Національний університет «Полтавська політехніка імені Юрія Кондратюка»
(повне найменування вищого навчального закладу)

Навчально-науковий інститут інформаційних технологій та робототехніки
(повна назва інституту)

Кафедра комп'ютерних та інформаційних технологій і систем
(повна назва кафедри)

Пояснювальна записка

до кваліфікаційної роботи

магістра
(ступінь вищої освіти)

на тему «**Програмний комплекс захисту даних від несанкціонованого використання із застосуванням вбудованих пристроїв»**

Виконав: студент II курсу, групи 602-ТН
спеціальності
122 Комп'ютерні науки
(шифр і назва спеціальності)

Павленко А.С.
(прізвище та ініціали)

Керівник д.ф.-м.н, професор Миронцов М.Л.
(прізвище та ініціали)

Рецензент _____
(прізвище та ініціали)

Полтава – 2025 рік

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

«ПОЛТАВСЬКА ПОЛІТЕХНІКА ІМЕНІ ЮРІЯ КОНДРАТЮКА»

НАВЧАЛЬНО НАУКОВИЙ ІНСТИТУТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА РОБОТОТЕХНІКИ

КАФЕДРА КОМП'ЮТЕРНИХ ТА ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І СИСТЕМ

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

спеціальність 122 «Комп'ютерні науки» на тему

«Програмний комплекс захисту даних від несанкціонованого використання із застосуванням вбудованих пристроїв»

Студент групи 602-ТН Павленко Артем Сергійович

Керівник роботи
д.ф.-м.н, професор
Миронцов М.Л.

Консультант
к.т.н., доцент Головко
Г.В.

Завідувач кафедри
кандидат фізико-
математичних наук,
Двірна О.А.

Полтава – 2025 рік

РЕФЕРАТ

Кваліфікаційна робота: 61 с., 9 рис., 5 табл., 11 джерел.

Із зростанням доступності закладних пристроїв, виникає проблема у виявлення технічних засобів в ПЕОМ (персональних електронно-обчислювальних машинах) та приміщень на об’єктах інформаційної діяльності. Ця загроза стає проблемою витоку конфіденційної інформації. Метою роботи є підвищення захищеності (персональних комп’ютерів) ПК від зняття (інформація з обмеженим доступом) ІзОД з використанням (закладних пристроїв) ЗП шляхом застосування методів статистичного аналізу роботи окремих складових персонального комп’ютера.

Для досягнення мети, в роботі вирішені наступні задачі:

- за результатами порівняльного аналізу закладних пристроїв показана різниця між побудовою та конструкцією;

- за результатами проведеної оцінки описано методи виявлення закладних пристроїв від перехоплення даних;

- запропоновано рекомендації щодо протидії роботи закладних пристроїв вбудованих в обладнанні ПЕОМ. Запропоновано вдосконалення методів захисту каналів витоку інформації в ЕОМ на об’єктах інформаційної діяльності, які розроблені за результатом аналізу статистичних досліджень та літератури з відкритих джерел.

ПРОГРАМНИЙ КОМПЛЕКС ЗАХИСТУ ДАНИХ ВІД НЕСАНКЦІОНОВАНОГО ВИКОРИСТАННЯ ІЗ ЗАСТОСУВАННЯМ ВБУДОВАНИХ ПРИСТРОЇВ.

ABSTRACT

Scope of work: the work is done on: 62 pages, 9 figures, 5 tables, 11 sources.. INCREASING THE SECURITY OF OBJECTS AGAINST DATA RECEPTION USING BUGGING DEVICES

With the increasing availability of embedded devices, there is a problem in identifying technical means in PCs (personal electronic computing machines) and premises at information activity facilities. This threat becomes a problem of leakage of confidential information. The purpose of the work is to increase the security of computer equipment against the removal of confidential information. To achieve the goal, the following tasks are solved in the work:

- according to the results of the comparative analysis of embedded devices, the difference between construction and construction is shown;

- based on the results of the assessment, the methods of identifying embedded devices from data interception are described4

- recommendations are offered to counteract the operation of embedded devices built into personal computer equipment. It is proposed to improve the methods of protection of information leakage channels in computers at the objects of information activity, which were developed based on the results of the analysis of statistical studies and literature from open sources.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АС – автоматизована система;

БФП – багатофункціональний пристрій;

ЕЖ – елемент живлення;

ЕОМ – електронно-обчислювальна машина;

ВП – вбудований пристрій;

ІзОД – інформація з обмеженим доступом;

КС – комп’ютерна система

КСЗІ – комплексна система захисту інформації;

НГМД – накопичувач на гнучких магнітних дисках;

ОЗП – оперативна пам'ять;

ОІД – об’єкт інформаційної діяльності;

ОС – операційна система;

ПЕОМ – персональна електронно-обчислювальна машина;

ПЗП – постійний запам'ятовувальний пристрій;

РЗП – радіозакладний пристрій;

СІА – конфіденційність (англ. confidentiality) цілісність (англ. integrity) доступність (англ. availability);

ТЗ – технічний засіб;

ТЗІ – технічний захист інформації.

ВСТУП

Стрімкий розвиток сучасних технологій та технічних засобів сприяє постійному розширенню можливих шляхів витоку конфіденційної інформації. Така ситуація визначає актуальність і важливість робіт з раннього виявлення поведінки вбудованих пристроїв та протидії їм [1]. При розробці систем захисту комп'ютерних систем особлива увага приділяється дослідженню та протидії поведінці вбудованих пристроїв (ВП). Постійний розвиток таких пристроїв та їх зростаюча доступність значно ускладнюють завдання надійного захисту інформації з обмеженим доступом, що циркулює всередині комп'ютерних систем. Тому виникає необхідність комплексного підходу до захисту усіх компонентів комп'ютерних систем [1]. Для виявлення несанкціонованих вбудованих портативних пристроїв, призначених для доступу до конфіденційної інформації, сьогодні широко проводяться спеціальні дослідження комп'ютерних систем, зокрема, для виявлення несанкціонованої модифікації компонентів комп'ютера та аналізу сигналів, що генеруються під час його роботи.

Це пов'язано з необхідністю проведення таких досліджень відповідно до НД ТЗІ 2.7-011-2012 [4] та високою точністю виявлення вбудованих пристроїв. З іншого боку, слід враховувати, що такі дослідження займають значний час, а роботу КС можна перевірити лише в заданому (тестовому) режимі роботи. Така ситуація ускладнює виявлення новітніх типів вбудованих пристроїв, здатних виявляти використання тестового режиму роботи комп'ютерних систем і, відповідно, знижує рівень демаскуючих можливостей щодо роботи комп'ютерних систем. Тому цікавою є розробка нових методів виявлення вбудованих пристроїв, здатних виявляти ефекти поведінки вбудованих портативних пристроїв на основі результатів аналізу поведінки компонентів комп'ютерних систем протягом тривалого періоду часу [1].

Одним з новітніх методів вирішення цієї проблеми є використання методики статистичного аналізу поведінки як користувачів комп'ютерних систем, так і окремих підсистем комп'ютерних систем (виявлення аномальних

змін, спричинених поведінкою вбудованих пристроїв). Це дозволяє на ранніх стадіях виявляти відхилення в поведінці комп'ютера на статистично значущому рівні і, таким чином, значно скорочує кроки, необхідні для виявлення присутності хробака. Однак обмеженням практичного застосування цих методів є те, що вони зосереджені на окремих компонентах комп'ютера, що обмежує можливості експертів з комплексного захисту інформації (КЗІ) виконати комплексну перевірку комп'ютера [1].

Метою даної роботи є підвищення захищеності комп'ютерів від зняття апаратних вбудованих портативних пристроїв шляхом застосування статистичних методів для аналізу поведінки компонентів комп'ютера. Зокрема, розглядається випадок дослідження поведінки системних блоків, периферійних пристроїв та пристроїв для автономної передачі інформації.

Для досягнення поставленої мети вирішуються наступні завдання:

1. Провести порівняльний аналіз за конфігурацією вбудованих пристроїв;

2. Оцінити методи виявлення вбудованих пристроїв від перехоплення даних.

3. Розробити рекомендації щодо протидії вбудованим пристроям в комп'ютерах.

4. Розробити рекомендації щодо використання вбудованих пристроїв в комп'ютерах.

5. Розробити рекомендації щодо використання вбудованих пристроїв в комп'ютерах.

6. Розробити рекомендації щодо використання вбудованих пристроїв в комп'ютерах. Об'єктом дослідження є методи виявлення вбудованих пристроїв в комп'ютерах, що використовуються для обчислень. Предметом дослідження є метод статистичного аналізу порушень в роботі підсистем персонального комп'ютера, викликаних роботою вбудованих пристроїв. Методи дослідження: теоретичні - аналіз, порівняння, систематизація та узагальнення авторської наукової літератури, електронних джерел.

РОЗДІЛ 1.
ОГЛЯД ПРИНЦИПІВ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ ВБУДОВАНИХ ПРИСТРОЇВ

1.1 Основні відомості про побудову вбудованих пристроїв

Необхідність забезпечення комплексної системи захисту інформації, тобто побудови комплексної системи захисту інформації в автоматизованих системах 1-го, 2-го та 3-го типів: НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем», необхідна для збереження конфіденційності, цілісності та доступності і в основному визначається вимогами нормативних документів або в деяких випадках рішенням власника інформаційного ресурсу [5].

Модель CIA часто використовується для характеристики основних властивостей інформації як об'єкта захисту, а її застосування дає критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу в рамках НД ТЗІ 2.5-004-99 [5]:

1. Конфіденційність (Confidentiality) - властивість інформації, яка полягає в тому, що інформація не може бути використана несанкціонованими користувачами.

2. Цілісність (Integrity) означає, що інформація не може бути змінена неавторизованими користувачами.

3. Крім того, використовуються також наступні властивості [5]:

4. Незаперечність - можливість довести, що автором є заявлена особа (юридична особа) і ніхто інший.

5. Підзвітність - властивість інформаційної системи, яка фіксує дії користувачів, використання пасивних об'єктів і чітко ідентифікує автора тієї чи іншої дії в системі.

6. Надійність - властивість, за якою інформація точно розпізнається, ймовірність того, що помилок не існує.

7. Автентичність - властивість, яка гарантує, що об'єкт або ресурс ідентичний заявленому.

1.2 Суб'єкти діяльності із захисту даних

У процесі забезпечення захисту даних беруть участь такі суб'єкти [5]:

- організація, що замовляє роботи із захисту даних (власник або розпорядник інформації, як визначено окремими нормативно-правовими актами або двосторонніми угодами);

- організація, що реалізує заходи із забезпечення захисту даних (виконавець).

Діяльність у сфері захисту інформації є дозволеною діяльністю і ліцензується Державною службою спеціального зв'язку та захисту інформації України; ТЗІ має ліцензію серії ВА № 501745 від 11 лютого 2010 року на проведення робіт у галузі технічного захисту інформації. - ДССЗЗІ (Державна служба спеціального зв'язку та захисту інформації) - контролюючий орган - орган, відповідальний за здійснення державної експертизи відповідно до Положення «Про державну експертизу в сфері технічного захисту інформації». 18 березня 2010 року. Відтоді ТЗІ включено до переліку організаторів державних експертиз (лист ДССЗЗІ № 8/3-86.12 від 18 березня 2010 року).

1.3 Класифікація вбудованих пристроїв

Одним з найефективніших способів негласного отримання приватної, комерційної або іншої інформації є приховане розміщення пристрою в найбільш ймовірному місці знаходження об'єкта спостереження (наприклад, конкурента). Одним з найбільш ефективних способів негласного отримання приватної, комерційної або іншої інформації є підхід, заснований на використанні вбудованих пристроїв, які можуть бути таємно розміщені в місцях найбільш ймовірного перебування об'єктів спостереження (наприклад, конкурентів) або

підключені до каналів зв'язку, якими вони користуються [7]. Наразі розробляється багато типів таких пристроїв, що відрізняються за принципом дії, радіусом дії, способами передачі інформації, розмірами та зовнішнім виглядом [7]. Найменші сучасні пристрої зберігання даних важать лише кілька грамів, а їхні лінійні розміри не перевищують кількох міліметрів. Зазвичай дальність передачі інформації таких пристроїв становить трохи більше десятка метрів. Більш потужні пристрої мають розмір у кілька сантиметрів і можуть передавати перехоплену інформацію на відстань від кількох сотень до тисячі метрів і більше. Такі пристрої часто непомітно вбудовуються в конструктивні елементи або інтер'єри будівель, носяться під одягом або маскуються під особисті речі [7].

Для того, щоб систематизувати наведені вище уявлення про пристрої, доцільно ввести п'ять ознак їх класифікації [8]:

- за каналом передачі інформації;
- за способом обміну інформації;
- за наявністю пристрою управління;
- за зовнішнім виглядом;
- за використанням засобів живлення.

Таблиця 1.1. Класифікація вбудованих пристроїв

Класифікація ЗП				
канал передачі інформації	спосіб сприйняття інформації	наявність пристрою управління	зовнішній вигляд	використання джерела живлення
радіозакладки	мікрофонного типу;	з безперервним випромінюванням;	у звичайному виконанні	з власним джерелом;
інфрачервоні закладки	вібраційного типу;	з дистанційним управлінням;	у закамуфльованому вигляді	з живленням від зовнішнього джерела.
закладки з передачею інформації електропровідними лініями	з підключенням до комунікаційних ліній.	з автоматичним включенням при появі сигналу.		
закладки із записом для подальшого вилучення				

Розглянемо особливості кожної з цих категорій окремо.

За способом передачі інформації можна виділити наступні типи вбудованих пристроїв [8]:

- бездротові ВП;
- інфрачервоні ВП;
- ВП, що передають інформацію через струмопровідні дроти;
- ВП, що містять записи для подальшого пошуку.

У бездротових вбудованих пристроях інформація передається за допомогою електромагнітної енергії. Ця енергія не впливає на органи чуття людини і може поширюватися на великі відстані, долаючи природні та штучні перешкоди. Ці дві характеристики електромагнітної енергії дозволяють пристроям радіомоніторингу відстежувати об'єкти, що цікавлять, практично з будь-якої віддаленої точки за допомогою спеціального приймального обладнання. Дальність передачі становить від 10 м до 1,5 км.

З технічної точки зору, радіомаяки можуть працювати практично у всіх радіодіапазонах. Однак, з огляду на конструктивні особливості, найчастіше використовуються частоти від 100 до 1000 МГц. Інфрачервоні вбудовані

пристрої також можуть використовувати енергію електромагнітної хвилі для передачі інформації, але ця електромагнітна хвиля не належить до радіочастотного діапазону, а відповідає такій частині світлового спектру, як інфрачервоний діапазон. Таке короткохвильове випромінювання поширюється вузьким пучком у фіксованому напрямку і тому його важко виявити навіть за допомогою спеціального обладнання. Дальність передачі інформації від інфрачервоного датчика становить близько 500 м. Однак використання таких пристроїв значно ускладнюється їхньою високою секретністю. Обов'язковою умовою є те, що інфрачервоний ВП завжди знаходиться в полі зору приймача оптичного випромінювання, а випадковий контакт з людьми, транспортними засобами чи іншими об'єктами або зміна погодних умов може значно погіршити якість сигналу і навіть спричинити його втрату в реєстраторі. Звичайно, такі датчики абсолютно неефективні в мобільних установках. З огляду на перераховані вище недоліки, інфрачервоні ВП рідко використовуються в польових розвідувальних операціях.

Дротові пристрої передачі даних використовують властивість електричних сигналів поширюватися на великі відстані по провідниках. Такі пристрої мають низку переваг над іншими типами пристроїв, наприклад, кращу прихованість передачі інформації, більшу відстань передачі та відсутність потреби в додатковому джерелі живлення. Вони також можуть бути успішно замасковані під частину електричного кола або колектора (трійники, розетки, подовжувачі, настільні лампи тощо). Завдяки цим особливостям цей тип підслуховуючих пристроїв часто використовується недобросовісними конкурентами для отримання конфіденційної інформації. Для підвищення конспірації передачу інформації по цьому каналу можна замінити записом на диктофон. Це доцільно у випадках, коли оперативна інформація не повинна бути доступною в режимі реального часу, а касета або магнітні стрічки можуть бути таємно вилучені і замінені. Для цього вбудований пристрій може бути обладнаний електронним засобом запису інформації замість передавача по одному з вищезгаданих каналів.

Цей спосіб зазвичай використовується, коли існує ризик того, що канал передачі інформації буде виявлений об'єктом спостереження (наприклад, за допомогою спеціальної апаратури спостереження).

Залежно від способу виявлення інформації розрізняють три типи вбудованих пристроїв [8]:

- мікрофонного типу;
- вібраційного типу;
- підключені до лінії зв'язку.

Принцип дії вбудованих пристроїв мікрофонного типу заснований на перетворенні акустичних коливань атмосфери в електричні сигнали, що передаються споживачеві одним із зазначених вище способів.

Закладні пристрої вібраційного типу (стетоскопи) перехоплюють акустичні коливання (коливання) твердого середовища, викликані тиском атмосферних акустичних хвиль на середовище [8]. Такі пристрої зазвичай використовують п'єзомікрофони, електронні мікрофони або датчики типу акселерометра як чутливі елементи. Вони найбільш ефективні при закріпленні на тонких поверхнях (наприклад, перегородках приміщень, склі, дверях). Як правило, такі пристрої часто називають бездротовими стетоскопами, оскільки для передачі інформації споживачеві використовуються бездротові канали [8]. Вбудовані пристрої, що підключаються до телекомунікаційних ліній зв'язку, призначені для негласного перехоплення інформації, що протікає по телефонних або оптоволоконних лініях. Такі пристрої можуть негласно отримувати інформацію про зміст телефонних розмов і текстових повідомлень (наприклад, телеграм, факсів, електронної пошти) [8]. Для передачі інформації від підключених пристроїв часто використовуються радіоканали. Такі станції називаються радіостанціями (РС). Залежно від способу підключення до телефонної лінії радіотрансляційні вбудовані пристрої можна розділити на дві групи: радіостанції з прямим підключенням і радіостанції з індуктивним підключенням. Вони підключаються паралельно абоненту одночасно до обох кабелів або до розриву в одному кабелі.

Таким чином, на вході радіотрансляційні вбудовані пристрої можна досягти високого рівня сигналу (хорошої якості), а живлення може здійснюватися від лінії. Однак безпосередньо підключені радіотрансляційні вбудовані пристрої можна легко виявити за зміною параметрів лінії.

Цей недолік значною мірою долається другою групою бездротових вбудованих пристроїв з індуктивним зв'язком. У цьому типі вбудованих пристроїв елементом виявлення є спеціально сконструйована антена, розміщена поблизу телефонної лінії. У цьому випадку електромагнітне поле, що оточує телефонну лінію, індукує в антені сигнали, які містять інформацію про характер конкретного повідомлення. Ці сигнали посилюються і перетворюються, а отримана інформація передається в точку запису. Вбудовані пристрої для зняття і зчитування інформації з волоконно-оптичних ліній відрізняються від вищезгаданих в основному лише способом зняття інформації. Для цього використовується спеціальний пристрій стиснення оптоволоконної лінії, який викликає інтерференційний процес на поверхні оптоволокна, що зчитується фотоприймачем.

Залежно від наявності або відсутності контрольного пристрою вбудовані пристрої можна умовно поділити на три групи [8].

Пристрої безперервного випромінювання є найпростішими та найдешевшими у виготовленні і призначені для отримання необхідної інформації протягом певного обмеженого часу. Робота цих приладів починається одразу після підключення джерела живлення. Якщо джерело живлення є автономним, час роботи таких детекторів не може перевищувати однієї-двох годин через високі витрати енергії на передачу сигналу. Час роботи накопичувачів, що живляться від мережі (електричної або телефонної), практично не обмежений. Однак є суттєві недоліки, притаманні всім пристроям безперервного випромінювання. Дистанційне керування пристроєм дозволяє йому переходити в режим випромінювання тільки тоді, коли об'єкт спостереження веде переговори або передає інформацію по відповідному каналу

зв'язку. Час випромінювання пристрою може бути додатково скорочений, якщо ВП оснащений пристроєм зберігання і стиснення сигналу.

Інший спосіб продовжити час роботи вбудованого пристрою - використання засобів, які автоматично вмикають передавач при появі сигналу (акустичного або електричного) на лінії зв'язку.

Пристрої, що активуються звуком, називаються акустичними пристроями (іноді їх називають системами VAS або VOX). ВП з таким пристроєм працюють у звичайному (черговому) режимі як звичайний акустичний приймач і споживають невелику кількість струму. При виявленні сигналу, наприклад, коли починається розмова між суб'єктом та іншою людиною, передавач подає живлення і переходить у режим випромінювання. Коли через певний проміжок часу (зазвичай кілька секунд) акустичний сигнал зникає (коли розмова припиняється), передавач вимикається, а самий ВП переходить у звичайний режим прийому. Використання передавачів акустичної сигналізації зазвичай подовжує час роботи вбудованих пристроїв у кілька разів. Однак особливістю використання акустичного пристрою є те, що перше слово зникає при кожному його вмиканні.

За зовнішнім виглядом розрізняють два типи підслуховуючих пристроїв [8]. Традиційний тип зазвичай має металевий корпус (пофарбований чи ні) і форму паралелепіпеда. Вони також є універсальними і можуть використовуватися в різних умовах. Такі пристрої часто використовують з одягом або предметами в приміщенні (книги, пластикові коробки, канцелярські прилади, кошики для документів, меблі і тому подібне). Ці електронні вбудовані пристрої також можуть використовуватися з локальними предметами, які передають акустичні та/або електромагнітні коливання (дерево, трава, фанера, зім'яті паперові або пластикові пакети і т.п.).

Пристрій в замаскованому вигляді використовується тільки в певних ситуаціях. Наприклад, вони використовуються у вигляді електричної або телефонної розетки тільки тоді, коли в приміщенні немає інших розеток, і вони повинні мати такий самий вигляд. Також їх використовують у вигляді особистих

речей (годинників, футлярів, шпильок, запальничок), коли вони відповідають загальному іміджу, характерному для стилю конкретної людини.

Як зазначалося вище, залежно від типу використовуваного джерела живлення, пристрої зберігання даних можна розділити на два типи [8].

До першого типу відносяться будь-які носії інформації з внутрішньою або акумуляторною батареєю.

До другого типу відносяться пристрої, що передають інформацію по лініях електропередач, або накопичувачі, що безпосередньо підключаються до ліній зв'язку. Час роботи таких пристроїв практично не обмежений.

1.4 Програмні методи та засоби захисту інформації

Захист від несанкціонованого доступу до інформації Для захисту інформації від несанкціонованого доступу встановлюються системи контролю доступу. Завданням системи контролю доступу є управління доступом користувачів до внутрішніх інформаційних ресурсів КС. Система складається з блоків ідентифікації та аутентифікації операцій, ініційованих конкретними користувачами, бази даних прав користувачів і блоків управління Коли необхідно виконати певну дію в ІС, користувач запускає програму. Операційна система запускає процес виконання програми, якій присвоєно атрибут користувача. Коли процес звертається до ресурсу ІС (програми, файлу або пристрою), система контролю доступу визначає, в чиїх інтересах був запущений процес, що вимагає доступу до ресурсу. Після авторизації процесу ІС контролю доступу вибирає інформацію про повноваження користувача з бази даних і порівнює її з вимогами до повноважень, визначеними для ресурсу. Якщо повноваження користувача не менші за запитувані, відповідний процес отримує дозвіл на виконання запитуваної дії над ресурсом. В іншому випадку операція відхиляється, а факт спроби порушення встановлених правил фіксується в спеціальному реєстрі. Для посилення стійкості ІС до несанкціонованого доступу

до інформації інформація на зовнішніх носіях шифрується, а тимчасові файли видаляються після закінчення обробки інформації.

1.5 Механізми захисту від несанкціонованої зміни технічної структури під час експлуатації ІС

На етапі експлуатації ІС зловмисник може виконати наступні несанкціоновані дії для зміни технічної (апаратної) структури підключити нестандартні блоки, пристрої або комп'ютери; модифікувати з'єднання ІС; оснастити стандартні блоки, пристрої або комп'ютери відповідними конструктивними компонентами зі зміненими характеристиками, змінивши режим роботи пристрою. Несанкціонованому доступу до апаратного та програмного забезпечення можна запобігти або суттєво ускладнити за допомогою таких заходів:

- захист приміщень, де встановлені апаратні засоби КС;
- заходи проти несанкціонованого проникнення в КС;
- заходи проти несанкціонованого підключення обладнання;
- захист внутрішніх засобів встановлення, управління та заміни обладнання від несанкціонованого втручання.

Загалом, контроль доступу до системи включає наступні операції:

- відкриття апаратного забезпечення;
- встановлення програмного забезпечення захисту інформації;
- ідентифікація та аутентифікація суб'єкта доступу;
- встановлення операційної системи;
- реєстрація суб'єкта доступу.

1.6 Несанкціоноване використання апаратного забезпечення комп’ютерних систем

Для запобігання розблокуванню можуть бути використані наступні методи:

- використання замка на блоці живлення;
- дистанційне керування блоком живлення;
- блокування керування блоком живлення.

У захищених системах перед звичайним завантаженням операційної системи та перед процесом завантаження операційної системи може бути встановлений програмний блок, який контролює процес ідентифікації та автентифікації. Цей блок відносно простий і захищає від несанкціонованих змін, забезпечуючи ідентифікацію, аутентифікацію та надійне завантаження операційної системи. Ідентифікація та аутентифікація суб'єкта доступу також може здійснюватися операційною системою після завершення завантаження операційної системи. Засоби і способи контролю доступу до пристрою повинні також слугувати для автоматичної реєстрації поведінки суб'єкта доступу. Реєстри подій можуть зберігатися на окремому комп'ютері або в мережі. Періодично або при виявленні порушень протоколу доступу адміністратори повинні переглядати реєстри для перевірки поведінки суб'єктів доступу. Контрольований доступ до системи завершується розблокуванням доступу та активацією системи контролю доступу для забезпечення санкціонованого доступу до ресурсів системи.

Для протидії загрозі неконтрольованих підключень пристроїв використовуються наступні методи.

Використання ідентифікаторів пристроїв. Контроль підключень пристроїв може бути досягнутий шляхом порівняння інформації про підключені пристрої з інформацією про зареєстровані пристрої в СК. Ця інформація включає тип і характеристики пристрою (обладнання), кількість і характеристики підключених зовнішніх пристроїв, режими роботи та іншу інформацію.

Ще більш надійним та ефективним методом контролю є використання спеціальних ідентифікаційних кодів пристроїв. Цей код може генеруватися апаратно або зберігатися в спеціальному запам'ятовуючому пристрої. Генератор може ініціювати видачу унікального номера пристрою контролю (в комп'ютерних мережах - робочому місцю адміністратора). Для захисту від несанкціонованого втручання, такого як зміна установки, заміна елементів або модифікація пристроїв, необхідно вжити таких заходів: - запобігання доступу до внутрішнього обладнання, органів управління та комутаційних пристроїв за допомогою замкнених дверей, кришок, захисних екранів тощо; - автоматичне керування ввімкненням та вимкненням пристроїв.

1.7 Мета і завдання роботи

Однією з найскладніших задач у сфері інформаційної безпеки є виявлення вбудованих пристроїв у комп'ютерні системи, через складну їх конфігурацію.

Це зумовлює актуальність вирішення проблеми пошуку та боротьби з НСД в комп'ютерній техніці. Метою даного дослідження є підвищення захищеності персональних комп'ютерів від вилучення інформації з обмеженим доступом з використанням вбудованих пристроїв шляхом застосування статистичних методів для аналізу поведінки окремих компонентів комп'ютера.

Для досягнення поставленої мети необхідно вирішити наступні завдання:

1. Проаналізувати конструкцію та принципи роботи вбудованих пристроїв для несанкціонованого зняття інформації з обмеженим доступом.
2. Оцінити методи виявлення вбудованих пристроїв від несанкціонованого доступу до даних.
3. Розробити рекомендації щодо протидії вбудованим пристроям в комп'ютерній техніці.

Висновки до розділу 1

У цьому розділі було описано типи, характеристики та класифікацію вбудованих пристроїв. Аналіз технічних аспектів та принципів роботи вбудованих пристроїв, що використовуються для перехоплення конфіденційної інформації, дозволив зробити наступні висновки:

1. Конструкція вбудованих пристроїв залежить від їх призначення та характеристик, а розуміння принципів роботи вбудованих пристроїв є важливим для ефективного виявлення та захисту.

2. Вивчення принципів роботи вбудованих пристроїв підтверджує потребу в сучасних технічних засобах захисту інформації.

РОЗДІЛ 2
ВИЯВЛЕННЯ ТА ХАРАКТЕРИСТИКА ВБУДОВАНИХ ПРИСТРОЇВ

2.1 Загальні методи виявлення вбудованих пристроїв

Одним з компонентів системи інформаційної безпеки є виявлення інтегрованих та функціонуючих вбудованих пристроїв. Цей процес здійснюється на основі двох великих груп методів і різних методів, що не входять до цих груп (рис. 2.1).

Рисунок 2.1– Методи виявлення ВП

До першої групи (пошук як фізичних об'єктів) відносяться методи виявлення, що базуються на пошуку АС як фізичних об'єктів з певними

властивостями, ваговими та розмірними характеристиками. До методів цієї групи належать [9]:

- візуальний огляд місць можливого знаходження СВУ, в тому числі з використанням лупи, дзеркал та спеціального освітлення;

- ретельний огляд важкодоступних місць з використанням засобів відеоспостереження;

- використання металодетекторів.

До другої групи (пошук як електронний пристрій) відносяться методи, що використовують характеристики СВП як електронних систем, наприклад [9]:

- використання індикаторів поля, які реагують на випромінювання радіовипромінювальних пристроїв і дозволяють виявити їх місцезнаходження;

- використання сигналів за певними характеристиками використання спеціальних радіоприймачів, призначених для пошуку та аналізу електромагнітної обстановки;

- використання відповідних комплексів радіопошуку та виявлення;

- обстеження об'єктів за допомогою нелінійної радіолокації.

Процес виявлення вбудованих пристроїв, як фізичного об'єкта є, звичайно, найбільш поширеним випадком, що підпадає під поняття огляду. Основні методи та використання спеціальних технічних засобів розглядаються нижче.

2.2 Методи виявлення вбудованих пристроїв як фізичних об'єктів (візуальний огляд)

Візуальний огляд об'єктів є дуже важливим методом, який не може бути замінений жодним приладом. Він призначений для пошуку у важкодоступних місцях без маскування людей або таким чином, щоб замаскувати людей. Його проводять у поєднанні з електронними засобами перед важливими зустрічами та в рамках періодичних перевірок.

Під час візуального огляду експерти рекомендують звертати увагу на нові подряпини, чистоту, сліди бруду (наприклад, залишки грунту від висаджених у

горщиках квітів) та інші особливості інтер'єру. Також слід звернути увагу на нові предмети інтер'єру, забуті речі, сувеніри та подарунки і, за необхідності, демонтувати їх повністю або частково. Огляньте телефони та аналогічне телекомунікаційне обладнання, а також лінії зв'язку, що ведуть до системи розподілу між абонентами. Також зверніть увагу на важкодоступні або незвичні місця (їх можна заховати у себе під носом і ніхто не помітить). Як було сказано вище, це дуже важливе і творче завдання, яке вимагає нестандартного підходу.

Для полегшення огляду об'єкта, що цікавить, використовуються спеціальні освітлювальні прилади (з різними режимами освітлення) і спеціальні дзеркала (дзеркальця). Спеціалізовані камери також використовуються для ергономіки та для доступу у важкодоступні місця.

2.2.1 Спеціалізовані камери для огляду. Ці інструменти можна розділити на дві групи:

- ендоскопічні інструменти;
- портативні системи відеообстеження.

Ендоскопічне обладнання включає фіброскопи, жорсткі бароскопи, відеоскопи та інше обладнання, що використовується для огляду важкодоступних ділянок.

Конструктивною особливістю цих приладів є невелика лінза на кінці гнучкої або прямої трубки, яка спрямовує об'єктив і забезпечує захист оптоволоконного кабелю або, у виняткових випадках, спеціальних систем лінз. Вони служать для передачі зображення з лінзи на ПЗС-матрицю або окуляр. Однак існують також типи, в яких ПЗС-матриця встановлюється безпосередньо за об'єктивом, і в цьому випадку використовуються звичайні кабелі передачі зображення або радіоканали.

Гнучкі бароскопи, як правило, використовуються для проходження через криволінійні просторові поверхні.

Жорсткі бароскопи пристосовані для спостереження прямих, вузьких щілин (порожнин) і використовують жорстку трубку замість гнучкої.

В результаті перевірки можуть здійснювати кілька людей, а не лише один працівник. Ще однією перевагою є те, що моніторинг можна здійснювати на відстані до 22 м від об'єкта.

Загальним недоліком ендоскопічних інструментів є те, що вони не підходять для коротких оглядів, а для більш тривалих, поглиблених обстежень.

У випадку бароскопів і фіброскопів якість зображення не зовсім задовільна, що повністю вирішується використанням відеоскопів, але швидке перенесення і підготовка до роботи неможливі.

2.2.2 Переносні відеосистеми для огляду. Це обладнання поєднує в собі переваги високої якості зображення з відносною простотою використання. Це досягається завдяки поєднанню телевізійної камери, регульованої штанги і відеомонітора з відповідною якістю зображення. Ці пристрої були розроблені в першу чергу для митних операцій, але зараз також використовуються для пошуку зброї масового знищення. Як приклад, прилад Alpha-4 має наступні особливості:

- телескопічна штанга з чорно-білою камерою та інфрачервоним підсвічуванням (для моніторингу на відстані до 2,5 метрів);

- невеликий LCD відеомонітор для роботи однією рукою;

- спеціальний футляр для перенесення іншого спеціального обладнання.

Футляр містить акумулятор, панель управління з дисплеєм, мікрофон і передавач з антеною. Останній використовується для передачі відеозображення на контрольний пункт, що дозволяє здійснювати спостереження за групою та подальший запис.

2.2.3 Металодетектори. Металодетектори є наступним етапом після візуального огляду, оскільки не завжди є можливість, час або проста неуважність (через тривале спостереження) для проведення якісного огляду. Під металодетекторним оглядом розуміють використання контактного або

безконтактного обладнання, яке виявляє нерівності на місцевості на основі фізичних характеристик. При виявленні таких аномалій видаються звукові або світлові сигнали. Таким чином, є можливість не тільки виявити об'єкти, а й визначити їх місцезнаходження. І при виявленні такої аномалії подається звуковий або світловий сигнал. Таким чином, є можливість не тільки виявити об'єкт, а й визначити його місцезнаходження. Металодетектори засновані на принципі виявлення металевих предметів у напівпровідниках і діелектриках (дереві, пластику, одязі тощо) і є одними з найпростіших детекторів, що використовуються для пошуку вибухових речовин. За конструктивними особливостями їх можна розділити на поясні (такі, що зустрічаються в аеропортах) і ручні, які підходять для вирішення таких завдань.

Наразі металодетектори практично ідентичні, за винятком особливостей експлуатації та характеристик користувача. Майже всі металошукачі пристосовані для пошуку чорних і кольорових металів на відстані від 10 до 500 мм. Характеристики також залежать від ваги об'єкта. Всі пристрої переважно розпізнають за звуком, а іноді і за світлом.

2.3 Методи виявлення вбудованих пристроїв

Відповідно до схеми основними методами виявлення електронних вбудованих пристроїв є використання індикаторів місцевості, використання спеціалізованих приймачів, використання систем радіоконтролю, використання нелінійних радарів.

Ці методи такі: використання індикатора місцевості, використання спеціалізованого приймача, використання системи радіоконтролю та використання нелінійних радарів. Всі ці методи базуються на наявності певної форми радіовипромінювання в АС. Це дуже важливий демаскуючий фактор і, як наслідок, його дуже легко виявити.

Крім того, випромінювання цих пристроїв має свої особливості, про які зараз піде мова. ключові показники випромінювання радіотрансляційних вбудованих пристроїв:

- відносно сильний сигнал випромінювання підходить для передачі сигналів на відносно великі відстані. Це відбувається за рахунок менших розмірів пристрою і якісної фільтрації прийнятого сигналу;

- поява нових сигналів (частотних діапазонів) у просторі;

- локалізація певних сигналів у просторі.

Це означає, що при повороті приймальної антени всі сигнали поводяться однаково, крім радіотрансляційних вбудованих пристроїв. Підходить лише для радіотрансляційних вбудованих пристроїв без інформаційного кодування. При використанні обладнання без інформаційного кодування оператор може чути дійсні акустичні сигнали. В апаратному режимі вони обробляються різними кореляторами для забезпечення постійної видимості. Цей спосіб не підходить при використанні інформаційного кодування. Йдеться про використання обладнання з дистанційною активацією радіотрансляційних вбудованих пристроїв або системи VOX. Особливістю таких радіотрансляційних вбудованих пристроїв є те, що сигнали з'являються під час «критичних» розмов або коли доступні лише акустичні сигнали (у випадку систем VOX).

2.4 Виявлення вбудованих пристроїв на основі непрямих даних

Виявлення ґрунтується на непрямих даних, тобто на раніше отриманих статистичних даних і поведінці цільового користувача. Воно може бути реалізоване з використанням обох підготовлених моделей правил [1].

1) При виявленні на основі статистичних відхилень дані, що характеризують поведінку законних користувачів, збираються в часові ряди. Аналізуючи ці дані за допомогою статистичних методів, можна з високим ступенем достовірності визначити потенційну небезпеку конкретного користувача. Найпоширенішими методами є використання порогових значень

частоти аномальної поведінки в системі та використання профілів поведінки (створюється профіль поведінки користувача та виявляються відхилення в поведінці).

2) Виявлення рішень на основі правил про те, що певні типи поведінки є поведінкою зловмисника. Найбільш поширеними є виявлення аномалій та виявлення вторгнень.

У інформаційному джерелі [3] описано актуальність статистичних досліджень поведінки користувачів для виявлення зловмисників, у тому числі тих, що використовують вбудовані в комп'ютер пристрої перехоплення інформації. Це є передумовою стандартизації та уніфікації статистичних спостережень і механізмів забезпечення конфіденційності даних.

Методи, засновані на обробці статистичної інформації [3], вимагають мінімальних витрат від організацій-користувачів, але їхня ефективність є достатньою. Методи, засновані на правилах, передбачають детальний аналіз систем і мереж, організовують захист від певних типів зловмисників і можуть ефективно захищати від нестандартних атак. Процес отримання статистичних даних з компонентів комп'ютера найпростіше здійснювати за допомогою готових або створених програмних засобів, тобто шляхом логування або запису в системний реєстр.

Слід розуміти, що цей метод не може виявити пристрої зберігання даних, які не підключені безпосередньо до комп'ютера, наприклад, камери, що працюють на батарейках, або камери з пам'яттю. Однак, якщо пристрій зберігання даних контактує з комп'ютером, наступні результати можуть бути записані в реєстр подій. - Споживання енергії, частота, температура, швидкість компонентів або інші умови можуть змінитися. Реєстри подій зазвичай зберігаються на диску з операційною системою або в деяких випадках на материнській платі. На основі даних про стан пристрою і завдання, зібраних за допомогою реєстрів за певний період часу, системний адміністратор, який повинен відповідати за збір і зберігання реєстрів, може створити базу даних або

інший формат для зберігання такої інформації і передати їх адміністратору безпеки.

На основі даних, отриманих двома описаними вище методами, адміністратор безпеки може зробити висновок про те, що - є користувачі комп'ютера, в реєстрах подій яких зафіксовані підозрілі або незвичні зміни в поведінці компонентів комп'ютера, і ці події можуть свідчити про те, що підозрюваний міг використовувати програмне забезпечення для наступних цілей машина могла бути підроблена. Хоча в наявній статистиці не було виявлено жодних підозрілих елементів, комп'ютери слід перевірити іншими методами, оскільки не все програмне забезпечення має значний вплив.

2.5 Характеристики та поширені місця розташування вбудованих пристроїв у технічних засобах

Вбудовані пристрої в персональних комп’ютерах і складних комп’ютерних системах є найпривабливішим місцем для зловмисників.

Згідно з Розпорядженням ВКНМР № 276-2021-р «Про затвердження схем захисту інформації в системах автоматизації 1 класу», до пристроїв АС (табл. 2.1) належать:

- системний блок (корпус (разом з блоком живлення), материнська плата, процесор, відеокарта, оперативна пам'ять, жорсткий диск (SSD));

- периферійні пристрої (монітор, клавіатура, миша, принтер, джерело безперебійного живлення, мережевий фільтр, флеш-накопичувачі).

Таблиця 2.1 Класифікація компонентів комп'ютерної техніки

Класифікація (типовий перелік елементів) компонентів ПЕОМ, що приймають участь у обробці ІзОД		
системний блок	периферійні пристрої	пристрої призначені для позамережного цифрового переміщення інформації
материнська плата	маніпулятор миша	накопичувачі на основі flash пам'яті
процесор	клавіатура	оптичний привід
оперативна пам'ять	монітор	НГМД
відеокарта	додатковий блок живлення	
жосткий диск (SSD)	принтер	
корпус (з блоком живлення)	проектор	
звукова плата	сканер	
	БФП	
	мережевий фільтр	
	мікрофон	
	звукові колонки;	
	головні телефони	
	web-камери	

У контексті сучасних і застарілих комп'ютерних комплектів перелік цих компонентів може включати:

- системні блоки: звукові карти;

- периферійні пристрої: проектори, сканери, МФУ, мікрофони, аудіоколонки, навушники, веб-камери;

- оптичні приводи, НГМД.

2.6. Механізми захисту від несанкціонованого доступу до програмного забезпечення в процесі експлуатації ІС

Захист від несанкціонованої модифікації структури програми застосовується для наступних цілей:

- захист від несанкціонованої модифікації програми обслуговуючим персоналом;

- захист від шкідливого програмного забезпечення.

Основними напрямками захисту від несанкціонованої модифікації програми обслуговуючим персоналом під час експлуатації є

- контроль цілісності програми;

- захист від несанкціонованого копіювання та перевірки програми;

- спеціальне регулювання процесу модифікації програми.

Програма повинна регулярно перевірятися на предмет несанкціонованих модифікацій за допомогою спеціальних методів, що дозволяють отримати контрольні характеристики незміненої природи досліджуваної програми. До них відносяться методи контрольних сум, використання хеш-функцій тощо. Контрольні характеристики повинні зберігатися або в зашифрованому вигляді, або в пам'яті, недоступній для зловмисників. Оскільки зловмисник не може внести необхідні зміни без вивчення алгоритмів роботи програми, для захисту від копіювання або подальшого вивчення програми використовуються найрізноманітніші апаратні та програмні засоби.

Важливою частиною забезпечення цілісності програми є організація процесу перегляду програми та виправлення помилок. Це вимагає особливого контролю за діями виконавців та документування змін. Радикальним способом запобігання потраплянню шкідливого програмного забезпечення в систему є використання в КС закритих програмних середовищ. У системі може працювати лише необхідна кількість перевірених прикладних програм, що завантажуються

в КС під час суворо регламентованих дій. Запуск незареєстрованих програм, які потрапляють в систему будь-якими шляхами, в тому числі каналами зв'язку, заборонений на технічному рівні.

Якщо умови експлуатації системи не дозволяють створити закрите програмне середовище, для боротьби зі шкідливими програмами використовуються два підходи.

Перший – це блокування потенційно небезпечного трафіку. Для обмеження можливості проникнення шкідливого ПЗ в систему використовуються міжмережеві екрани (брандмауери). Основна функція цих інструментів - фільтрувати трафік за певними правилами.

Основним захистом від шкідливого ПЗ є антивірусна система, яка виконує наступні завдання:

- виявляє шкідливе ПЗ в КС;

- блокує поведінку шкідливого ПЗ;

- усуває наслідки дії шкідливого ПЗ.

Антивірусне програмне забезпечення зазвичай використовує два методи для виявлення шкідливого програмного забезпечення:

- сканує файли для виявлення відомих шкідливих програм (інформація про шкідливі програми є в антивірусній базі даних);

- виявляє підозрілу поведінку програм, схожу на поведінку зараженої програми виявляє підозрілу поведінку програм, схожу на поведінку зараженої програми.

Якщо комп'ютер заражений, необхідно виконати наступні дії:

1. Відключити комп'ютер від інформаційної мережі і спробувати видалити шкідливе програмне забезпечення за допомогою встановленого антивірусу і доступних утиліт.

2. Якщо наслідки зараження не вдається усунути, комп'ютер необхідно вимкнути, щоб знищити резидентний вірус.

3. Запустіть операційну систему та антивірусну систему зі знімного носія, який точно не містить шкідливого програмного забезпечення.

4. Збережіть важливі файли без резервних копій на знімний носій.

5. За допомогою антивірусного програмного забезпечення видаліть вірус і відновіть файли та обсяг пам'яті. Якщо роботу комп'ютера буде відновлено, переходьте до пункту 9, якщо ні - переходьте до пункту 6.

6. Завершіть видалення та маркування (форматування) незнімних зовнішніх носіїв інформації.

7. Відновіть операційну систему, інші програмні системи та файли з дистрибутивів і резервних копій, створених до зараження.

8. Ретельно перевірте файли, збережені після виявлення зараження, видаліть віруси та за потреби відновіть файли.

9. Ретельне сканування комп'ютера всіма доступними антивірусними засобами для повного відновлення інформації.

Висновок до розділу 2

У цьому розділі були розглянуті методи та методики, які можуть бути використані для виявлення та ідентифікації вбудованих пристроїв. Було запропоновано рішення для підвищення точності виявлення вбудованих пристроїв.

Рішення базується на врахуванні особливостей пошуку фізичних об'єктів та електронних пристроїв в інформаційних системах. Крім того, для виявлення підозрілої поведінки аналізується поведінка користувачів комп'ютерів. Перевага запропонованого рішення полягає в тому, що вбудовані пристрої можуть бути виявлені на ранній стадії використання комп'ютера. Це може запобігти загрозі витоку конфіденційної інформації. Також представлені пропозиції щодо виявлення вбудованих пристроїв. Однак обмеженням запропонованого рішення є низька точність виявлення невеликих вбудованих пристроїв.

РОЗДІЛ 3
ОСОБЛИВОСТІ ВИЯВЛЕННЯ ТА ЗАХИСТУ КОМП'ЮТЕРНОЇ ТЕХНІКИ ВІД ВБУДОВАНИХ ПРИСТРОЇВ

У цьому розділі розглядаються способи пошуку вбудованих пристроїв в комп'ютерній техніці, яка поділяється на три групи (системні блоки, периферійні пристрої та пристрої для автономної передачі цифрової інформації).

Залежно від їх розташування в комп'ютерному обладнанні сформульовані рекомендації щодо поліпшення пошуку вбудованих пристроїв. Кожен компонент працюючого комп'ютерної системи, може мати наступні характеристики, які розпізнаються і доступні для виявлення вбудованих пристроїв [10]:

- заздалегідь визначені технічні дані про компоненти;
- реєстри операцій і запитів;
- споживана потужність;
- частота;
- температура;
- швидкість роботи компонента;
- інтенсивність випромінювання, включаючи звук і світло.

Вимірювання цих параметрів можна контролювати в більшості випадків для коректної роботи комп'ютера. Крім використання цих даних для виявлення вбудованих пристроїв, можна також збирати статистику змін параметрів для фонового моніторингу, щоб запобігти тривалій роботі в разі попереднього пошуку вбудованих пристроїв на основі виявлених таким чином нестандартних значень і раптового підключення вбудованих пристроїв. Однак вплив вбудованих пристроїв на роботу комп'ютера не настільки великий, щоб його можна було виявити статистично, тому стандартні методи виявлення та боротьби з вбудованими пристроями залишаються актуальними.

Згідно з таблицею 2.1, всі компоненти комп'ютера можна розділити на

- системні блоки;

- периферійні пристрої;

- пристрої, призначені для автономної передачі інформації.

Залежно від того, до якої з цих груп вони належать, можна розглядати особливості виявлення та протидії вбудованим пристроям в комп'ютерній системі.

3.1 Вбудовані пристрої в компонентах системного блоку ПК

Компоненти системного блоку можна розділити на три категорії: обробка та передача інформації, зберігання інформації та живлення. Материнські плати належать до всіх категорій одночасно, залежно від їхнього призначення.

Таблиця 3.1. Складові частини системного блоку

Компоненти системного блоку		
обробка та передача інформації	зберігання інформації	електроживлення
материнська плата		
процесор	жорсткий диск (SSD)	корпус, блок живлення, система охоложення
відеокарта	оперативна пам'ять	
звукова плата		

3.1.1 Обладнання для обробки та передачі інформації. Всі компоненти, пов'язані з обробкою інформації, тісно пов'язані з іншими групами компонентів і надзвичайно чутливі до пристроїв пам'яті, встановлених до запуску комп'ютера.

Для прикладу розглянемо материнську плату класу Supermicro (рис. 3.1) [10].

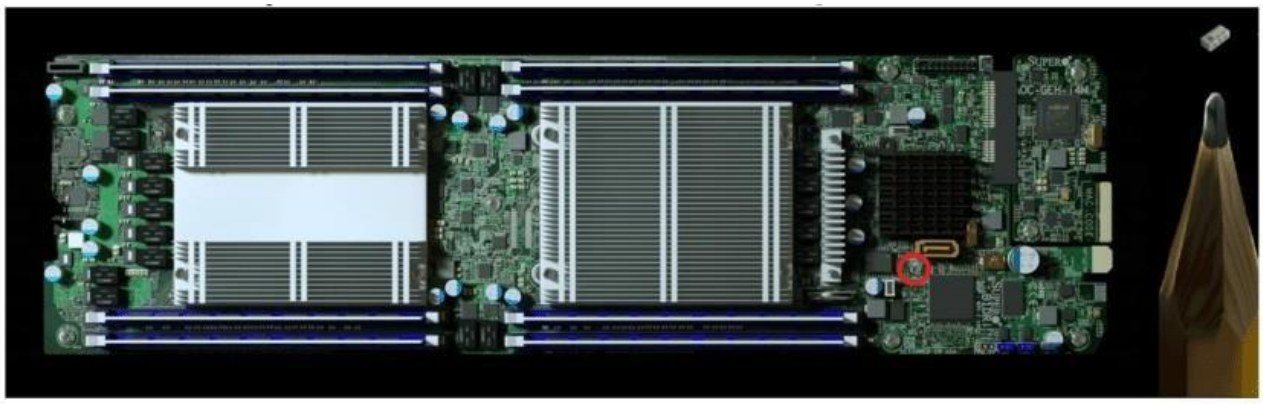

Рисунок 3.1 - Материнська плата Supermicro з невеликим вбудованим пристроєм

Вбудовані пристрої настільки малі, що виявити їх та ефективно протидіяти їм можна лише шляхом вивчення схеми материнської плати під мікроскопом, а потім порівняння її з аналогічними виробами. Це надзвичайно трудомісткий і тривалий процес.

Другий спосіб - перевірка ваги компонента (ефективно, якщо пам'ять не вказана в експлуатаційній документації).

Також раціональним є проведення перевірки та моніторингу навколишнього середовища на предмет випромінювання, яке випромінює вбудований компонент.

Крім того, іншими засобами виявлення вбудованих пристроїв є перевірка портів і роз'ємів. А також перевірка та порівняння енергоспоживання із заявленим енергоспоживанням (коли комп'ютерні компоненти цього типу простоюють, застосовувати такий спосіб неефективно). Такі комп'ютерні компоненти споживають більшу частину енергії машини навіть у режимі очікування, а наявність фонових процесів операційної системи унеможливлює моніторинг стрибків споживання.

По можливості варто використовувати механізми, що унеможливлюють моніторинг зовнішнього радіо- та електромагнітного випромінювання.

Можливість проникнення рентгенівського або іншого випромінювання в компоненти/пристрої.

Шляхом перевірки, моніторингу та збору значень властивостей компонентів можна збирати статистику за допомогою комп'ютерних реєстрів і за їх допомогою виявляти портативні вбудовані пристрої.

3.1.2 Пристрої для зберігання даних. До пристроїв зберігання інформації слід віднести оперативну пам’ять, жорсткі диски, інші накопичувачі (слід зазначити, що подібні накопичувачі є швидкодіючими пристроями і тому мають більш високі показники випромінювання та енергоспоживання порівняно з аналогічними компонентами) мають наступні важливі відмінності від компонентів обробки та передачі даних - відсутність активної обробки інформації, що призводить до дуже низького рівня випромінювання, а також відсутність компонентів з непровідними характеристиками випромінювання інформації, таких як ОЗП та ПЗП. Виходячи з цих характеристик, ефективні заходи для виявлення потративних вбудованих пристроїв можна вжити наступним чином:

- шляхом порівняння енергоспоживання пам'яті з технічними характеристиками пристрою, в деяких випадках в першу чергу шляхом перевірки дисків, які служать для зберігання даних, що не використовуються системою; - шляхом перевірки портів і роз'ємів;

- контроль можливого проникнення в компоненти/пристрої рентгенівського або іншого випромінювання;

- метрологічний контроль компонентів, ефективний, коли портативний вбудований пристрій не зазначено в експлуатаційній документації;

- контроль надлишкового випромінювання, що випускається компонентами, і моніторинг навколишнього середовища;

- радіочастотний контроль з використанням механізмів, що перешкоджають його передачі.

Особливу увагу слід звернути на характеристики джерела живлення, швидкодію компонентів, задані технічні дані компонентів, реєстри роботи та опитування і частоти.

3.1.3. Елементи системи електроживлення. Компоненти живлення - це комп'ютерні компоненти з важливою установкою і розташуванням пам'яті, які виконують свою функцію за рахунок електромагнітних властивостей пристрою.

Як правило, цифрове електронне обладнання забезпечує синхронізовану роботу логічних пристроїв. Тому, коли кожен логічний пристрій перемикається, енергія концентрується в синхронізованих дрібних імпульсних компонентах, які при накладанні можуть генерувати більш високі сумарні рівні випромінювання, ніж ті, які можуть генеруватися окремими пристроями. Характеристики негативної шини джерела живлення та заземлення мають значний вплив на рівень генерування електромагнітних імпульсів. Навіть радіочастотний друкований провідник більше схожий на котушку, ніж на замикаючий провід, тому це з'єднання повинно мати дуже низький імпеданс.

У багатьох випадках основним джерелом випромінювання є кабелі, які передають інформацію в цифровому вигляді. Такі кабелі знаходяться всередині обладнання або з'єднують обладнання між собою. Використання заземлюючих перемичок з обплетення кабелю призводить до того, що кабель поводиться як передавальна антена, оскільки характеризується високими значеннями індуктивності та активного опору до радіочастотних завад і не забезпечує хорошої якості заземлення екрану. При аналізі можливості витоку інформації необхідно враховувати наступні характеристики радіотехнічного каналу витоку інформації з цифрового електронного обладнання [11]:

- для відновлення інформації, крім знання рівня електромагнітного імпульсу, необхідно знати її структуру - інформація в цифровій електронній апаратурі являє собою послідовність прямокутних імпульсів найкращим приймачем для перехоплення EMI є детектор, оскільки вона передається за допомогою EMI - факт наявності сигналу важливий сам по собі, а його форма відома, тому відновити сигнал легко;

- не всі ЕМІ є небезпечними з точки зору фактичного витоку інформації. Як правило, найвищі рівні відповідають неінформаційним випромінюванням (найвищі рівні в ЕМІ генеруються синхронізованими системами);

- через наявність великої кількості паралельних електричних ланцюгів інформаційні та неінформаційні випромінювання можуть перекриватися в діапазоні (взаємна інтерференція). Імпульсний характер інформаційного сигналу викликає різке збільшення смуги пропускання приймача, що призводить до підвищення рівнів власних і заважаючих шумів;

- періодичне повторення сигналу збільшує діапазон, доступний для прослуховування - використання паралельних кодів у більшості випадків робить відновлення інформації під час ЕМІ-прослуховування практично неможливим.

Важливим питанням технічного захисту об'єктів комп’ютерних телекомунікаційних систем є виявлення каналів витоку інформації з комп'ютерів. Такі канали утворюються безпосередньо під час роботи комп'ютера та в режимі очікування. Їх джерелами є - електромагнітні поля - струми і напруги в струмопровідних системах (силових, заземлюючих і з'єднувальних лініях) - надлишкові випромінювання оброблюваної інформації на завадоутворюючих частотах елементів і пристроїв комп'ютерної техніки - надлишкові випромінювання оброблюваної інформації на частотах контрольно-вимірювальних приладів. Крім перерахованих каналів, в силу походження і технічних особливостей процесів, що відбуваються в комп'ютерах, в комп'ютерах, що поставляються на ринок, можуть бути навмисно створені додаткові канали витоку інформації.

Для створення таких каналів може бути використано наступне [11]:

- розміщення в комп'ютерах вбудованих пристроїв (замаскованих під певні електронні блоки) для запису звукових сигналів або оброблюваної інформації;

- розміщення в комп'ютерах радіомаяків;

- встановлення в комп'ютерах вбудованих пристроїв, що забезпечують руйнування комп'ютера ззовні (схемне);

- встановлення елементної бази помилок. Свідоме використання таких конструктивних і схемотехнічних рішень збільшує електромагнітні випромінювання в певних ділянках спектра. У групі каналів, де основним видом обробки даних є апаратна обробка, можливі наступні канали витоку;

- спеціально спроектовані апаратні з'єднання з комп'ютерами, що забезпечують доступ до інформації;

- використання спеціальних технічних заходів для блокування електромагнітних випромінювань, що виходять від комп'ютерного обладнання.

Виходячи з цих характеристик, ефективно запобігти встановленню несанкціоновано вбудованих пристроїв можна наступними методами [11]:

- перевірка портів і роз'ємів;

- мікроскопічне дослідження схем;

- використання захисних/детекторних механізмів для відкриття компонентів;

- візуальний огляд;

- можливе проникнення рентгенівського або іншого випромінювання в компонент/пристрій;

- контроль і моніторинг навколишнього середовища надлишкового випромінювання, що випромінюється компонентом;

- збір статистичної інформації шляхом перевірки, моніторингу та збору значень для відстежуваних характеристик компонента за допомогою комп'ютерних реєстрів, виявлення з їх допомогою вбудованих пристроїв.

Коли це можливо, використовуйте механізми, що запобігають зовнішньому радіо- та електромагнітному випромінюванню, що відстежується. Контролювати наступні потенційні шляхи витоку інформації:

- побічні електромагнітні випромінювання в діапазоні частот від 10 Гц до 5 ГГц;

- сигнальні наведення на лінії електропередач, лінії заземлення та лінії зв'язку;

- внаслідок впливу високочастотних електромагнітних полів на різні лінії, встановлені в приміщеннях, які можуть бути приймальними антенами, канали витоку інформації.

У цьому випадку випробування проводяться в діапазоні частот від 20 кГц до 1 ГГц.

3.2 Периферійні пристрої

Периферійні пристрої поділяються на чотири категорії:

- механічна обробка інформації;

- електромагнітна обробка інформації (включаючи світлове випромінювання),

- обробка звукової інформації та периферія електроживлення.

Таблиця 3.2. Периферійні пристрої

Периферійні пристрої			
механічна робота з інформацією	інформація, що транслюється електромагнітним випромінюванням (включаючи видиме світло)	інформація, що транслюється за допомогою звуку (аудіо)	периферійні пристрої електроживлення.
маніпулятор миша	монітор	звукові колонки;	мережевий фільтр
Клавіатура	принтер	головні телефони	додатковий блок живлення
	проектор	мікрофон	
	сканер		
	БФП		
	web-камери		

3.2.1 Механічні компоненти, що містять інформацію. Компоненти, пов'язані з інформаційно-місткими механічними завданнями, найімовірніше, є

«бортовими клавіатурами/мишами» або подібними пристроями. Розглянемо, наприклад, клавіатуру Logitech G510 (Рис. 3.2).

Деякі маніпулятори також мають додаткові функції та мікросхеми, що їх забезпечують.

Рисунок 3.2 - LOGITECH G510 - клавіатура з інтегрованим роз'ємом jack та звуковою картою

Ефективно вжити наступних запобіжних заходів:

- якщо пристрій не має зайвих функцій, візуально визначте наявність зайвих елементів у схемі, порівнявши її з іншими подібними маніпуляторами;

- якщо додаткові функції присутні, слід вжити заходів, щоб забезпечити їхню роботу з компонентами обробки та передачі інформації;

- особливу увагу слід звернути на характеристики джерела живлення;

- попередньо визначені специфікації компонентів, робочі регістри та регістри запитів, температуру, інтенсивність та частоту випромінювання, в тому числі звукового та світлового;

- перевірка портів і роз'ємів;

- можливе проникнення рентгенівського та іншого випромінювання в компоненти/пристрої;

- мікроскопічне дослідження схем;

- використання механізмів захисту від несанкціонованого втручання/виявлення.

- там, де це можливо, використання засобів, що запобігають моніторингу зовнішніх радіо- та електромагнітних хвиль;

- візуальна перевірка.

3.2.2 Засоби електромагнітної обробки інформації. Операційні компоненти, які обробляють електромагнітну інформацію, особливо чутливі до ЕМВ, пов'язаних зі значними ризиками для конфіденційності інформації, такі як камери, відеоскімери та подібні пристрої. Існують також пристрої з додатковими функціями, пов'язаними з випромінюванням у невидимому для людини спектрі, і мікросхеми, які їх забезпечують.

Враховуючи, що подібні типи портативних вбудованих пристроїв доступні на споживчому ринку, і що деякі зловмисники можуть створити міні-камери, які працюють з цим пристроєм, виявленню портативних вбудованих пристроїв можна ефективно протидіяти за допомогою наступних заходів:

- перевірка та порівняння фактичного енергоспоживання та заявленого енергоспоживання є хорошим способом переконатися у високому енергоспоживанні;

- перевірка енергоспоживання та порівняння його із заявленим енергоспоживанням є неефективним при живленні пристроїв з високим енергоспоживанням.

Рисунок 3.3 - SQ11, невелика, легкодоступна камера, може бути використана як вбудований пристрій, якщо її встановити у відсік всередині принтера.

Оскільки такі компоненти комп’ютерних систем споживають велику кількість електричної енергії під час роботи, а також існує нерівномірне енергоспоживання принтерів, сканерів, Amoled-дисплеїв та подібних частин пристрою, неможливо відстежити стрибки енергоспоживання.

Особливу увагу слід звернути на характеристики:

- джерела живлення, визначені технічні дані компонента, записи про експлуатацію та вимоги, температуру, інтенсивність випромінювання, включаючи звук, світло та частоту;

- використання елементів захисту та виявлення при вмиканні компонента;

- якщо можливо, використання засобівв, що запобігають зовнішньому радіо- та електромагнітному відстеженню;

- візуальний огляд.

3.2.3 Компоненти обробки звукової інформації (аудіо). Компоненти обробки інформації, пов'язані з аудіо, є особливо чутливими для портативних вбудованих пристроїв щодо ризику порушення конфіденційності інформації

через підслуховуючі пристрої, спрямовані мікрофони, додаткові антени для дротових/бездротових навушників та подібні пристрої.

Деякі пристрої також здатні відтворювати звук на високому рівні гучності. Це означає, що звук може відтворюватися з енергією, достатньою для передачі вібрацій через стіни, за умови, що існують задані значення характеристик пасивних засобів звукозахисту, таких як стіни.

Слід також враховувати, що через аномалії в електромагнітному випромінюванні існують частоти, які не можуть бути виявлені людиною і потребують додаткових пристроїв виявлення.

У зв'язку з особливостями звуку і пов'язаних з ним пристроїв, слід мати на увазі, що мембрани, встановлені на акустичних і записуючих пристроях, можуть використовуватися в обох режимах, оскільки всі вони конструктивно ідентичні, а ці пристрої можна виявляти і ефективно боротися з ними обома способами - слід перевіряти і порівнювати споживану і заявлену потужність. Додаткові антени і записуючі пристрої можуть мати значний вплив на необхідну потужність у відсотковому відношенні.

Особливу увагу слід звернути на характеристики джерела живлення, попередньо визначені специфікації компонентів, реєстри роботи та опитування, температуру, інтенсивність випромінювання, включаючи звук і світло, та частоту.

3.2.4 Периферійні компоненти живлення. Периферійні компоненти електричного живлення відрізняються від компонентів живлення всередині комп'ютера за кількома параметрами, найважливішим з яких є їхнє розташування. Ці компоненти не мають прямого доступу до блоку живлення машини і тому практично не можуть передати зловмиснику інформацію, що обробляється комп’ютерною системою, але вони підключені до блоку живлення комп’ютерної системи і можуть маскувати енергоспоживання запам'ятовуючих пристроїв, таких як камери, антени, мікрофони і диктофони.

Виходячи з цих особливостей, наступні методи можуть бути використані для ефективного запобігання виявленню пристроїв живлення:

- перевірка споживаної потужності та порівняння її із заявленою неефективна, оскільки такі комп'ютерні компоненти споживають велику кількість машинної енергії під час роботи;

- перевірка та контроль роз'ємів;

- перевірка ваги компонентів (ефективна, якщо вага портативних вбудованих пристроїв не вказана в експлуатаційній документації);

- можливе проникнення в компоненти/пристрої рентгенівського або іншого випромінювання;

- перевірка та моніторинг необґрунтованих випромінювань, що випромінюються в навколишнє середовище;

- за можливості, використовувати механізми, що унеможливлюють моніторинг зовнішнього радіо- та електромагнітного випромінювання.

- контролювати, відстежувати та збирати значення характеристик компонентів, які можна відстежувати за допомогою комп'ютерних реєстрів для збору статистики і за допомогою цього виявляти наявність портативних вбудованих пристроїв.

Особливу увагу слід приділяти реєстрам і частотним характеристикам операцій і запитів.

3.3 Немережеві пристрої для передавання інформації

Пристрої, призначені для немережевої передачі цифрової інформації, відрізняються від постійних запам’ятовуючих пристроїв мобільністю та функціональністю (Таблиця 3.3).

Зауважте, що такі пристрої можуть бути відкрито обладнані антенами, мікрофонами, камерами тощо, що має бути ретельно продумано організацією при їх придбанні. Крім того, оскільки накопичувачі на гнучких дисках практично не використовуються, цей пункт не вартий подальшого розгляду.

Таблиця 3.3 Обладнання, призначене для позамережевого передавання інформації

Пристрої призначені для позамережевого цифрового переміщення інформації	
Оптичний привід	Накопичувачі на основі flash пам’яті

3.3.1 Оптичні накопичувачі. Компоненти, пов'язані з обробкою інформації на дисках, наражаються на ризик втручання в роботу пристроїв копіювання інформації, підключаючись до комп’ютерних систем як посередник для передачі інформації, оскільки дискові пристрої зазвичай потребують адаптера. У випадку з бездротовими функціями також існує ризик втрати конфіденційності інформації через додаткові антени.

Деякі пристрої також мають можливість безпосередньо зв'язуватися з компонентами відтворення відео та аудіо на комп'ютері. Враховуючи ці особливості, для ефективної протидії застосуванню портативних вбудованих пристроїв можна використовувати наступні методи:

- перевірка портів і роз'ємів;
- перевірка ваги компонентів (корисно, якщо вона не вказана в експлуатаційній документації ВП);
- перевірка і моніторинг навколишнього середовища на предмет надмірного випромінювання компонентів;
- мікроскопічне дослідження мікросхем;
- використання механізмів захисту від несанкціонованого втручання/виявлення;
- якщо можливо, використання пристроїв, що перешкоджають моніторингу зовнішнього радіо- і електромагнітного випромінювання;
- по-можливості візуальний огляд;
- можливе проникнення рентгенівського або іншого випромінювання в компоненти/пристрої;

- перевірка, моніторинг та збір значень характеристик компонентів, що відслідковуються, з використанням комп'ютерних реєстрів для збору статистики та використання її для виявлення портативних вбудованих пристроїв.

Особливу увагу слід приділяти характеристикам потужності, реєстрам роботи та запитів, температурі, інтенсивності випромінювання, включаючи звук і світло, швидкості та частоті компонентів.

У випадку з бездротовими пристроями також існує ризик порушення конфіденційності інформації через додаткові антени. Деякі пристрої також мають можливість безпосередньо взаємодіяти з відео- та аудіопрогравачами комп'ютера.

Ми також розглянемо USB та подібні роз'єми, але слід розуміти, що ця тема тісно пов'язана з розділами «системні блоки» та «периферійні пристрої», згаданими у розділі про роз'єми.

У цьому розділі ми розглянемо загрозу від пам'яті в роз'ємі на прикладі Cottonmouth - сімейства апаратних вбудоваок, що складаються з повнофункціональних мікроконтролерів архітектури ARM, замаскованих під USB-кабелі та USB-порти. Окрім мікрокомп'ютера Trinity, до складу цих портативних вбудованих пристроїв також входить радіомодуль Howlmonkey для організації двосторонніх радіоканалів середньої та малої дальності CM-I - це стандартний USB-кабель (див. рис. 3.4), який можна використовувати як подовжувач USB або з будь-яким USB CM-I та CM-II, припаяним до материнської плати (замість стандартного порту USB+Ethernet). Основною функцією цього портативного вбудованого пристрою є завантаження помилок програмного забезпечення та організація бездротових мереж стільникового зв'язку короткого радіусу дії. Для завантаження програмного забезпечення портативний вбудований пристрій може емулювати USB-клавіатури та інші маніпулятори.

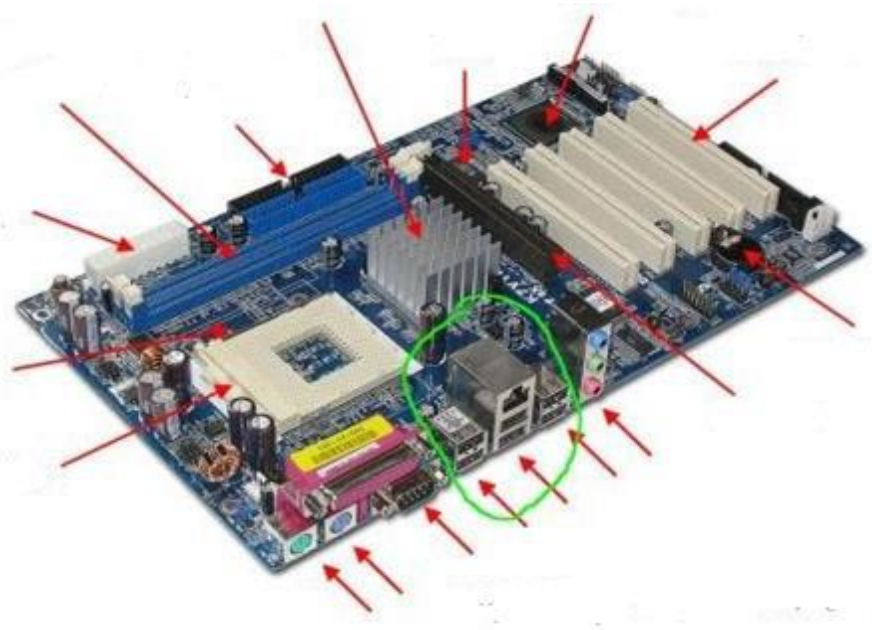

Рисунок 3.4 - Можливі місця розташування СМ-І на материнській платі

Порт USB на материнській платі підключається до джерела живлення та комп'ютерної мережі. На рентгенівському знімку материнської плати важко виявити СМ-ІІІ через вертикальне розташування плати управління TRINITY.

Firewalk - це варіант Cottonmouth, дуже схожий на СМ-ІІІ. Разом з Howlermonkey, Firewalk можна використовувати для пасивного прослуховування Ethernet-трафіку на вбудованих материнських платах або вбудовування його в мережеві карти. Дистанційно керований мережевий сніффер, здатний таємно впроваджувати користувацькі пакети через прихований радіоканал.

Починаючи з 2010-х років, 400 МГц ARM 9 матиме 32 МБ флеш-пам'яті (з можливістю розширення), 64 МБ оперативної пам'яті та ПЛІС + 128 МБ DDR2 модуль для мікропрограмного забезпечення. Результатом є дуже маленька, надзвичайно універсальна плата, яку можна вбудовувати або припаювати практично в будь-що, включаючи материнські плати, телефони та маршрутизатори.

Єдине, що обмежує масове розповсюдження - це її ціна, яка становить кілька тисяч доларів за штуку.

З огляду на ці характеристики, виявлення портативного вбудованого пристрою можна здійснити наступним чином:

- перевірка портів і роз'ємів;

- перевірка ваги компонентів (корисно, якщо вона не вказана в експлуатаційній документації);

- перевірка та моніторинг навколишнього середовища на предмет невиправданих випромінювань від компонентів;

- якщо можливо, використання пристроїв, що запобігають моніторингу зовнішнього радіо- або електромагнітного випромінювання;

- візуальний огляд;

- можливе проникнення в компоненти/пристрої рентгенівського або іншого випромінювання;

- перевірка, моніторинг та збір значень характеристик компонентів, які можна відстежувати за допомогою комп'ютерних реєстрів для збору статистики і з їх допомогою виявляти портативні вбудовані пристрої.

Особливу увагу слід приділяти енергетичним характеристикам, записам про роботу і попит, температурі, інтенсивності випромінювання, включаючи звук і світло, попередньо визначеним технічним характеристикам компонентів і частотам компонентів.

3.4 Програмно-апаратні засоби для захисту від несанкціонованого використання інформації

Блокові шифри [6, 7, 10] є різновидом спеціальних шифрів, які призначені для захисту від несанкціонованого використання інформації, Блокові шифри є різновидом симетричних шифрів. Для блокових шифрів характерна обробка блоку з декількох байт за одну ітерацію (зазвичай 8 або 16). Режими роботи блокових шифрів складається з наступних операцій. Робота блокових шифрів у найпростішому режимі, тобто коли функція шифрування застосовується до блоку даних (проста підстановка), викликає серйозні проблеми: статистичні

властивості відкритих даних частково зберігаються. У випадку великих обсягів даних (відео, аудіо) це може надати криптоаналізу інформацію про зміст даних.

Видалення статистичних залежностей відкритого тексту можливе при попередньому архівуванні, але воно не вирішує проблему повністю і може бути технічно неможливим, оскільки у файлі залишається власна інформація програми-архіватора.

Другим ефективним засобом захисту від несанкціонованого використання інформації є циклічне кодування.

Циклічне кодування («категоризація») даних використовується для вирішення вищезгаданих проблем. Суть цього рішення полягає в накладанні статистичних даних у тривимірному просторі та присвоєнні рейтингу кожній групі даних. В результаті цього процесу області з низьким рейтингом усуваються, а кодовані області відокремлюються від «порожніх» комбінацій.

3.4.1 Вибори методу шифрування. Існує багато алгоритмів шифрування. Конкурс Advanced Encryption Standard (AES), проведений Національним інститутом стандартів і технологій США (NIST), обрав найпопулярніші з них. Переможець Rijndael отримав 86 голосів, Serpent - 59, Twofish - 31, RC6 - 23 і MARS - 13. NIST обрав Rijndael як модель; Serpent і Rijndael насправді дуже схожі, з основними відмінностями в тому, що Rijndael швидший, а Serpent безпечніший.

Advanced Encryption Standard (AES), також відомий під назвою Rijndael — Симетричний блоковий алгоритм шифрування (розмір блоку 128 біт, ключ 128/192/256 біт), фіналіст конкурсу AES і прийнятий урядом США як стандарт шифрування США.

В принципі, алгоритм, запропонований Дейцманом і Рейманом, не є тотожним AES. Алгоритм Рендольфа [10] підтримує широкий діапазон розмірів блоків і ключів: AES має фіксовану довжину 128 біт і довжину ключа 128, 192 або 256 біт. Алгоритм Рендольфа підтримує розміри блоків і ключів з кроком 32 біта від 128 до 256. Оскільки розмір блоку фіксований, AES працює з масивами

4 x 4 байти, які називаються станами (у версіях алгоритму з більшими розмірами блоків додаються стовпці). Для 128-бітного ключа алгоритм має 10 раундів, в яких послідовно виконуються наступні операції:

- *subBytes*();
- *shiftRows*();
- *mixcolumns*() (у 10-му раунді пропускається);
- *xorRoundKey*().

Процедура шифрування SubBytes() обробляє кожен байт стану незалежно і виконує нелінійну підстановку байтів, використовуючи таблицю підстановок (S-box). Це гарантовано забезпечує нелінійність алгоритму шифрування: побудова шифрування S-box складається з двох кроків. Спочатку отримується її обернена в оболонці Галуа. Потім над кожним байтом b S-боксу виконується наступна операція:

$$B'_i = b_i \oplus b_{(i+4) \bmod 8} \oplus b_{(i+5) \bmod 8} \oplus b_{(i+6) \bmod 8} \oplus b_{(i+7) \bmod 8} \oplus c_i$$

де $0 \leq i < 8$, і де b_i є i-й біт b, а c_i — i-й біт константи $c = 63_{16} = 99_{10} = 01100011_2$.

Таким чином, забезпечується захист від атак, заснованих на простих алгебраїчних властивостях.

S-box можна відобразити таблицею простої підстановки:

\	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	63	7c	77	7b	f2	6b	6f	c5	30	01	67	2b	fe	d7	ab	76
1	ca	82	c9	7d	fa	59	47	f0	ad	**d4**	a2	af	9c	a4	72	c0
2	b7	fd	93	26	36	3f	f7	cc	34	a5	e5	f1	71	d8	31	15
3	04	c7	23	c3	18	96	05	9a	07	12	80	e2	eb	27	b2	75
4	09	83	2c	1a	1b	6e	5a	a0	52	3b	d6	b3	29	e3	2f	84
5	53	d1	00	ed	20	fc	b1	5b	6a	cb	be	39	4a	4c	58	cf
6	d0	ef	aa	fb	43	4d	33	85	45	f9	02	7f	50	3c	9f	a8
7	51	a3	40	8f	92	9d	38	f5	bc	b6	da	21	10	ff	f3	d2
8	cd	0c	13	ec	5f	97	44	17	c4	a7	7e	3d	64	5d	19	73
9	60	81	4f	dc	22	2a	90	88	46	ee	b8	14	de	5e	0b	db
a	e0	32	3a	0a	49	06	24	5c	c2	d3	ac	62	91	95	e4	79
b	e7	c8	37	6d	8d	d5	4e	a9	6c	56	f4	ea	65	7a	ae	08
c	ba	78	25	2e	1c	a6	b4	c6	e8	dd	74	1f	4b	bd	8b	8a
d	70	3e	b5	66	48	03	f6	0e	61	35	57	b9	86	c1	1d	9e
e	e1	f8	98	11	69	d9	8e	94	9b	1e	87	e9	ce	55	28	df
f	8c	a1	89	0d	bf	e6	42	68	41	99	2d	0f	b0	54	bb	16

Рисунок 3.5 – Матриця подстановки за методом шифрування S-box

Наприклад, на вході 19 на виході отримаємо d4.

Фактично це звичайний шифр простої підстановки.

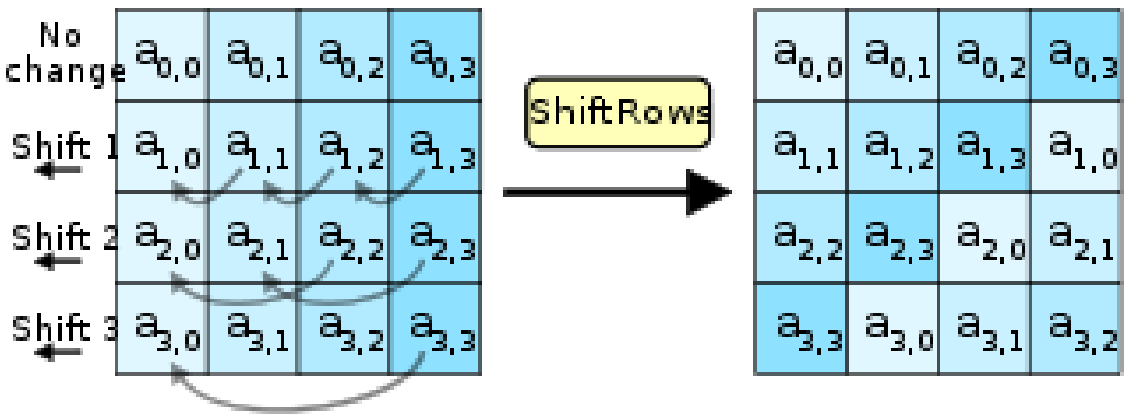

Рисунок 3.6 – Схема подстановки за методом шифрування S-box

ShiftRows зсуває рядки у таблиці Status. При цьому перетворенні рядки таблиці Status циклічно зсуваються по горизонталі на r байт відповідно до номера рядка: Для рядка 0, r = 0, для рядка 1, r = 1 і т.д. Таким чином, кожен рядок вихідного стану після застосування процедури ShiftRows складається з байт з кожного рядка початкового стану; в алгоритмі Rijndael схема зсуву рядків для 128-бітових і 192-бітових рядків однакова. Однак різниця полягає в тому, що для 256-бітових блоків другий, третій і четвертий рядки зсуваються на один, три і чотири байти відповідно.

Фактично це проста перестановка байтів таблиці 4x4 State.

Метод MixColumns

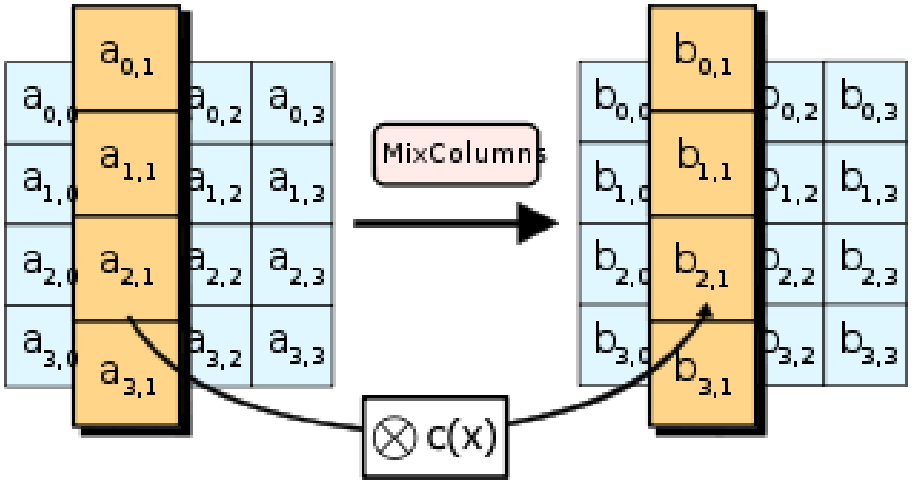

Рисунок 3.7 – Схема подстановки за методом шифрування MixColumns

У процедурі **MixColumns** чотири байти кожного стовпчика стану змішуються за допомогою оберненого лінійного перетворення; **MixColumns** обробляє стан стовпчик за стовпчиком і розглядає кожен стовпчик як поліном четвертого порядку. Разом з **ShiftRows**, **MixColumns** вносить дифузію в шифр.

Під час цієї операції, кожен стовпчик множиться на матрицю, яка для 128-бітного ключа має вигляд:

$$\begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix}$$

Метод AddRoundKey

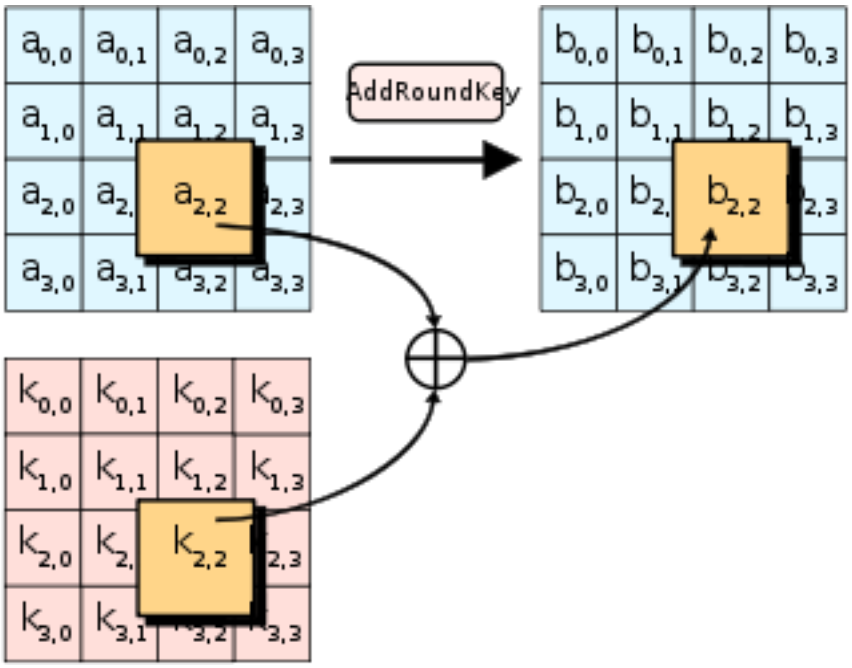

Рисунок 3.8 – Схема подстановки за методом шифрування AddRoundKey

У процедурі AddRoundKey, RoundKey для кожного раунду поєднується зі статусом. RoundKey для кожного раунду отримується з CipherKey за допомогою процедури KeyExpansion.

Ця процедура виконує побітове XOR кожного байта статусу і кожного байта ключа раунду. На практиці це просте побайтове XOR байтів ключа і байтів таблиці стану.

Висновки до розділу 3.

У цьому розділі описано методи виявлення вбудованих пристроїв у комп'ютерній техніці та вжиття заходів проти них. Запропоновано рішення для підвищення точності виявлення вбудованих пристроїв у комп'ютерному обладнанні, такому як системні блоки, периферійні пристрої та обладнання, призначене для цифрової передачі інформації.

Представлено рішення проблеми виявлення апаратних засобів всередині комп'ютерних компонентів. Воно полягає у використанні таких інструментів, як візуальний огляд, реалізація механізмів запобігання зовнішньому радіо- та електромагнітному моніторингу, а також контроль доступу до обладнання за допомогою методів фізичного захисту. Обмеженням запропонованого рішення є те, що малі розміри знижують точність виявлення пристроїв.

ВИСНОВКИ

У даній кваліфікаційній роботі запропоновано метод підвищення захищеності комп'ютерної техніки від перехоплення конфіденційної інформації. Для досягнення поставленої мети були вирішені наступні завдання.

1. За результатами порівняльного аналізу через побудову та проектування захисних пристроїв визначено наступне:

- структура вбудованих пристроїв залежить від їх призначення та характеристик. Розуміння принципів їх побудови є важливим кроком на шляху до ефективного виявлення та захисту. Це допомагає розпізнати характеристики вбудованих пристроїв, такі як приховане розташування, механізми перехоплення даних та канали зв'язку для передачі інформації;

- огляд принципів побудови вбудованих пристроїв підкреслює необхідність постійного вдосконалення технічних засобів захисту інформації. З розвитком технологій та появою нових методів атак заходи безпеки необхідно постійно оновлювати та адаптувати для протидії сучасним загрозам;

2. На основі результатів оцінки описано, як виявляти вбудовані пристрої, що перехоплюють дані.

З метою підвищення точності виявлення вбудованих пристроїв запропоновано рішення, що базується на особливостях пошуку фізичних об'єктів та електронних пристроїв у комп’ютерних системах та дослідженні поведінки користувачів персональних комп'ютерів з метою виявлення підозрілих дій.

Однією з переваг запропонованого рішення є те, що воно може виявляти вбудовані пристрої на ранніх стадіях використання персонального комп'ютера, що допомагає запобігти потенційним загрозам витоку конфіденційної інформації. Однак слід зазначити, що одним з обмежень запропонованого рішення є низька точність виявлення невеликих вбудованих пристроїв.

3. Запропоновано рекомендації щодо боротьби з поведінкою вбудованих пристроїв у комп'ютерному обладнанні:

- візуальний контроль, зовнішній радіо- та електромагнітний моніторинг, впровадження профілактичних заходів та контроль доступу до обладнання методами фізичного захисту.

Однак обмеженням запропонованих рішень є те, що малі розміри вбудованих пристроїв знижують точність виявлення. Отримані дані можуть бути використані на практиці для статистичного виявлення загроз від вбудованих пристроїв та детального вивчення поведінки зловмисників на основі режимів роботи комп'ютера та класифікації компонентів.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Методи та засоби технічного захисту інформації. [Електронний ресурс] : навч. посіб. для здобувачів ступеня бакалавра за освітньою програмою «Системи технічного захисту інформації» спеціальності 125 «Кібербезпека» / КПІ ім. Ігоря Сікорського; уклад.: В.М. Луценко, Д.О. Прогонов. – Київ : КПІ ім. Ігоря Сікорського, 2021. – 289 с.

2. Захист інформації в комп'ютерних системах та мережах /Семенов С.Г. / [Електронний ресурс] Режим доступу: http://www.dgma.donetsk.ua/docs/kafedry/avp/metod/_БКМ_Пос_бник.pdf.

3. Офіційна статистика в системі національної інформаційної безпеки /Осауленко О. Г/.: монографія. Київ: ТОВ «Август Трейд», 2017. 367 с.

4. НД ТЗІ 2.7–011-2012«Захист інформації на об’єктах інформаційної діяльності. Методичні вказівки з розробки Методики виявлення закладних пристроїв» [Електронний ресурс] Режим доступу: https://tzi.com.ua/downloads/2.7-011-2012.pdf.

5. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу» [Електронний ресурс] Режим доступу: https://tzi.ua/assets/files/%D0%9D%D0%94-%D0%A2%D0%97%D0%86-2.5-004-99.pdf.

6. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп’ютерних системах від несанкціонованого доступу» [Електронний ресурс] Режим доступу: https://tzi.ua/assets/files/1.1_003_99.pdf.

7. Виявлення та блокування засобів негласного отримання інформації на об'єктах інформаційної діяльності/Навчальний посібник [Електронний ресурс] Режим доступу: https://dut.edu.ua/uploads/l_2031_50136601.pdf.

8. Спеціальні технічні засоби негласного збору інформації/Стаття [Електронний ресурс] Режим доступу: http://irbis-nbuv.gov.ua/cgibin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&I

MAGE_FILE_DOWNLOAD=1&Image_file_name=PDF/Npchduct_2013_229_217_10.pdf.

9. Ідентифікаційні ознаки спектрального складу випромінювання демаскуючого розсіювача в нелінійній радіолокації : дис. канд. техн. наук : 172 / .– НТУУ «КПІ», 2017. – 144 с.

10. HaTCh: A Formal Framework of Hardware Trojan Design and Detection /K. H.Syed, J. Chenglu, A. Masab, M. S. Devu / [Електронний ресурс] United Technologies Research Cente. – 2015. – Режим доступу до ресурсу: https://www.researchgate.net/profile/Masab-Ahmad/publication/335389265_HaTCh_A_Formal_Framework_of_Hardware_Trojan_Design_and_Detection/links/5d62067792851c619d745481/HaTCh-A-Formal-Framework-of-Hardware-Trojan-Design-and-etection.pdf?origin=publication_detail.

11. Телекомунікаційні системи та мережі. Структура й основні функції.Том 1 / [В. В. Поповський, О. В. Лемешко, В. К. Ковальчук та ін.]., 2018. – (ТОВ Компанія СМІТ). – (Видання; т. 2)./ [Електронний ресурс] Режим доступу: https://www.znanius.com/3853.html.