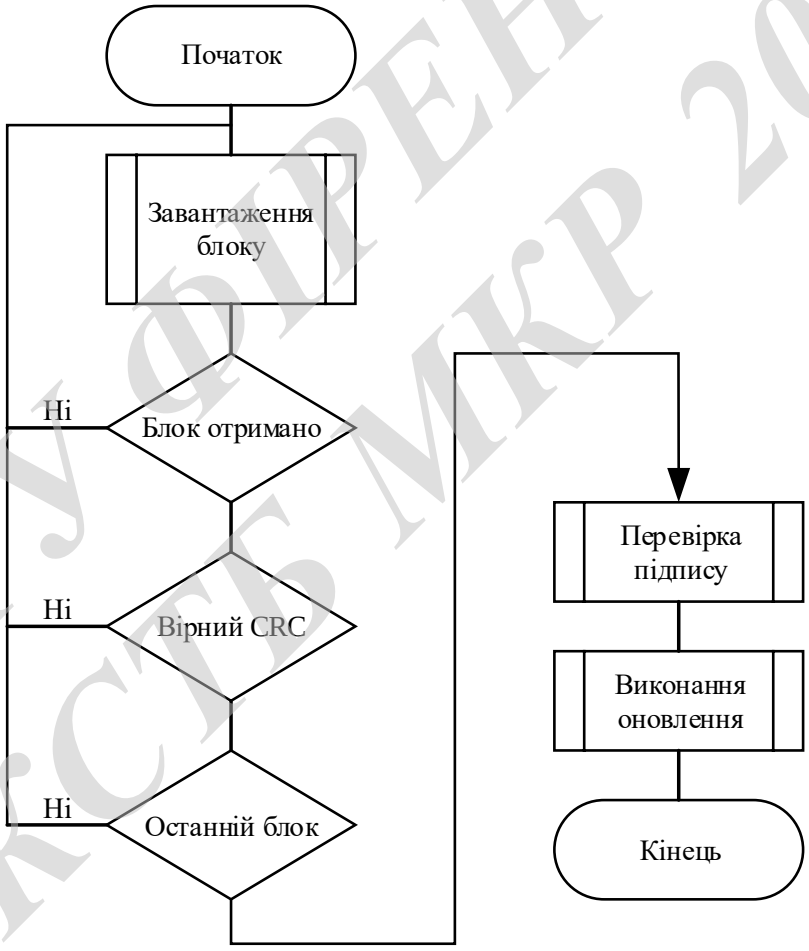


Рисунок 4.8 - Алгоритму перевірки автентичності пакета поновлення

Спочатку варто сказати, що в операційній системі пропонується застосовувати три групи оновлень: персональні поновлення (поновлення, які необхідно встановити на певний пристрій); групові оновлення (оновлення, які

призначені для цілого класу пристроїв); загальні оновлення (оновлення, призначені для всіх пристроїв, працюючих на основі розробленої ОС).

Крім вищевказаного розподілу, оновлення також мають різний рівень критичності: критичні оновлення (оновлення, які виправляють фатальні помилки в роботі операційної системи); оновлення безпеки (поновлення, що впливають на процес забезпечення безпеки операційної системи); поновлення прикладного програмного забезпечення.

Аналіз ефективності застосування в мобільній ОС

Метод захисту: безпечне оновлення ПЗ.

Відмінні риси: перевірка справжності оновлень, категоризація оновлень.

4.9 Висновки до розділу 4

В даному розділі буде акцентовано увагу на результати виконаної роботи. Технічні характеристики розробленої операційної системи багато в чому обумовлені двома факторами: середовищем застосування операційної системи - мобільні системи; вимогами інформаційної безпеки.

У розробленій операційній системі підсистема інформаційної безпеки глибоко інтегрована в системні служби. ОС забезпечує ешелоновану систему захисту від найбільш актуальних загроз безпеки, які були описані у другому розділі.

Вся система захисту операційної системи побудована в ключі, запропонованому в [11]. Два основні підходи, що описують дану концепцію побудови підсистем захисту це:

- забезпечення безпеки взаємодії процесів є прямим завданням операційної системи (операційна система зобов'язана забезпечити безпеку взаємодії своїх "клієнтів");
- для забезпечення вимог безпеки операційна система може вимагати від процесу виконання деяких вимог.

Далі буде узагальнена загальна структура розроблених підсистем захисту мобільної операційної системи.

Підсистема аутентифікації. Кількісна оцінка стійкості стандартної пральний системи аутентифікації користувачів виконується відповідно до наступної формули.

$$P = \frac{VT}{A^L}$$

де

A - потужність алфавіту символів, з яких складається пароль;

L - довжина пароля;

V - швидкість перебору паролів зловмисником;

T - термін дії паролів;

P - ймовірність підбору паролів зловмисником за час t, менше терміну дії паролів.

Підсистема аутентифікації операційної системи підтримує гнучке налаштування пральний політики. Пароль користувача може включати в себе символи латинського алфавіту, цифри, спеціальні символи. Передбачено захист від перебору (стандартно: блокування доступу на 5 хвилин після 3 невдалих спроб ввести пароль). Для прикладу, пароль в 6 символів (символи латинського алфавіту, цифри, спеціальні символи) і терміном дії в 1 рік має можливість вибору пароля протягом терміну дії пароля в гіршому випадку становить приблизно.

Для безпечного віддаленого управління операційною системою передбачена можливість використання аутентифікації з використанням одноразових паролів. Картка паролів передбачає використання цифрових паролів розміром в 8 символів. В даному випадку простір паролів значно менше порядку. Але так як скорочується час використання одного пароля, значення ймовірності підбору пароля протягом терміну дії пароля має порівнянні значення. Що дозволяє також ефективно застосовувати даний метод аутентифікації.

Додатково підсистема аутентифікації ОС надає можливість захисту користувачів від змушують атак. За потреби може бути згенерований додатковий набір альтернативної пральний інформації. В роботі була запропонована схема організації підсистеми аутентифікації локальних користувачів на основі отрицаемого шифрування.

Криптографічна підсистема операційної системи має розвинену структуру ключової інфраструктури. Даний підхід дозволяє в деяких випадках економити ресурси системи шляхом застосування менш стійких алгоритмів шифрування без шкоди її безпеки [11]. Підсистема реалізує як стандартні криптографічні алгоритми, так і додатково розроблені.

В ході дослідження було запропоновано ефективний алгоритм, що заперечується шифрування на основі блокових шифрів [8]. Швидкість простого алгоритму отрицаемого шифрування з використанням блочного шифру (див. Розділ Алгоритм отрицаемого шифрування).

Було досягнуто збільшення продуктивності ЗОШ в продуктивності в 2u раз. Даний факт дозволяє використовувати заперечне шифрування в розробленій мобільну операційну систему. Заперечується шифрування застосовується в операційній системі: в підсистемі аутентифікації; в

підсистемі захисту від налагодження; в криптографічній підсистемі (як функція).

Економія ресурсів системи. У зв'язку з обмеженою кількістю ресурсів було прийнято рішення застосовувати в операційній системі схеми почергового виконання завдань спеціалізованим сервісом. Дана схема доступна для використання в прикладних програмних продуктах з фонової завданнями. Схема застосовується в наступних підсистемах: сервіс контролю доступу до ФС; системі захисту переданих даних; криптографічній підсистемі.

Дане рішення дозволило заощадити оперативну пам'ять мобільної операційної системи. Що дозволить запускати більшу кількість додатків. Наприклад, реалізація функцій доступу до файлової системи в режимі API функцій для одного процесу вимагає виділення оперативної пам'яті в розмірі не менше 2 кбайт. З огляду на розмір оперативної пам'яті цільових платформ приблизно 20-40 кбайт, таке марнотратство неприпустимо в мобільних системах. Схема застосування спеціалізованих служб виконання завдань дозволяє не виділяти пам'ять для реалізації функцій доступу до файлової системи кожному процесу.

Захист програмного забезпечення від налагодження. В ході дослідження були розроблені методи захисту прикладного програмного забезпечення від налагодження з використанням алгоритмів, що заперечується шифрування [6]. У даних методах ЗОШ застосовується як додаткова перешкода для використання алгоритмів аналізу програмного забезпечення. В роботі запропоновані методи захисту від: статичного аналізу машинного коду (дизассемблирования); активного аналізу додатки з використанням отладчиков шляхом введення хибних гілок коду; використання елементів аналізу зовнішнього середовища.

Віртуальне середовище виконання. Дуже великою загрозою операційній системі є прикладне програмне забезпечення. Прикладні програми приносять в системи помилки програмістів, виняткові ситуації і навіть спеціальні програмні закладки. Для захисту від даного виду загроз була обрана найбільш безпечна схема контролю програмного забезпечення віртуальне середовище виконання додатків. На базі операційної системи реалізований компілятор програмного забезпечення, який призводить програмний код в зручний вид для віртуального середовища виконання.

Застосування штатного компілятора дозволить в подальшому впровадити в систему алгоритми аналізу програмного коду на наявність декларованих можливостей. Для написання програмного забезпечення пропонується використовувати мову, подібний мови ASSEMBLER. У віртуальному середовищі виконання реалізовані основні функції мови

ASSEMBLER. Для додаткового захисту в зв'язці з віртуальним середовищем виконання працює підсистема контролю пам'яті, яка дозволяє надійно ізолювати пам'ять процесів.

Резервування ресурсів. Мобільна операційна система відрізняється наявністю природних загроз функціонування, які пов'язані з особливостями експлуатації операційної системи (наприклад, можливістю раптового відключення). Захист програмного забезпечення від можливих наслідків експлуатації виконується цілим рядом рішень:

- система контролю пам'яті забезпечує резервування оперативною пам'яттю важливих процесів в незалежній пам'яті;
- наявність різних режимів роботи ядра операційної системи;
- записування файлових операцій для можливості подальшого відновлення.

Триразове резервування даних прикладних програм дозволяє експлуатування розроблену ОС в мобільних системах.

Комплексне використання підсистем захисту різного типу дозволяє значно збільшити загальну захищеність системи. В цьому розділі вирішені наступні завдання дослідження: розробка методів захисту програмного забезпечення від дизасемблювання.

5 ЕКОНОМІЧНА ЧАСТИНА

5.1 Визначення рівня комерційного потенціалу дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX

Метою проведення технологічного аудиту є оцінювання комерційного потенціалу дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX, створеної в результаті науково-технічної діяльності. В результаті оцінювання можна буде зробити висновок щодо напрямів (особливостей) організації подальшого її впровадження з врахуванням встановленого рейтингу.

Для проведення технологічного аудиту залучимо 3-х незалежних експертів. У нашому випадку такими експертами будуть керівник магістерської роботи та провідні викладачі випускової та споріднених кафедр.

Оцінювання комерційного потенціалу дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX будемо здійснювати за 12-ю критеріями згідно рекомендацій.

Результати оцінювання комерційного потенціалу дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX заносимо до таблиці 5.1.

Таблиця 5.1. - Результати оцінювання комерційного успіху дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX

Критерії	Експерти		
	Стальченко О.В., к.т.н., доцент	Стальченко О.В., к.т.н., доцент	Стальченко О.В., к.т.н., доцент
	Бали, виставлені експертами		
1	2	2	2
2	3	1	3
3	2	2	3
4	3	1	2
5	3	2	3
6	2	2	2
7	3	2	3
8	2	2	2
9	3	2	1
10	3	3	3

11	2	2	3
12	3	3	2
Сума балів	31	24	29
Середньоарифметична сума балів, СБ	28		

За даними таблиці 5.1 робимо висновок щодо рівня комерційного потенціалу дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX. При цьому користуємося рекомендаціями, наведеними в таблиці 5.2.

Таблиця 5.2 – Рівні комерційного потенціалу розробки

Середньоарифметична сума балів, розрахована на основі висновків експертів	Рівень комерційного потенціалу розробки
0 – 10	Низький
11 – 20	Нижче середнього
21 – 30	Середній
31 – 40	Вище середнього
41 – 50	Високий

Таким чином, робимо висновок, щодо рівня комерційного потенціалу нашої дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX – середній.

Прогнозування витрат на виконання науково-дослідної, дослідно-конструкторської та конструкторсько-технологічної роботи

5.2 Розрахунок витрат, що стосуються виконавців дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX

Основна заробітна плата кожного із розробників (дослідників) Зо, якщо вони працюють в наукових установах бюджетної сфери:

$$Зо = \frac{М}{Тр} \cdot t, \qquad (5.1)$$

де М – місячний посадовий оклад конкретного розробника (інженера, дослідника, науковця тощо), грн.

У 2019 році величини окладів (разом з встановленими доплатами і надбавками) рекомендується брати в межах (5000…10000) грн. за місяць; Тр – число робочих днів в місяці; приблизно Тр = (21…23) дні; t – число робочих днів роботи розробника (дослідника).

Зроблені розрахунки зводимо до таблиці 5.3.

Таблиця 5.3 – Заробітна плата розробників

Посада	Місячний посадовий оклад, грн.	Оплата за робочий день, грн.	Число днів роботи	Витрати на заробітну плату, грн.
Керівник	10000	455	5	2275
Інженер-програміст	7500	341	5	1705
Консультанти	5000	227	5	1135
Всього:				5115

Додаткова заробітна плата Зд всіх розробників та робітників, які брали участь у виконанні даного етапу роботи, розраховується як (10…12)% від суми основної заробітної плати всіх розробників та робітників, тобто:

$$Зд = 0{,}1 \cdot (Зр + Зо) = 0{,}1 \cdot (5115) = 511{,}5 \text{ грн.} \quad (5.4)$$

Нарахування на заробітну плату Нзп розробників та робітників, які брали участь у виконанні даного етапу роботи, розраховуються за формулою:
де Зо – основна заробітна плата розробників, грн.; Зр – основна заробітна плата робітників, грн.; Зд – додаткова заробітна плата всіх розробників та робітників, грн.; β – ставка єдиного внеску на загальнообов'язкове державне соціальне страхування, % (приймаємо для 1-го класу професійності ризику 22%).

$$Нзп = 0{,}22 \cdot (Зр + Зо + Зд) = 0{,}22 \cdot (5115 + 511{,}5) = 1237 \text{ грн.} \quad (5.5)$$

Амортизація обладнання, комп'ютерів та приміщень А, які використовувались під час (чи для) виконання даного етапу роботи.

Дані відрахування розраховують по кожному виду обладнання, приміщенням тощо.

У спрощеному вигляді амортизаційні відрахування А в цілому бути розраховані за формулою:

$$А = \frac{Ц \cdot На}{100} \cdot \frac{Т}{12},$$

де Ц – загальна балансова вартість всього обладнання, комп'ютерів, приміщень тощо, що використовувались для виконання даного етапу роботи, грн.; На – річна норма амортизаційних відрахувань. Для нашого випадку можна прийняти, що На = (10...25)%; Т – термін, використання обладнання, приміщень тощо, місяці.

Таблиця 5.4 - Амортизаційні відрахування

Найменування	Ціна, грн.	Норма амортизації, %	Термін використання, м.	Сума амортизації
Комп'ютер	7900	20	1	132
Лабораторний стенд	22000	20	1	367
Всього	499			

Витрати на комплектуючі К, що були використані під час виконання даного етапу роботи, розраховуються за формулою:

$$К = \sum_1^n Ні \cdot Ці \cdot Кі, грн$$

де Ні – кількість комплектуючих і-го виду, шт.; Ці – ціна комплектуючих і-го виду, грн.; Кі – коефіцієнт транспортних витрат, Кі = (1,1…1,15); n – кількість видів комплектуючих.

Таблиця 5.5 - Комплектуючі, що використані на розробку

Найменування матеріалу	Ціна за одиницю, грн.	Витрачено	Вартість, грн.
Полікорова гібридна плата	18,3	1	18,3
Пермикач двопозиційний	14,8	1	14,8
НВЧ діод	15,4	1	15,4
Котушка індуктивності з феритовим осердям	4,65	1	4,65

Резистор	0,75	2	1,5
Конденсатор – 3,3 нФ	2,05	1	2,05
Конденсатор – 47 нФ	2,2	1	2,2
Роз'єми	8,1	2	16,2
Коаксіальний кабель з вхідним опором 50 Ом	8,4	1	8,4
Всього, з урахуванням коефіцієнта транспортних витрат	315		

Витрати на силову електроенергію Ве, якщо ця стаття має суттєве значення для виконання даного етапу роботи, розраховуються за формулою:

$$Ве = В \cdot П \cdot Ф \cdot Кп, грн$$

В – вартість 1 кВт-год. електроенергії, в 2019 р. В ≈ 8,45 грн./кВт; П – установлена потужність обладнання, кВт; Ф – фактична кількість годин роботи обладнання, годин, Кп – коефіцієнт використання потужності; Кп < 1.

Потужність обладнання складає – 0,5 кВт.

Кількість годин роботи складає – 700 годин.

Коефіцієнт викор. потужності -0,9.

Ве=2662 грн.

Інші витрати Він охоплюють: витрати на управління організацією, оплата службових відряджень, витрати на утримання, ремонт та експлуатацію основних засобів, витрати на опалення, освітлення, водопостачання, охорону праці тощо.

Інші витрати Ів можна прийняти як (100…300)% від суми основної заробітної плати розробників та робітників, які були виконували дану роботу, тобто:

$$Ів = 1 \cdot (Зо + Зр) = 1 \cdot (5115) = 5115 \text{ грн.} \qquad (5.6)$$

Сума всіх попередніх статей витрат дає витрати на виконання даної частини (розділу, етапу) роботи – В.

$$В = 15454 \text{ грн.}$$

5.3 Розрахунок загальних витрат на дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX

Загальна вартість всієї наукової роботи визначається за Взаг формулою:

$$\text{Взаг} = \frac{\text{Ів}}{\alpha} = \frac{5115}{0{,}6} = 8525 \text{ грн}, \quad (5.7)$$

де α – частка витрат, які безпосередньо здійснює виконавець даного етапу роботи, у відн. одиницях.

5.4 Прогнозування витрат на виконання та впровадження дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX

Прогнозування загальних витрат ЗВ на виконання та впровадження дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX здійснюється за формулою:

$$\text{ЗВ} = \frac{\text{Взаг}}{\beta} = \frac{8525}{0{,}1} = 85250 \text{ грн}, \quad (5.8)$$

де β – коефіцієнт, який характеризує етап (стадію) виконання даної роботи.

Так, якщо розробка знаходиться: на стадії науково-дослідних робіт, то β ≈ 0,1; на стадії технічного проектування, то β ≈ 0,2; на стадії розробки конструкторської документації, то β ≈ 0,3; на стадії розробки технологій, то β ≈ 0,4; на стадії розробки дослідного зразка, то β ≈ 0,5; на стадії розробки промислового зразка, β ≈ 0,7; на стадії впровадження, то β ≈ 0,9.

5.5 Прогнозування комерційних ефектів від реалізації дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX

З метою прогнозування комерційних ефектів від реалізації дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX складемо таблицю вихідних показників, за рахунок яких і відбуватиметься отримання комерційного ефекту.

Таблиця 5.6 – Вихідні дані для прогнозування комерційного ефекту від реалізації дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX

Рік реалізації розробки	1
Кількість од. реалізації, шт.	1

Збільшення чистого прибутку підприємства Пі для кожного із років, протягом яких очікується отримання позитивних результатів від впровадження розробки, розраховується за формулою:

$$\Delta\text{Пі} = \sum_1^n (\Delta\text{Ц0} \cdot N + \text{Ц0} \cdot \Delta N)\text{і} \cdot \rho \cdot \gamma \cdot (1 - \frac{v}{100}) \quad (5.9)$$

де ΔПо – покращення основного оціночного показника від впровадження результатів розробки у даному році. Зазвичай таким показником може бути ціна одиниці нової розробки; N – основний кількісний показник, який визначає діяльність підприємства у даному році до впровадження результатів наукової розробки; ΔN – покращення основного кількісного показника діяльності підприємства від впровадження результатів розробки; Цо – основний оціночний показник, який визначає діяльність підприємства у даному році після впровадження результатів наукової розробки; n – кількість років, протягом яких очікується отримання позитивних результатів від впровадження розробки; λ– коефіцієнт, який враховує сплату податку на додану вартість. У 2018 р. ставка податку на додану вартість дорівнює 20%, а коефіцієнт – 0,8333. З 2014 року ставка податку на додану вартість встановлена на рівні 17%, а коефіцієнт – 0,8547; ρ– коефіцієнт, який враховує рентабельність продукту. Рекомендується приймати – 0,2…0,3; υ– ставка податку на прибуток. У 2018 році – 21%, у 2013 році – 19%, а з 2014 року – 16%.

Збільшення чистого прибутку підприємства Пі протягом першого року складе: 167334 грн.

5.6 Розрахунок ефективності вкладених інвестицій та період їх окупності

5.6.1 Визначення абсолютної ефективності вкладених інвестицій у дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX

Для цього користуються формулою:

$$\text{Еабс} = (\text{ПП} - PV), \quad (5.10)$$

де ПП – приведена вартість всіх чистих прибутків, що їх отримає підприємство (організація) від реалізації результатів наукової розробки, грн.; PV – теперішня вартість інвестицій PV = ЗВ, грн.

У свою чергу, приведена вартість всіх чистих прибутків ПП розраховується за формулою:

$$ПП = \sum_1^т \frac{ΔПі}{(1+\tau)^t} \quad (5.11)$$

де ΔПі– збільшення чистого прибутку у кожному із років, протягом яких виявляються результати виконаної та впровадженої НДДКР, грн.; т – період часу, протягом якого виявляються результати впровадженої НДДКР, роки; τ– ставка дисконтування, за яку можна взяти щорічний прогнозований рівень інфляції в країні; для України цей показник знаходиться на рівні 0,1; t – період часу (в роках) від моменту отримання чистого прибутку до точки „0”.

$$ПП = 167334 \text{ грн.},$$
$$Еабс = 167334 - 85250 = 82084 \text{ грн.}$$

Оскільки Еабс > 0, то результат від проведення наукових досліджень та їх впровадження принесе прибуток, але це також ще не свідчить про те, що інвестор буде зацікавлений у фінансуванні дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX.

5.6.2 Розрахунок відносної ефективності вкладених коштів в НДДКР дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX

Для цього користуються формулою:

$$Ев = \sqrt[т]{1 + \frac{Еабс}{PV}} - 1 \quad (5.12)$$

де Еабс – абсолютна ефективність вкладених інвестицій, грн..; PV – теперішня вартість інвестицій PV = ЗВ, грн.; Тж – життєвий цикл наукової розробки, роки.

$$Ев = 0{,}37$$

Далі, розрахована величина Ев порівнюється з мінімальною (бар'єрною) ставкою дисконтування, що дорівнює:

$$\tau = d + f, \quad (5.13)$$

де d – середньозважена ставка за депозитними операціями в комерційних банках; в 2018 році в Україні d = (0,14...0,2); f – показник, що характеризує ризикованість вкладень; зазвичай, величина f = (0,05...0,1), але може бути і значно більше.

$$\text{Ев} = 0{,}37 \geq \tau = 0{,}2 + 0{,}1 = 0{,}3.$$

Оскільки величина Ев > τмін, то інвестор може бути зацікавлений у фінансуванні даної наукової розробки.

5.6.3 Розрахунок терміну окупності коштів, вкладених в наукову дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX

Термін окупності вкладених у реалізацію наукового проекту інвестицій Ток можна розрахувати за формулою:

$$\text{Ток} = \frac{1}{\text{Ев}} = \frac{1}{0{,}37} = 2{,}7 \text{ роки}. \quad (5.14)$$

Оскільки Ток < 3…5-ти років, то фінансування даної наукової дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX є доцільним.

6 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

Виробнича безпека, яку вивчає охорона праці, відіграє велику роль для працюючих тому, що якраз вона контролює фізичний стан трудівника, що не може не відображатись на його здоров'ї, житті, а також результативності праці зокрема і у сфері радіоелектроніки.

У даному розділі наводиться розгляд небезпечних, шкідливих [1] та уражаючих для людини і навколишнього довкілля факторів, які утворюються під час проведення дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX. Тут розглядаються, зокрема, технічні рішення з виробничої санітарії та гігієни праці, визначення допустимої довжини провідника (антени), при якій напруженість магнітного поля на робочому місці знаходиться в межах норми, технічні рішення з промислової та пожежної безпеки під час проведення дослідження, безпека в надзвичайних ситуаціях.

6.1 Технічні рішення з виробничої санітарії та гігієни праці

6.1.1 Мікроклімат та склад повітря робочої зони

Визначаємо для приміщення для проведення дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX, категорію важкості робіт за фізичним навантаженням – легка Іа.

Відповідно до [2] допустимі параметри мікроклімату у робочій зоні для холодного та теплого періодів року наведені в таблиці Р.1 додатку Р.

При опроміненні менше 25% поверхні тіла працівника, допустима інтенсивність теплового опромінення сладає 100 Вт/м^2.

Вміст шкідливих речовин в повітрі робочої зони не повинен перевищувати гранично допустимих концентрацій (ГДК) у повітрі робочої зони і підлягає систематичному контролю для запобігання можливості перевищення ГДК, значення яких для роботи з ЕОМ наведено в таблиці Р.2 додатку Р.

При використанні ЕОМ джерелом зараження повітря є також іонізація молекул речовин, що містяться в повітрі. Рівні позитивних та негативних іонів повинні відповідати [4] та приведені в таблиці Р.3 додатку Р.

З метою забезпечення нормованих параметрів мікроклімату і складу повітря робочої зони передбачено:

1) в приміщенні повинна бути встановлена система опалення для холодного і кондиціонування для теплого періодів року;

2) застосування вентиляції, яка видаляє забруднення або нагріте повітря з приміщення, а також за допомогою неї контролюється швидкість руху повітря і вологість.

6.1.2 Виробниче освітлення

Для забезпечення раціональних гігієнічних умов на робочих місцях великі вимоги висуваються до кількісних та якісних показників освітлення.

З точки зору задач зорової роботи в приміщенні, в якому проводиться робота з дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX, відповідно до [3] знаходимо, що вони відносяться до IV розряду зорових робіт. Приймаємо контраст об'єкта з фоном – великий та характеристику фону – середню, яким відповідає підрозряд зорових робіт *г*.

Нормовані значення коефіцієнта природного освітлення (КПО) та мінімальні значення освітленості для штучного освітлення наведені в таблиці Р.4 додатку Р.

Оскільки приміщення знаходиться у м. Вінниця (2-га група забезпеченості природним світлом), а світлові пройми розташовані за азимутом 225°, то для таких умов КЕО визначатиметься за формулою [3, 4]

$$e_N = e_н m_N \, [\%], \tag{6.1}$$

де $e_н$ – табличне значення КЕО для бокового освітлення, %;

m_N – коефіцієнт світлового клімату;

N – номер групи забезпеченості природним світлом.

Підставляючи відомі значення одержимо нормовані значення КПО для бокового та суміщеного освітлення:

$$e_{N.б} = 1{,}5 \cdot 0{,}85 = 1{,}28 \ (\%);$$
$$e_{N.с} = 0{,}9 \cdot 0{,}85 = 0{,}77 \ (\%).$$

Для забезпечення нормативних значень параметрів освітлення запропоновано:

1) при недостатньому природному освітлені в світлу пору доби доповнення штучним завдяки використанню газорозрядних ламп з утворенням системи суміщеного освітлення;

2) використання загального штучного освітлення в темну пору доби.

6.1.3 Виробничі віброакустичні коливання

Зважаючи на те, що під час експлуатації пристроїв крім усього іншого обладнання використовується устаткування, робота якого супроводжується шумом та вібрацією, необхідно передбачити захист від шуму та вібрації.

Визначено, що приміщення, в якому проводиться робота з дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX може містити робочі місця із шумом та вібрацією, що створюється вентиляторами блоку живлення комп'ютера і кулерами мікропроцесора, відеоадаптера.

З метою запобігання травмуванню працюючих під дією шуму він підлягає нормуванню. Головним нормативом з питань виробничого шуму, діючим в нашій країні, є [5], у відповідності з яким допустимі рівні звукового тиску, рівні звуку і еквівалентні рівні шуму на робочих місцях у виробничих приміщеннях не повинні бути більшими ніж значення, що приведені в таблиці Р.5 додатку Р. Норми виробничих вібрацій наведені в таблиці Р.6 додатку Р для локальної вібрації.

Для встановлення допустимих параметрів шуму та вібрації в приміщенні запропоновано:

1) оздоблення стін спеціальними перфорованими плитами, панелями з метою шумопоглинання;

2) контроль рівня шуму та вібрації не менше 1 разу на рік.

6.1.4 Виробничі випромінювання

Проведений аналіз умов праці показав, що приміщення, в якому проводиться робота з дослідження може містити електромагнітні випромінювання.

Гранично допустимі рівні електромагнітних полів наведені в таблиці 6.1.

Таблиця 6.1 – Гранично допустимі значення електромагнітних полів на робочих місцях згідно [14]

Параметри та одиниці вимірювання	Граничні значення в діапазонах частот					
	1-10 кГц	10-60 кГц	0,06-3 МГц	3-30 МГц	30-50 МГц	50-300 МГц
$E_{ГД}$, В/м	1000	700	500	300	80	
$ЕН_{Егд}$, $(В/м)^2 \cdot год$	120000	40000	20000	7000	800	
$Н_{ГД}$, А/м	75	57	50	–	3,0	–
$ЕН_{Нгд}$, $(А/м)^2 \cdot год$	675	390	200	–	0,72	–

Для забезпечення захисту та досягнення нормованих рівнів випромінювань потрібно використовувати екранування робочого місця і скорочення часу опромінення за рахунок перерв на відпочинок.

Для забезпечення захисту та досягнення нормованих рівнів випромінювань потрібно використовувати екранування робочого місця і скорочення часу опромінення за рахунок перерв на відпочинок.

Визначимо допустиму довжину провідника (антени), по якому протікає струм силою в $I = 5{,}4$ А, при якій напруженість магнітного поля на робочому місці, віддаленому на $r = 0{,}28$ м, знаходиться в межах норми.

Біля джерела ЕМВ виділяють ближню зону (зону індукції), що знаходиться на відстані $r \le \lambda / 2\pi$, і далеку зону (зону випромінювання), для якої $r > \lambda / 2\pi$, де λ – довжина хвилі, м.

Допустиму довжину провідника (антени) в умовах магнітного поля для ближньої зони можна визначити з формули

$$H_{бл} = \frac{IL}{4\pi r^2} \text{ [А/м]}, \tag{6.2}$$

звідки

$$L = \frac{4\pi r^2 H_{бл}}{I} \text{ [м]}, \tag{6.3}$$

де $H_{бл}$ – напруженість магнітного поля ближньої зони, А/м;

r – віддаленість робочого місця, м;

I – сила струму, А.

Для діапазону частот 0,06…3 МГц $H_{ГД} = 50$ А/м.

Підставляючи відомі значення у формулу (6.3), отримаємо:

$$L = \frac{4 \cdot 3{,}14 \cdot 0{,}28^2 \cdot 50}{5{,}4} = 9{,}118 \text{ (м)}.$$

6.2 Технічні рішення щодо промислової та пожежної безпеки під час проведення дослідження

6.2.1 Безпека щодо організації робочих місць

Робочі місця з відеодисплейним терміналом зобов’язані розміщатися на віддалі не менше ніж 1,5 м від стіни з віконними прорізами, від інших стін –

на віддалі 1 м, одне від одного на віддалі не менше як 1,5 м. У випадку розміщення робочих місць потрібно виключити ймовірність прямого засвічування екрану джерелом природного освітлення. Робоче місце доцільно розміщати так, щоб природне освітлення знаходилось збоку, переважно зліва [7].

Поверхня екрана має знаходитись на віддалі 400-700 мм від органів зору користувача. Висота робочої поверхні столу при виконанні роботи сидячи має регулюватися в межах 680-800 мм. Робочий стіл повинен мати простір для ніг висотою не менше 600 мм, шириною не менше як 500 мм, глибиною на рівні колін не менше 450 мм та на рівні витягнутої ноги не менше як 650 мм [8].

6.2.2 Електробезпека

У середині приміщення, в якому здійснюється робота з дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX, особливу увагу потрібно надати уникненню загрози ураження електричним струмом. У відповідності до [9] це приміщення належить до приміщень із підвищеною небезпекою ураження електричним струмом через наявність високої (понад 75 %) відносної вологості. Через це безпека використання електрообладнання має гарантуватись рядом заходів, що передбачають застосування ізоляції струмовідних елементів, захисного заземлення, захисних блокувань та ін [10].

6.2.3 Пожежна безпека

Відповідно до [11] приміщення, в якому проводиться робота з дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX, відноситься до категорії пожежної небезпеки В. Дане приміщення відноситься до 2-го ступеня вогнестійкості, в якому приміщення знаходяться в будівлі з несучими та огороджувальними конструкціями з природних або штучних кам’яних матеріалів, бетону, залізобетону із застосуванням листових і плитних негорючих матеріалів.

Мінімальні межі вогнестійкості будівельних конструкцій приміщення, що розглядається наведені в таблиці 6.7. В таблиці 6.8 приведено протипожежні норми проектування будівель і споруд.

Встановлюємо, що приміщення, де проводиться робота з дослідження, має бути обладнане двома вогнегасниками, пожежним щитом, а також ємністю з піском [12].

6.3 Безпека у надзвичайних ситуаціях. Дослідження безпеки роботи системи бездротових мереж в умовах дії загрозливих чинників НС

Надзвичайні ситуації (НС) та їхні загрозливі фактори можуть негативно впливати на безпеку роботи системи бездротових мереж, спрямованої на забезпечення послугами цифрового безпровідного зв'язку. Встановлено, що найбільшу небезпеку серед НС для даної системи становлять іонізуючі випромінювання та електромагнітний імпульс.

Дія іонізуючих випромінювань приводить як до оборотних, так і необоротних змін електричних властивостей інтегральних схем і твердотільних приладів. Так як вказані перетворення можуть спричиняти відмови електронних підсистем, значні зусилля в останні роки скеровуються на розробку методів, що дозволяють обминути погіршення параметрів радіоелектронної апаратури (РЕА) під час опромінення.

Електромагнітний імпульс (ЕМІ) пошкоджує напівпровідникові прилади, конденсатори, резистори тощо. Це становить велику небезпеку для РЕА, добре захищеної від впливу інших загрозливих чинників. Тому потрібно пам'ятати про те, що захист РЕА від механічних пошкоджень ушкоджень не оберігає від дії ЕМІ. Апаратури може втратити працездатність, знаходячись в безпечних захисних спорудженнях.

За відсутності спеціальних заходів захисту електромагнітний імпульс може спричиняти пошкодження радіоелектронної апаратури управління зв'язку, порушення роботи електричних пристроїв, підключених до зовнішніх ліній. Особливо піддаються дії електромагнітного імпульсу напівпровідникові, газорозрядні, вакуумні прилади, а також опори та конденсатори.

6.3.1 Дослідження безпеки роботи системи бездротових мереж в умовах дії іонізуючих випромінювань

Беручи до уваги елементну базу, яка застосовується при реалізації системи бездротових мереж, складемо таблицю рівнів радіації для кожного компонента $P_{зв.і}$, що викликають початок зворотних змін (табл. 6.1).

Знаходимо елемент, що найбільше піддається дії випромінювання, тобто елемент із найменшим значенням $P_{зв.min} = 10^4$ Р.

Розраховуємо граничне значення потужності експозиційної дози:

$$P_{гр} = K_{над} \cdot P_{в.min} \cdot K_{посл} \text{ [Р/год]}; \quad (6.9)$$

$$P_{гр} = 0{,}93 \cdot 10^4 \cdot 2 = 18600 \text{ (Р/год)},$$

де $K_{над}$ – коефіцієнт надійності (приймається $K_{над}$ = 0,93);

$P_{зв}$ – потужність експозиційної дози, яка відповідає початку зворотних змін в елементах;

$K_{посл}$ – коефіцієнт послаблення радіації (приймається $K_{посл}$ = 2).

Таблиця 6.1 – Рівні радіації кожного компонента

№	Елементи системи бездротових мереж	$P_{зв.і}$, Р/год	$P_{зв.min}$, Р/год
1	Транзистори серії КП	10^4	10^4
2	Діоди 1N4004	10^4	
3	Конденсатори СР-13.020	10^7	
4	Мікросхеми К1533	10^5	
5	Резистори СМД	10^8	

Отже, безпечне функціонування системи бездротових мереж в умовах дії іонізуючих випромінювань забезпечується при $P_{зв} <$ 18600 Р/год, а допустимий час його безвідмовної роботи може скласти:

$$t_{доп} = \left(\frac{Д_{гр} K_{посл}}{2P_1} + \sqrt{t_n} \right)^2 \text{ [год];} \qquad (6.10)$$

$$t_{доп} = \left(\frac{10^6 \cdot 2}{2 \cdot 18600} + \sqrt{1} \right)^2 = 2999{,}03 \text{ (год).}$$

6.3.2 Дослідження безпеки роботи системи бездротових мереж в умовах дії електромагнітного імпульсу

Вихідні дані: напруга живлення $U_{ж}$ = 12 ± 5% В; максимальна довжина горизонтальної струмопровідної частини електричної принципової схеми l_B = 0,28 м.

За критерій безпеки роботи РЕА в цих умовах приймаємо коефіцієнт безпеки:

$$K_в = 20 \lg \frac{U_д}{U_{в(г)}} \geq 40 \text{ [дБ],} \qquad (6.11)$$

де $U_д$ – допустимі коливання напруги живлення, В;

$U_{в(г)}$ – напруга наведення за рахунок електромагнітного імпульсу в вертикальних (горизонтальних) струмопровідних частинах, В.

Розраховуємо спочатку допустиме коливання напруги живлення:

$$U_д = U_ж + \frac{U_ж}{100} N \text{ [В]}, \tag{6.12}$$

$$U_Д = 12 + \frac{12}{100} \cdot 5 = 12{,}6 \text{ (В)};$$

де $U_ж$ – робоча напруга живлення, В;

N – допустимі коливання напруги, %.

Розраховуємо максимально очікувану напруга в горизонтальних лініях:

$$U_в = \frac{U_д}{10^{K/20}} \text{ [В]}; \tag{6.13}$$

$$U_в = \frac{12{,}6}{10^{40/20}} = 0{,}126 \text{ (В)};$$

де K – коефіцієнт безпеки (K = 40 дБ).

Визначаємо горизонтальну складову напруженості електромагнітного поля за формулою:

$$E_г = \frac{U_в}{l_в} \text{ [В/м]}; \tag{6.14}$$

$$E_г = \frac{0{,}126}{0{,}28} = 0{,}45 \text{ (В/м)};$$

Розраховуємо горизонтальну складову напруженості електромагнітного поля за формулою

$$E_в = 10^3 E_г \text{ [В/м]}, \tag{6.15}$$

$$E_в = 10^3 \cdot 0{,}45 = 450 \text{ (В/м)}.$$

Згідно з виконаними розрахунками безпека роботи системи бездротових мереж в умовах впливу електромагнітного імпульсу можлива при напруженості вертикальної складової електричного поля $E_в$ < 450 В/м.

6.3.3 Розробка превентивних заходів по підвищенню безпеки роботи системи бездротових мереж в умовах надзвичайних ситуацій

З метою зниження негативної дії уражаючих на РЕА системи бездротових мереж потрібно застосувати наступні заходи.

Боротьба з впливом іонізуючого випромінювання може бути здійснена новітнім вітчизняним методом, який полягає у захисному покритті радіоелектронної апаратури, що розташовуються на поверхнях цих елементів, які піддаються впливу іонізуючого випромінювання, при цьому захисне покриття виконане у вигляді наноструктури, яка містить сукупність атомів рідкоземельних елементів, введених у будову армованої атомно-молекулярної металічної матриці, або утворює її захисний прошарок.

Боротьба з впливом електромагнітного імпульсу виконується струмопровідними сітками та плівковим покриттям вікон, стільниковими металевими конструкціями для повітрозбірників і вентиляційних отворів, а також пружинними контактними прокладками, що розташовуються по периметру дверей і люків.

Товщину захисного екрану знаходимо за формулою:

$$t = \frac{A}{k\sqrt{f}} \text{ [см];} \qquad (6.16)$$

$$t = \frac{14}{5{,}2 \cdot \sqrt{15000}} = 0{,}022 \text{ (см)} = 0{,}22 \text{ (мм)},$$

де A – перехідне затухання енергії електричного поля стальним екраном (A = 14 дБ);

k – коефіцієнт, що для стального екрана дорівнює 5,2;

f – найбільш характерна частота (f = 15000 Гц).

6.4 Висновки до розділу 6

Отже в даному розділі нами було розглянуто такі питання охорони праці, як технічні рішення з гігієни праці та виробничої санітарії, технічні рішення з промислової та пожежної безпеки.

Також у даному розділі нами було досліджено безпеку роботи системи бездротових мереж в умовах впливу загрозливих факторів НС. Запропоновано превентивні заходи із підвищення безпеки роботи системи бездротових мереж в умовах НС. Визначено, що допустимий час безвідмовної роботи системи в умовах дії радіації може скласти майже 3000 год при коефіцієнті ослаблення радіації $K_{осл}$ = 2. Розраховано, що екранування стальним екраном товщиною 0,22

мм захищає системи бездротових мереж від дії електромагнітного імпульсу для перехідного затухання енергії електричного поля в 14 дБ.

В результаті написання цього розділу було розглянуто такі питання охорони праці та безпеки в надзвичайних ситуаціях, як технічні рішення з гігієни праці та виробничої санітарії, визначення допустимої довжини провідника (антени), при якій напруженість магнітного поля на робочому місці знаходиться в межах норми, технічні рішення з промислової та пожежної безпеки під час проведення дослідження методів забезпечення інформаційної безпеки в системі бездротових мереж WiMAX, безпека у надзвичайних ситуаціях.

ВИСНОВКИ

Цілями цієї роботи є дослідження методів захисту інформації в розподілених бездротових мережах, в умовах впливу навмисних атак та розробка алгоритму кодування для зебезпечення передачі інформації в мережах з радіодоступом.

Для досягнення поставлених цілей були вирішені наступні завдання:

1. Були розглянуті основні види загроз інформації, в бездротових мережах. Розкрито специфіку загроз в бездротових розподілених мережах. Проаналізовано рекомендації стандартів забезпечення безпеки в бездротових мережах. Розглянуто існуючі методи захисту інформації в бездротових мережах, описані їхні переваги і недоліки. Показано, що більшість існуючих методів є вузькоспеціалізованими при протидії загрозам інформації, а також не застосовні в силу різних обмежень для захисту деяких видів інформації.

Це зумовлює необхідність розробки і реалізації спеціалізованих методів захисту інформації, переданої в бездротових мережах, спрямованих на вирішення поставлених завдань.

У представленій роботі запропонована альтернативна методика захисту конфіденційності та забезпечення доступності інформації, переданої в бездротових мережах. Дана методика заснована на застосуванні додатки динамічної маршрутизації «маршрутизації сервіс» і дозволяють вирішувати задачу захисту інформації без застосування алгоритмів шифрування.

В результаті виконання роботи досліджений алгоритм динамічної маршрутизації трафіку. На основі даного алгоритму реалізований «маршрутизації сервіс» передачі даних через розподілені мережі. Вироблені основні компоненти, необхідні для функціонування системи. Дано оцінки вірогідності мережевих атак на передану інформацію в разі застосування «маршрутизації сервісу».

Отримані оцінки реалізації мережевих атак показують, що застосування додатка «маршрутизації сервіс» дозволяє підвищити безпеку передачі інформації в розподілених бездротових мережах. Підвищення захищеності інформації в розподілених бездротових мережах при використанні SM досягається за рахунок підвищення захисту її конфіденційності, цілісності і доступності. Цілісність і конфіденційність інформації, що передається забезпечується зменшенням ймовірності реалізації мережевих атак на контрольованих ділянках проходження трафіку в разі застосування маршрутизації сервісу. Доступність обґрунтовується стійкістю системи до блокування порушником одного або декількох довірених серверів.

В результаті виконаного дослідження вирішені важливі науково-технічні завдання розробки продуктивних методів і алгоритмів псевдовероятностного захисного перетворення, що задовольняють критерію обчислювальної нерозрізненості від імовірнісного захисного перетворення, і універсальної захищеної мобільної операційної системи, яка забезпечує переносимість програмних засобів захисту інформації на різні типи мобільних пристроїв (технічних платформ) і забезпечує захист користувачів системи та інформації від атак з примусом за рахунок застосування псевдовероятностного захисного перетворення. Рішення даних завдань дозволило досягти заявленого скорочення термінів і зменшення витрат по розробці мобільних захищених інформаційних технологій.

Основні результати дослідження:

1. розроблений метод аутентифікації користувачів з використанням одноразових паролів, що генеруються за допомогою алгебраїчного алгоритму псевдовероятностного захисного перетворення, який забезпечує захист від примушують атак;

2. розроблений метод псевдовероятностного захисного перетворення інформації, що забезпечує захист інформації від несанкціонованого доступу в разі атак на примусову працю;

3. розроблений метод захисту програмного забезпечення від дизассемблирования, заснований на введенні помилкових гілок коду за допомогою псевдовероятностного захисного перетворення коду;

4. розроблений метод протидії активної налагодженні програмного забезпечення з використанням псевдовероятностного захисного перетворення для введення хибних гілок коду;

5. розроблений метод зберігання ключів шифрування, заснований на застосуванні псевдовероятностного захисного перетворення для забезпечення можливості приховування наявності резервних серій ключів;

6. розроблений протокол аутентифікації з використанням одноразових паролів на основі алгебраїчного алгоритму псевдовероятностного захисного перетворення. Протокол забезпечує додатковий захист віддалених користувачів від примушує атаки;

7. запропонована схема підсистеми аутентифікації локальних користувачів операційної системи, в якій передбачений захист від примушує атаки. В основі даного алгоритму лежить алгоритм псевдовероятностного захисного перетворення.

В процесі роботи проводилася розробка механізмів застосування отрицаемого шифрування в механізмах захисту інформації операційних систем.

Новизна роботи полягає в тому, що застосування універсальної операційної системи в мобільних пристроях телекомунікаційних та інформаційних систем, в тому числі в системах захисту інформації, дозволить уніфікувати підходи до забезпечення безпеки при розробці таких систем. Даний підхід значно скоротить витрати на розробку і виробництво мобільних пристроїв на схожих апаратних платформах. Область застосування ОС: аунтетифікуючі пристрої (маркери, ідентифікатори), системи охорони, пристрої захисту програмного забезпечення, персональні пристрої зберігання даних (захищені файлові сховища), апаратні засоби шифрування (криптопровайдери).

СПИСОК ЛІТЕРАТУРИ

1. Параметры прогнозирования и идентификации атак в информационнокоммуникационных системах / [Азарсков В. Н., Гизун А. И., Грехов А. М., Скворцов С. А.] // Науково-практичний журнал “Захист інформації”. – 2014. – Т. 16. – № 1. – С. 89–95.

2. Корченко А. О. Система виявлення та ідентифікації порушника в інформаційно-комунікаційних мережах / А. О. Корченко, В. В. Волянська, Гізун А. І. // Науково-практичний журнал “Безпека інформації”. – 2013. – Т. 19. – № 3. – С. 158–162.

3. Шевченко А. С. Метод оцінювання ризиків з урахуванням впливу механізмів захисту інформації на параметри безпроводових інформаційнотелекомунікаційних систем під час інформаційних операцій / А. С. Шевченко, О. В. Кокотов // Науково-практичний журнал “Безпека інформації”. – 2014. – Т. 20. – № 1. – С. 7–11.

4. Славінський С. Деякі питання метрологічного забезпечення у цифрових телекомунікаціях й системах зв’язку / С. Славінський // Стандартизація, сертифікація, якість. – 2009. – № 3. – С. 28–34.

5. Системна безпека технологій безпровідного зв’язку: моделі загроз та захисту мовної інформації / [Дудике- вич В. Б., Микитин Г. В., Ребець А. І., Банах Р. І.] // Матеріали ІІІ міжнародної науково-технічної конференції “Захист інформації і безпека інформаційних систем”. – Львів, 5–6 червня, 2014. – С. 50–51.

6. Лавровская Т. В. Анализ методов повышения защищенности в LTE-системах / Т. В. Лавровская // Системи обробки інформації. – 2014. – Вип. 5 (121). – С. 139–141.

7. Столлингс, Вильямс. Операционные системы, 4-е издание. Москва: Издательский дом "Вильямс", 2014.

8. Шаньгин В.Ф. Защита в компьютерных системах и сетях. Москва: ДМК Пресс, 2012.

9. Оладько А.Ю. Подсистема мониторинга и аудита информационной безопасности в операционной системе Linux // Известия Южного федерального университета. Технические науки, No. 12, 2012.

10. Качанов М.А. Анализ безопасности информационных потоков в операционных системах семейства GNU/Linux // Прикладная дискретная математика, No. 3, 2010.

11. Брыкова Е.И. Основные принципы построения безопасных операционных систем // Вестник Астраханского государственного

технического университета. Серия: Управление, вычислительная техника и информатика , No. 2, 2013. С. 52-57.

12. Сумкин К.С., Байков И.В., Горелкин Д.О. Безопасность в операционных системах, модель безопасности операционных систем // Промышленные АСУ и контроллеры, No. 7, 2011. С. 59-60.

13. Морозова Е.В., Мондикова Я.А., Молдовян Н.А. Способы отрицаемого шифрования с разделяемым ключом // Информационно-управляющие системы, No. 6, 2013. С. 73-78.

14. Молдовян Н.А., Щербаков А.В. Протокол бесключевого отрицаемого шифрования // Вопросы защиты информации, No. 2, 2016. С. 9-14.

15. Березин А.Н., Рыжков А.В., Гурьянов Д.Ю. Понятие отрицаемого шифрования в дисциплине «криптографические методы защиты информации» // Современное образование: содержание, технологии, качество, 2012. С. 246-248.

16. Березин А.Н., Молдовян А.А., Молдовян Н.А. Потоковое отрицаемое шифрование, вычислительно неотличимое от вероятностного шифрования // Международная конференция по мягким вычислениям и измерениям. 2015. С. 95-97.

17. Молдовян Н.А., Горячев А.А., Вайчикаускас М.А. Расширение криптосхемы рабина: алгоритм отрицаемого шифрования по открытому ключу // Вопросы защиты информации, No. 2, 2014.

18. Горбунов В.В. Требования к операционным системам реального времени // Журнал научных публикаций аспирантов и докторантов, No. 9, 2012. С. 78-79.

19. Ли И.В., Балса А.Р. Современные подходы к разработке операционных систем для масштабируемых многоядерных систем // Информационные технологии и системы: управление, экономика, транспорт, право, No. 1, 2014. С. 6-14.

20. Андреева О.Н. Создание процесса обработки в вычислительных системах реального времени // Вестник науки и образования северо-запада России, No. 1, 2015. С. 173-177.

21. Бокова О.И., Михайлов Д.М., Фроимсон М.И. Выработка и анализ требований к защищенной мобильной операционной системе // Вестник воронежского института МВД России, No. 4, 2013. С. 242-247.

22. Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: Учебное пособие. СПб.: СПбГУЭФ, 2010.

23. Шаньгин В.Ф. Защита в компьютерных системах и сетях. Москва: ДМК Пресс, 2012.

24. Абденов А.Ж., Голяков С.А. Аутентификация методом динамического графического пароля // Сборник научных трудов Новосибирского государственного технического университета. Новосибирск. 2013. С. 78-83.

25. Капустин Ф.А., Долгова Т.Г. Двухэтапная аутентификация в интернет-сервисах // актуальные проблемы авиации и космонавтики, No. 9, 2013.

26. Бельфер Р.А., Богомолова Н.Е. Аутентификация в сетях передачи данных на базе виртуальных каналов // Фундаментальные проблемы радиоэлектронного приборостроения, No. 6, 2012. С. 34-37.

27. Васильев А.С., Керш С.В. Анализ алгоритма аутентификации подключаемых модулей аутентификации // Россия молодая: передовые технологии – в промышленность!, No. 2, 2015.

28. Гроссе Э., Упадхаяй М. Многофакторная аутентификация // Открытые системы. СУБД, No. 2, 2013. С. 42-47.

29. Царёв Е. Аутентификация сегодня и завтра // Защита информации. Инсайд , No. 4, 2014. С. 39-41.

30. Березин А.Н., Биричевский А.Р., Молдовян Н.А., Рыжков А.В. Способ отрицаемого шифрования // Вопросы защиты информации, No. 2, 2013. С. 18-21.

31. Козачок А.В., Голембиовская О.М., Туан Л.М. Прототип системы контролируемого разграничения доступа к файлам документальных форматов // Вестник брянского государственного технического университета, No. 4, 2015.

32. Королев И.Д., Поддубный М.И., Носенко С.В. Применение сегмента матрицы доступов хру в анализе информационной безопасности систем, реализующих мандатное разграничение доступа // Политематический сетевой электронный научный журнал кубанского государственного аграрного университета, No. 101, 2014. С. 1811-1823.

33. Сизоненко А.Б. Арифметико-логическое представление матрицы доступа в дискреционной модели разграничения доступа // Вестник воронежского института МВД России, No. 3, 2012. С. 201-206.

34. Молдовян Н.А., Биричевский А.Р., Мондикова Я.А. Отрицаемое шифрование на основе блочных шифров // Информационно управляющие системы, No. 5, 2014. С. 80-86.

35. Биричевский А.Р. Практическое применение алгоритмов отрицаемого шифрования. Информационная безопасность и защита персональных данных: Проблемы и пути их решения // Материалы VI Межрегиональной научно-практической конференции. Брянск. 2014. С. 17-18.

36. Биричевский А.Р. Отрицаемое шифрование как механизм защиты приложений от отладки. // Комплексная защита объектов информатизации и измерительные технологии: сб. науч. тр. Всероссийской науч.-практической конф. с международным участием. 16-18 июня 2014. СПб. 2014. С. 8-12.

37. Биричевский А.Р. Способ применения отрицаемого шифрования для хранения ключей // Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2015 г. СПб. 2015. С. 98-99.

38. Таныгин М.О. Методика обеспечения безопасного хранения данных на постоянных носителях // Известия юго-западного государственного университета., No. 2, 2013. С. 45-48.

39. Таныгин М.О., Глазков А.С. Принципы организации программно-аппаратной защиты файлов на жёстких дисках персональных компьютеров // Молодой ученый, No. 11, 2010. С. 104-106.

40. Биричевский А.Р. Использование архитектуры «черного ящика» в аппаратных средствах криптографической защиты информации // Юбилейная XIII Санкт-Петербургская международная конференция региональная информатика «РИ-2012». Санкт-Петербург, 24-26 октября 2012. С. 19.

41. Максимов В.А. Архитектура системы управления виртуальными машинами // Электронное периодическое издание информационная среда образования и науки, No. 11, 2012. С. 30-34.

42. Хашковский В.В., Прокопенко А.В. О применении интерфейса прикладного программирования для управления виртуальными машинами // Материалы v международной научно-практической конференции. 21 век: фундаментальная наука и технологии. 2014. С. 128-129.

43. Иванов Д.Г. Организация резервирования в системах распределенного хранения данных // Весник национального техничного университету Украины "Киевский политехничний институт", No. 56, 2012. С. 160-164.

44. Черноусов Н.С., Зуев М.С. Системы резервирования данных // Психолого-педагогический журнал Гаудеамус, Vol. 2, No. 20, 2012. С. 161-162.

45. Гатчин Ю.А., Теплоухова О.А. Реализация контроля целостности образа операционной системы, загружаемого по сети на тонкий клиент // Научно-технический вестник информационных технологий, механики и оптики, No. 6, 2015. С. 1115-1121.

46. Авезова Я.Э., Фадин А.А. Вопросы обеспечения доверенной загрузки в физических и виртуальных средах // Вопросы кибербезопасности, No. 1, 2016. С. 24-30.

47. Биричевский А.Р. Подход к обеспечению безопасности взаимодействия процессов при разработке операционных систем. //

Информационная безопасность регионов России (ИБРР-2013). И 74 VIII Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 23-25 октября 2013 г. СПб. 2013. С. 49-50.

48. Биричевский А.Р. Использование распределенной ключевой системы в аппаратных средствах криптографической защиты информации // Юбилейная XIII Санкт-Петербургская международная конференция региональная информатика «РИ-2012». Санкт-Петербург, 24-26 октября 2012. С. 19.

49. Биричевский А.Р. Универсальная мобильная операционная система с подсистемами аутентификации и защиты информации на основе псевдовероятностного преобразования // Труды СПИИРАН, No. 3, 2016. С. 128-138.

50. ГОСТ 12.0.003-74.ССБТ. Опасные и вредные производственные факторы. Классификация.

51. ДСН 3.3.6.042-99. Санітарні норми мікроклімату виробничих приміщень.

52. ДБН В.2.5-28-2006. Природне і штучне освітлення.

53. Пособие по расчету и проектированию, естественного, искусственного и совмещенного освещения НИИСФ – М.: Стройиздат. 1985. – 384 с.

54. ДСН 3.3.6-037-99. Санітарні норми виробничого шуму, ультразвуку та інфразвуку.

55. ДСН 3.3.6.039 99. Державні санітарні норми виробничої та загальної вібрацій.

56. ГОСТ 12.2.032-78. ССБТ. Рабочее место при выполнении работ сидя. Общие эргономические требования.

57. Березюк О. В. Охорона праці. Підсумкова державна атестація спеціалістів, магістрів в галузях електроніки, радіотехніки, радіоелектронних апаратів та зв’язку : навчальний посібник / О. В. Березюк, М. С. Лемешев. – Вінниця : ВНТУ, 2017. – 104 с.

58. Правила улаштування електроустановок. 2-е вид., перероб. і доп. – Х: "Форт", 2009. – 736 с.

59. ДБН В.2.5-27-2006. Захисні заходи електробезпеки в електроустановках будинків і споруд.

60. ДБН В.1.1.7-2002. Пожежна безпека об’єктів будівництва.

61. НАПБ Б.03.001-2004. Типові норми належності вогнегасників.

62. СНиП 2.09.02-85. Противопожарные нормы проектирования зданий и сооружений.

63. ДСанПіН 3.3.6-096-2002. Державні санітарні норми і правила при роботі з джерелами електромагнітних полів.

ДОДАТКИ

Додаток А
(Технічне завдання)

Додаток Б
(обов’язковий)

Структура системи захисту від загроз порушення конфіденційності

Додаток В
(обов’язковий)

Блок-схема процесу аутентифікації локальних користувачів

Додаток Г
(обов’язковий)

Структурна схема служби доступу до файлової системи

Додаток Д
(обов’язковий)

Алгоритм заперечного шифрування

Додаток Е
(обов’язковий)

Блок-схема алгоритму базового заперечного шифрування

Додаток Є
(обов’язковий)

Алгоритм використання заперечного шифрування для зберігання резервних серій ключової інформації

Додаток Ж
(обов’язковий)

Алгоритм шифрування файлу в файловій системі EFS

Додаток З
(обов’язковий)

Структурна схема служби передачі даних

Додаток К
(обов’язковий)

Структурная схема блоку криптографічного сховища інформації

Додаток Л
(обов’язковий)

Структурна схема пристрою ідентифікації

Додаток М
(обов’язковий)

Архітектура віртуального програмного середовища

Додаток Н
(обов’язковий)

Алгоритм роботи завантажувача операційної системи

Додаток О
(обов’язковий)

Алгоритм роботи безпечного завантажувача фірми Atmel

Додаток П
(обов’язковий)

Алгоритм перевірки автентичності пакета оновлення ПЗ

Додаток Р
(довідниковий)

ДОДАТКИ

Додаток А

(обов’язковий)

ВНТУ

ЗАТВЕРДЖУЮ

Зав.кафедри ТКСТБ ВНТУ,

канд. техн. наук, професор

Г.Г.Бортник

. “__” _____ 2019 р.

ТЕХНІЧНЕ ЗАВДАННЯ

на виконання магістерської кваліфікаційної роботи

ПІДВИЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В БЕЗПРОВІДНИХ МЕРЕЖАХ WiMAX

08-34.МКР.012.00.000 ТЗ

Керівник роботи

к.т.н., доц. кафедри ТКСТБ ВНТУ

Городецька О.С.

Виконавець: ст. гр. ТТК-18м

Чуба В.В.

Вінниця-2019

1 ПІДСТАВА ДЛЯ ВИКОНАННЯ РОБОТИ

Робота проводиться на підставі наказу ректора по Вінницькому національному технічному університету від “02” 10 2019 року № 254 та індивідуального завдання на магістерську кваліфікаційну роботу.

Дата початку роботи: 02.09.2019 р.

Дата закінчення: 09.12.2019 р.

2 МЕТА І ПРИЗНАЧЕННЯ МКР

Метою даної магістерської кваліфікаційної роботи є дослідження методики захисту інформації в розподілених бездротових мережах, в умовах впливу навмисних атак та розробка алгоритму кодування для зебезпечення передачі інформації в мережах з радіодоступом.

Задачами магістерської кваліфікаційної роботи є:

- розробка технічного завдання;
- дослідження алгоритмів динамічної маршрутизації трафіку в розподілених мережах;
- дослідження методів захисту інформації в розподілених бездротових мережах;
- аналіз алгоритму динамічної маршрутизації інформації при передачі в розподілених бездротових мережах в умовах впливу навмисних атак;
- аналіз алгоритму генерації потоку мережевих атак;
- аналіз прототипу маршрутизациї сервісу для експериментальної перевірки запропонованої методики захисту;
- аналіз протоколу WEP;
- дослідження функцій кодування для забезпечення гармоійного вихідного повідомлення;
- аналіз розробленої системи кодування на відповідність значень правилам псевдовипадковості;

- визначення ключових послідовностей кодуючої функції для забезпечення псевдовипадкового характеру.

Об'єкт дослідження є процеси захисного перетворення переданої по відкритих каналах інформації на основі вимог обчислювальної нерозрізненості по шифротексту від імовірнісного захисного перетворення.

Предмет дослідження є метод аутентифікації користувачів на основі використання одноразових паролів, що генеруються за допомогою алгебраїчного алгоритму псевдовипадкового захисного перетворення.

Основними завданнями роботи є:

- техніко-економічне обґрунтування доцільності даної розробки;

- виконання аналізу функціональних можливостей і особливостей реалізації існуючих мобільних операційних систем і на його основі розробки моделі загроз інформаційній безпеці об'єкту дослідження, архітектури та програмного коду універсальної захищеної операційної системи для мобільних систем;

- розробка методу аутентифікації користувачів, стійкого до примусових атак;

- розробка методу захисного перетворення переданої інформації по відкритих каналах інформації, стійкого до атак з примусом користувача розкрити ключ захисного перетворення;

- розробка методу захисту програмного забезпечення від дизасемблювання;

- розробка методу захисту інформації, що зберігається, стійкого до атак з примусом користувача розкрити ключ захисного перетворення.

- аналіз економічної ефективності проведеної розробки;

- дослідження питань безпеки життєдіяльності.

Практична значимість полягає в тому, що застосування універсальної операційної системи в мобільних пристроях телекомунікаційних та інформаційних систем, в тому числі в системах захисту інформації,

дозволить уніфікувати підходи до забезпечення безпеки при розробці таких систем. Даний підхід спростить розробку і виробництво мобільних пристроїв. Область застосування розробленої ОС включає розробку захищених аутентифікуючих пристроїв (токенів, ідентифікаторів), систем охорони, пристроїв захисту програмного забезпечення, персональних пристроїв зберігання даних (захищених файлових сховищ), апаратних засобів для виконання захисних перетворень даних.

3 ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ МКР

Робота базується на результатах звіту з переддипломної практики “Підвищення інформаційної безпеки в безпровідних мережах WiMAX”, який виконувався у ВНТУ 2019/2020 н.р. Під час підготовки магістерської кваліфікаційної роботи будуть використані матеріали цього звіту.

Список використаних джерел розробки:

3.1 Скляр Б. Цифровая связь. Теоретические основы и применение / Бернард Скляр ; [пер. с англ]. – М.: Изд. Дом “Вильямс”, 2003. – 1104с.

3.2 Молдовян Н.А., Щербаков А.В. Протокол бесключевого отрицаемого шифрования // Вопросы защиты информации, No. 2, 2016. С. 9-14.

3.3 Березин А.Н., Молдовян А.А., Молдовян Н.А. Потоковое отрицаемое шифрование, вычислительно неотличимое от вероятностного шифрования // Международная конференция по мягким вычислениям и измерениям. 2015. С. 95-97.

3.4 Андреева О.Н. Создание процесса обработки в вычислительных системах реального времени // Вестник науки и образования северо-запада России, No. 1, 2015. С. 173-177.

3.5 Васильев А.С., Керш С.В. Анализ алгоритма аутентификации подключаемых модулей аутентификации // Россия молодая: передовые технологии – в промышленность!, No. 2, 2015.

3.6 Козачок А.В., Голембиовская О.М., Туан Л.М. Прототип системы контролируемого разграничения доступа к файлам документальных форматов // Вестник брянского государственного технического университета, No. 4, 2015.

3.7 Биричевский А.Р. Способ применения отрицаемого шифрования для хранения ключей // Информационная безопасность регионов России (ИБРР-2015). IX Санкт-Петербургская межрегиональная конференция. Санкт-Петербург, 28-30 октября 2015 г. СПб. 2015. С. 98-99.

3.8 Гатчин Ю.А., Теплоухова О.А. Реализация контроля целостности образа операционной системы, загружаемого по сети на тонкий клиент // Научно-технический вестник информационных технологий, механики и оптики, No. 6, 2015. С. 1115-1121.

3.9 Авезова Я.Э., Фадин А.А. Вопросы обеспечения доверенной загрузки в физических и виртуальных средах // Вопросы кибербезопасности, No. 1, 2016. С. 24-30.

3.10 Биричевский А.Р. Универсальная мобильная операционная система с подсистемами аутентификации и защиты информации на основе псевдовероятностного преобразования // Труды СПИИРАН, No. 3, 2016. С. 128-138.

3.11 Положення про кваліфікаційну роботу у Вінницькому національному технічному університеті / Уклад. О. Н. Романюк, Р. Р. Обертюх, Т. О. Савчук, Л. П. Громова – Вінниця : ВНТУ, 2015 – 27 с.

3.12 Кухарчук В.В., Ігнатенко О.Г., Обертюх Р.Р. Методичні вказівки до оформлення дипломних проектів (робіт) для студентів всіх спеціальностей.- В.: ВДТУ, 2002.

3.13 Козловський В.О. Техніко-економічні обгрунтування та економічні розрахунки в дипломних проектах та роботах. Навчальний посібник. – В.: ВДТУ, 2003.

3.14 ДСТУ 3008-2015. Інформація та документація, звіти у сфері науки і техніки.- К.: ДП «УкрНДНЦ», 2016.

3.15 Разработка и оформление конструкторской документации радиоэлектронной аппаратуры. Справочник. Под ред. Э.Т.Романычевой.- М: Радио и связь, 1989.

3.16 Бортник Г.Г., Васильківський М.В. Методичні вказівки до підготовки магістерських кваліфікаційних робіт для студентів спеціальності «Телекомунікації та радіотехніка» усіх форм навчання.- Вінниця:ВНТУ, 2018.- 50 с.

4 ВИКОНАВЕЦЬ

Вінницький національний технічний університет, кафедра телекомунікаційних систем та телебачення, студент групи ТКС-18м Чубою В.В.

5 ВИМОГИ ДО ВИКОНАННЯ МКР

Пропонується виконати дослідження методики захисту інформації в розподілених бездротових мережах, в умовах впливу навмисних атак та розробка алгоритму кодування для зебезпечення передачі інформації в мережах з радіодоступом.

Технічні вимоги, яким повинна відповідати розробка, наступні:

- режим роботи алгоритму шифрування – RC5;
- швидкість шифрування інформаційного повідомлення – 10,92 кбіт/с;
- швидкість шифрування базового алгоритму – 2728,211 кбіт/с;
- тип алгоритму шифрування основного файлу – симетричні алгоритми 3DES або AES;
- тип криптографічного обчислювального блоку – ATSAM3U4C;
- тип ідентифікуючого пристрою блоку шифрування - STM32F103RE;
- тип ядра криптографічного блоку – Cortex-M3;
- тактова частота ЦП – 96 МГц;

- ПЗП ЦП – 256 Кбайт;
- ОЗП ЦП – 52 Кбайт;
- тип зовнішнього інтерфейсу – USB 400 Мбіт/с.

При розробці безпровідної мережі слід максимально використовувати стандартні та уніфіковані НВЧ деталі.

6 ЕТАПИ МКР І ТЕРМІНИ ЇХ ВИКОНАННЯ

№	Назва та зміст етапу	Термін виконання		Очікувані результати	Звітна документ-тація
		початок	закінчення		
1.	Розробка технічного завдання (ТЗ)	02.09.2019р.	06.09.2019р.	Розроблене ТЗ	Додаток А
2.	Методи захисту інформації в сучасних бездротових мережах	09.09.2019р.	13.09.2019р.	Проведений аналіз	Вступ. Розділ 1.
3.	Розробка методів аутентифікації і розмежування доступу	16.09.2019р.	04.10.2019р.	Розроблений метод	Розділ 2
4.	Розробка методів захисту інформації при зберіганні та передаванні в безпровідних мережах	07.10.2019р	25.10.2019р.	Розроблений метод	Розділ 3
5.	Розробка безпечної мобільної операційної системи та підсистеми захисту програмного забезпечення	28.10.2019р.	08.11.2019р.	Характеристики і параметри	Розділ 4
6.	Аналіз економічної ефективності	11.11.2019р.	15.11.2019р.	Економічна частина МКР	Розділ 5
7.	Охорона праці та безпека в надзвичайних ситуаціях	18.11.2019р.	22.11.2019р.	Частина ОТ та БНС	Розділ 6

8.	Оформлення пояснювальної записки (ПЗ) та графічної частини	25.11.2019р.	29.11.2019р.	Оформлена документація	ПЗ та графічна частина
9.	Нормоконтроль, попередній захист, рецензування МКР	02.12. 2019р.	06.12.2019р.	Позитивні відзиви	Відзив. рецензія
10.	Захист МКР ЕК		09.12. 2019р.	Позитивний захист	Протокол ЕК

7 ОЧІКУВАНІ РЕЗУЛЬТАТИ ТА ПОРЯДОК РЕАЛІЗАЦІЇ МКР

В результаті виконання роботи будуть розроблені:

- структура системи захисту від загроз порушення конфіденційності;
- блок-схема процесу аутентифікації локальних користувачів;
- структурна схема служби доступу до файлової системи;
- алгоритм заперечного шифрування;
- блок-схема алгоритму базового заперечного шифрування;
- алгоритм використання заперечного шифрування для зберігання резервних серій ключової інформації;
- алгоритм шифрування файлу в файловій системі EFS;
- структурна схема служби передачі даних;
- структурна схема блоку криптографічного сховища інформації;
- структурна схема пристрою ідентифікації;
- архітектура віртуального програмного середовища;
- алгоритм роботи завантажувача операційної системи;
- алгоритм роботи безпечного завантажувача фірми Atmel;
- алгоритм перевірки автентичності пакета оновлення ПЗ;
- економічна частина МКР;
- розділ ОП та БНС;
- рекомендації щодо подальшого використання структурної схеми блоку криптографічного сховища інформації.

Результати, отримані в процесі виконання даної роботи, будуть впроваджені в галузі телекомунікацій:

- Регіональний Центр експлуатації телекомунікаційної мережі України шляхом впровадження системи захисту від загроз порушення конфіденційності;

- ПАТ “Укртелеком” шляхом впровадження служби доступу до файлової системи.

Очікуваний техніко-економічний ефект. При впроваджені результатів досліджень очікується уніфікування підходів до забезпечення безпеки при розробці безпровідних НВЧ систем та мереж. Даний підхід спростить розробку і виробництво мобільних пристроїв.

8 МАТЕРІАЛИ, ЯКІ ПОДАЮТЬ ПІСЛЯ ЗАКІНЧЕННЯ РОБОТИ ТА ПІД ЧАС ЕТАПІВ

За результатами виконання МКР до ЕК подаються пояснювальна записка, графічна частина МКР, відзив і рецензія.

9 ПОРЯДОК ПРИЙМАННЯ МКР ТА ЇЇ ЕТАПІВ

Поетапно результати виконання МКР розглядаються керівником роботи та обговорюються на засіданні кафедри.

Захист магістерської кваліфікаційної роботи відбувається на відкритому засіданні ЕК.

10 ВИМОГИ ДО РОЗРОБЛЮВАНОЇ ДОКУМЕНТАЦІЇ

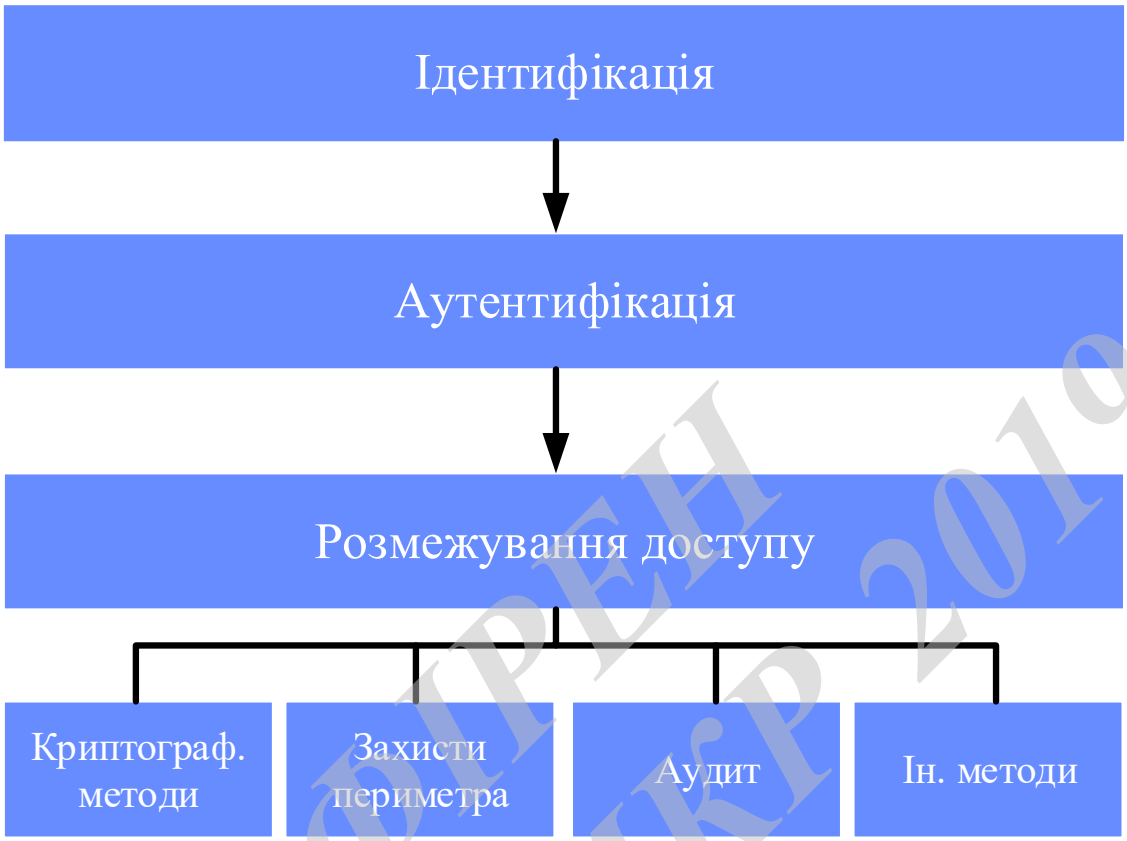
Документація, що розробляється в процесі виконання досліджень повинна містити:

- техніко-економічне обґрунтування розробки;
- структуру системи захисту від загроз порушення конфіденційності;

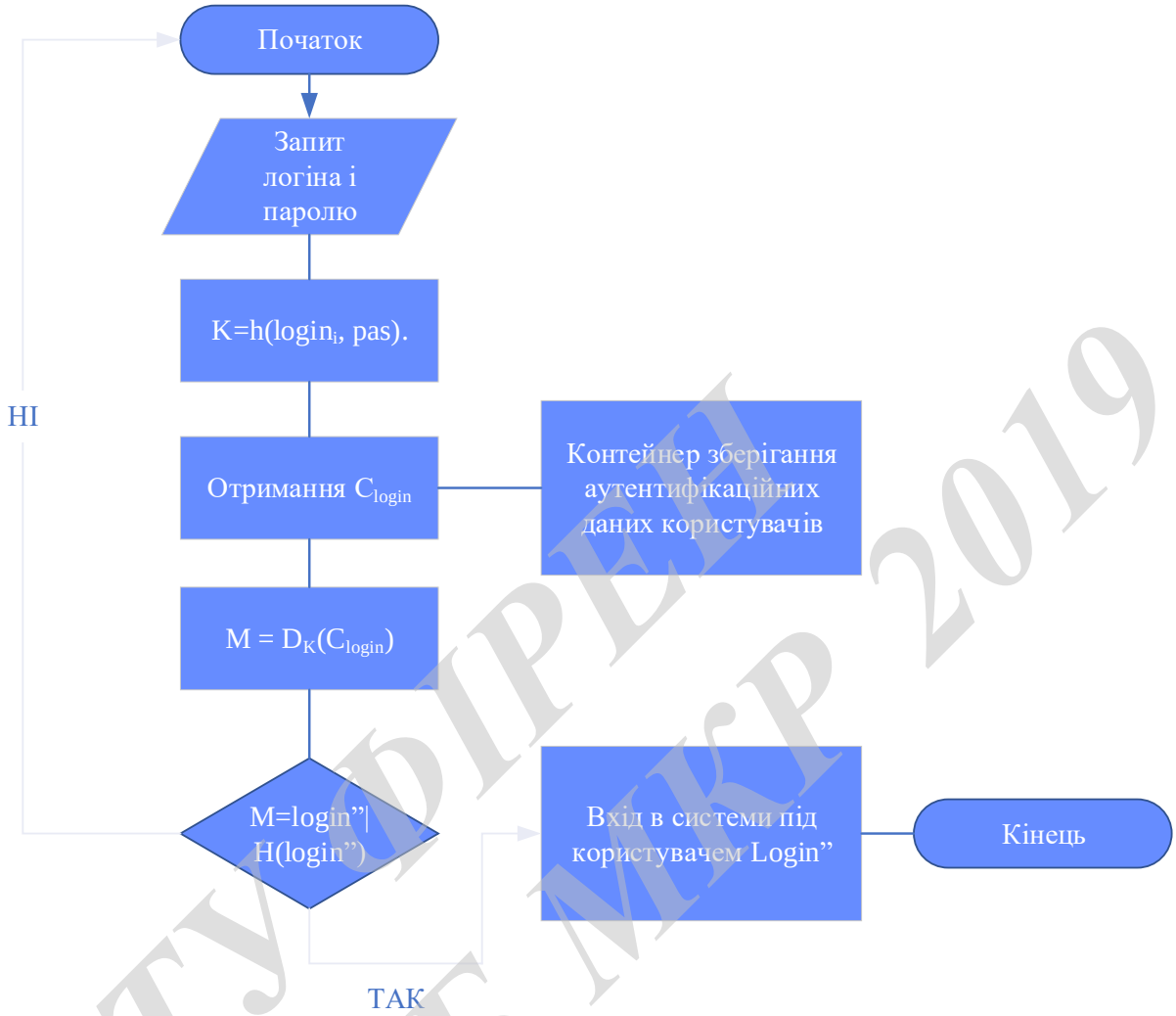
- блок-схему процесу аутентифікації локальних користувачів;
- структурну схему служби доступу до файлової системи;
- алгоритм заперечного шифрування;
- блок-схему алгоритму базового заперечного шифрування;
- алгоритм використання заперечного шифрування для зберігання резервних серій ключової інформації;
- алгоритм шифрування файлу в файловій системі EFS;
- структурну схему служби передачі даних;
- структурну схему блоку криптографічного сховища інформації;
- структурну схему пристрою ідентифікації;
- архітектуру віртуального програмного середовища;
- алгоритм роботи завантажувача операційної системи;
- алгоритм роботи безпечного завантажувача фірми Atmel;
- алгоритм перевірки автентичності пакета оновлення ПЗ;
- економічну частину та розділ БЖД і ЦЗ;
- рекомендації щодо подальшого використання структурної схеми блоку криптографічного сховища інформації.

11 ВИМОГИ ЩОДО ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ

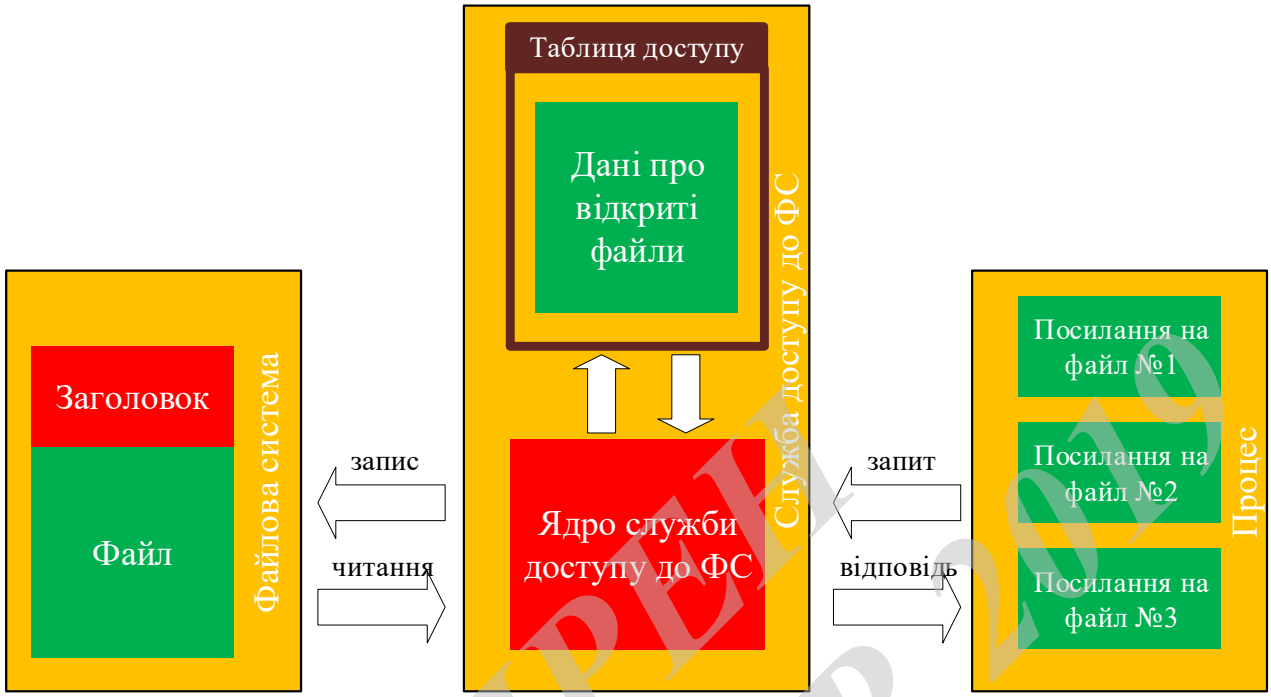
У зв’язку з тим, що інформація не є конфіденційною, заходи з її технічного захисту не передбачаються.



					08-34. МКР.012.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Чуба В.В.			Структура системи захисту від загроз порушення конфіденційності	Літ.	Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.					
Реценз.						ВНТУ, гр. ТТК-18м	
Н. Контр.		Городецька О.С.					
Затверд.		Бортник Г.Г.					

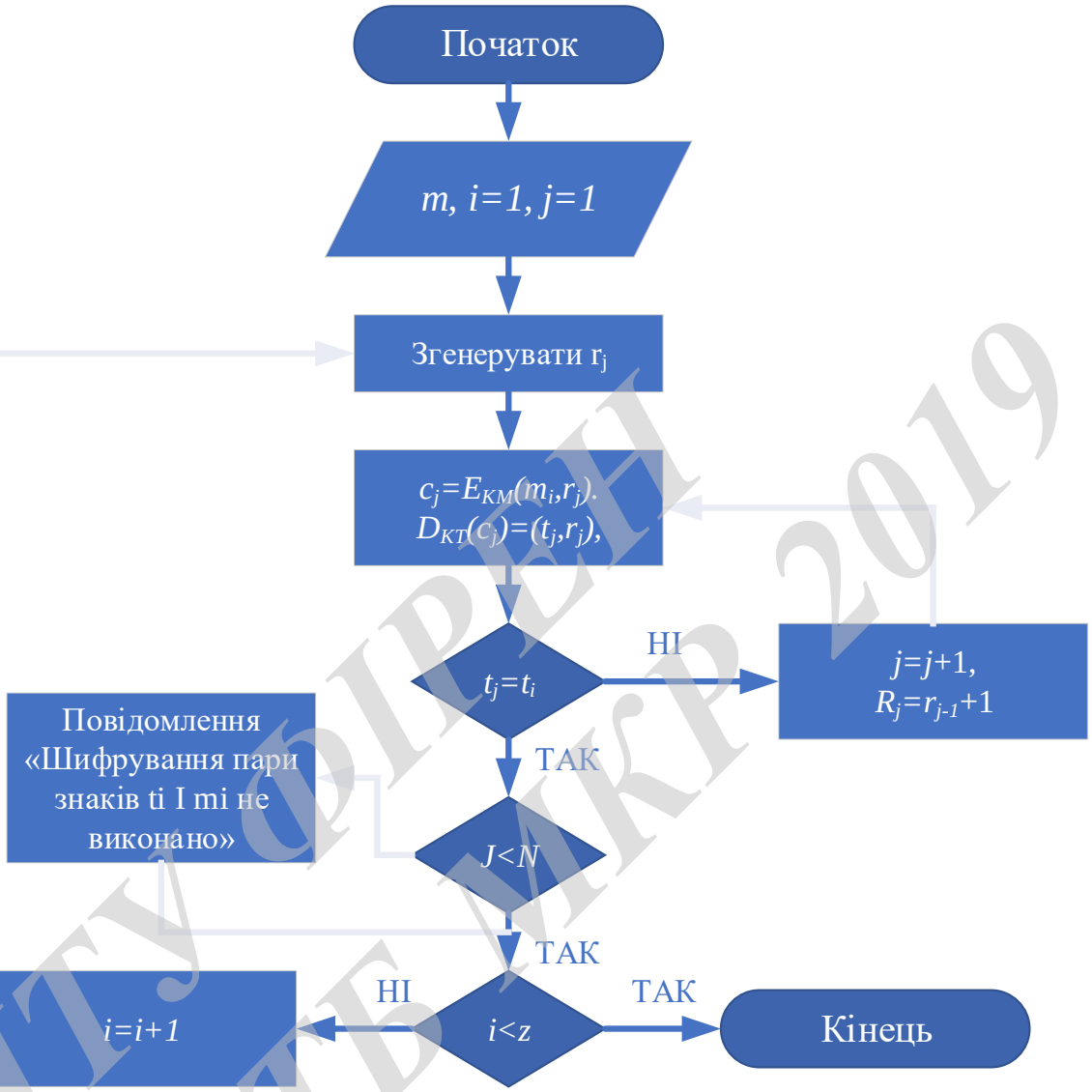


					08-34. МКР.012.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Чуба В.В.			Блок-схема процесу аутентифікації локальних користувачів	Літ.	Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.					
Реценз.						ВНТУ, гр. ТТК-18м	
Н. Контр.		Городецька О.С.					
Затверд.		Бортник Г.Г.					

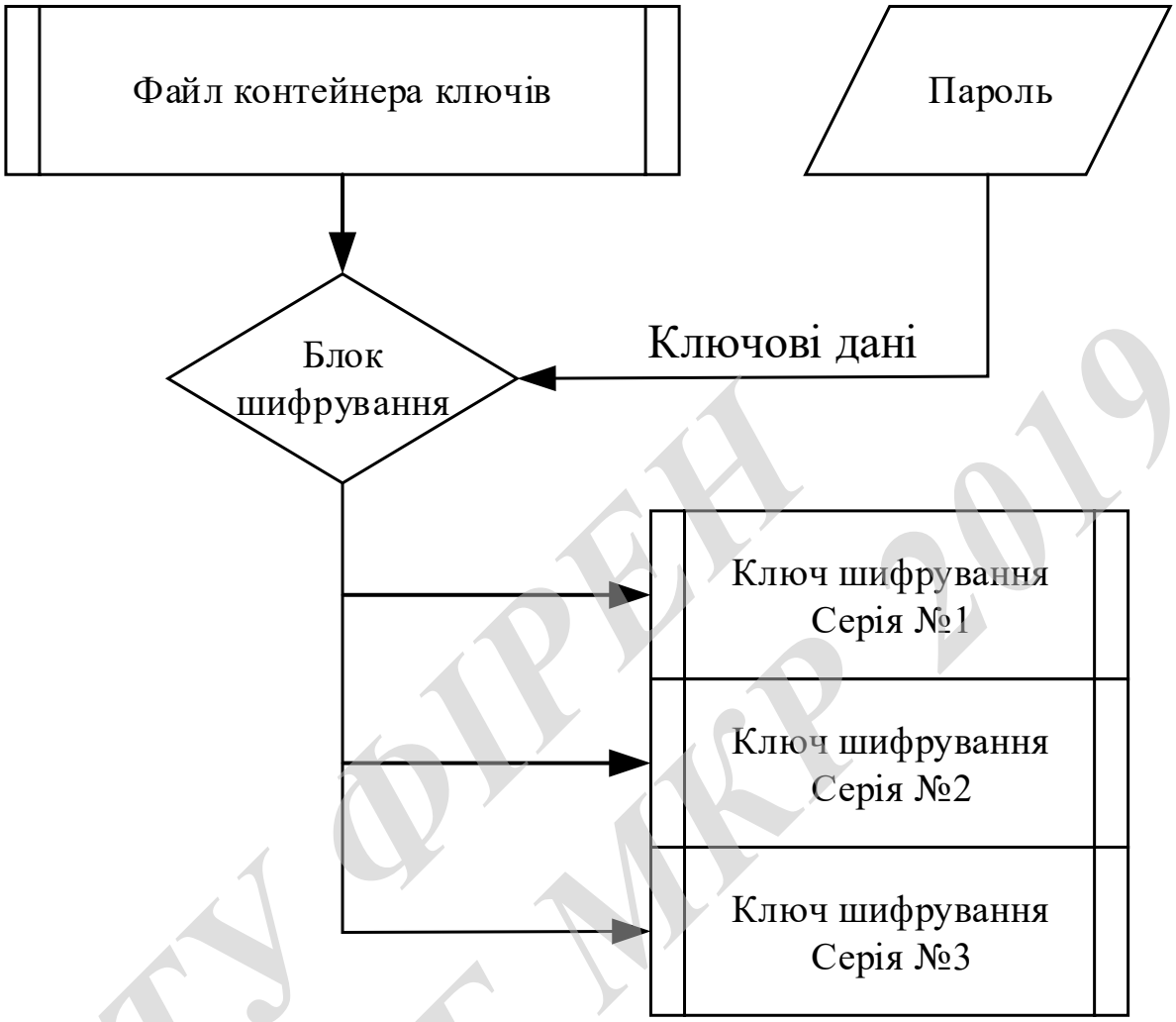


					08-34. МКР.012.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Чуба В.В.			Структурна схема служби доступу до файлової системи	Літ.	Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.					
Реценз.						ВНТУ, гр. ТТК-18м	
Н. Контр.		Городецька О.С.					
Затверд.		Бортник Г.Г.					

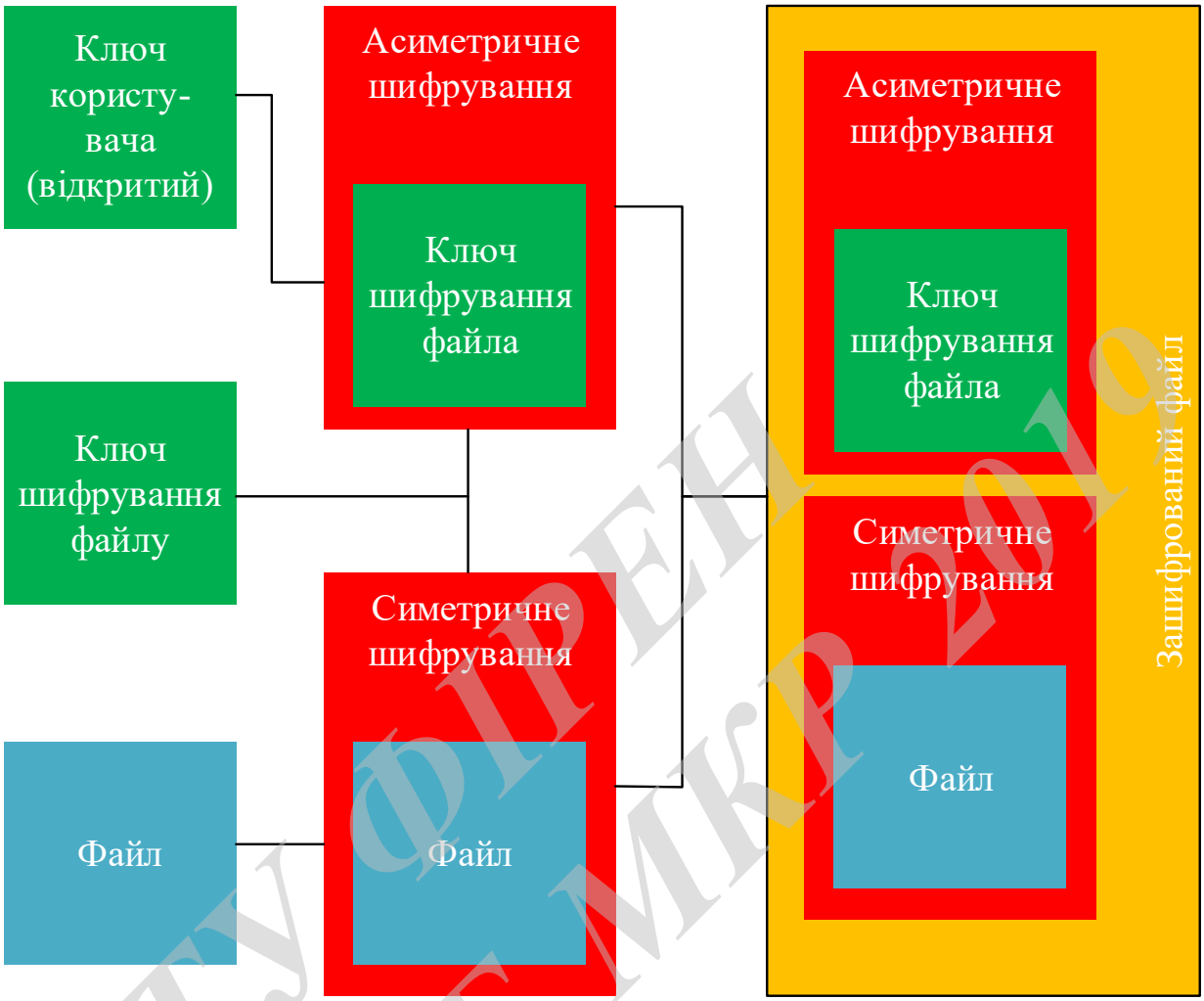
					08-34. МКР.012.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Чуба В.В.			Алгоритм заперечного шифрування	Літ.	Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.					
Реценз.						ВНТУ, гр. ТТК-18м	
Н. Контр.		Городецька О.С.					
Затверд.		Бортник Г.Г.					



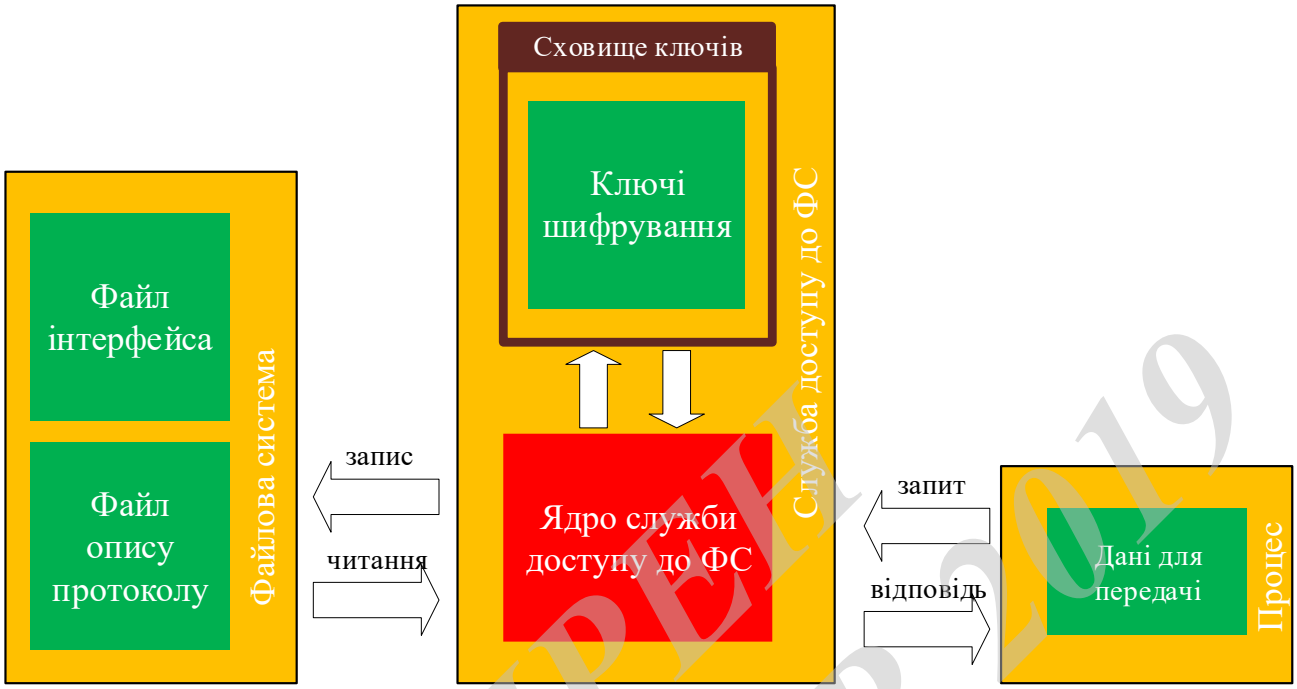
					08-34. МКР.012.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Чуба В.В.			Блок-схема алгоритму базового заперечного шифрування	Літ.	Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.					
Реценз.						ВНТУ, гр. ТТК-18м	
Н. Контр.		Городецька О.С.					
Затверд.		Бортник Г.Г.					



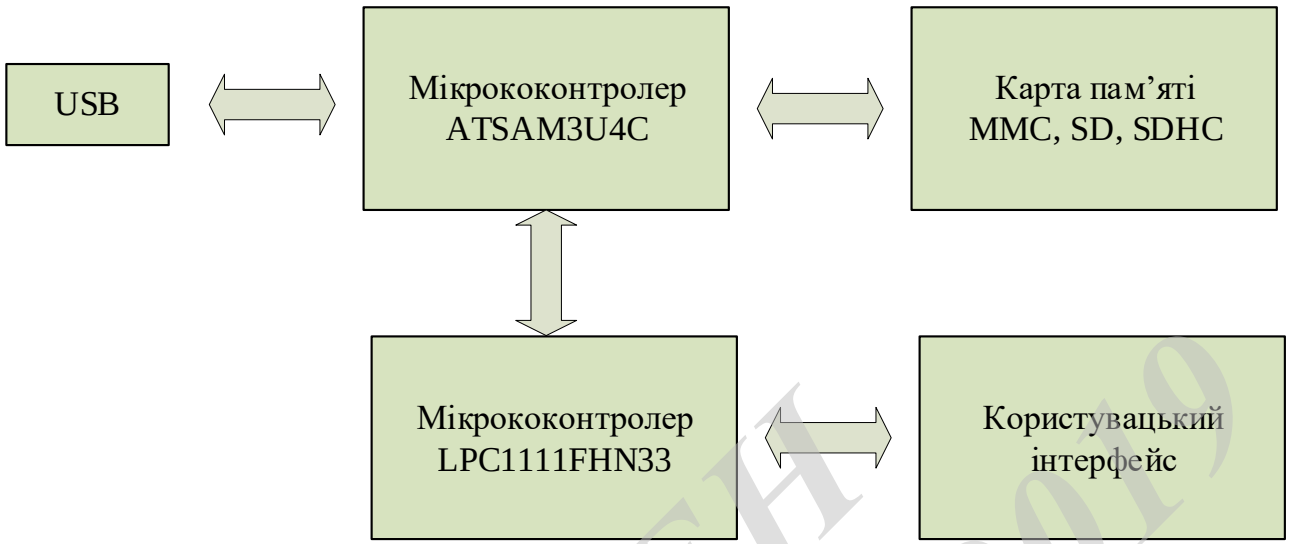
					08-34. МКР.012.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Чуба В.В.			Алгоритм використання заперечного шифрування для зберігання резервних серій ключової інформації	Літ.	Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.					
Реценз.						ВНТУ, гр. ТТК-18м	
Н. Контр.		Городецька О.С.					
Затверд.		Бортник Г.Г.					



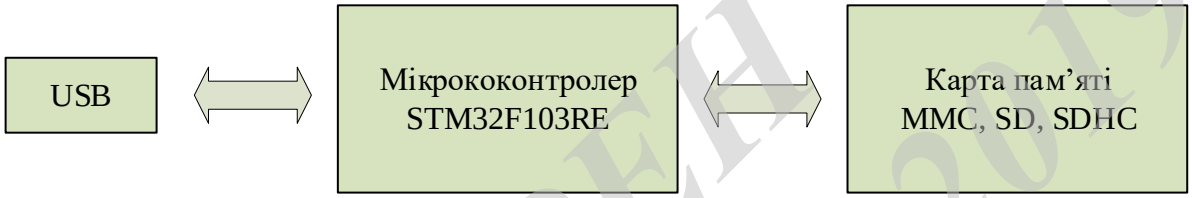
					08-34. МКР.012.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Чуба В.В.			Алгоритм використання заперечного шифрування для зберігання резервних серій ключової інформації	Літ.	Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.					
Реценз.						ВНТУ, гр. ТТК-18м	
Н. Контр.		Городецька О.С.					
Затверд.		Бортник Г.Г.					



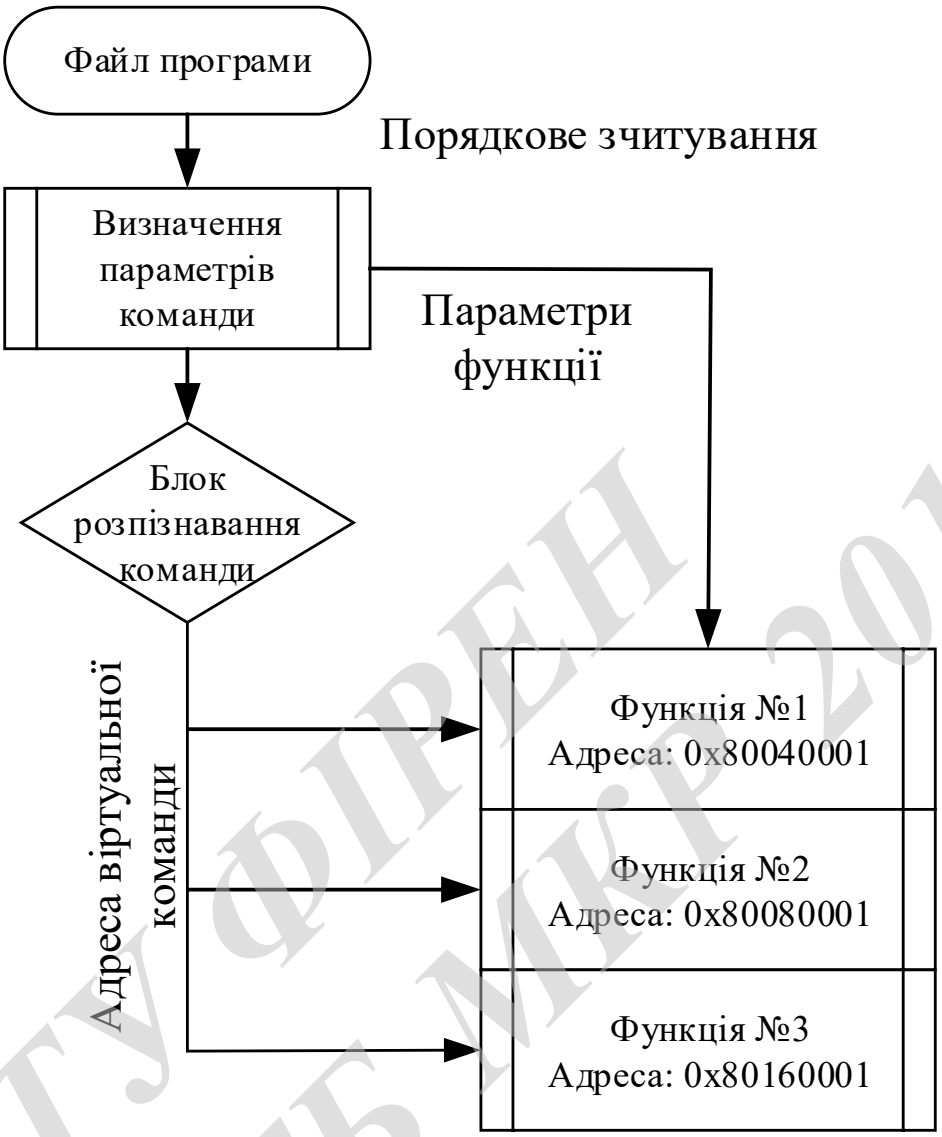
					08-34. МКР.012.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Чуба В.В.			Структурна схема служби передачі даних	Літ.	Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.					
Реценз.						ВНТУ, гр. ТТК-18м	
Н. Контр.		Городецька О.С.					
Затверд.		Бортник Г.Г.					



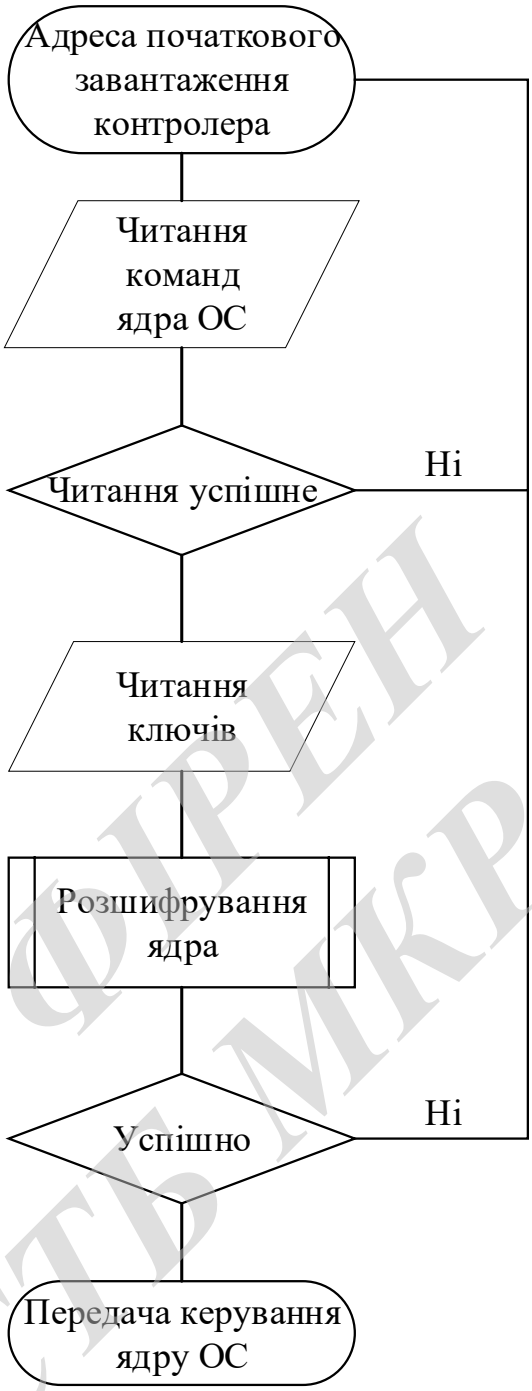
					08-34. МКР.012.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Чуба В.В.			Структурная схема блоку криптографічного сховища інформації	Літ.	Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.					
Реценз.						ВНТУ, гр. ТТК-18м	
Н. Контр.		Городецька О.С.					
Затверд.		Бортник Г.Г.					



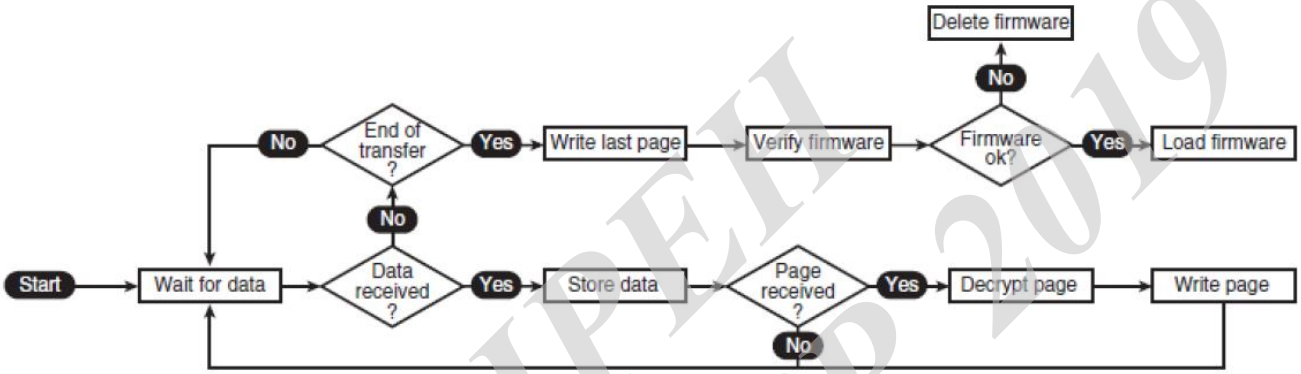
					08-34. МКР.012.00.000 Е8		
Змн.	Лист	№ докум.	Підпис	Дата			
Розроб.		Чуба В.В.			Структурна схема пристрою ідентифікації	Літ.	Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.					
Реценз.						ВНТУ, гр. ТТК-18м	
Н. Контр.		Городецька О.С.					
Затверд.		Бортник Г.Г.					



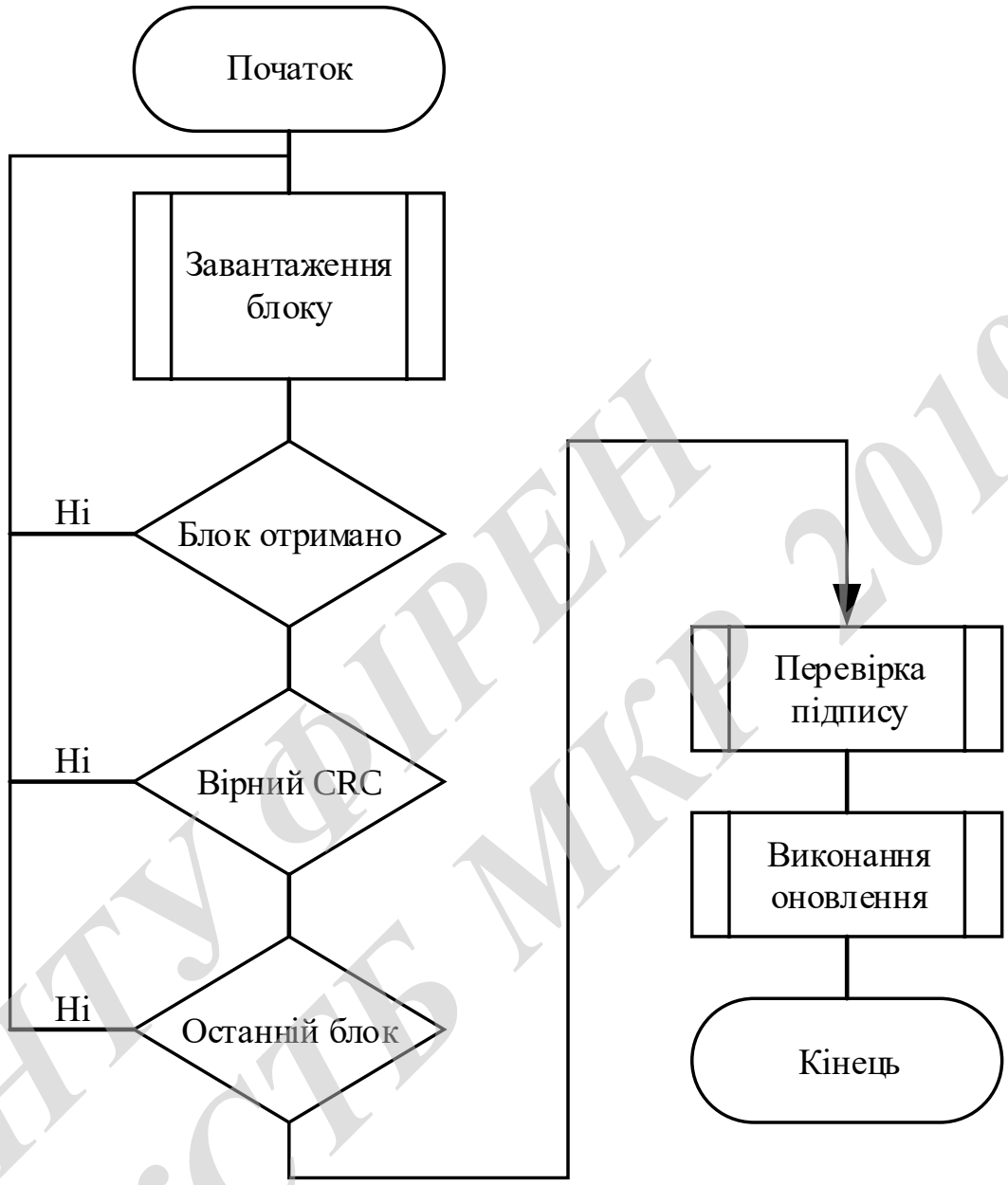
					08-34. МКР.012.00.000 Е8	
Змн.	Лист	№ докум.	Підпис	Дата		
Розроб.		Чуба В.В.			Архітектура віртуального програмного середовища	Літ. / Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.				
Реценз.						ВНТУ, гр. ТТК-18м
Н. Контр.		Городецька О.С.				
Затверд.		Бортник Г.Г.				



					08-34. МКР.012.00.000 Е8	
Змн.	Лист	№ докум.	Підпис	Дата		
Розроб.		Чуба В.В.			Алгоритм роботи завантажувача операційної системи	Літ. / Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.				
Реценз.						ВНТУ, гр. ТТК-18м
Н. Контр.		Городецька О.С.				
Затверд.		Бортник Г.Г.				



					08-34. МКР.012.00.000 Е8	
Змн.	Лист	№ докум.	Підпис	Дата		
Розроб.		Чуба В.В.			Алгоритм роботи безпечного завантажувача фірми Atmel	Літ. / Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.				
Реценз.						ВНТУ, гр. ТТК-18м
Н. Контр.		Городецька О.С.				
Затверд.		Бортник Г.Г.				



					08-34. МКР.012.00.000 Е8	
Змн.	Лист	№ докум.	Підпис	Дата		
Розроб.		Чуба В.В.			Алгоритм перевірки автентичності пакета оновлення ПЗ	Літ. / Арк. 1 / Аркушів 1
Перевір.		Городецька О.С.				
Реценз.						ВНТУ, гр. ТТК-18м
Н. Контр.		Городецька О.С.				
Затверд.		Бортник Г.Г.				

Додаток Р

Допустимі значення виробничих факторів

Таблиця Р.1 – Допустимі показники мікроклімату

Період року	Категорія робіт	Температура повітря, °С для робочих місць		Відносна вологість повітря, %	Швидкість руху повітря, м/с
		постійних	непостійних		
Холодний	Іа	21-25	18-26	75	≤0,1
Теплий		22-28	20-30	55 при 28°С	0,1-0,2

Таблиця Р.2 – Гранично допустимі концентрації шкідливих речовин [4]

Назва шкідливої речовини	ГДК, мг/м^3	Агрегатний стан	Клас небезпеки
Озон	0,1	Пара	4
Оксиди азоту	5	Пара	2
Пил	4	Аерозоль	2

Таблиця Р.3 – Кількість іонів у 1 см^3 повітря приміщення при роботі на ЕОМ

Рівні	*Мінімально необхідні*	Оптимальні	Максимально допустимі
додатній	400	1500-3000	50000
від’ємний	600	3000-5000	50000

Таблиця Р.4 – Нормовані значення коефіцієнта природного освітлення та мінімальні освітленості для штучного освітлення

Характеристика зорової роботи	Найменший розмір об’єкта розрізнення, мм	Розряд зорової роботи	Підрозряд зорової роботи	Контраст об’єкта розрізнення з фоном	Характеристика фону	Освітленість при штучному освітленні, лк			КПО для бокового освітлення, %	
						комбіноване		загальне	Природного	Суміщеного
						всього	у т. ч. від загального			
Середньої точності	0,5-1	IV	г	великий	середній	300	150	150	1,5	0,9

Таблиця Р.5 – Нормовані рівні шуму і еквівалентні рівні звуку

Рівні звукового тиску в дБ в октавних полосах із середньо-геометричними частотами, Гц									Рівні звуку та еквівалентні рівні звуку, дБА
31,5	63	125	250	500	1000	2000	4000	8000	
86	71	61	54	49	45	42	40	38	50

Таблиця Р.6 – Нормовані рівні вібрації [6]

Гранично допустимі рівні віброприскорення, дБ, в октавних полосах із середньо-геометричними частотами, Гц								Коректовані рівні віброприскорення, дБА
8	16	31,5	63	125	250	500	1000	
73	73	79	85	91	97	103	109	76

Таблиця Р.7 – Значення мінімальних меж вогнестійкості приміщення [11]

Ступінь вогнестійкості будівлі	Стіни				Колони	Східчасті майданчики	Плити та інші несучі конструкції	Елементи покриття	
	Несучі та східчасті клітки	Самонесучі	Зовнішні несучі	Перегородки				Плити, прогони	Балки, ферми
2	REI 120 М0	REI 60 М0	Е 15 М0	EI 15 М0	R 120 М0	R 60 М0	REI 45 М0	REI 15 М0	R 30 М0

Примітка. R – втрати несучої здатності; Е – втрати цілісності; І – втрати теплоізолювальної спроможності; М – показник здатності будівельної конструкції поширювати вогонь (межа поширення вогню); М0 – межа поширення вогню дорівнює 0 см.

Таблиця Р.8 – Протипожежні норми проектування будівель і споруд [13]

Об’єм приміщення, тис. $м^3$	Категорія пожежної небезпеки	Ступінь вогнестійкості	Відстань, м, для щільності людського потоку в загальному проході, осіб/$м^2$			Кількість людей на 1 м ширини евакуаційного виходу	Відстань між будівлями та спорудами, м, для ступеня їх вогнестійкості			Найбільша кількість поверхів	Максимально допустима площа поверху, $м^2$, для кількості поверхів		
			до 1	2-3	4-5		I,II	III	IV, V		1	2	3 і більше
до 15	В	2	100	60	40	110	9	9	12	8	н.о.	н.о.	н.о.

Примітки: н.о. – не обмежується.