Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня магістра

студента *Кузьмінової Марії Сергіївни*

академічної групи *125м-19-1*

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему *Методика захисту інформації з обмеженим доступом від несанкціонованих дій при використанні зовнішніх flash-носіїв*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	професор Корнієнко В.І.			
розділів:				
спеціальний	ст.викладач Кручінін О.В.			
економічний	к.е.н, доцент Пілова Д.П.			

Рецензент				

Нормоконтролер	ст.викладач Тимофєєв Д.С.			

Дніпро
2020

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту ***Кузьміновій М.С.*** **академічної групи** ***125м-19-1***
(прізвище та ініціали) (шифр)

спеціальності ***125 Кібербезпека***

спеціалізації

за освітньо-професійною програмою ***Кібербезпека***

на тему ***Методика захисту інформації з обмеженим доступом від несанкціонованих дій при використанні зовнішніх flash-носіїв***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 22.10.2020 № 888-с

Розділ	**Зміст**	**Термін виконання**
Стан питання. Постановка задачі	Дослідження загроз та вразливостей інформаційної безпеки при порушенні політики використання flash-носіїв	03.09.2020 – 21.09.2020
Спеціальна частина	Розробка методики захисту інформації	22.09.2020 – 19.11.2020
Економічна частина	Розрахунок економічної складової	20.09.2020 – 03.12.2020

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)
Дата видачі завдання: 01.09.2020
Дата подання до екзаменаційної комісії: 10.12.2020
Прийнято до виконання _____ Кузьмінова М.С.
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 121 с., 18 рис., 3 табл., 8 додатків, 27 джерел

Об'єкт досліджень: захист інформації з обмеженим доступом від несанкціонованих дій внутрішніх порушників при використанні зовнішніх flash-носіїв.

Предмет досліджень: розроблення методики захисту інформації від несанкціонованих дій при використанні зовнішніх flash-носіїв.

Мета дипломної роботи: покращення захисту інформації від несанкціонованих дій при використанні зовнішніх знімних flash-носіїв в автоматизованих системах.

В першому розділі проаналізовані інциденти витоку даних за останні декілька років при використанні зовнішніх носіїв інформації, розглянуті сучасні зовнішні flash-носії та визначені загрози інформаційної безпеки, пов'язані з несанкціонованими діями при використанні носіїв інформації.

В другій частині дипломної роботи розроблена методика захисту інформації за рахунок посиленої ідентифікації зовнішніх носіїв та розроблено додатковій пристрій для flash-носіїв, який забезпечує підсилений контроль використання зареєстрованого flash-носія в АС.

В економічній частині проведений розрахунок капітальних витрат на розробку методики захисту інформації за рахунок застосування додаткового пристрою flash-носіїв, а також обґрунтована економічна ефективність цієї методики.

Ключові слова: МЕТОДИКА ЗАХИСТУ ІНФОРМАЦІЇ, ВНУТРІШНІ ПОРУШЕННЯ, НЕСАНКЦІОНОВАНІ ДІЇ, ІДЕНТИФІКАЦІЯ ЗОВНІШНІХ FLASH-НОСІЇВ, ПРИСТРІЙ НА МІКРОКОНТРОЛЕРІ

THE ABSTRACT

Explanatory note: 121 pp., 18 fig., 3 tab., 8 appendices, 27 sources

Object of research: protection of information with limited access from unauthorized actions of internal violators when using external flash media.

Subject of research: development of methods for protecting information from unauthorized actions when using external flash media.

The purpose of the thesis: improving the protection of information from unauthorized actions when using external removable flash media in automated systems.

The first section analyzes data leakage incidents over the past few years using external storage media, examines current external flash drives, and identifies information security threats associated with unauthorized use of storage media.

In the second part of the thesis a method of information protection due to enhanced identification of external media is developed and an additional device for flash media is developed, which provides unambiguous use of the reserved flash media.

In the economic part, the calculation of capital costs for the development of a method for protecting information through the use of an additional flash-media device was made, and the economic efficiency of this method was substantiated.

Key words: INFORMATION PROTECTION METHODOLOGY, INTERNAL VIOLATIONS, UNAUTHORIZED ACTIONS, IDENTIFICATION OF EXTERNAL FLASH-MEDIA, MICRO DEVICES

РЕФЕРАТ

Пояснительная записка: 121 с., 18 рис., 3 табл., 8 приложений, 27 источников

Объект исследования: защита информации с ограниченным доступом от несанкционированных действий внутренних нарушителей при использовании внешних flash-носителей.

Предмет исследования: разработка методики защиты информации от несанкционированных действий при использовании внешних flash-носителей.

Цель дипломной работы: улучшение защиты информации от несанкционированных действий при использовании внешних съемных flash-носителей в автоматизированных системах.

В первом разделе проанализированы инциденты утечки данных за последние несколько лет при использовании внешних носителей информации, рассмотрены современные внешние flash-носители и определенные угрозы информационной безопасности, связанные с несанкционированными действиями при использовании носителей информации.

Во второй части дипломной работы разработана методика защиты информации за счет усиленной идентификации внешних носителей и разработан дополнительной устройство для flash-носителей, который обеспечивает усиленный контроль использования зарегистрированного flash-носителя в АС.

В экономической части произведен расчет капитальных затрат на разработку методики защиты информации за счёт применения дополнительного устройства для flash-носителей, а также обоснована экономическая эффективность этой методики.

Ключевые слова: МЕТОДИКА ЗАЩИТЫ ИНФОРМАЦИИ, ВНУТРЕННИЕ НАРУШЕНИЯ, НЕСАНКЦИОНИРОВАННЫЕ ДЕЙСТВИЯ, ИДЕНТИФИКАЦИЯ ВНЕШНИХ FLASH-НОСИТЕЛЕЙ, УСТРОЙСТВО НА МИКРОКОНТРОЛЛЕРЕ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

АС – автоматизована система;

ГБ – гігабайт;

ЕОМ – електронно-обчислювальна машина;

ІзОД – інформація з обмеженим доступом;

КЕП - кваліфікований електронний підпис;

ЕЦП - електронний цифровий підпис;

КЗЗ – комплекс засобів захисту;

ЛОМ – локальна обчислювальна мережа;

МБ – мегабайт;

НД ТЗІ – нормативний документ з технічного захисту інформації;

ОЗП – оперативний запам'ятовуючий пристрій;

ОС – операційна система;

ПЗ – програмне забезпечення;

ПЗП – постійний запам'ятовуючий пристрій;

ПЕОМ – персональна електронно-обчислювальна машина;

ПК - персональний комп'ютер;

ППКЗН – пристрій посиленого контролю зовнішніх носіїв;

ППС - прикладна програмна система;

РСО – режимно-секретні органи;

ТБ – терабайт;

ТЗ – технічне завдання;

У/В – увід/вивід;

BIOS - basic input/output system;

DLP - Data Leak Prevention;

MDM - Mobile Device Management;

PnP - Plug and Play;

USB - Universal Serial Bus.

ЗМІСТ

ВСТУП

У сучасному суспільстві у зв'язку з дедалі більшими потребами людини виникають проблеми інформаційного забезпечення усіх сфер її діяльності, тобто надання всієї необхідної інформації. За своєю значимістю та актуальністю проблема інформатизації є найважливішою для сучасного суспільства. Однак вона породжує цілий ряд серйозних супутніх проблем, без вирішення яких немає ефективної інформатизації.

Однією з таких супутніх проблем є надійний захист інформації, що циркулює в системах обробки інформації, який забезпечував би попередження знищення інформації, а також унеможливлював би її зловмисне отримання, використання або несанкціоновану модифікацію. Особливої гостроти ця проблема набуває у зв'язку з повсюдною та масовою комп'ютеризацією інформаційних процесів, і насамперед у зв'язку з об'єднанням комп'ютерів в інформаційно-обчислювальні мережі, що забезпечує масовий доступ будь-яких користувачів до їх ресурсів.

Несанкціонований доступ до конфіденційної інформації - основна загроза інформаційній безпеці. Для захисту інформації, що обробляється на робочих станціях, від несанкціонованого доступу повинен застосовуватися цілий комплекс заходів: забезпечення надійної автентифікації, реалізація правил розмежування доступу, контроль витоків інформації на знімні носії і по мережі і багато інших.

Знімні носії увійшли в життя сучасного суспільства і зараз є дуже зручним і ефективним засобом зберігання інформації, архівації та виконання операцій імпорту/експорту. Сьогодні можна з упевненістю стверджувати, що найважливішим активом будь-якої сучасної компанії є інформація. Як і всякий критично важливий актив, інформація потребує захисту, а в разі її витоку компанія несе досить серйозні збитки. Активне забезпечення інформаційної безпеки даних є однією з ключових завдань у області захисту інформації.

USB-флеш-накопичувач - один з типів носіїв на флеш-пам'яті, що з'явився на ринку в 2001 р За формою USB-флеш-накопичувач нагадує брелок довгастої форми. Працювати з пристроєм дуже зручно - для цього не потрібно ніяких додаткових пристроїв. Тому даний винахід впевнене увійшло в життя сучасної людини, і зараз користується попитом. Але при появі нового способу зберігання інформації, з'являються і нові канали витоку інформації. І якщо фахівці з інформаційної безпеки в достатній мірі освоїли і застосовують інструменти захисту від зовнішніх порушників, то з внутрішніми справа йде не так гладко.

Розроблена методика протидії несанкціонованим діям при використанні зовнішніх flash-носіїв характеризується, як спосіб додаткового захисту інформації при використанні знімних носіїв.

1 СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз інцидентів витоку інформації

За перші 9 місяців 2020 року в базу Експертно-аналітичного центру InfoWatch внесено 1773 випадки витоку інформації обмеженого доступу з комерційних компаній, державних організацій і органів влади у всьому світі.

В результаті зареєстрованих випадків «витікло» 9,93 млрд записів персональних даних і платежів. У порівнянні з аналогічним періодом 2019 року в цілому (в світі) число витоків знизилося на 7,4%, а число скомпрометованих записів – на 1,4%.

Зниження числа зареєстрованих (стали відомими) витоків в світі головним чином можна пояснити впливом пандемії коронавируса на бізнес і держсектор: внаслідок нагальної перебудови процесів і переведення значної частки співробітників на віддалену роботу контроль над інформаційними активами у багатьох компаніях міг бути ослаблений, а значна частина інцидентів перестала фіксуватися.

17 липня 2020 року експертно-аналітичний центр InfoWatch опублікував результати щорічного дослідження з витоків конфіденційної інформації в світі. За 2019 рік зафіксовано 2509 витоків даних з розташованих по всьому світу комерційних і державних організацій, а також органів влади. У порівнянні з 2018 роком число витоків зросло на 10,8%.

Персональні дані і платіжна інформація в сумі склали 86% витоків. Всього було скомпрометовано 14,8 млрд записів, це більш ніж удвічі перевищило число витікших записів персональних даних і платежів в 2018 році.

Автори дослідження констатують, що в 2019 році зареєстрований цілий ряд витоків, що торкнулися повної популяції або як мінімум більшість жителів окремих країн. Подібні «витоки національного масштабу» зафіксовані в Еквадорі (20,8 млн записів), в Канаді (15 млн записів), в Чилі (понад 14 млн записів), в Болгарії (5 млн записів). У 2020 році виявлено випадки компрометації величезних

державних баз даних. Зокрема, з'явилася інформація про витік персональних даних всіх громадян Грузії, а також особистої інформації громадян Ізраїлю, які мають право голосу.

Спровоковані внутрішніми порушниками витоки привели до втрати 9,8 млрд записів, що складають 67,6% загального масиву інформації, конфіденційність якої було порушено. Відповідно в результаті дій зовнішніх порушників витекло близько 4,7 млрд записів або 32,4% всього обсягу скомпрометованих записів (Рис.1.1).

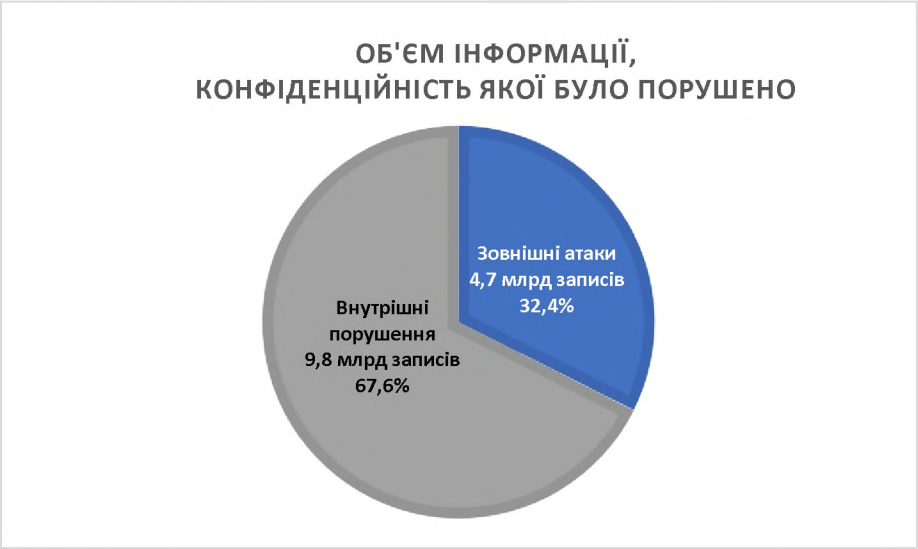


Рисунок 1.1 - Об’єм інформації, конфіденційність якої було порушено за 2019 рік

У 41% витоків винуватцями виявлялися діючі співробітники, в 2% - керівництво компаній. Ще 4,6% припало на підрядників, 2,1% інцидентів були ініційовані колишніми співробітниками, а 0,3% системними адміністраторами. Майже половина витоків - 49,7% - відбулися в результаті хакерських атак і інших дій ззовні (Рис.1.2). У порівнянні з 2018 роком, відзначено вибухове зростання хакерської активності. В результаті число виявлених випадків витоків з вини зовнішніх зловмисників зросла більш ніж на 45%.

Найбільш привабливими галузями для внутрішніх порушників автори дослідження виділяють банки і фінансовий сектор, держоргани і силові

структури, що пояснюється високою ліквідністю даних, які обробляються в зазначених вертикалях.

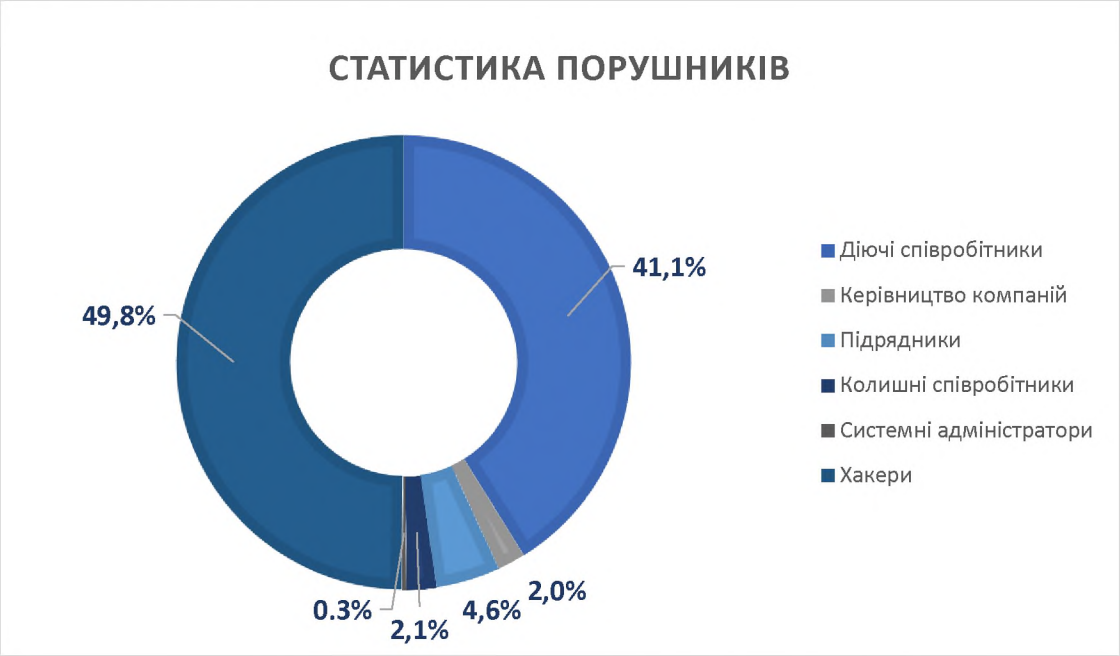


Рисунок 1.2 - Статистика порушників

Автори дослідження прийшли до висновку, що в 2019 році майже на третину побільшало порушень, спровокованих умисними діями персоналу з метою отримання вигоди від використання довірених співробітникам масивів персональних даних клієнтів, відомостей категорії «комерційна таємниця» та інших інформаційних активів. Також викликає тривогу лавиноподібне зростання числа витоків з неправильно сконфігурованих хмарних сховищ. Певною мірою через це число записів персональних даних і платіжної інформації, що витекли в результаті дій внутрішніх порушників, вдвічі перевищило число записів, вкрадених зовнішніми зловмисниками.

З розвитком інформаційних систем загрози, які виходять від співробітників організацій (інсайдерів), давно стали дуже серйозними, а збиток від їх дій обчислюється десятками мільярдів доларів. Постійно зростає потік повідомлень про інциденти, пов'язані з порушенням своїх зобов'язань і прав авторизованими користувачами, які навмисно саботують свою компанію і передають інформацію

конкурентам. Одночасно змінюється і бізнес-середовище, яке все більше покладається на аутсорсинг, підрядні компанії і сторонні технологічні платформи, що призводить до того, що цінний бізнес-інформація стає доступною все більшій кількості людей [1].

У США на замовлення компанії SanDisk було проведено спеціальне дослідження на тему ризиків, пов'язаних з використанням незахищених USB-накопичувачів. Його результати вражають: виявляється, більшість компаній щонайменше вдвічі недооцінюють ризики використання працівниками незахищених флешок.

Компактність, простота у використанні і мобільність - ось головні переваги USB-накопичувачів. Але саме вони і створюють дуже високий ризик втрати даних. Результати анонімних опитувань, проведених на замовлення SanDisk, показали, що найчастіше користувачі копіюють на особисті флешки конфіденційні дані про замовників (25%), інформацію фінансового характеру (17%), бізнес-плани (15%), інформацію про співробітників своєї компанії (13%), маркетингові плани (13%), об'єкти інтелектуальної власності (6%), а також вихідні коди програмного забезпечення (ПЗ) (6%) (Рис.1.3).

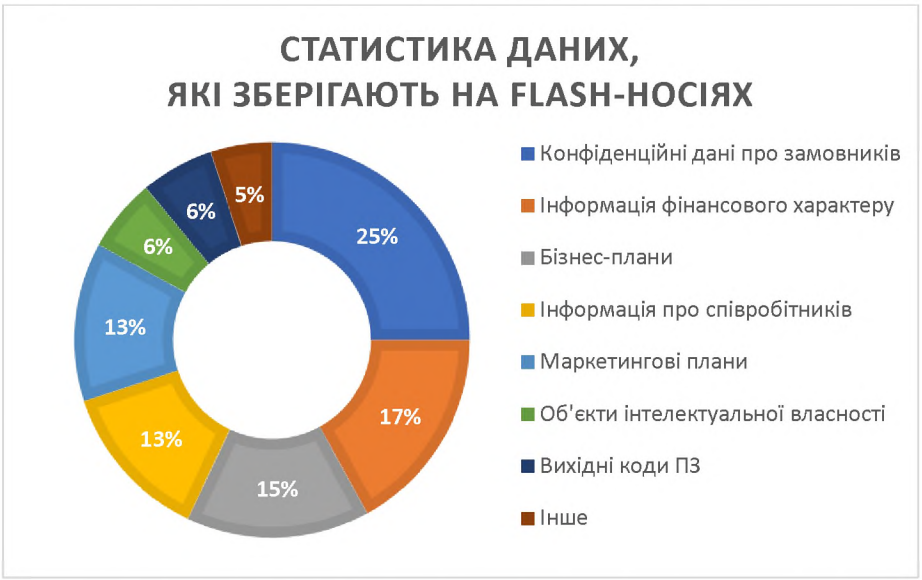


Рисунок 1.3 - Статистика даних, які зберігають на flash-носіях

При цьому керівники IT-підрозділів і внутрішніх служб безпеки в більшості випадків навіть не мають уявлення про реальні масштаби поширення незахищених флеш-накопичувачів в своїх організаціях.

Статистична інформація про те, що 77% співробітників використовують особисті флеш накопичувачі для зберігання і перенесення службових даних, стала справжнім шоком для більшості фахівців з інформаційної безпеки. До цього найсміливіші з опитаних IT-фахівців оцінювали частку співробітників, що використовують особисті флешки в службових цілях, не більше ніж в 35% [2].

Отже, витік інформації через використання USB-flash носіїв внутрішніми робітниками організацій залишається актуальною проблемою на сьогоднішній день.

1.2 Сфери використання зовнішніх знімних носіїв інформації

З розвитком технологій збереження даних в паперовому вигляді поступово відійшло на задній план і стали використовувати дані в електронному вигляді. Цей вид інформації спростив обмін даними між користувачами, а саме: інформацію або дані в електронному вигляді було простіше передати або переслати на далекі відстані.

Комп'ютерна техніка теж не стояла на місці і зробила великий прорив у розвитку. Тепер для зберігання і транспортування інформації потрібні портативні пристрої на які можна записувати, а потім зчитувати інформацію. Тому в 2000 році стали популярні портативні прилади, такі як знімні носії [3].

До знімних носіїв даних можна віднести будь-який пристрій, призначене для перенесення інформації від одного обчислювального пристрою до іншого. Найбільш поширені такі знімні носії [4]:

- дискети (вже рідко застосовуються);
- оптичні диски;
- пристрою флеш-пам'яті;

- флеш карти;
- знімні вінчестери.

Останнім часом широку популярність набули носії інформації на основі мікросхем флеш-пам’яті. За популярністю в наш час їм немає рівних: карти пам’яті в фотоапаратах, стільникових телефонах, плеєрах, USB флеш брелоки, а з недавнього часу ще й SSD диски.

І така популярність не випадкова: по практичності «флешкам» теж немає рівних. Великий, постійно зростаючий об’єм, який обчислюється вже гігабайтами і десятками гігабайт, досить високу швидкодію, а також заявлена надійність і довговічність.

Flash-пам’ять отримала свою назву завдяки тому, як проводиться записування та стирання даного виду пам’яті [5].

USB-флеш-накопичувач, флешка — носій інформації, що використовує флеш-пам'ять для збереження даних та підключається до комп'ютера чи іншого пристрою через USB-порт.

USB-флеш-накопичувачі зазвичай підтримують перезаписування. Розмір - близько 5 см, вага - менше, ніж 60 г. Надзвичайну популярність здобули у 2000-ні у зв'язку з тим, що вони дуже компактні, легкі і мають великий об'єм пам'яті.

Основне призначення — зберігання й перенесення файлів та обмін ними, резервне копіювання, завантаження операційних систем (ОС) тощо [6].

Прогрес у розвитку просунувся дуже далеко і зробив флешки незамінним помічником людини. Адже кожен з нас має вдома комп'ютер, і в кожного з нас рано чи пізно виникає потреба перенести інформацію або скопіювати файл і передати одному, і зараз це дуже зручно зробити, адже всього лише потрібно мати флешки. Більшість обладнання має порт USB, який може зчитувати інформацію з флешки [3].

Найбільш поширене використання флешок є перенесення і зберігання будь-яких файлів. Часто флешки використовують для відновлення BIOS або UEFI материнських плат.

Більшість сучасних персональних комп'ютерів (ПК) підтримують не тільки установку ОС з використанням завантажувальної флешки, але можливість завантаження з USB-пристрою, що дозволяє операційній системі завантажитися з флешки. Така конфігурація часто серед користувачів називається Live USB. Ця особливість допоможе не тільки в клонування ОС і надалі її перенесення на аналогічний комп'ютер, виконати маніпуляції з файлами не завантажуючи основну ОС і зробити боротьбу з шкідливим ПЗ.

USB-накопичувальний пристрій підтримує шифрування, що дуже важливо для безпечного зберігання інформації і не втрачає актуальності і при резервному копіюванні. Флеш накопичувачі можуть використовуватися як ключ для активації (USB Keys) додатків [7].

Крім того, що флешки використовують для зберігання и перенесення данних, їх застосовують як токен, який призначений для забезпечення інформаційної безпеки користувача, віддаленого доступу до інформації та використовується для ідентифікації його власника.

Токен – це захищений носій ключової інформації, який являє собою пристрій, призначений для безпечного зберігання ключів КЕП (ЕЦП), оскільки на ньому зберігається інформація про електронний підпис.

Головною задачею токену є безпечне зберігання інформації та ідентифікація користувача. Тобто, токен є захищеним носієм ключової інформації. Найпоширеніший тип захищених носіїв в Україні - токени у вигляді USB-флешки [8].

Отже, найпопулярнішим зовнішнім знімним носієм інформації є USB-флеш-накопичувач - сучасний пристрій зберігання, перенесення, шифрування,

резервного копіювання та ще більшого функціоналу. Все це полегшує життя людини у сучасному світі.

1.3 Використання знімних носіїв інформації в автоматизованних системах

Автоматизована система (АС) являє собою організаційно-технічну систему, що об'єднує ОС, фізичне середовище, персонал і оброблювану інформацію. Вимоги до функціонального складу КЗЗ залежать від характеристик оброблюваної інформації, самої ОС, фізичного середовища, персоналу і організаційної підсистеми.

Згідно з НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» за сукупністю характеристик АС виділено три ієрархічні класи АС (Рис.1.4), вимоги до функціонального складу комплекс засобів захисту (КЗЗ) яких істотно відрізняються.

Рисунок 1.4 – Класи автоматизованих систем

Виходячи з даних трьох ієрархічних класів АС можна визначити з якою метою використовуються знімні носії в кожному классі АС.

Клас «1» — одномашинний однокористувачевий комплекс, який оброблює інформацію однієї або кількох категорій конфіденційності.

Істотні особливості:

- в кожний момент часу з комплексом може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка оброблюється;

- технічні засоби (носії інформації і засоби У/В) з точки зору захищеності відносяться до однієї категорії і всі можуть використовуватись для збереження і/або У/В всієї інформації.

Приклад — автономна персональна електронно-обчислювальна машина (ЕОМ), доступ до якої контролюється з використанням організаційних заходів [9].

Автономні робочі станції (один або декілька ПК, не зв'язаних між собою. На будь-якому з них користувачі працюють роздільно в часі. Обмін інформацією відбувається тільки через змінні носії).

Об'єкти захисту в автономних робочих станціях [10]:

- власне робоча станція;

- змінні носії інформації;

- користувачі і робочий персонал;

- пристрої візуального представлення інформації (монітор, принтер тощо);

- прилади-джерела побічних електромагнітних випромінювань і наведень.

В таких системах знімні носії використовуються для імпорту та експорту даних, оскільки в таких системах не має ніяких зовнішніх підключень для обміну інформацією. В захищених системах класу «1» використовують двухфакторну автентифікацію користувачів на підставі пароля і носія даних автентифікації. Також зовнішні носії застосовують для зберігання резервних копій даниих.

Клас «2» — локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу — наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності [9].

Приклад — локальна обчислювальна мережа (ЛОМ).

Локальні системи колективного користування (створюються для колективної обробки інформації і (або) сумісного використання ресурсів; устаткування розміщене в межах одного приміщення, будівлі або групи близько розташованих будівель).

Структури локальних систем колективного користування [10]:

1. Без виділеного сервера (однорангові мережі) (не вимагають централізованого управління; будь-який користувач сам робить свої ресурси доступними іншим; використовується однотипна операційна система).

2. З виділеним сервером/серверами (побудовані на робочих станціях і серверах; вимагають централізованого адміністративного управління).

3. Багато термінальні системи на базі малих і великих комп'ютерів (основні ресурси зосереджені на сервері. Робочі станції – термінали. Загальне керівництво здійснює адміністратор. На центральному комп'ютері і робочих станціях використовуються різні ОС).

4. Багатосегментні локальні мережі (складаються з декількох сегментів, будь-який з яких є мережею з виділеним сервером. Об'єднання здійснюється через міст, в якості якого може використовуватися або виділений сервер, або спеціальний пристрій. Будь-яким сегментом управляє свій адміністратор. У будь-якому сегменті може використовуватися своя ОС).

5. Змішані мережі (включають всі раніше розглянуті системи).

Об'єкти захисту:

- всі робочі станції;

- виділені сервери і центральний комп'ютер;

- локальні канали зв'язку;

- реквізити доступу.

В АС класу «2» зовнішні знімні носії використовуются для імпорту та експорту данних, для встановлення программного забезпечення, для зберігання резервних копій. Оскільки така система є багатокористувачевою, актуальним є питання автентифікації користувачів в системі. Зовнішні носії використовуються для двухфакторної ідентифікації як ключ, яким володіє користувач.

Клас «3» — розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності.

Істотна відміна від попереднього класу — необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки [9].

Приклад - глобальна мережа.

Глобальні системи колективного користування (розміщені на значній відстані один від одного; об'єднані через глобальні канали зв'язку, які не належать власнику).

Використовуються для сумісної обробки інформації і сумісного використання ресурсів.

Відмінності від локальних систем:

- можуть знаходитися на значній відстані одна від одної;

- канали зв'язку не належать власнику системи;

- канали зв'язку є комутованими і взаємозв'язаними;

- для використання каналів зв'язку необхідний пристрій сполучення;

- подібні системи відкриті і підключитися до ним можуть всі охочі.

Об'єкти захисту включають в себе все те ж, що й в локальних системах колективного користування, а також [10]:

1. глобальні канали зв'язку;

2. інформація, що передається по глобальних каналах зв'язку;

3. інформація про реквізити доступу в глобальні системи колективного користування.

В АС класу «3» знімні носії використовуються переважно для автентифікації користувачів в системі, оскільки в таких системах є вихід в Інтернет для обміну даними. Також можна зберігати резервні копії на хмарних сервісах.

Проаналізувавши цілі використання зовнішніх носіїв інформації в АС трьох класів можна зробити висновок, що застосування зовнішніх носіїв є актуальним в системах класу «1» та «2», оскільки немає зв'язку із зовнішньою мережею, а, отже, немає можливості переміщувати та зберігати якусь інформацію без застосування зовнішнього накопичувача.

1.4 Класифікація зовнішніх носіїв інформації

З розвитком технологій запам'ятовуючі пристрої зазнали значних змін. На сьогоднішній день існують запам'ятовуючі пристрої різних форм і розмірів, а також є типи запам'ятовуючих пристроїв, які можуть використовуватися з різними пристроями і виконувати різні функції.

Пристрої, що запам'ятовують також називають носіями даних. Розмір цифрових пристроїв вимірюється в мегабайтах (МБ), гігабайти (ГБ), а на сьогодні - вже і в терабайт (ТБ).

Деякі пристрої, що запам'ятовують для комп'ютерів забезпечують постійне зберігання інформації, а інші призначені тільки для тимчасового зберігання. Кожен комп'ютер має первинний і вторинний пристрій. Первинний працює як короткочасний пристрій, а вторинний - як довгострокове.

До первинних запам'ятовуючих пристроїв належить оперативний запам'ятовуючий пристрій (ОЗП). ОЗП забезпечує виконання повсякденних завдань, таких як відкриття додатків, завантаження веб-сторінок, редагування

документів або функціонування ігор, а також дозволяє швидко перемикатися між завданнями без втрати тієї частини роботи, яка вже була виконана.

ОЗП - енергозалежна пам'ять, що означає, що вона не забезпечує зберігання інформації після виключення системи. ОЗП дозволяє комп'ютеру отримувати доступ до даних в довільному порядку, забезпечуючи їх більш швидке зчитування і запис, на відміну від вторинного пристрою, що запам'ятовує.

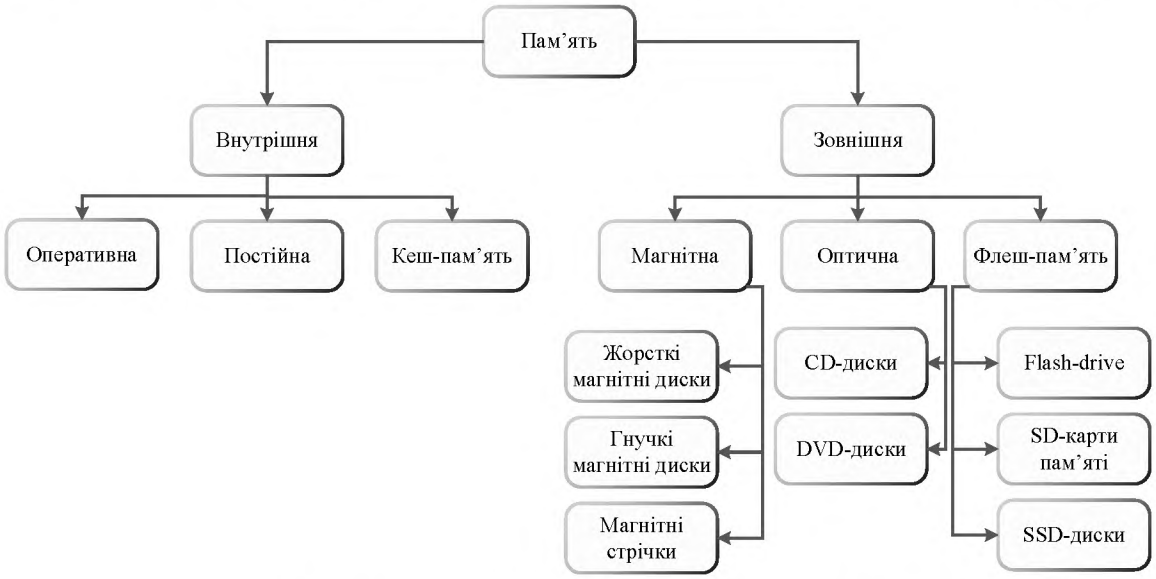


Рисунок 1.5 - Класифікація носіїв інформації

Крім ОЗП на кожному комп'ютері також є інший накопичувач інформації, який використовується для довгострокового зберігання - вторинне пристрій. Будь-який файл, який створюється або завантажується на комп'ютер, зберігається на його вторинний пристрій. Вторинні запам’ятовуючі пристрої часто є знімними, тому їх можна замінювати або модернізувати, а також переміщати знімні накопичувачі на інші комп'ютери.

У комп'ютерах в якості вторинних використовуються два типи запам'ятовуючих пристроїв:

- жорсткі диски (HDD);
- твердотільні накопичувачі (SSD).

HDD - це оригінальні жорсткі диски. Це магнітні запам'ятовуючі пристрої, які існують з 1950-х років, хоча з часом вони сильно еволюціонували.

Твердотільні накопичувачі з'явилися набагато пізніше, в 90-х роках. У них немає ніяких магнітів і дисків, замість цього використовується флеш-пам'ять типу NAND. У твердотільних накопичувачах використовуються напівпровідники, які зберігають інформацію, змінюючи електричний струм ланцюгів, що містяться в накопичувачі. Це означає, що, на відміну від жорстких дисків, твердотільні накопичувачі не мають рухомих частин.

Тому твердотільні накопичувачі не тільки працюють швидше і плавніше, ніж жорсткі диски (жорстких дисків потрібно більше часу для збору інформації через механічну природи їх пластин і головок), а й, як правило, служать довше (через велику кількість складних рухомих частин жорсткі диски більше схильні до пошкоджень і зносу).

Крім носіїв інформації, розміщених в комп'ютері, існують також зовнішні цифрові пристрої, що запам'ятовують. Вони зазвичай використовуються з метою збільшення обсягу місця для зберігання, коли на комп'ютері мало місця, а також щоб забезпечити більшу мобільність і полегшити передачу файлів з одного пристрою на інший. Вони є енергонезалежні та можуть використовувати різні фізичні принципи зберігання інформації – магнітний, оптичний, електронний.

В якості зовнішніх накопичувачів можна використовувати як жорсткі диски, так і твердотільні накопичувачі. Як правило, серед зовнішніх запам'ятовуючих пристроїв вони забезпечують найбільший обсяг місця: зовнішні жорсткі диски - до 20 ТБ пам'яті, а зовнішні твердотільні накопичувачі (за розумною ціною) - до 8 ТБ.

Зовнішні жорсткі диски і твердотільні накопичувачі працюють так само, як і їх внутрішні аналоги. Більшість зовнішніх накопичувачів можна підключити до будь-якого комп'ютера; вони не прив'язані до одного пристрою, тому можуть відмінно використовуватися для передачі файлів між пристроями.

Компакт-диски, DVD-диски і диски Blu-Ray використовуються не тільки для відтворення музики і відео, але і як пристрої, що запам'ятовують. Вони

відносяться до категорії оптичних запам'ятовуючих пристроїв, або оптичних дисків.

Двійковий код зберігається на цих дисках у вигляді крихітних виїмок на доріжці, що йде по спіралі з центру диска. Працюючий диск обертається з постійною швидкістю, а лазер на дисковому накопичувачі сканує доріжку на диску. Те, як промінь лазера відбивається або розсіюється на ділянці доріжки, визначає, записаний на ньому 0 або 1 в бінарному коді.

DVD має більш вузьку спіральну доріжку, ніж компакт-диск, що дозволяє зберігати більше даних при тому ж розмірі диска, а в дисководах DVD використовується більш тонкий червоний лазер, ніж в дисководах компакт-дисків. DVD також можуть бути двошаровими, що збільшує їх ємність.

Blu-Ray - це технологія більш високого рівня, що забезпечує зберігання даних на декількох шарах з ще вужчими доріжками, для зчитування яких потрібно ще більш точний синій лазер.

CD-ROM, DVD-ROM і BD-ROM відносяться до категорії оптичних дисків, призначених тільки для читання, що означає, що записані на них дані зберігаються назавжди і не можуть бути видалені або перезаписані. Вони зазвичай використовуються для зберігання дистрибутивів ПЗ, але не як жорсткий диск для персональної інформації.

На диски формату CD-R, DVD-R і BD-R можна записувати інформацію, але вони не передбачають перезапису. Які б дані ви не зберегли на чистому диску одноразової записи, вони залишаться на ньому назавжди. На цих дисках можна зберігати дані, але вони не забезпечують такої гнучкості, як інші пристрої, що запам'ятовують.

CD-RW, DVD-RW і BD-RE передбачають перезапис, тому можна постійно записувати на них нові дані і видаляти непотрібні. Диски CD-RW довгий час були найкращим варіантом зовнішнього сховища, так як більшість настільних

комп'ютерів і багато ноутбуки мають дисковод для CD- або DVD-дисків, хоча їх місце поступово займають нові технології, такі як флеш-пам'ять.

На компакт-диску можна зберігати до 700 МБ даних, на DVD-DL - до 8,5 ГБ, а на Blu-Ray - від 25 до 128 ГБ.

Дискети були першими широко доступними портативними знімними запам'ятовують. Зараз ці пристрої вважаються застарілими. Вони працюють за тим же принципом, що і жорсткі диски, але в набагато меншому масштабі.

Ємність дискет ніколи не перевищувала 200 МБ, поки CD-RW і флеш-накопичувачі не стали популярними носіями інформації. iMac став першим персональним комп'ютером, випущеним без дисковода гнучких дисків в 1998 році, і з цього моменту закінчилося більш ніж 30-річне панування гнучких дисків.

Пристрої флеш-пам'яті складаються з трильйонів взаємопов'язаних осередків флеш-пам'яті, в яких зберігаються дані. Ці осередки містять мільйони транзисторів, які при включенні і виключенні представляють одиниці і нулі в двійковому коді, а комп'ютер зчитує і записує інформацію на основі електричного струму, що проходить через транзистори.

Мабуть, найвідоміший тип пристрою флеш-пам'яті - це USB-накопичувач. Ці невеликі портативні пристрої, що запам'ятовують, також відомі як флеш-накопичувачі, або просто «USB», довгий час були популярним варіантом додаткових комп'ютерних запам'ятовуючих пристроїв. USB-накопичувачі використовують для переміщення файлів з одного пристрою на інший.

В наші дні USB-накопичувач може вмістити до 2 ТБ даних. Якщо порахувати вартість зберігання гігабайта даних, USB-накопичувач буде дорожче, ніж зовнішній жорсткий диск. Хоча флеш-накопичувачі нечасто використовують для зберігання всіх персональних даних, вони популярні для тимчасового зберігання і перенесення невеликих файлів завдяки своїй простоті і зручності.

Крім USB-накопичувачів, до пристроїв флеш-пам'яті також відносяться SD-карти і карти пам'яті інших типів, які часто використовуються в якості носіїв інформації в цифрових камерах [11].

Переваги використання USB-накопичувачів:

- мала маса, безшумність під час роботи, портативність;
- усі сучасні комп'ютери, телевізори, материнські плати та DVD-програвачі обладнані USB-гніздами;
- експлуатація у широкому діапазоні температур;
- висока щільність запису;
- мають змогу зберігати дані автономно протягом 5-10 років;
- більш стійкі до механічних впливів (ударів) порівняно з твердим диском;
- відсутність рухливих частин, що знижує енергоспоживання у 3—4 рази;
- не чутливі до подряпин та пилу, які є значною проблемою для дискет, CD- та DVD-дисків.

Ці переваги обумовлюють актуальність використання usb-накопичувачів у сучасному світі.

1.5 Аналіз вразливостей та загроз при використанні зовнішніх flash-носіїв

Захист інформації включає повний комплекс заходів по забезпеченню цілісності та конфіденційності інформації за умови її доступності для користувачів, що мають відповідні права.

Поняття конфіденційності, цілісності, доступності наведені згідно з НД ТЗІ 1.1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

Цілісність - поняття, що визначає збереження якості інформації та її властивостей.

Конфіденційність передбачає забезпечення секретності даних і доступу до певної інформації окремим користувачам.

Доступність - якість інформації, що визначає її швидке і точне знаходження конкретними користувачами [12].

На рисунку 1.6 представлені базові загрози, які мають вплив на конфіденційність, цілісність та доступність інформаційних ресурсів.

Рисунок 1.6 – Базові загрози безпеці інформаційних ресурсів

USB-накопичувачі залишаються серйозною загрозою для інформаційної безпеки підприємств. З огляду на зростаючі швидкості роботи накопичувачів, їх ємність, але не людський фактор. Співробітник, навмисне або випадково, може сприяти витоку великих обсягів важливих даних.

Зростання кількості умисних витоків обумовлений виникненням нових можливостей, пов'язаних з обробкою, зберіганням, передачею інформації в цифровому вигляді. З кожним днем розширюється спектр послуг, що надаються на онлайн-майданчиках і з застосуванням даних електронного формату, збільшується обсяг інтелектуальної власності [13].

Основними об'єктами порушень є:

- відомості (незалежно від виду їхнього представлення), віднесені до інформації з обмеженим доступом (ІзОД) або інших видів інформації, що підлягають захисту, обробка яких здійснюється в АС і які можуть знаходитись на паперових, магнітних, оптичних та інших носіях;

- інформаційні масиви та бази даних, програмне забезпечення, інші інформаційні ресурси;

- обладнання АС та інші матеріальні ресурси, включаючи технічні засоби та системи, не задіяні в обробці ІзОД, але знаходяться у контрольованій зоні, носії інформації, процеси і технології її обробки. Технічні області, в яких необхідно захищати інформаційне та програмне забезпечення - робоча станція, комунікаційні канали (фізична мережа) та комутаційне обладнання, сервери, засоби друку та буферизації для утворення твердих копій, накопичувачі інформації;

- засоби та системи фізичної охорони матеріальних та інформаційних ресурсів, організаційні заходи захисту;

- користувачів (персонал) АС, власників інформації та АС, а також їхні права.

Уся інформація, яка циркулює в АС, поділяється на відкриту та з обмеженим доступом. За правовим режимом ІзОД поділена на таємну, службову, конфіденційну, іншу інформацію, необхідність захисту якої встановлено законом. До таємної інформації віднесена інформація, що містить відомості, які становлять державну, а також іншу, передбачену законом таємницю. Інформація, що становить державну таємницю, в свою чергу, поділяється на категорії відповідно до Закону України “Про державну таємницю” [14].

Для проведення аналізу ризиків необхідно розробити модель загроз для інформації та модель порушника.

При використанні зовнішніх знімних носії основним способом здійснення загрози є несанкціоновані дії, які здійснюються з метою використання інформації або нав’язування хибної інформації.

Загрози для інформації, що обробляється в АС, залежать від характеристик ОС, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні.

Випадковими загрозами суб’єктивної природи є дії, які здійснюються персоналом або користувачами по неуважності, недбалості, незнанню тощо, але без навмисного наміру:

- дії, що призводять до відмови АС (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв’язку, видалення даних, програм та ін.);

- ненавмисне пошкодження носіїв інформації;

- неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання тестуючих або технологічних процесів, які здатні призвести до незворотних змін у системі (наприклад, форматування носіїв інформації);

- неумисне зараження ПЗ комп’ютерними вірусами;

- невиконання вимог до організаційних заходів захисту чинних в АС розпорядчих документів;

- помилки під час введення даних в систему, виведення даних за невірними адресами пристроїв, внутрішніх і зовнішніх абонентів тощо;

- будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо;

- неправомірне впровадження і використання забороненого політикою безпеки ПЗ.

Навмисними загрозами суб'єктивної природи, спрямованими на дезорганізацію роботи АС (окремих компонентів) або виведення її з ладу, проникнення в систему і одержання можливості несанкціонованого доступу до її ресурсів, можуть бути:

- порушення режимів функціонування АС (обладнання і ПЗ);
- впровадження і використання комп'ютерних вірусів;
- використання (шантаж, підкуп тощо) з корисливою метою персоналу АС;
- крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо);
- несанкціоноване копіювання носіїв інформації;
- читання залишкової інформації з оперативної пам'яті ЕОМ, зовнішніх накопичувачів;
- одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача ("маскарад").

Модель порушника — абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце дії і т.ін. По відношенню до АС порушники можуть бути:

- внутрішніми (з числа співробітників, користувачів системи);
- зовнішніми (сторонні особи або будь-які особи, що знаходяться за межами контрольованої зони).

Метою порушника можуть бути:

- отримання необхідної інформації у потрібному обсязі та асортименті;
- мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);
- нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Порушників можна класифікувати за наступними критеріями:

- за рівнем можливостей, що надаються їм засобами АС;
- за рівнем знань про АС;
- за місцем здійснення дії.

Класифікація за рівнем можливостей є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

- перший рівень визначає найнижчий рівень можливостей ведення діалогу з АС — можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

- другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

- третій рівень визначається можливістю управління функціонуванням АС, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

- четвертий рівень визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення АС, аж до включення до складу АС власних засобів з новими функціями обробки інформації.

Ступінь інформованості порушника залежить від багатьох факторів, включаючи реалізовані на об'єктах АС конкретні організаційні заходи і компетенцію порушників. Тому об'єктивно оцінити обсяг знань ймовірного порушника в загальному випадку практично неможливо.

За місцем здійснення дії порушниками можуть бути ті особи, які мають доступ до робочих місць кінцевих користувачів АС та до місць накопичення і зберігання даних [14].

Найбільш небезпечними ймовірними порушниками є користувачі АС і уповноважений персонал розробників АС, який на договірній основі має право на технічне обслуговування і модифікацію компонентів АС.

Кожній системі захисту притаманна наявність слабких місць, що призводять до утворення каналів витоку інформації. Загалом, усі загрози інформаційній безпеці можна поділити на внутрішні та зовнішні.

Найслабкішим місцем систем захисту електронної інформації є внутрішні загрози. Проведені дослідження щодо співвідношення внутрішніх та зовнішніх загроз подано на рисунку 1.7.

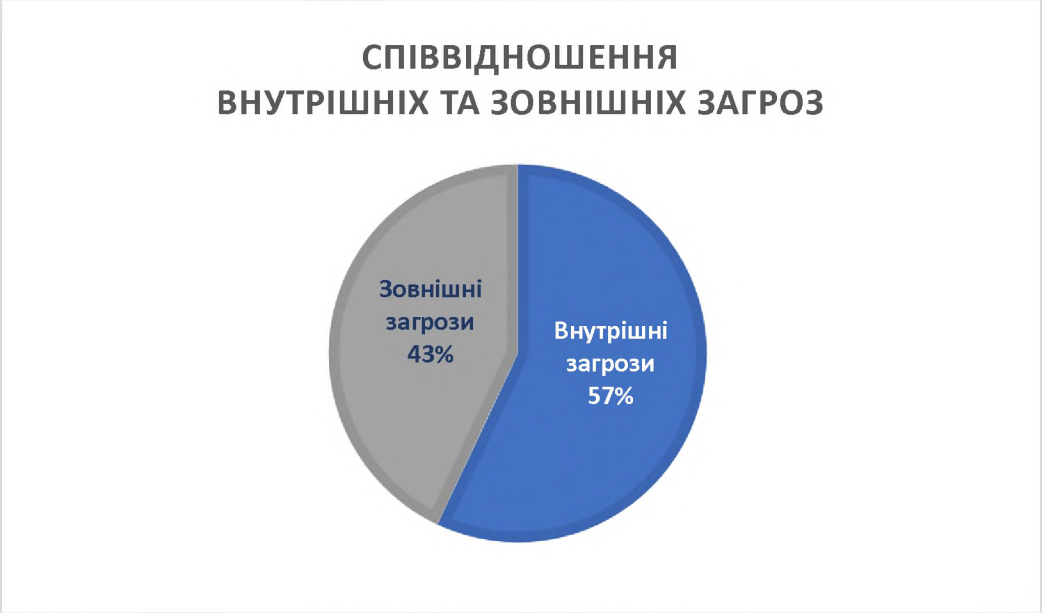


Рисунок 1.7 - Співвідношення внутрішніх та зовнішніх загроз

Здебільшого дії персоналу, що має безпосередній легальний доступ до АС, контролюються нормативними та організаційними заходами. Але при спробі здійснення несанкціонованого доступу їх буде замало.

Умисні витоки даних здійснюються інсайдерами або зовнішніми зловмисниками. Інсайдери мають доступ до важливої інформації всередині організації, тому заплановану витік такого роду можна розділити на два типи: працівник використовує наявні в нього дані заради особистої вигоди. Персонал має доступ до інформації, в якій не потребує для виконання посадових обов'язків (перевищення прав доступу), і застосовує його для отримання грошей або в інших інтересах. Зловмисники користуються відсутністю (або поганою організацією)

системи інформаційної безпеки компанії, ненавмисним або навмисним порушенням заходів щодо захисту даних.

Користувач, який має безпосередній легальний доступ до автоматизованої системи, може реалізувати такі загрози:

– здійснити крадіжку конфіденційної інформації — користувач може скопіювати інформацію на портативні пристрої, чи на зовнішні носії, опублікувати її на веб-сайті, відправити за помилковим поштовим індексом. Може реалізовуватися через помилку користувача або через його навмисні дії;

– порушити авторські права на інформацію — здійснення несанкціонованого копіювання авторського документу чи його частини, шифрування документу з власним паролем, підробка реквізитів іншого користувача чи компанії. Найчастіше реалізується через навмисні дії користувачів;

– шахрайство — спотворення фінансової документації, перевищення повноважень під час роботи з базами даних, модифікація важливих даних. Реалізується через навмисні дії задля досягнення певної мети;

– саботаж інформації — реалізується навмисно задля досягнення певної мети чи для помсти.

Проаналізувавши можливості з утворювання користувачами каналів витоку інформації, можна перелічити їх у порядку зменшення ймовірності реалізації (Рис. 1.8):

- зовнішні носії — 45 %;
- пересилання файлів мережею Internet — 25 %;
- друк файлів на принтері — 13 %;
- фотографування документів на цифрові камери — 12 %;
- інші — 5 %.

Рисунок 1.8 - Імовірність реалізації внутрішніх каналів витоку інформації

Проаналізовані джерела виділяють внутрішні загрози як основну причину спричинення каналу витоку інформації.

У свою чергу, зовнішні пристрої накопичування даних є головним засобом здійснення витоку інформації через її копіювання самим користувачем для подальших неправомірних дій із нею.

Загрози, що виникають при використання USB накопичувачів:

- втрата носія з конфіденційною інформацією;
- витік конфіденційної інформації, при неправильному зберіганні конфіденційної інформації;
- несанкціоновані ненавмисні дії користувачів;
- при пошкодженні USB - носія доступ до інформації може бути неможливий;
- exploit програми впроваджені в прошивку USB накопичувача зловмисником;
- уразливості операційної системи дозволяють виконувати файли при підключенні знімного носія;

- відмова знімного носія в обслуговування, при не якісному обладнанні (внаслідок чого порушується доступ до інформації);
- тіньове копіювання даних при підключенні до комп'ютера переносних запам'ятовуючих пристроїв;
- збої в роботі устаткування і ПЗ;
- шкідливе ПЗ, що приводить до пошкодження компонентів обладнання;
- розкрадання виробничих відходів (роздруківок, записів, списаних носіїв і т.п.);
- відновлення (в тому числі і фрагментарне) захищається інформації та інформації про АІТС шляхом аналізу виведених з ужитку і стали після цього доступними порушнику знімних носіїв інформації;
- зчитування або відновлення інформації (в тому числі і фрагментарне) по залишковим слідах на носіях інформації, що захищається інформації, зданих в ремонт, на обслуговування, переданих для використання іншими користувачами або для використання за межами АС;
- негласне (приховане) тимчасове вилучення або розкрадання знімних носіїв інформації, що захищається, автентифікуючої або ключовий інформації;
- негласна (прихована) модифікація інформації, що захищається, що зберігається на носіях інформації (в тому числі на знімних носіях інформації);
- модифікація програмних засобів АС з використанням шкідливих програм, розміщених на знімних носіях інформації;
- витік, модифікація, блокування або знищення захищається з використанням шкідливих програм, розміщених на знімних носіях інформації.

Кожній загрозі можуть бути співставлені різні уразливості, усунення або істотне ослаблення яких впливає на ймовірність реалізації загроз ІБ [15].

Отже, можливості внутрішнього порушника істотно залежать від діючих в межах контрольованої зони обмежувальних факторів, з яких основним є реалізація комплексу режимних та організаційно-технічних заходів, в тому числі по підбору, розстановці і забезпечення високої професійної підготовки кадрів, допуску фізичних осіб всередину контрольованої зони і контролю за порядком проведення робіт, спрямованих на запобігання і припинення несанкціонованих дій.

1.6 Аналіз існуючих методів захисту інформації від несанкціонованих дій при використанні зовнішніх носіїв

Основні прийоми захисту від цілеспрямованих шкідливих дії інших людей полягають у забезпеченні заборони несанкціонованого доступу до ресурсів комп'ютера, а також до підключеним до нього пристроям; неможливість несанкціонованого використання ресурсів комп'ютера після отримання до них доступу; своєчасне виявлення факту несанкціонованих дій і усунення їх причин та наслідків.

Засоби захисту інформації - це сукупність інженерно-технічних, електричних, електронних, оптичних та інших пристроїв і пристосувань, приладів та технічних систем, а також інших речових елементів, які використовуються для вирішення різних завдань із захисту інформації, у тому числі попередження витоку і забезпечення безпеки захищається інформації.

В цілому засоби забезпечення захисту інформації в частині запобігання навмисних дій залежно від способу реалізації можна поділити на групи: технічні (апаратні) засоби, програмні засоби та організаційні методи.

Організаційні методи складаються з організаційно-технічних (підготовка приміщень з комп'ютерами, прокладка кабельної системи з урахуванням вимог обмеження доступу) та організаційно-правових (національні законодавства і правила роботи, встановлені керівництвом конкретного підприємства).

До організаційно – адміністративних заходів відносяться (Рис.1.9): охорона комп'ютерних систем, підбір персоналу, виключення випадків ведення особливо важливих робіт тільки однією людиною, наявність плану відновлення працездатності центру після виходу його з ладу, обслуговування обчислювального центру сторонньою організацією або особами, незацікавленими в приховуванні фактів порушення роботи центру, універсальність засобів захисту від усіх користувачів (включаючи вище керівництво), покладання відповідальності на осіб, що повинні забезпечити безпеку центру, вибір місця розташування центру.

Рисунок 1.9 – Організаційно-адміністративне забезпечення безпеки

Переваги організаційних засобів полягають у тому, що вони дозволяють вирішувати безліч різнорідних проблем, прості в реалізації, швидко реагують на небажані дії в мережі, мають широкі можливості модифікації і розвитку. Недоліки організаційних засобів - висока залежність від суб'єктивних факторів, у тому числі від загальної організації роботи із захисту інформації.

До інженерно – технічних заходів (Рис. 1.10) можна віднести захист від несанкціонованого доступу до комп'ютерної системи, резервування важливих комп'ютерних систем, забезпечення захисту від розкрадань і диверсій, резервне електроживлення, розробку і реалізацію спеціальних програмних і апаратних комплексів безпеки тощо [10].

Рисунок 1.10 – Інженерно-технічне забезпечення безпеки

Технічні (апаратні) засоби - це різні за типом пристрою (механічні, електромеханічні, електронні та ін.), які апаратними засобами вирішують завдання захисту інформації. Вони або перешкоджають фізичній проникненню, або, якщо проникнення все ж таки відбулося, перешкоджають доступу до інформації, у тому числі за допомогою засобів маскування. Першу частину завдання вирішують запірні пристрої, грати на вікнах, захисна сигналізація. Другу - мережеві фільтри, генератори шуму, скануючі радіоприймачі і безліч інших пристроїв, «перекривають» потенційні канали витоку інформації. У практиці діяльності будь – якої організації знаходить широке застосування різна

апаратура: від телефонного апарату до розроблених автоматизованих інформаційних систем, що забезпечують її виробничу діяльність. Основна задача апаратних засобів – стійка безпека комерційної діяльності.

Фізичні засоби містять у собі різні інженерні засоби, що перешкоджають фізичному проникненню зловмисників на об'єкти захисту, що захищають персонал (особисті засоби безпеки), матеріальні засоби і фінанси, інформацію від протиправних дій.

Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб'єктивних факторів. Слабкі сторони підходу-недостатня гнучкість, відносно великі обсяг і маса, висока вартість.

Програмні засоби включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової інформації типу тимчасових файлів, тестового контролю системи захисту та ін. Переваги програмних засобів - універсальність, гнучкість, надійність, простота установки, здатність до модифікації і розвитку. Недоліки групи - обмежена функціональність мережі, використання частини ресурсів файл-сервера і робочих станцій, висока чутливість до випадкових або навмисним змінам, можлива залежність від типів комп'ютерів.

Ідентифікація користувача включає в себе реєстрацію в системі безпеки обчислювального пристрою унікального реєстраційного імені користувача (логіна) і відповідного цьому користувацькому імені - пароля. Встановлення автентичності користувача (автентифікація) полягає в перевірці істинності його повноважень. Для особливо надійного впізнання при ідентифікації і автентифікації користувача іноді використовуються спеціальні технічні засоби, що фіксують і розпізнають індивідуалізують людини фізичні та лінгвістичні характеристики (голос, відбитки пальців, структура зіниці, мовні особливості і т.д.). Однак такі методи вимагають значних витрат і тому використовуються

рідко, так що основним і найбільш масовим засобом ідентифікації залишається парольний доступ.

У ряді випадків при необхідності забезпечити високий ступінь захисту інформації, яка знаходиться в комп'ютері або обробляється обчислювальним пристроєм, використовуються також спеціальні криптографічні методи захисту інформації.

Криптографічні засоби – це спеціальні математичні та алгоритмічні засоби захисту інформації, переданої по мережах зв'язку, збереженої та обробленої на комп'ютерах з використанням методів шифрування. При шифруванні інформації відбувається її оборотне перетворення в деяку уявну випадкової послідовність знаків, яка називається шифротекст, або криптограмою. Для створення і роботи з криптограмою потрібне знання алгоритму і ключа шифрування [16].

Змішані програмно-апаратні засоби реалізують ті ж функції, що апаратні і програмні засоби окремо, і мають проміжні властивості.

Велика частина традиційних засобів захисту таких як антивіруси, міжмережеві екрани (Firewall) і системи запобігання вторгнень (IPS) не здатні забезпечити ефективний захист від внутрішніх порушників (інсайдерів), метою яких може бути передача інформації за межі компанії для подальшого використання - продажу, передачі третім особам, опублікування у відкритому доступі і т.д.

Наразі застосовують такі методи захисту від внутрішніх загроз витоку інформації:

- оснащення приміщень компанії камерами спостереження;
- суворий режим допуску на територію компанії, особливо в зони зберігання і обробки конфіденційної інформації;
- шифрування якомога більшої кількості важливої інформації;
- персональна відповідальність посадових осіб за видачу дозволу на доступ співробітників до конфіденційних документів;

- шифрування USB флеш-карт, CD, DVD, розділів з даними на мобільних пристроях;
- впровадження корпоративної системи управління мобільними пристроями MDM (Mobile Device Management);
- оснащення серверів компанії засобами миттєвого знищення інформації;
- зберігання важливої інформації на зарубіжних довірених майданчиках.

Також використовують наступні методи протидії соціальним загрозам витоку інформації:

- впровадження професійних DLP-систем;
- обмеження доступу персоналу до певних документів компанії;
- моніторинг роботи користувачів з корпоративними ресурсами;
- моніторинг внутрішнього і зовнішнього трафіку користувачів;
- складання та контроль дотримання політики інформаційної безпеки;
- персональна відповідальність співробітників за ввірені йому носії інформації;
- регламентація роботи персоналу з корпоративними документами;
- використання термінального режиму роботи користувачів для централізації периметра безпеки.

Вирішити проблему випадкових і навмисних витоків конфіденційних даних, покликані системи запобігання витоків даних (DLP - Data Loss Prevention).

Подібного роду системи створюють захищений «цифровий периметр» навколо організації, аналізуючи всю витікаючу, а в ряді випадків і вхідну інформацію. Контрольованої інформацією виступає не тільки інтернет-трафік, але і ряд інших інформаційних потоків: документи, які виносяться за межі захищається контуру безпеки на зовнішніх носіях, роздруковуються на принтері, що відправляються на мобільні носії через Bluetooth, WiFi і т.д.

DLP - системи здійснюють аналіз потоків даних, які перетинають периметр захищається інформаційної системи. При виявленні в цьому потоці

конфіденційної інформації спрацьовує активна компонента системи і передача повідомлення (пакета, потоку, сесії) блокується. Виявлення конфіденційної інформації в потоках даних здійснюється шляхом аналізу змісту і виявлення спеціальних ознак: грифа документа, спеціально введених міток, значень хеш-функції з певної множини і т.д [17].

Інші пункти реалізуються за рахунок використання програмно-апаратних комплексів засобів захисту. В Україні найбільш популярними КЗЗ є «Гриф-4» та «Лоза».

Засіб технічного захисту інформації від несанкціонованого доступу (НСД) «Комплекс «Гриф» версії 4 призначений для забезпечення захисту ІзОД, оброблюваної в АС класу 1 та в АС класу 2, що побудовані на базі ПЕОМ (у випадку АС класу 2 – об'єднаних в однорангову локальну обчислювальну мережу), які функціонують під управлінням ОС корпорації Microsoft.

На відміну від політики довірчого управління доступом, яка реалізується штатними засобами захисту ОС, використання комплексу «Гриф» версії 4 дозволяє забезпечити реалізацію політики адміністративного управління доступом до ІзОД, тобто такого розмежування доступу, при якому призначати права доступу користувачів до захищених інформаційних ресурсів можуть тільки спеціально уповноважені користувачі (адміністратори). Комплекс повністю заміняє штатні засоби ОС власними засобами, які підтримують реалізацію адміністративного розмежування доступу до захищених ресурсів.

Комплекс забезпечує захист інформації, яка представлена у вигляді файлів даних довільного типу (електронних документів, електронних таблиць, конструкторських креслень, даних геоінформаційних систем і т.п.).

Комплекс «Гриф» версії 4 реалізує наступні основні функції захисту:

- ідентифікацію та автентифікацію користувачів на підставі імені (псевдоніма), пароля та персонального носія даних автентифікації (дискети, пристрою Flash Drive, CD-RW, DVD-RW або іншого знімного файлового носія);

- розподіл обов'язків користувачів та виділення декількох ролей адміністраторів, які можуть виконувати різні функції з адміністрування (реєстрацію захищених ресурсів, реєстрацію користувачів, призначення прав доступу, оброблення протоколів аудиту, тощо);

- розмежування доступу користувачів до обраних каталогів файлової системи незнімних носіїв ПЕОМ (у тому числі різних ПЕОМ, що функціонують у складі ЛОМ) та файлів, що містяться у них, що дозволяє організувати спільну роботу декількох користувачів, які мають різні службові обов'язки та права по доступу до захищеної інформації;

- управління потоками інформації та блокування потоків інформації, що можуть призвести до зниження її рівня конфіденційності;

- керування створеними на знімних або незнімних носіях ПЕОМ захищеними логічними дисками, вся інформація на яких зберігається у зашифрованому вигляді, та розмежування доступу до їх вмісту з використанням механізмів "прозорого" розшифрування/зашифрування даних у момент їх читання/ запису, що дозволяє забезпечити захист конфіденційності збереженої інформації навіть у випадку крадіжки ПЕОМ або відповідних носіїв;

- контроль цілісності захищених логічних дисків, що дозволяє забезпечити захист від несанкціонованої модифікації збереженої на них інформації при відключених засобах захисту або у випадку крадіжки відповідних носіїв;

- контроль за виведенням інформації на пристрої друку з можливістю маркування друкованих аркушів документів (у форматі "Office Open XML") відповідно до вимог діючих нормативних документів в сфері охорони державної таємниці;

- контроль за експортом інформації на знімні носії та за імпортом інформації зі знімних носіїв із забезпеченням можливості реєстрації змінних носіїв та обмеження (для певних користувачів) переліку використовуваних знімних носіїв тільки зареєстрованими;

- гарантоване знищення інформації з обмеженим доступом при видаленні відповідних файлів;

- розмежування доступу прикладних програм до обраних каталогів та файлів, що містяться у них, що дозволяє забезпечити захист інформації від випадкового видалення або пошкодження, а також забезпечити дотримання технології її оброблення;

- контроль цілісності прикладного ПЗ та ПЗ комплексу, а також блокування завантаження програм, цілісність яких порушено, що дозволяє забезпечити захист від шкідливих програм (комп'ютерних вірусів) та дотримання технології оброблення ІзОД;

- контроль за використанням дискового простору користувачами, що виключає можливість блокування одним із користувачів можливості роботи інших користувачів;

- можливість блокування пристроїв інтерфейсу користувача (клавіатури, миші, монітора) на час його відсутності;

- контроль цілісності та самотестування комплексу при старті та за запитом адміністратора;

- відновлення функціонування комплексу у випадку збоїв, що гарантує доступність інформації при дотриманні правил доступу до неї;

- реєстрацію, аналіз та надання уповноваженим адміністраторам можливості оброблення інформації про події, які мають безпосереднє відношення до безпеки оброблюваної інформації, що дозволяє адміністраторам контролювати доступ до ІзОД, слідкувати за тим, як використовується комплекс, а також правильно його конфігурувати;

- ведення архівів зареєстрованих даних аудита;

- взаємодію з прикладними програмними системами (ППС) через визначений розробником комплексу інтерфейс, що дозволяє забезпечити

безперервність захисту ІзОД при її обробці як штатними засобами ОС, так і засобами різноманітних ППС.

Розробка комплексу «Гриф» версії 4 виконана у відповідності з вимогами НД ТЗІ 2.5-012-2015, НД ТЗІ 2.5-008-2002 та рекомендаціями НД ТЗІ 2.4-015-2018. Комплекс «Гриф» версії 4 пройшов державну експертизу за критеріями технічного захисту інформації та має експертний висновок, зареєстрований в Адміністрації Держспецзв'язку 08.10.2020 г. за № 1171 [18].

Система ЛОЗА-1 — це програмний засіб захисту інформації від несанкціонованого доступу в автоматизованих системах класу «1». Система ЛОЗА-1 може працювати під керуванням операційних систем Windows 7/8/8.1/10/ Server 2008/2012/2016/2019 (32- та 64-розрядних версіях).

Система ЛОЗА-1 реалізує всі стандартні функції, необхідні для надійного захисту інформації від несанкціонованого доступу і для побудови комплексної системи захисту інформації.

Система ЛОЗА-1 може використовуватись для захисту інформації, що становить державну таємницю, — це підтверджено експертним висновком №1095, виданим Державною службою спеціального зв'язку та захисту інформації України 02 квітня 2020р.

Система ЛОЗА-1 має наступні особливості:

Захист від несанкціонованого доступу до інформації:

- забезпечує надійний захист документів Microsoft Word та Microsoft Excel за рахунок тісної інтеграції з Microsoft Office (відключаються небезпечні команди, макроси, шаблони тощо); підтримуються версії Microsoft Office 2007/2010/2013/2016/2019;

- дозволяє захистити будь-які дані на знімних та стаціонарних носіях; захист здійснюється на рівні папок Windows та знімних дисків.

- дозволяє контролювати роботу із знімними дисками: дискетами, компакт-дисками та «флешками», для «флешек» дозволи на доступ до диска можуть

встановлюватись для окремих носіїв (вони ідентифікуються за «залізним» серійним номером);

- дозволяє встановлювати дозволи або заборони на запуск процесів.

Контроль друку та експорту:

- забезпечує можливість встановлення дозволу/заборони друку та експорту на рівні окремих документів;

- для підсилення контролю система ЛОЗА-1 дозволяє забезпечити присутність адміністратора або іншої уповноваженої особи під час друку та експорту (за рахунок необхідності введення пароля).

Контроль входу користувачів до системи:

- у конфігурації «Підвищена безпека» вхід здійснюється тільки після введення пароля та встановлення ключового диска (може використовуватись звичайна дискета, «флешка» або CD/DVD-диск); діє жорстка політика паролів та політика блокування користувачів, яка протидіє підбору паролів;

- у конфігурації «Стандартна безпека» для входу достатньо ввести пароль; політика паролів менш жорстка, ніж в конфігурації «Підвищена безпека».

Реєстрація подій:

- система веде захищений журнал, в якому реєструються всі події, важливі для захисту інформації;

- аналіз журналу та протоколів роботи не потребує спеціальної кваліфікації;

- журнал подій ніколи не перезаписується: після досягнення граничного розміру журналу всі події зберігаються у файлі на жорсткому диску;

- система забезпечує докладну реєстрацію подій друку та експорту; поряд із стандартною інформацією у журналі фіксуються гриф та обліковий номер документа, а також серійний номер носія, на якому зберігається документ, та носія, на який здійснюється експорт; адміністратор має можливість формування протоколу друку документів [19].

Реєстрація носіїв інформації в таких системах не є надійною, адже можна підмінити зареєстрований носії, скопіювавши файл, записаний системою, на інший носій та використовувати його для копіювання даних. Тому необхідно однозначно ідентифікувати пристрій за його внутрішніми параметрами. Для цього треба розробити такий пристрій, який буде підключатися між зовнішнім носієм і системою через USB-інтерфейс та порівнювати параметри пристрою з тими, які пристрій зберігає у своїй внутрішній пам'яті. Завдяки цьому пристрою до системи буде допускатися тільки той flash-носій, який записано на перехідному ідентифікуючому пристрої.

1.7 Постановка задачі

Задача захисту від здійснення несанкціонованих дій при використанні зовнішніх flash-носіїв є найбільш актуальною в автоматизованих системах класу «1» та «2», де носії інформації використовуються для переміщення даних. Загрозу безпеці ІзОД становлять внутрішні порушники, які мають доступ до системи та мають змогу підключати зовнішні пристрої для переміщення даних із системи на знімний пристрій або ж завантажувати з зовнішнього пристрою шкідливі файли та вірусні програми.

В наш час найпоширенішими у використанні зовнішні пристрої є USB-flash-носії, оскільки вони мають малий розмір, достатній об'єм пам'яті та зручні у використанні. Майже у кожної людини є флешка, яка слугує засобом зберігання інформації та переміщення даних між різними системами. Однак такі носії не є захищеними. Зареєстрований в системі носії можна підмінити та використовувати зовсім іншу флешку, яка не контролюється організацією. Таким чином можна нанести шкоду інформації та організації, якій вона належить за рахунок копіювання та компрометації, модифікації, підміни або видаленню даних з обмеженим доступом.

Проаналізувавши існуючі методики захисту від несанкціонованих дій при використанні flash-носіїв в системі, можна зробити висновок, що цього недостатньо для того, щоб захистити інформацію від несанкціонованих дій внутрішніх порушників. Тому є необхідність розробити нову методику захисту інформації з обмеженим доступом від несанкціонованих дій при використанні зовнішніх flash-носіїв.

2 СПЕЦІАЛЬНА ЧАСТИНА

2.1 Вимоги до методики захисту інформації від несанкціонованих дій при використанні зовнішніх flash-носіїв інформації в автоматизованних системах

Під час підключення носія до АС виконується одностороння автентифікація пристрою по його статичним параметрам. При обміні даних між системою та зовнішніми носіями є загроза витіку інформації шляхом підміни легітимного flash-носія. Виходячи з цього необхідно розробити методику захисту для протидії цій загрозі.

Для того, щоб уникнути несанкціоноване копіювання, модифікацію або знищення інформації методика повинна забезпечувати достовірний зв'язок між довіреною системою та підключеним носієм. Також потрібно контролювати події, які виконувалися з носієм.

Не допускається внесення змін в операційну систему та у встановлені програмні надлаштування над операційною системою для забезпечення захисту інформації. Методика виконуватиме захисні функції окремо від ОС.

Розроблена методика не повинна вносити змін в апаратну частину автоматизованої системи. Для реалізації методики достатньо наявності USB-порту в системному блоці ЕОМ для підключення знімних накопичувачів та інших USB-пристроїв.

Методика захисту від несанкціонованих дій користувачів АС при використанні зовнішніх носіїв повинна бути легкою та прозорою у застосуванні. Для використання методики не має потреби у додатковому навчанні персоналу. Робітникам немає необхідності мати підвищений рівень кваліфікації, достатньо володіти знанями ПК на рівні користувача.

Розроблювана методика захисту інформації від несанціонованих дій внутрішніх порушників при використанні зовнішніх flash-носіїв включає в себе створення додаткового пристрою для посиленої ідентифікації flash-носія та опис роботи адміністратора безпеки та користувача системи. Для того, щоб

реалізувати рішення протидії порушенням, потрібно визначити основні вимоги до методики.

Застосування методики не повинно допускати спотворення данних, які передаються між системою і зовнішнім носієм. Пристрій тільки ідентифікує та автентифікує підключений до нього USB-пристрій. Якщо підключений пристрій легітимний, то він має працювати як шлюз і не впливати на дані, які через нього протікають.

В результаті роботи потрібно отримати додатковий пристрій для USB-flash-носіїв, який забезпечить підключення та доступ до ЕОМ тільки одного носія, який зареєстрований у пристрої. Ініціалізацію flash-носія повинен проводити адміністратор безпеки у режимі адміністратора, а користувач має тільки підключати свій носії інформації до системного блоку через даний пристрій. Працювати з розробленим пристроєм має бути легко та зрозуміло.

2.2 Обґрунтування вибору методики захисту інформації від несанкціонованих дій

Захист інформації з обмеженим доступом в автоматизованих системах і засобах обчислювальної техніки, призначених для формування, пересилання, приймання, перетворення, відображення та зберігання інформації, забезпечується комплексом організаційних, програмних і технічних заходів.

Для реального здійснення попередження неправомірних дій з інформаційними ресурсами необхідно обмежувати дії авторизованого користувача зі здійснення підключення незареєстрованих пристроїв, а також контролювати розповсюдження важливої інформації, що знаходиться на його знімних носіях.

У розроблюваній методиці необхідно застосовувати комплексний підхід для реалізації захисту, враховуючи організаційні заходи, програмну та апаратну складові.

Організаційні заходи спрямовані на чіткий розподіл відповідальності персоналу в процесах опрацювання інформації, створення декількох рубежів контролю, запобігання зовнішнім та інсайдерським загрозам, навмисному або випадковому знищенню й модифікуванню інформації. Для протидії внутрішнім порушенням при використанні зовнішніх знімних носіїв може застосовуватись контроль дозволених пристроїв. Кожен пристрій, якій дозволено використовувати в системі, реєструється у спеціальному відділі та закріплюється за тим користувачами, якому він належить. Зберігаються знімні пристрої в спеціальних сховищах, виносити їх за межі контрольованої зони неможна. Для контролю знімних носіїв ведеться обліковий журнал, в якому уповноважена особа веде запис видачі та прийняття носіїв. Такий підхід зменшує вірогідність реалізації витоку інформації за межі організації, але не є ідеальним, оскільки враховується людський фактор (змова, підкуп в т.п.). Також це не виключає змогу пронести сторонній зовнішній носій, який не зареєстрований у відділі контролю носіїв.

Програмні засоби захисту інформації необхідні для виконання логічних і інтелектуальних функцій захисту. Операційні системи та різні програми мають функцію контролю підключень зовнішніх носіїв. Програмою отримуються унікальні параметри носія, йому присвоюється всередині системи номер та записується в список зареєстрованих програмою носіїв. Також вони дають змогу блокувати підключення окремих зареєстрованих пристроїв або груп пристроїв у налаштуваннях. Однак при наявності знімного носія зловмисник має змогу зчитати ці параметри носія та скопіювати їх на інший носій, який не є легітимним і користуватися їм в системі, як дозволеним пристроєм. Також параметри носіїв є лише теоретично унікальними. Насправді вони можуть повторюватись. Тобто

один виробник може випустити дві абсолютно однакові флешки з однаковими параметрами. Тому використання програмних продуктів не дозволяє повноцінно захисти систему та її внутрішні ресурси від несанкціонованих підключень зовнішніх flash-носіїв. Отже, програмні методи не забезпечують однозначне визначення носія. Виходячи з цього пропонується застосувати програмно-апаратне рішення.

Принцип роботи програмно-апаратної частини базується на використанні внутрішніх параметрів flash-носіїв, так названих дескрипторів, а також на кількості секторів пам'яті. На основі отриманих параметрів підключеного до пристрою носія генерується хеш-значення, яке зберігається у внутрішній енергонезалежній пам'яті пристрою. При повторному підключені носія відбувається зчитування параметрів, генерується хеш-значення та порівнюється з тим, яке зберігається в пристрої. Якщо хеш-значення співпадають, то пристрій надає наскрізний доступ до системи, якщо ні – носії не підключається до системи.

Враховуючи організаційні заходи слід зазначити, що процес ініціалізації flash-носія в пристрої виконується уповноваженою особою, яка має кваліфікацію з безпеки інформації. Після того, як flash-носій зареєстровано у пристрої, їх необхідно об'єднати в один монолітний корпус, який опечатується.

2.2.1 Аналіз взаємодії автоматизованих систем з зовнішніми носіями

У наш час на ЕОМ широко використовуються операційні системи сімейства Windows. Тому на прикладі роботи ОС Windows розглянемо процес взаємодії з USB-flash-носіями.

Підключення будь-якого нового обладнання пов'язане з виконанням модулями ядра системи Windows зумовлених фаз опитування і ініціалізації. Починається все з того, що при підключенні пристрою до гнізда USB, контролером USB (вбудованим в чіпсет на материнській платі) генерується апаратне переривання. Драйвер USB, відповідальний за обробку даного

переривання, запитує статус порту, і якщо статус вказує на підключений пристрій, то відповідальними підсистемами ядра проводиться послідовність дій, яку умовно можна розділити на дві стадії:

1. нумерування пристрою;
2. установка драйвера пристрою.

Ядро ініціює до знову підключеного пристрою серію запитів GET_DESCRIPTOR з різними типами запитуваних дескрипторів (Device, Configuration, LangID, iProduct). Основні дескриптори приведені в Додатку В. Запити опитують пристрій на предмет наявності серії дескрипторів, що представляють собою структури даних, що описують можливості USB пристрою.

У відповідь на подібного роду запити, мікрокод пристрою повертає з ПЗУ необхідну інформацію. Дані, які повертаються пристроєм у відповідь на запити різноманітних дескрипторів, є важливими для операційної системи, оскільки саме частина цих даних є різного роду ідентифікатори, що використовуються системою в подальшому в процесі нумерування пристрою.

Для підтримки виробників, чиї пристрої через функціональних особливостей не підходять під стандартний набір класів, Microsoft розробила набір спеціальних класів і власних дескрипторів. Прикладне і системне ПЗ може ідентифікувати пристрої, що належать до розроблених Microsoft класів пристроїв шляхом опитування пристрою на предмет наявності дескрипторів Microsoft. Пристрої, що підтримують дескриптори Microsoft, повинні зберігати спеціальний строковий дескриптор в прошивці з фіксованим індексом 0xEE. Операційні системи Windows XP SP1 і більш пізні запитують цей строковий дескриптор у пристрої при першому його підключенні.

Таким чином, кожен USB пристрій повинен мати, як мінімум: ідентифікатор виробника (VID, Vendor ID), ідентифікатор продукту (PID, Product ID), і серійний номер (Serial). На основі цих параметрів формується унікальний

ідентифікатор обладнання, тим самим забезпечується Унікалізація USB-пристрої в межах системи і вносяться зміни в конфігурацію обладнання.

Після того, як у пристрої запитані ключові параметри, для USB пристрою створений унікальний ідентифікатор HardwareID (CompatibleID), однозначно ідентифікує пристрій / клас пристрою. Драйвер USB-концентратора повідомляє спеціалізований модуль ядра під назвою Диспетчер Plug-n-Play (PnP Manager) про новий пристрій. Диспетчер PnP отримує ідентифікатори HardwareID і CompatibleID пристрою і намагається виявити пристрої з аналогічними ідентифікаторами HardwareID / CompatibleID. У цей момент в системі створюється вузол пристрою (devnode), що є, по суті, першим відбитком USB пристрою в системі. Якщо схожий пристрій знайдено, то проводиться установка відповідних драйверів в автоматичному режимі, якщо ж не знайдено, то Диспетчер PnP виводить повідомлення про новий пристрій і далі діє за певними правилами.

Представлені вище параметри і їх значення, фактично формують відбиток для кожного USB пристрою, оскільки сліди підключення USB пристрою в системі Windows складаються з подібних унікальних значень / назв [20].

В програмних комплексах засобів захисту є функції обліку та контролю подій при роботі з зовнишніми носіями. Адміністратор КЗЗ може зареєструвати в базі комплексу знімні носії, попередньо поставлені на облік в РСО, і дозволити певним користувачам виконання операцій імпорту / експорту тільки з використанням таких носіїв. Всі операції з файлами, що знаходяться на пристроях імпорту / експорту фіксуються в протоколах аудиту із зазначенням дати / часу, імені користувача, атрибутів додатків і імені файлу.

Для реєстрації носія необхідно заповнити реєстраційний номер (номер носія в РСО), рівень конфіденційності, дату взяття носія на облік (за замовчуванням стоїть поточна дача), відповідальна за носій особа. Після збереження даних програма заповнює поля «Ідентифікатор» і «Дата реєстрації»,

а також поля «Файлова система», «Тип» і «Серійний номер» заповнюються програмою адміністратора КЗЗ (Рис.2.1) [21].

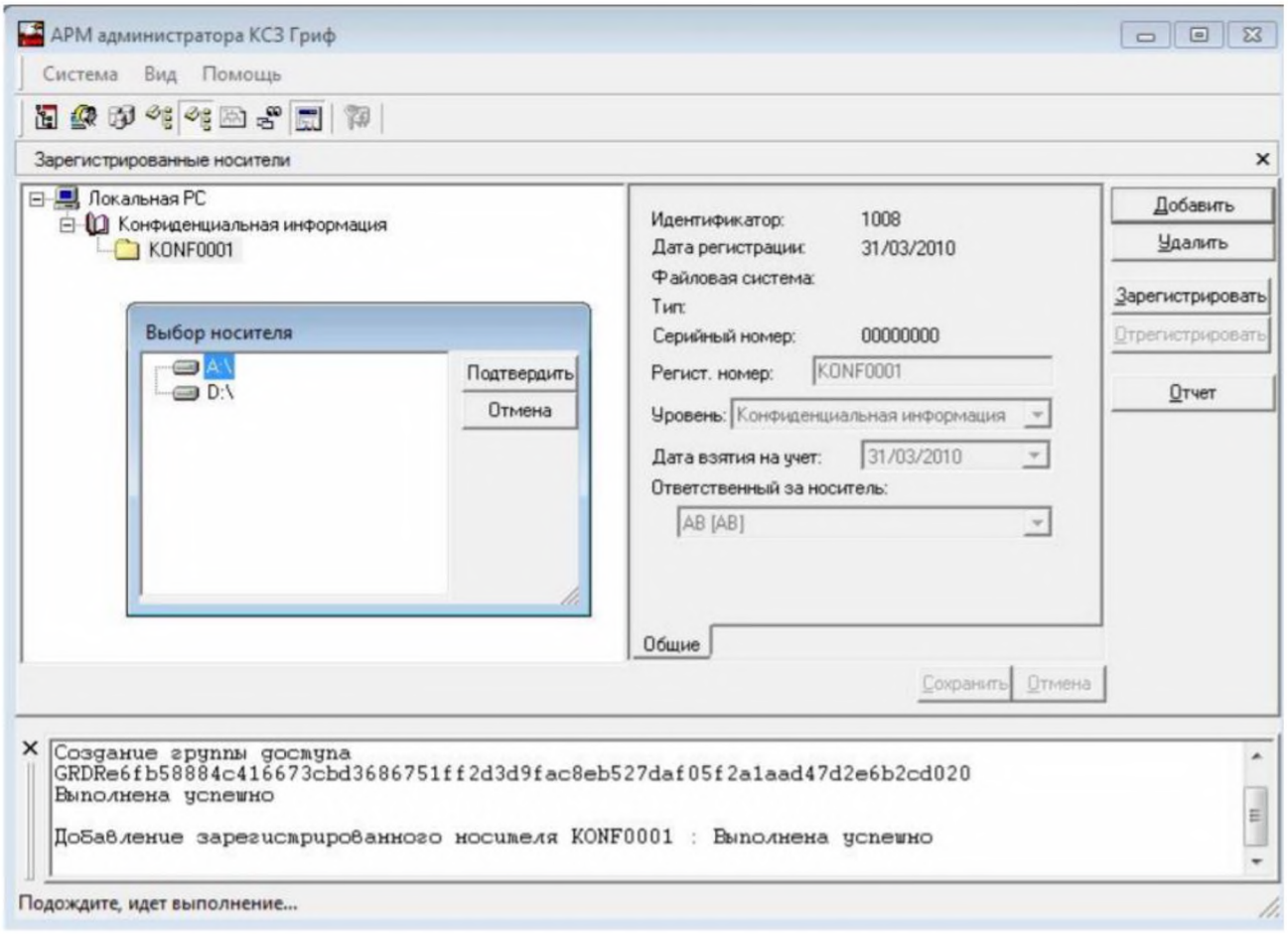


Рисунок 2.1 – Реєстрація носія в КЗЗ

Такий спосіб захисту використовує тільки програмний засіб реєстрації та контролю носіїв інформації, прив'язуючись до внутрішнього ідентифікатора носія. У разі використання копії носія, з такими ж дескрипторами, що записані у зареєстрованому носії, захищена система буде вважати, що до неї підключено дозволений носій і надасть доступ до роботи з інформацією.

В програмних комплексах функція контролю подій, які виконуються з носієм, відстежує дії лише всередині захищеної АС, але не має можливості визначити де і як ще був застосован носій. Це дозволяє користувачам використовувати носії на інших ЕОМ та неконтрольовано розповсюджувати інформацію з обмеженим доступом.

Проаналізувавши взаємодію зовнішніх носіїв з АС було зроблено висновок, що програмна реалізація контролю та обмеження підключень не захищає від використання копій носіїв, тому програмних засобів для захисту від несанкціонованих дій недостатньо для того, щоб уникнути загрози витоку інформації. Тому необхідно вирішити проблему підробки носіїв, використовуючи комплекс програмних та апаратних засобів захисту.

2.2.2 Структурна схема пристрою посиленого контролю flash-носіїв в автоматизованих системах

В якості програмно-апаратного комплексу засобів захисту пропонується розробити зовнішній пристрій посиленого контролю зовнішніх носіїв (ППКЗН) на мікроконтролері, який буде додатковим засобом захисту до програмних комплексів. Пристрій повинен мати вхідний порт, до якого підключається USB-носій, а з іншої сторони – USB-інтерфейс, за допомогою якого пристрій приєднується до блоку ПК. Пристрій повинен реалізовувати наступні функції:

- ідентифікація та автентифікація АС, до якої підключається пристрій;
- ідентифікація USB-flash-носія, який підключений до пристрою;
- ведення журналу подій та порівнювання його з журналом подій в АС;
- робота пристрою в різних режимах.

Для реалізації цих функцій пристрій повинен містити в собі порт USB-хост, USB-інтерфейс, центрального процесору, ОЗП, ПЗП, модуль годинника реального часу з підключеною до нього батарейкою, порти вводу/виводу для підключення світлодіода та перемикача режимів роботи та стабілізатор напруги (Рис.2.2).

USB-хост виявляє підключення і відключення USB-пристрою, управління передачею даних (тобто пакетів по шині USB), забезпечує живленням підключені до нього пристрої.

Інтерфейс USB призначений для підключення пристрою до персонального комп'ютера. Інтерфейс USB з'єднує між собою USB-хост ПК і пристрій. Хост

знаходиться всередині персонального комп'ютера і керує роботою всього інтерфейсу.

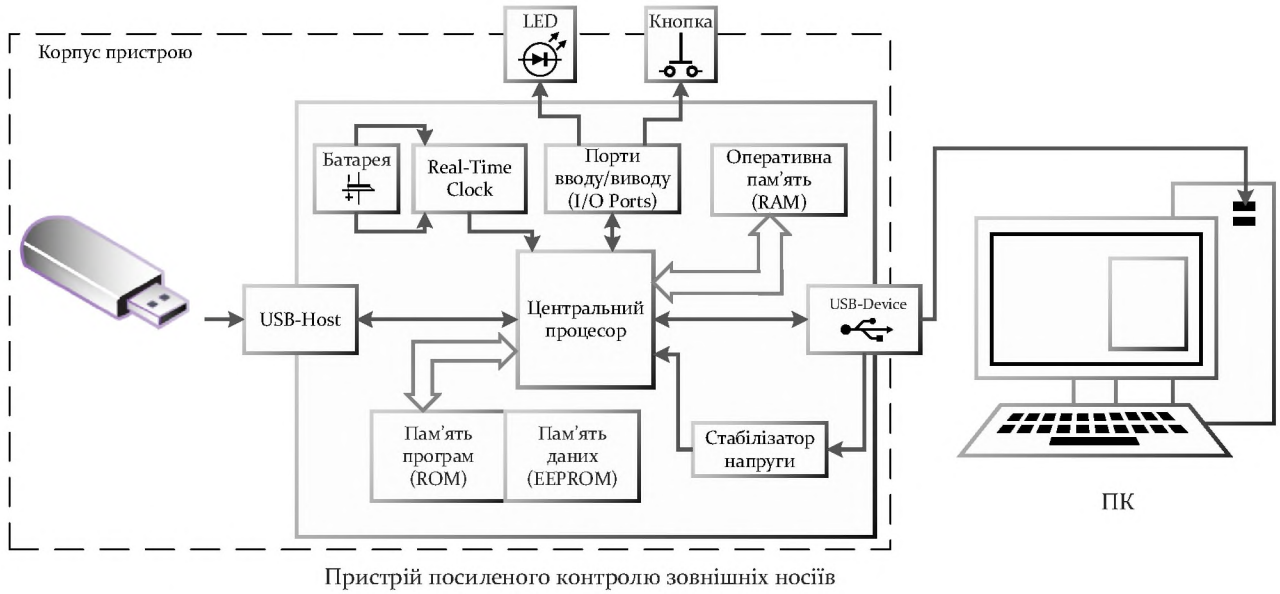


Рисунок 2.2 – Структурна схема пристрою посиленого контролю зовнішніх носіїв

Центральний процесор здійснює налаштування роботи пристрою, ведення журналу подій, приймання і передавання даних та реалізує криптографічний протокол ідентифікації. ПК повинен містити вбудований USB-порт для підключення ППКЗН.

ОЗП слугує для зберігання даних і команд для подальшої їх передачі процесору для обробки, виконує функції зберігання результатів обчислень, виконаних процесором, зчитування (або запис) вмісту осередків. При запуску програм інформація надходить в ОЗП з ПЗП, в якому зберігаються програми. Поки йде робота з програмою вона присутня в оперативній пам'яті.

ПЗП складається з двох частин: відкрита область (RAM) та захищена область (EEPROM). Відкрита область дозволяє виконувати читання даних та запис. У цій області зберігаються пам'ять програм, які виконуються центральним процесором, дескриптори flash-носіїв, які зчитуються при підключенні знімних пристроїв до ППКЗП, локальний журнал подій. В захищеній області пам'яті зберігаються хеш-значення, які генеруються з дескрипторів flash-носіїв, хеш-

значення записів журналу подій, сертифікати автентифікації пристрою з довіреною захищеною системою (Рис.2.3).

Рисунок 2.3 – Карта ПЗП

Наявність модуля годинника реального часу потрібно застосувати для того, щоб фіксувати події, які відбуваються з підключеним flash-носієм, у часі. Оскільки пристрій не має джерела постійного живлення, а годинник повинен постійно працювати, до модуля під'єднується батарейка, яка надає постійне живлення годиннику.

Порти вводу/виводу використовуються для управління підключених до пристрою світлодіода та кнопки. Світлодіод відображає режим роботи пристрою, а кнопка забезпечує їх перемикання.

Стабілізатор напруги забезпечить захист пристрою від ненормальних режимів роботи, таких як перепади напруги в мережі і високий або низький його рівень. Можливості стабілізатора дозволяє поліпшити ефективність використання енергії.

2.2.3 Обґрунтування вибору протоколу ідентифікації flash-носіїв

В будь-яких комп'ютерних системах існує необхідність аутентифікації. В ході цієї процедури комп'ютерна система перевіряє, чи дійсно користувач той, за кого себе видає. Для того, щоб отримати доступ до АС, користувачеві необхідно переконливо довести АС, що "він є та сама персона", а не хто-небудь ще. Для цього він повинен пред'явити системі якусь автентифікаційну інформацію, на підставі якої модуль аутентифікації даної системи виносить рішення про надання йому доступу до необхідного ресурсу (доступ дозволений / ні).

Для такої перевірки застосовується інформація трьох видів:

- унікальна послідовність символів, яку користувач повинен знати для успішного проходження автентифікації. Найпростіший приклад - парольна аутентифікація, для якої досить ввести в систему свій ідентифікатор (наприклад, логін) і пароль;

- унікальний вміст або унікальні характеристики предмета. Найпростіший приклад - ключ від будь-якого замку. У разі ж комп'ютерної аутентифікації в цій якості виступають будь-які зовнішні носії інформації: смарт-карти, електронні таблетки iButton, USB-токени і т.д.;

- біометрична інформація, яка невід'ємна від користувача. Це може бути відбиток пальця, малюнок райдужної оболонки ока, форма обличчя, параметри голосу і т.д.

Дуже часто комбінують декілька видів інформації, по якій проводиться автентифікація. Типовий приклад: автентифікаційна інформація зберігається на смарт-карті, до якої для отримання доступу потрібно ввести пароль. Така автентифікація називається двухфакторною.

У ряді випадків потрібна і взаємна аутентифікація - коли обидва учасники інформаційного обміну перевіряють один одного. Щоб зберегти в таємниці унікальну інформацію, при пересиланні використовується безліч протоколів аутентифікації.

Найпростіший протокол аутентифікації - доступ по паролю (Password Access Protocol, PAP): вся інформація про користувача (логін і пароль) передається в мережі у відкритому вигляді. Отриманий сервером пароль порівнюється з еталонним паролем даного користувача, який зберігається на сервері. Але така схема має недолік: будь-який зловмисник, здатний перехоплювати мережеві пакети, може отримати пароль користувача за допомогою найпростішого аналізатора пакетів типу sniffer. А отримавши його, зловмисник легко пройде автентифікацію під ім'ям власника пароля.

У сімейство протоколів по процедурі перевірки "запит-відповідь" входить кілька протоколів, які дозволяють виконати автентифікацію користувача без передачі інформації по мережі. До протоколів сімейства "запит-відповідь" відноситься, наприклад, один з найбільш поширених - протокол CHAP (Challenge-Handshake Authentication Protocol.

Автентифікуючою інформацією в даному випадку служить ключ, на якому виконується шифрування випадкового числа. Даний ключ ніколи не передається по мережі, а лише бере участь в обчисленнях, що становить безперечну перевагу протоколів даного сімейства.

Процедура перевірки включає як мінімум чотири кроки:

- користувач посилає серверу запит на доступ, що включає його логін;
- сервер генерує випадкове число і відправляє його користувачеві;
- користувач шифрує отримане випадкове число симетричним алгоритмом шифрування на своєму унікальному ключі, результат шифрування відправляється до сервера;
- сервер розшифровує отриману інформацію на тому ж ключі і порівнює з вихідним випадковим числом. При збігу чисел користувач вважається успішно автентифікованим, оскільки визнається власником унікального секретного ключа.

Основний недолік подібних систем автентифікації - необхідність мати на локальному комп'ютері клієнтський модуль, що виконує шифрування.

Протоколи типу "запит-відповідь" легко "розширюються" до схеми взаємної аутентифікації. В цьому випадку в запиті на автентифікацію користувач (крок 1) посилає своє випадкове число (N1). Сервер на кроці 2, крім свого випадкового числа (N2), повинен відправити ще й число N1, зашифроване відповідним ключем. Тоді перед виконанням кроку 3 користувач розшифровує його і перевіряє: збіг розшифрованого числа з N1 вказує, що сервер має необхідний секретний ключ, тобто це саме той сервер, який потрібен користувачу. Така процедура аутентифікації часто називається рукостисканням. Автентифікація буде успішна тільки в тому випадку, якщо користувач попередньо зареєструвався на даному сервері і будь-яким чином обмінявся з ним секретним ключем [22].

Основним міжнародним стандартом по криптографічним протоколам автентифікації є стандарт Міжнародної організації зі стандартизації та Міжнародної електротехнічної комісії ISO / IEC 9798 - Information technology - Security techniques - Entity authentication. Стандартом ISO / IEC 9798-2 передбачена взаємна автентифікація з використанням випадкових чисел.

Алгоритми шифрування поділяються на дві категорії, відомі як симетричне і асиметричне шифрування. Принципова відмінність між цими двома методами полягає в тому, що алгоритми симетричного шифрування використовують один ключ, в той час як асиметричні використовують два різних, але пов'язаних між собою ключа.

У той час як алгоритми симетричного шифрування використовують один і той же ключ для виконання цієї функції, алгоритм асиметричного шифрування навпаки, використовує один ключ для шифрування даних та інший для його дешифрування. В асиметричних системах ключ, який використовується для шифрування відомий як відкритий (публічний), може вільно передаватися іншим

користувачам. З іншого боку, ключ, який використовується для розшифровки є приватним і повинен зберігатися в секреті.

Основний недолік симетричного шифрування є необхідність передачі ключів "з рук в руки". Цей недолік дуже серйозний, оскільки унеможливлює використання симетричного шифрування в системах з необмеженим числом учасників. Однак в іншому симетричне шифрування має лише переваги, які добре видно на тлі серйозних недоліків шифрування асиметричного.

До недоліків асиметричного шифрування можна віднести низьку швидкість виконання операцій шифрування і розшифрування, обумовлену наявністю ресурсномістких операцій. Зайві труднощі створює і необхідність захисту відкритих ключів від підміни - підмінивши відкритий ключ легального користувача, зловмисник зможе забезпечити шифрування важливого повідомлення на своєму відкритому ключі і згодом легко розшифрувати його своїм секретним ключем. У свою чергу, асиметричне шифрування вирішує проблему розподілу ключів, використовуючи відкриті ключі для шифрування, а приватні для дешифрування. Компроміс полягає в тому, що асиметричні системи дуже повільні в порівнянні з симетричними і вимагають набагато більшої обчислювальної потужності через довжину ключа [23].

Розроблюваний пристрій для виконання обчислювальних операцій використовує центральний процесор, який має малу обчислювальну потужність. Тому доцільно використовувати симетричне шифрування з використанням одного секретного ключа.

Для взаємної автентифікації між ППКЗН и АС було обрано протокол рукостискання. У якості функції шифрування доцільно використовувати алгоритм симетричного шифрування.

При первинному підключенні flash-носія до системи необхідно пройти процедуру ініціалізації. Для цього АС отримує від ППКЗН ідентифікатор flash-носія та генерує для нього секретний ключ. АС зберігає ключ в базі даних та

передає пару ідентифікатор та секретний ключ до пристрою, які зберігаються у захищеній пам'яті ППКЗН.

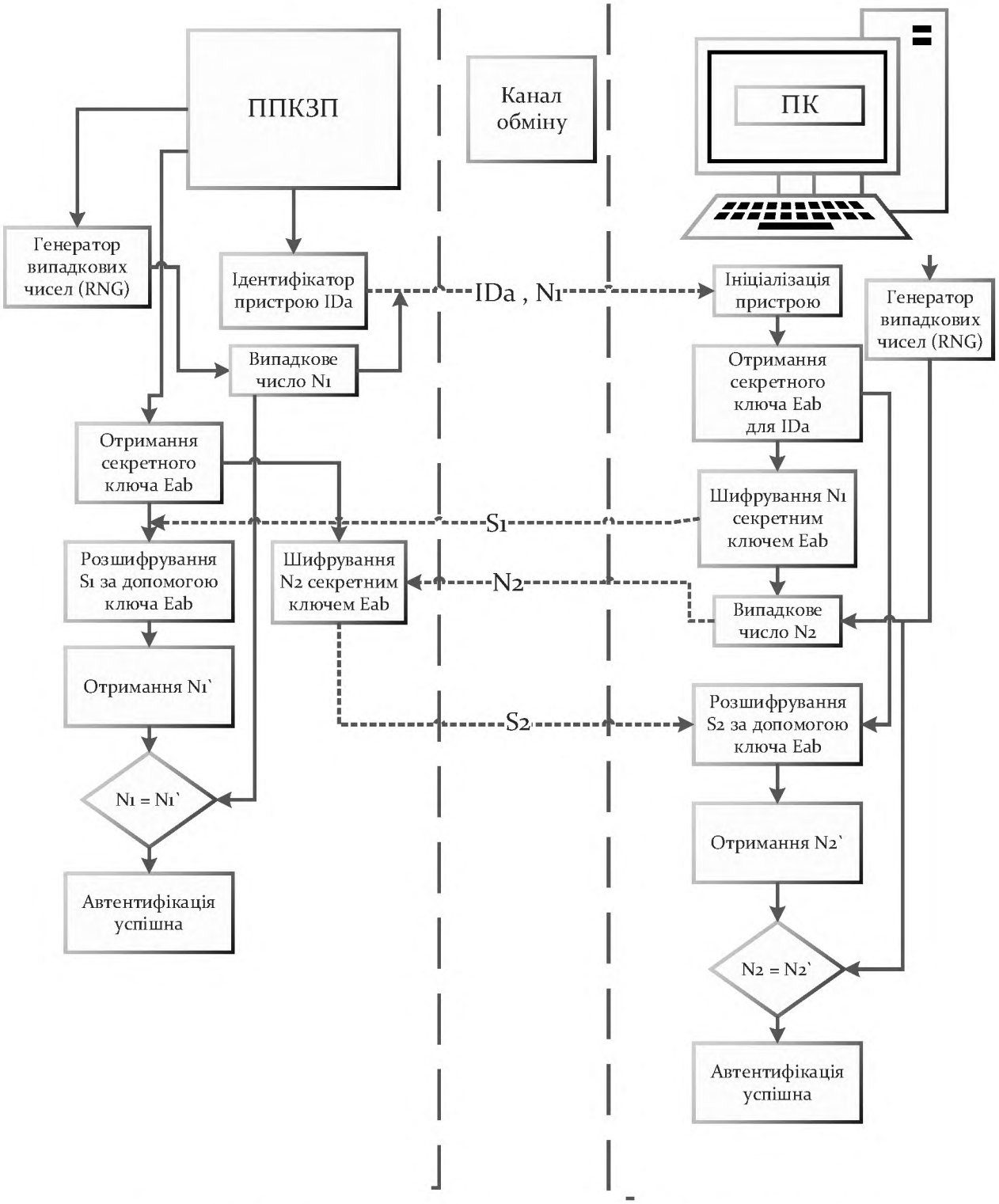


Рисунок 2.4 – Схема взаємної автентифікації ППКЗП та АС

Для автентифікації (Рис.2.4) ППКЗН надсилає до АС ідентифікатор flash-носія, який підключений до пристрою. АС перевіряє, чи ініціалізовано даний носій. Якщо пристрій пройшов попередню процедуру ініціалізації, АС знаходить секретний ключ, що відповідає ідентифікатору flash-носія.

Далі ППКЗН генерує випадкове число та надсилає АС. АС зашифровує отримане число та генерує інше випадкове число та надсилає їх до ППКЗН. ППКЗН розшифровує перше отримане значення та перевіряє: якщо сгенероване та отримане значення співпадають, то АС автентифікована успішно. Також ППКЗН зашифровує отримане від АС число та надсилає до АС зашифроване значення. АС розшифровує повідомлення та перевіряє отримане значення з тим, яке випадково було сгенеровано. Якщо значення співпали, то ППКЗН успішно автентифікована в АС.

2.2.4 Алгоритм роботи пристрою з flash-носієм та з автоматизованою системою

Розглянемо принцип роботи пристрою (Рис.2.5). При підключенні ППКЗП до ПК подається живлення, пристрій вмикається. В локальному журналі подій робиться запис про увімкнення пристрою. У центральний процесор завантажується програма для ініціалізації flash-носія.

Пристрій має два режими роботи:

- технологічний – режим, в якому може працювати лише адміністратор безпеки для реєстрації та ініціалізації flash-носіїв в ППКЗП;
- робочій – режим, в якому працюють користувачі flash-носіїв.

Програма визначає в якому режимі працює пристрій: у технологічному режимі або в робочому. Якщо встановлено технологічний режим, запускається підпрограма ініціалізації flash-носія. Якщо встановлено робочій режим, виконується підпрограма перевірки носія.

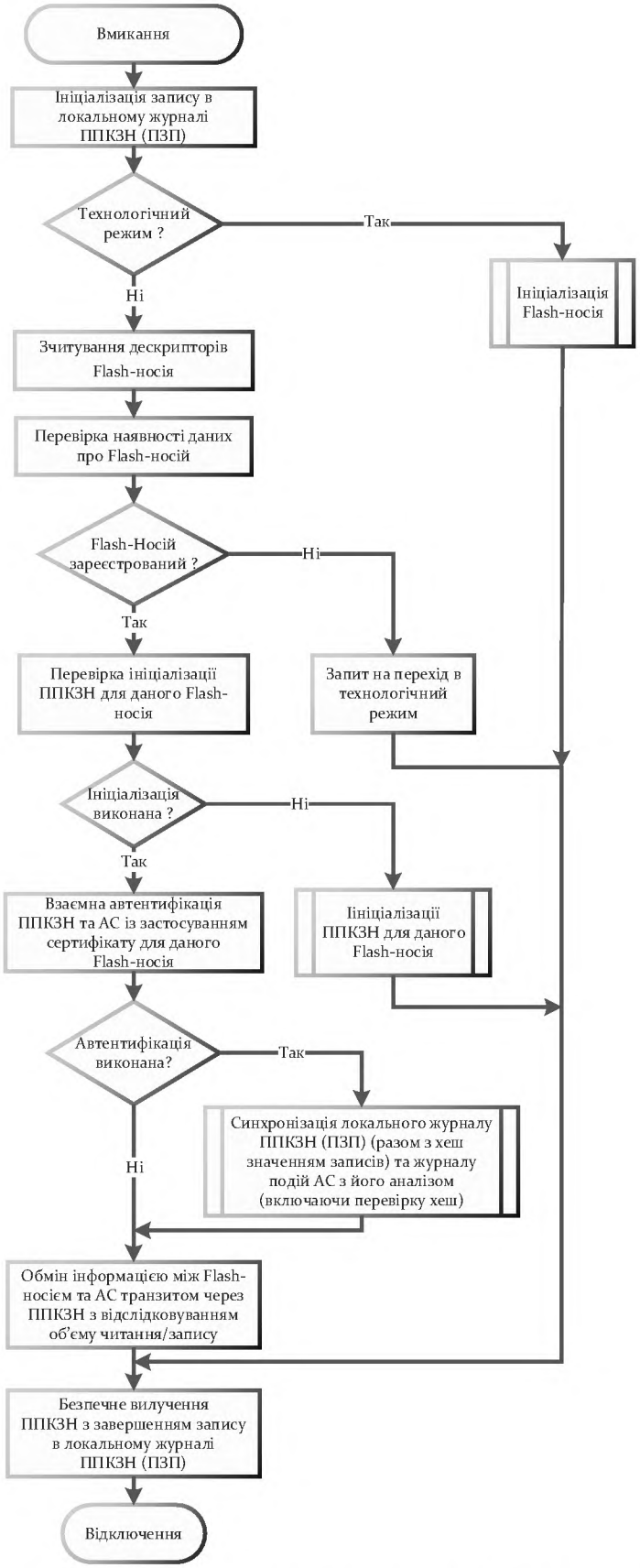


Рисунок 2.5 – Загальна блок-схема алгоритму роботи ППКЗН

Робочій режим

Для перевірки з підключеного flash-носія зчитуються внутрішні дескриптори, з яких генерується хеш-значення. Отриманий хеш порівнюється з тими, які записані у пам'яті пристрою. Якщо хеш-значення flash-носія не знайдено, то пристрій протоколює у локальному журналі подію, використовуючи час підключення та отриманий хеш носія та завершує роботу. Якщо хеш знайдено, то носій зареєстрований і має доступ до роботи з пристроєм.

Після того, як flash-носій перевірено, необхідно ініціалізувати його. Для цього здійснюється перевірка сертифікату автентифікації з системою. Якщо сертифікатів немає, в журналі пристрою виконується запис події, на ПК виводиться попередження, що необхідно провести ініціалізацію flash-носія. Для цього необхідно звернутися до адміністратора КЗЗ. Після того, як повідомлення закрили, пристрій завершує роботу.

Якщо для підключеного носія знайдено сертифікат, пристрій переходить до процесу взаємної автентифікації з АС, до якої він підключений. Далі встановлюється зв'язок із системою для перевірки сертифікату. Якщо автентифікація виконана успішно, це свідчить про те, що пристрій підключено до довіреної системи.

Усі обміни даними проходять через пристрій та протоколюються в журналі ППКЗП. Запис містить у собі час події, ідентифікатор носія, подію, об'єм даних та хеш, які оброблялися. Після того, як користувач завершує роботу з носієм, у журналі робиться запис про завершення сеансу з відзначенням часу. Пристрій витягується з блоку ПК та вимикається.

Після успішної автентифікації з АС завантажується з пристрою локальний журнал подій, відбувається звірення подій в журналі пристрою та в журналі АС (Рис.2.6). У журналі ППКЗП визначається кількість записів. Кількість записів в локальному журналі фіксована і може мати не більше 100 записів. Якщо журнал переповнено, необхідно, щоб адміністратор безпеки його очистив. Далі

проходить перевірка на співпадіння кожного запису. Якщо усі записи співпадають, то flash-носій готовий до роботи, користувачу доступна можливість обміну даними між АС та носієм.

У випадку, коли в результаті аналізу журналів подій записи не співпали, на ПК виводиться повідомлення про те, що були несанкціоновані підключення або некоректне завершення роботи. В такому разі необхідно запросити адміністратора безпеки для розслідування подій, які не зареєстровані в журналі системи. Після проведення розслідування адміністратор безпеки очищує в локальному журналі ППКЗН події та пристрій знову готовий до роботи.

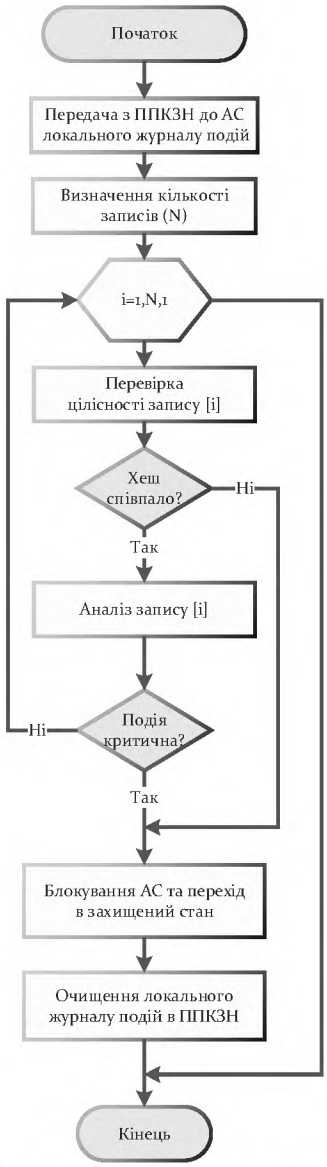


Рисунок 2.6 – Блок-схема алгоритму перевірки подій в журналі ППКЗН

Якщо під час запиту на взаємну автентифікацію система не відповідає, це свідчить про те, що в системі не реалізовано фунціонал взаємної автентифікації з пристроєм. Оскільки usb-flash-носій можна використовувати в інших системах, пристрій надає доступ для обміну даними з неавтентифікованою системою. При цьому в локальному журналі подій робиться запис з інформацією про час підключення, подіями, які відбувалися в системі та даними про інформацію, яка передавалася з носія до системи та навпаки. Після завершення роботи з носієм, в журналі робиться запис з часом завершення та пристрій вимикається.

Технологічний режим

У технологічному режимі працює адміністратор безпеки. Він проводить реєстрацію flash-носію у пристрої. Після того, як пристрій приєднано до ПК та включено, адміністратор натискає кнопку тим самим вмикаючи технологічний режим. Далі вмикає flash-носії до пристрою. Програма зчитує дескриптори підключеного носія та генерує з них хеш-значення. Отриманий хеш записується у ПЗП пристрою. Процес реєстрації носія завершено.

Також у технологічному режимі може працювати адміністратор КЗЗ. Після того, як адміністратор безпеки провів реєстрацію носія у пристрої, пристрій та flash-носій опечатуються та передаються адміністратору КЗЗ. Він, в свою чергу, проводить ініціалізацію flash-носія в АС (Рис.2.7). В з ППКЗН надсилається ідентифікатор підключеного носія до АС. Система генерує секретній ключ для АС та секретний ключ для пристрою. Ці дані є сертифікатом автентифікації, вони передаються до пристрою. А в АС зберігається ідентифікатор носія та секретній ключ АС.

Після формування секретних ключів відбувається процес взаємної автентифікації між пристроєм та АС та процес ініціалізації завершується. Якщо автентифікація виконана успішно, сертифікат записується в захищену пам'ять пристрою. Якщо сталася якась помилка, виводиться повідомлення про помилку та пристрій завершує роботу.

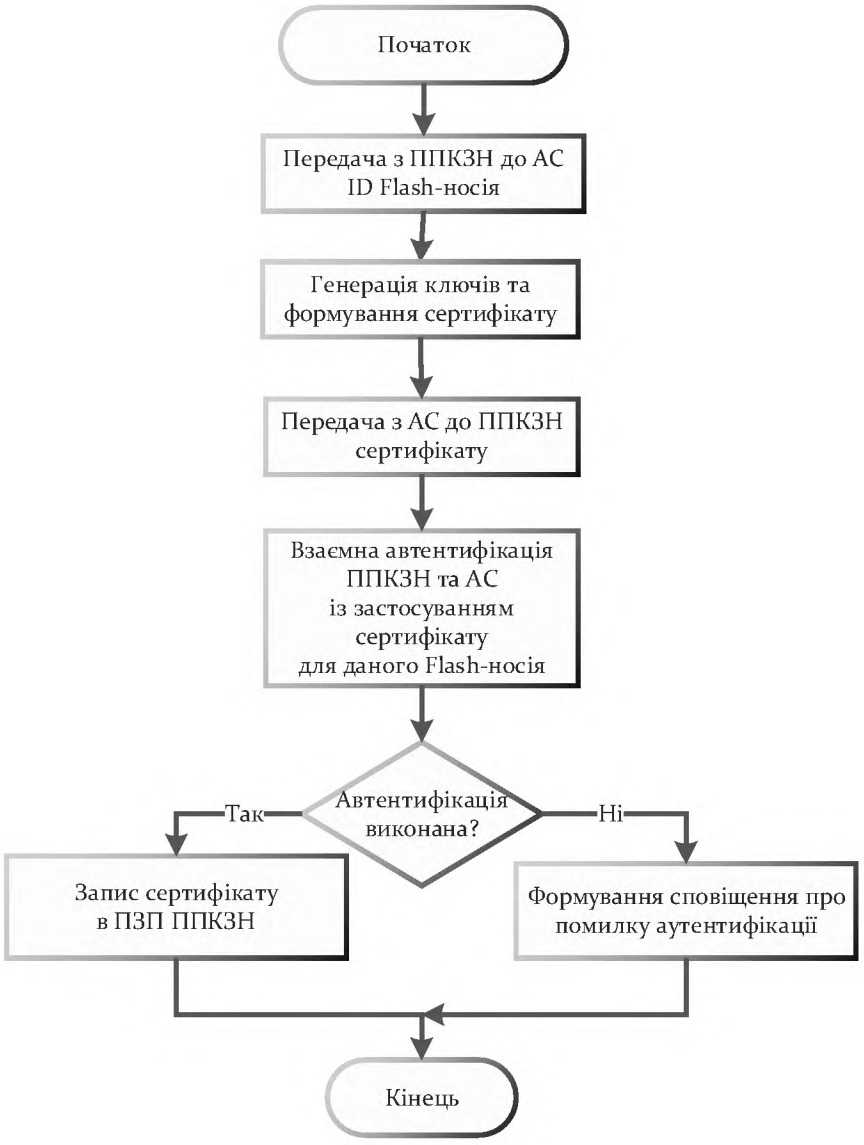


Рисунок 2.7 – Блок-схема алгоритму ініціалізації ППКЗН

2.2.5 Обґрунтування вибору програмно-апаратних засобів для створення пристрою для посиленої ідентифікації flash-носіїв

Для реалізації апаратної частини пристрою необхідно обрати мікроконтроллер, який у своєму складі має усі перелічені у пункті 2.2.3 компоненти.

Мікроконтролер - маленький за габаритами, не надто швидкий комп'ютер, з обмеженим розміром оперативної пам'яті, невисокою тактовою частотою, малої розрядністю оброблюваних команд. Зазвичай він являє собою 8 бітний RISC

процесор, розташований на одному чіпі з системами введення-виведення, оперативної та перепрограммируемой пам'яттю.

Маючи досить скромні можливостями обробки інформації, вони, тим не менш, дозволяють повністю покрити весь обсяг необхідного контролю обладнання. При цьому їх більш низька ціна, мінімальне енергоспоживання, пасивне охолодження, крихітні розміри, порівняно з «великими» комп'ютерами, - пріоритетний плюс в даній області застосування.

Найкращим вибором для реалізації ППКЗП є мікроконтроллер ATMega2560 фірми ATMel.

Мікроконтролер представлений RISC процесором, розробленим AVR і функціонуючим на частоті 16Мгц, яка максимальна зі всієї лінійки продуктів ATMel. На кристалі його чіпа розташовані всі пристрої, що відносяться до загального поняття комп'ютерної системи: оперативна і перепрограмувальна постійна, а також flash пам'ять, інтерфейсні мости, умножитель.

Процесор характеризується, як обчислювач одного за часом відгуку, на виконання будь-якої команди, незалежно від її складності. Розрядність шини адрес і внутрішніх регістрів - 8 біт. Максимальний розмір підключається, зовнішньої пам'яті SRAM - 64 Кбайт. Генератор тактової частоти знаходиться в складі самої мікросхеми контролера.

Найбільші плюси ATMega2560 порівняно з моделями контролерів інших виробників - це універсальність, відпрацьована система розробки коду процесора Arduino IDE, документованість можливостей, наявність модулів розширення. У Додатку В наведено технічні характеристики обраного мікроконтролера.

2.3 Розробка прототипу ППКЗП на базі апаратно-програмних засобів Arduino

Перед тим, як реалізовувати ППКЗП, необхідно протесувати роботу функцій, які він повинен виконувати. Для цього можливо використовувати готові програмно-апаратні рішення, які містять усі необхідні елементи для реалізації. На сучасному ринку існують різні варіанти готових контролерів. Найпопулярнішими з них є продукти, розроблені компанією Arduino.

Arduino - це апаратна обчислювальна платформа для аматорського конструювання, основними компонентами якої є плата мікроконтролера з елементами вводу/виводу та середовище розробки Processing/Wiring на мові програмування, що є спрощеною підмножиною C/C++. Arduino може використовуватися як для створення автономних інтерактивних об'єктів, так і підключатися до програмного забезпечення, яке виконується на комп'ютері. Інформація про плату (рисунок друкованої плати, специфікації елементів, програмне забезпечення) знаходяться у відкритому доступі і можуть бути використані тими, хто воліє створювати плати власноруч.

Плата Arduino складається з мікроконтролера Atmel AVR, а також елементів обв’язки для програмування та інтеграції з іншими пристроями. На багатьох платах наявний лінійний стабілізатор напруги +5В або +3,3В. Тактування здійснюється на частоті 16 або 8 МГц кварцовим резонатором. У мікроконтролер записаний завантажувач (bootloader), тому зовнішній програматор не потрібен.

Інтегроване середовище розробки Arduino це багатоплатформовий додаток на Java, що включає в себе редактор коду, компілятор і модуль передачі прошивки в плату. Середовище розробки засноване на мові програмування Processing та спроектоване для програмування новачками, не знайомими близько з розробкою програмного забезпечення. Мова програмування аналогічна мові

Wiring. Загалом, це C++, доповнений деякими бібліотеками. Програми обробляються за допомогою препроцесора, а потім компілюються [24].

Існує кілька версій платформ Arduino. Для створення пристрою найбільш підходить Arduino Mega ADK. Це версія стандартної плати Mega 2560 з підтримкою USB-host інтерфейсу для зв'язку з телефонами на Android і іншими пристроями з USB інтерфейсом [25]. USB Host інтерфейс реалізований на мікросхемі MAX3421e. Також як Mega 2560 плата має 54 цифрових входу / виходів (14 з яких можуть використовуватися як виходи ШІМ), 16 аналогових входів, 4 послідовних порту UART, кварцовий генератор 16 МГц, USB коннектор, роз'єм живлення, роз'єм ICSP і кнопку перезавантаження.

Хоча платформа має багато непотрібних для реалізації пристрою модулів, проте це не завадить зробити прототип. Тому далі розробка прототипу буде виконуватися на платі Arduino Mega ADK.

2.3.1 Реалізація прототипу пристрою

Розроблений прототип пристрою частково реалізує функціональні можливості ППКЗП. Прототип виконує функцію ініціалізації підключеного flash-носія. Листінг програми наведено у Додатку Г. Функціональна схема прототипу представлена на Рисунку 2.8.

Прототип складається з плати Adruino Mega ADK на базу мікроконтролеру ATMega2560, до якої підключені кнопка та світлодіоди. Світлодіоди підключені через опори номіналом 220 Ом та слугують для індикації стану роботи пристрою: синій світлодіод індикує режим, в якому працює пристрій (технологічний – світлодіод горить, робочій – вимкнений), RGB сітлодіод індикує статус підключення flash-носія. Кнопка підключена через опір номаналом 10 кОм та використовується для вмикання та вимикання технологічного режиму. Додаткові компоненті розміщені на макетній платі.

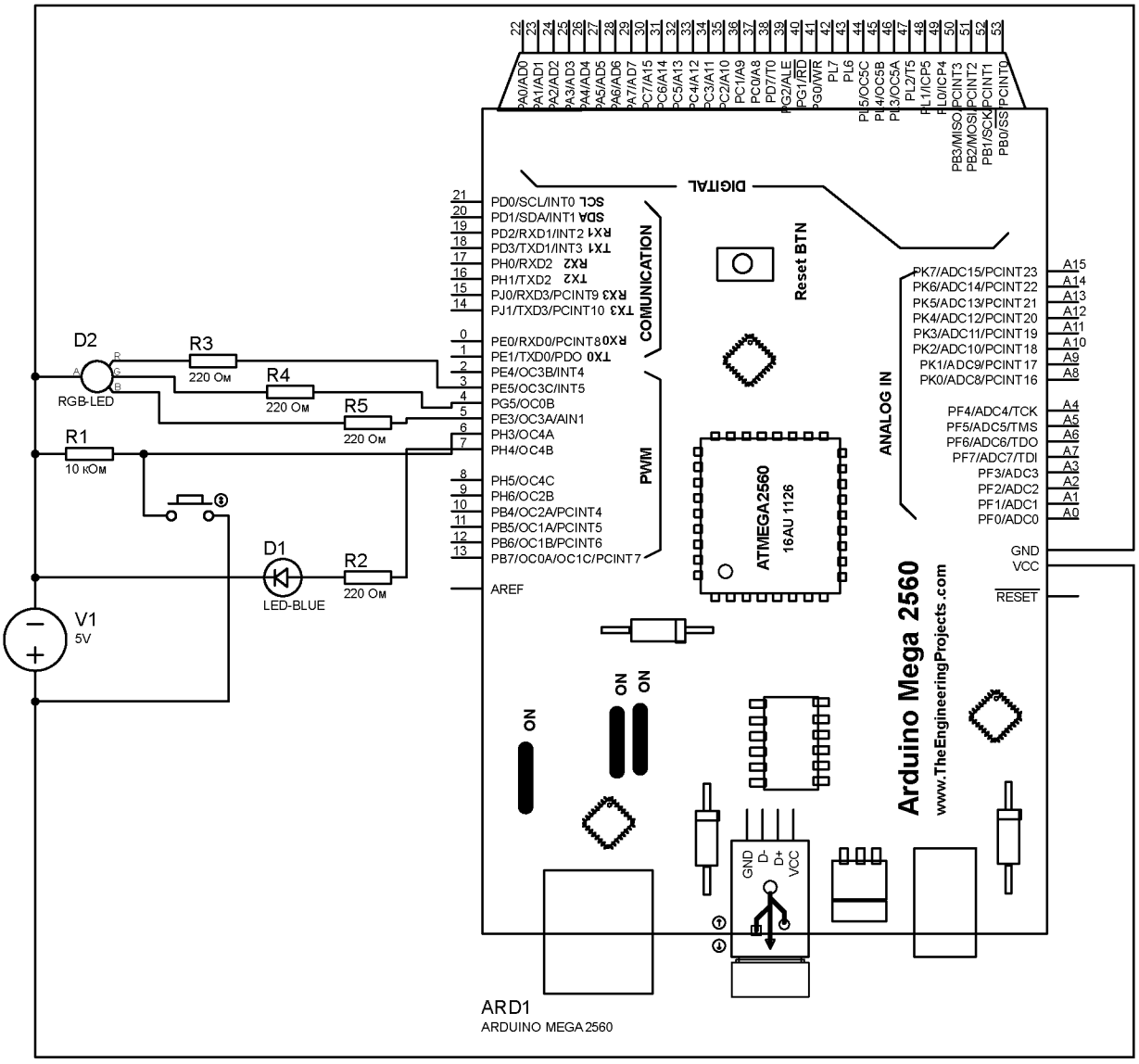


Рисунок 2.8 – Функціональна схема ППКЗН

Алгоритм роботи пристрою представлено на рисунку 2.9.

1. Підключаємо прошитий пристрій до ПК з ОС Windows до USB-порту, з якого буде надаватися живлення;

2. Програма завантажується з внутрішньої FLASH-пам’яті пристрою до RAM;

3. Програма постійно у циклі проводить опитування USB-порту вбудованого у плату Arduino USB-host пристрою, якщо знімний носій не підключений, програма фіксує цей статус у змінній current_state и приймає значення 12;

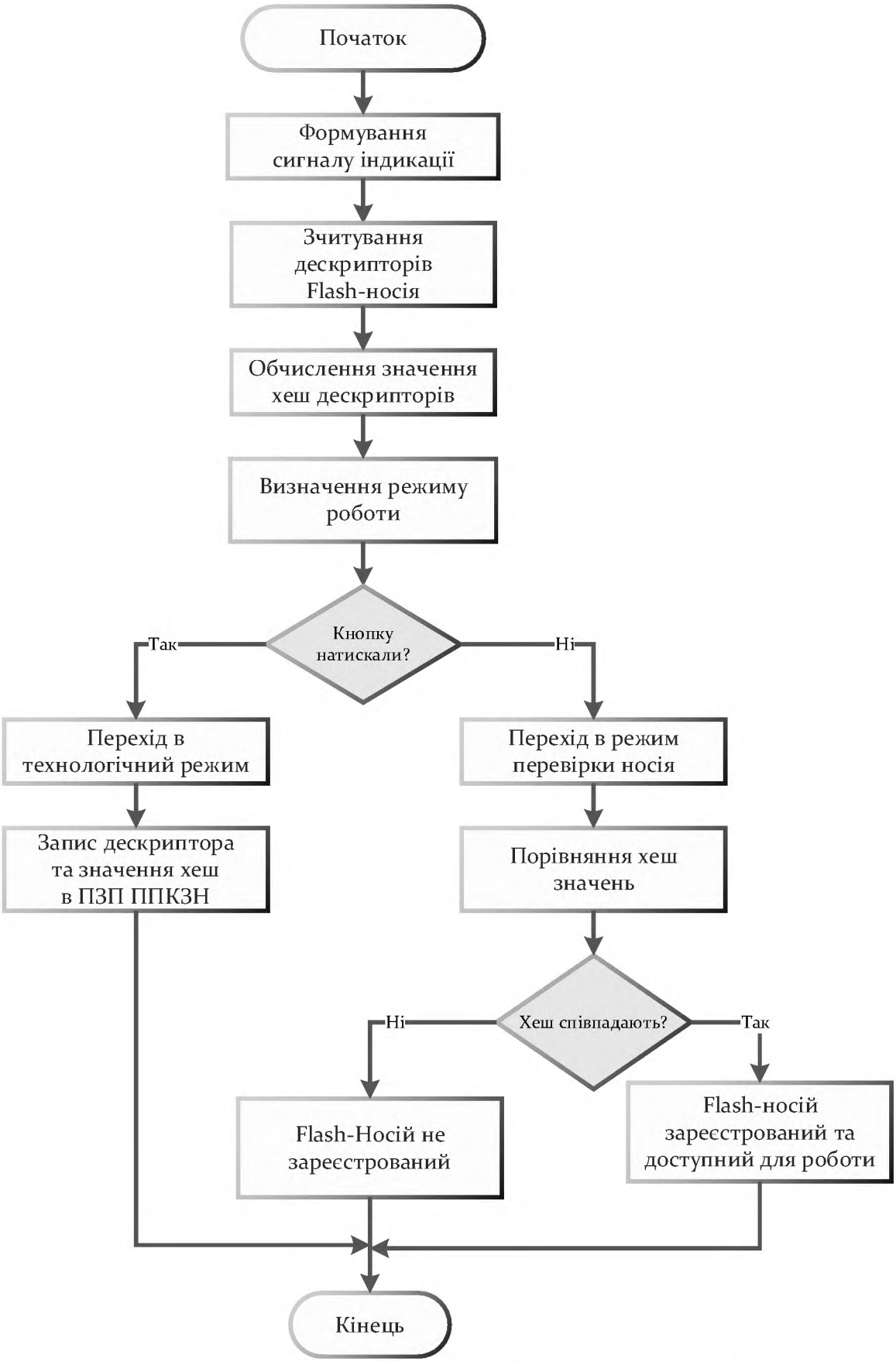


Рисунок 2.9 – Блок-схема алгоритму ініціалізації flash-носія

4. При натисканні кнопки змінній isAdmin присвоюється значення true і пристрій переходить у технологічний режим, це супроводжується загорянням синього LED діоду;

5. При підключенні змінного носія програма проводить процедуру його ідентифікації, це супроводжується загорянням LED RGB-діоду (колір Magenta);

6. Після ідентифікації змінного носія програма проводить зчитування параметрів носія (VID, PID, серійний номер та кількість фізичних секторів носія), генерації hash-строки на основі цих параметрів і записує цю строку у RAM у змінну hash, після чого LED RGB-діод загоряється зеленим кольором;

7. При натисканні на кнопку програма переходить із технологічного режиму у режим користувача, це супроводжується вимиканням синього LED діоду. При відсутності носія (зйомна FLASH-пам'ять) у USB-порті пристрою LED RGB-діоду вимкнений. У цьому режимі при подальшому підключенні носія проходить його ідентифікація, зчитування його вишезгаданих параметрів, генерація hash-строки на основі цих параметрів та зрівняння цієї строки зі значенням змінної hash (це також супроводжується загорянням LED RGB-діоду (колір Magenta));

8. Якщо значення hash-строки та значення змінної hash співпадають, LED RGB-діод загоряється зеленим кольором (користувач пройшов аутентіфікацію);

9. Якщо значення hash-строки та значення змінної hash не співпадають, LED RGB-діод загоряється красним кольором (користувач не пройшов аутентіфікацію).

2.4 Висновок до другого розділу

У другому розділі були проаналізовані варіанти протидії несанкціонованим діям при використанні зовнішніх носіїв та зроблено висновок, що існуючих методів недостатньо для захисту інформації від витоків через flash-носії.

Виходячи з результатів аналізу було зроблено висновок, що необхідно розробити методику захисту інформації від несанкціонованих дій при використанні зовнішніх flash-носіїв. Для реалізації завдань методики було запропоновано програмно-апаратне рішення у вигляді пристрою посиленого контролю зовнішніх носіїв.

За рахунок ведення журналу подій, який реалізує розроблений пристрій, забезпечується контроль підключень зовнішніх носіїв до АС. Таким чином вирішена проблема неконтрольованих дій користувачів з зовнішніми носіями.

Для опрацювання деяких функцій пристрою було розроблено прототип на базі програмно-апаратного комплексу Arduino Mega ADK, який частково реалізує функціонал методики. Робота прототипу успішно виконує реєстрацію usb-flash-носія у пристрої в технологічному режимі роботи та демонструє неможливість підключення flash-носія, який не зареєстровано у пристрої.

Запропоноване рішення може бути додатком до існуючих комплексів засобів захисту, що посилить захист витоку інформації з обмеженим доступом від несанкціонованих дій користувачів АС.

3 ЕКОНОМІЧНА ЧАСТИНА

Застосування знімних flash-носіїв є невід'ємною частиною роботи користувачів автоматизованих систем при роботі з інформацією з обмеженим доступом. Тому необхідно забезпечити додатковий захист від витоку ІзОД при використанні зовнішніх носіїв, які не обліковані в РСО. Для цього необхідно впровадити додатковий USB-модуль, який однозначно визначає знімний носій, який до нього підключається. Таке рішення забезпечить посилений захист інформації від несанкціонованих дій користувачів в системі при роботі з зовнішніми носіями.

В даному розділі проводяться економічні розрахунки витрат на розробку та технічну реалізацію методу ідентифікації USB-flash-носія. Розробка нового методу дозволить зменшити ризик втрати та компрометації даних з обмеженим доступом від несанкціонованого використання сторонніх зовнішніх носіїв, що в свою чергу має зменшити вірогідність збитків від втрати або розповсюдження ІзОД.

3.1 Визначення трудомісткості розробки методики захисту

Трудомісткість розробки методики захисту інформації від несанкціонованих дій користувачів при використанні зовнішніх flash-носіїв визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання (ТЗ) і закінчуючи оформленням документації (за умови роботи одного оператора).

Трудомісткість розробки й дослідження можна розрахувати за формулою:

$$t = t_{тз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{Д}\text{, годин,} \qquad (3.1)$$

де $t_{тз}$ – тривалість складання технічної документації та алгоритмів;

$t_{в}$ – тривалість вивчення ТЗ, літературних джерел за темою;

$t_{а}$ – тривалість розробки блок-схеми алгоритму;

$t_{пр}$ – тривалість розробки апаратної частини та програмування пристою за готовою блок-схемою;

$t_{опр}$ – тривалість опрацювання методики на ПК;

$t_д$ – тривалість підготовки технічної документації.

Для обчислення трудомісткості розробки необхідно визначити умовну кількість операторів Q, які примають участь у розробці методики.

Умовна кількість операторів:

$$Q = q*c*(1+p), \text{ штук,} \quad (3.2)$$

де q – очікувана кількість операторів;

c – коефіцієнт складності розроблення методики;

p – коефіцієнт корекції методів в процесі їх опрацювання.

Коефіцієнт складності розробки методики ***c*** визначає відносну складність виконання щодо типового завдання, складність якого дорівнює одиниці. Діапазон його зміни – 1,25…2,0. Коефіцієнт корекції рекомендацій ***p*** береться з діапазону 0,05...0,1, що відповідає внесенню 3...5 корекцій і переробці 5-10% готової програми.

Розрахуємо цей показник, припускаючи, що коефіцієнт складності c=1,6, а коефіцієнт рекомендацій p=0,06. Також припустимо, що для початкової розробки необхідно 20 осіб: 2 менеджера по проекту, 2 спеціалісти з інформаційної безпеки, 2 інженери-електроніки, 10 розробників, 1 системний адміністратор та 3 тестувальника.

$$Q = 20*1,6*(1+0,06) = 34 \text{ особи}$$

Тривалість складання технічної документації на розробку методики оцінемо у 80 годин.

Тривалість вивчення технічного завдання, опрацювання довідкової літератури з урахуванням уточнення ТЗ і кваліфікацію виконавця оцінюється за формулою:

$$t_в = \frac{Q \cdot B}{(75...85) \cdot k}, \text{ годин,} \quad (3.3)$$

у якій B – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання. B = 1,2...1,5;

k – коефіцієнт, що враховує кваліфікацію виконавця і визначається стажем роботи за фахом.

Для розробки даної методики припустимо, що коефіцієнт B = 1,3, а коефіцієнт, що враховує кваліфікацію виконавця візьмемо як k = 1,1, що відповідає 3-річному стажу роботи виконавця.

Тоді, за формулою 3.3, розрахуємо тривалість вичення ТЗ:

$$t_{\text{в}} = \frac{34*1,3}{80*1,1} = \frac{44,2}{88} = 0,5, \text{ годин}$$

Тривалість розробки блок-схеми алгоритму розраховується за наступною формулою:

$$t_{\text{а}} = \frac{Q}{(20...25)*k}, \text{ годин} \quad (3.4)$$

Оскільки в розробці методики приймають участь виконавці різної спеціалізації з різною кваліфікацією, розрахуємо за формулою 3.4 тривалість розробки блок-схеми алгоритму t_a для окремих груп.

Менеджери зі стажем роботи 2 роки (коефіцієнт k=1):

$$t_{\text{а,м}} = \frac{3}{22*1} = 0,14 \text{ , годин}$$

У розробці блок-схеми алгоритму роботи повинні приймати участь розробники вищої кваліфікації, які мають стаж роботи 6 років. Тому для розрахунку тривалості виконання цього етапу роботи програмістами коефіцієнт k = 1,35.

$$t_{\text{а,р}} = \frac{27}{22*1,35} = 0,9 \text{ , годин}$$

Припустимо, що у розробці тест-кейсів для тестування методики прийматимуть участь тестувальники зі стажем роботи 4 роки (коефіцієнт k=1,2):

$$t_{\text{а,т}} = \frac{4}{22*1,2} = 0,15 \text{ , годин}$$

Тоді загальна тривалість виконання блок-схеми дорівнює:

$$t_{\text{а}} = t_{\text{а,м}} + t_{\text{а,р}} + t_{\text{а,т}}, \text{ годин} \quad (3.5)$$

$$t_{\text{а}} = 0{,}14 + 0{,}9 + 0{,}15 = 1{,}2, \text{ годин}$$

Тривалість створення програми за готовою блок-схемою розраховується за формулою:

$$t_{\text{пр}} = \frac{Q}{(20...25)*k}, \text{ годин} \quad (3.6)$$

У створенні програми приймають участь розробники та тестувальники, тому розрахуємо це значення окремо для кожної групи:

$$t_{\text{пр,р}} = \frac{27}{22*1{,}35} = 0{,}9, \text{ годин}$$

$$t_{\text{пр,т}} = \frac{4}{22*1{,}2} = 0{,}2, \text{ годин}$$

Загальна тривалість створення програми за готовою блок-схемою складає:

$$t_{\text{пр}} = t_{\text{пр,р}} + t_{\text{пр,т}} = 0{,}9 + 0{,}2 = 1{,}1, \text{ годин}$$

Тривалість опрацювання та тестування програми на ПК розраховується за наступною формулою:

$$t_{\text{опр}} = \frac{1{,}5*Q}{(4...5)*k}, \text{ годин} \quad (3.7)$$

$$t_{\text{опр,р}} = \frac{1{,}5*27}{4*1{,}35} = 7{,}5, \text{ годин}$$

$$t_{\text{опр,т}} = \frac{1{,}5*4}{4*1{,}2} = 1{,}3, \text{ годин}$$

$$t_{\text{опр}} = 7{,}5 + 1{,}3 = 8{,}8, \text{ годин}$$

Тривалість підготовки технічної документації розраховується також для кожної групи виконавців окремо за формулою:

$$t_{\text{д}} = \frac{Q}{(20...25)*k} + \frac{Q}{(20...25)*k} * 0{,}75, \text{ годин} \quad (3.8)$$

$$t_{\text{д,м}} = \frac{3}{22*1} + \frac{3}{22*1} * 0{,}75 = 0{,}14 + 0{,}1 = 0{,}24, \text{ годин}$$

$$t_{\text{д,р}} = \frac{27}{22*1{,}35} + \frac{27}{22*1{,}35} * 0{,}75 = 0{,}9 + 0{,}68 = 1{,}58, \text{ годин}$$

$$t_{\text{д,т}} = \frac{4}{22*1{,}2} + \frac{4}{22*1{,}2} * 0{,}75 = 0{,}15 + 0{,}11 = 0{,}26, \text{ годин}$$

$$t_{\text{д}} = 0{,}24 + 1{,}58 + 0{,}26 = 2{,}1, \text{ годин}$$

У таблиці 3.1 визначена тривалість виконання кожного етапу розробки методики.

Таблиця 3.1.

Змінна	Назва процесу	Тривалість, год.
$t_{тз}$	Складання технічної документації для розробки методики захисту інформації	80
$t_{в}$	Вивчення ТЗ, літературних джерел про роботу та процес реєстрації знімних носіїв в комплексах засобів захисту	0,5
$t_{а}$	Розробка блок-схеми алгоритму роботи розробленої методики	1,2
$t_{пр}$	Програмування апаратного пристрою за готовою блок-схемою	1,1
$t_{опр}$	Опрацювання роботи пристрою на ПК	8,8
$t_{д}$	Підготовка технічної документації та оцінка стану захищеності інформації при використанні сторонніх знімних flash-носіїв в захищеній системі	2,1

Отже, виходячи з отриманих даних, загальна трудомісткість виконання роботи:

$$t = 80 + 0{,}5 + 1{,}2 + 1{,}1 + 8{,}8 + 2{,}1 = 94 \text{ , години}$$

3.2 Розрахунок витрат на впровадження методики

Витрати на створення програмного продукту $К_{пз}$ складаються з витрат на заробітну плату виконавця програмного забезпечення $З_{зп}$ і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК $З_{мч}$:

$$К_{пз} = З_{зп} + З_{мч} \quad (3.9)$$

Заробітна плата виконавців враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби, визначається за формулою:

$$З_{зп} = t * З_{пр}\text{ , грн.} \quad (3.10)$$

де t – загальна тривалість створення ПЗ, годин;

$З_{пр}$ - средньогодинна заробітна плата виконавця з нарахуваннями, грн/годину.

Оскільки розробка методики буде виконуватися в межах України, де нормована тривалість робочого тижня не повинна перевищувати 40 годин, будемо вважати, що тривалість робочого дня – 8 годин. Проаналізувавши середні місячні заробітні плати проект-менеджерів, програмістів, спеціалістів з інформаційної безпеки, тестувальників, можемо розрахувати середньогодинну заробітну плату кожного виконавця за формулою:

$$З_{пр} = \frac{З_{см}}{20 * t_{дн}}\text{ , грн.} \quad (3.11)$$

де $З_{см}$ – середньомісячна заробітна плата робітника, гривень;

$t_{дн}$ – тривалість робочого дня.

За даними сайту пошуку роботи Work.ua середня місячна заробітна плата кожного виконавця методики складає:

- менеджер по проекту – 20000 грн.;
- спеціаліст з інформаційної безпеки – 15000 грн.;
- програміст C++ - 62500 грн.;
- системний адміністратор – 15000 грн.;
- інженер-електроник – 15500 грн.;
- тестувальник – 17500 грн.

Розрахуємо середньогодинну заробітну плату кожного виконавця:

$$З_{пр,м} = \frac{20000}{20*8} = 125\text{ , грн./год.}$$

$$З_{пр,іб} = \frac{15000}{20*8} = 93{,}75\text{ , грн./год.}$$

$$З_{пр,р} = \frac{62500}{20*8} = 390{,}63 \text{ , грн./год.}$$

$$З_{пр,са} = \frac{15000}{20*8} = 93{,}75 \text{ , грн./год.}$$

$$З_{пр,е} = \frac{15500}{20*8} = 96{,}88 \text{ , грн./год.}$$

$$З_{пр,т} = \frac{17500}{20*8} = 109{,}38 \text{ , грн./год.}$$

Розрахуємо заробітну плату кожного виконавця на розробку методики захисту:

$$З_{зп,м} = 125 * 94 = 11750 \text{ , грн.}$$

$$З_{зп,іб} = 93{,}75 * 94 = 8813 \text{ , грн.}$$

$$З_{зп,р} = 390{,}63 * 94 = 36719 \text{ , грн.}$$

$$З_{зп,са} = 93{,}75 * 94 = 8813 \text{ , грн.}$$

$$З_{зп,е} = 96{,}88 * 94 = 9107 \text{ , грн.}$$

$$З_{зп,т} = 109{,}38 * 94 = 10282 \text{ , грн.}$$

Отже, середня заробітна плата виконавця методики становить:

$$З_{зп} = \frac{З_{зп,м} + З_{зп,іб} + З_{зп,р} + З_{зп,са} + З_{зп,е} + З_{зп,т}}{6} =$$

$$= \frac{11750+8813+36719+8813+9107+10282}{6} = 14248 \text{ , грн.}$$

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = С_{мч} * t_{опр} + t_д, \text{ грн,} \qquad (3.12)$$

у якій $t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

В свою чергу, вартість 1 години машинного часу ПК визначається за формулою:

$$C_{мч} = P * C_e + \frac{Ф_{зал} + Н_а}{F_p} + \frac{К_{ліз} + Н_{аіз}}{F_p}, \text{ грн,} \qquad (3.13)$$

у якій Р – встановлена потужність ПК, кВт. Р = 1,5 кВт;

C_e – тариф на електричну енергію, грн/кВт·година. C_e = 1,68 грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу; $F_р$ = 1993 для 40-годинного робочого тижня.

Амортизація – це систематичне розподілення вартості основних засобів, яка амортизується протягом строку їх корисного використання (експлуатації).

Мінімально допустимий строк корисного використання $Т_а$ ПК складає 5 років, тобто річна норма амортизації не має перевищувати:

$$Н_а = \frac{1}{Т_а} \cdot 100\% \qquad (3.14)$$

$$Н_а = \frac{1}{5} \cdot 100\% = 20\%$$

Мінімальний строк дії права користування ліцензійним програмним забезпеченням складає не менш ніж 1 рік, тому $Н_{апз}$ не має перевищувати 100%.

Визначимо залишкову вартість одного ПК $Ф_{зал}$ як середньою вартість необхідних для розробки пристроїв, які зазначені у таблиці 3.2.

Таблиця 3.2

Кількість пристроїв	Назва пристрою	Специфікація	Вартість за пристрій
27	Ноутбук ASUS ZenBook 14 UX433FAC	Екран 14.0" IPS (1920x1080) Full HD, процесор Intel Core i7-10510U (1.8 - 4.9 ГГц), оперативна пам’ять RAM 16 ГБ, жорсткий диск SSD 1 ТБ, відеокарта Intel UHD Graphics 620	34000 грн.
Продовження таблиці на с.85			

Продовження таблиці 3.2			
Кількість пристроїв	Назва пристрою	Специфікація	Вартість за пристрій
4	Ноутбук HP Pavilion Notebook 15-cw1005ua	Екран 15.6” IPS (1920x1080) Full HD, процесор AMD Ryzen 5 3500U (2.1 - 3.7 ГГц), жорсткий диск RAM 16 ГБ, оперативна пам’ять SSD 512 ГБ, відеокарта AMD Radeon Vega 8	19500 грн.
3	ПК	Процесор Intel Core i5-10400F (2.9 - 4.3 ГГц), оперативна пам’ять RAM 16 ГБ, жорсткий диск SSD 1 ТБ, відеокарта nVIdia GeForce RTX 3060 Ti, 8 ГБ	40000 грн.
Загальна вартість			1116000 грн.

Загальна вартість $К_{аз}$ становить 1116000 грн. Середня балансова вартість ПК $Ф_{зал}$ становить 32824 тис. грн.

Розрахуємо вартість ліцензійного програмного забезпечення на один рік як загальну вартість таких ліцензій, які визначені у таблиці 3.3.

Таблиця 3.3

Назва програмного продукту	Вартість ліцензії на один рік, грн.
PHPStorm	56000 (5600) грн.
Windows 10 Pro license	204000 (6000) грн.
Microsoft Office Professional 2016 Plus	4000 (500) грн.
Програмний комплекс захисту інформації від несанкціонованого доступу "Гриф" версії 4	52000 (13000) грн.
Загальна вартість	316000 грн.

Таким чином, загальна вартість ліцензійного програмного забезпечення $К_{лпз}$ дорівнюється 316000 грн.

Оскільки маємо усі дані для розрахунків, визначимо вартість 1 години машинного часу пристроїв за формулою 3.13:

$$C_{\text{мч}} = 1{,}5 * 1{,}68 + \frac{32824*0{,}2}{1993} + \frac{316000*1}{1993} = 2{,}52 + 3{,}29 + 158{,}56 = 164{,}4 \text{ грн.}$$

Вартість машинного часу для розробки запропонованого методу:

$$З_{\text{мч}} = 164{,}4 * 8{,}8 + 2{,}1 = 1449 \text{ грн.}$$

Отже, вартість створення ПЗ Кпз є частиною одноразових капітальних витрат разом з витратами на придбання і налагодження апаратури системи захисту інформації дорівнює:

$$К_{\text{пз}} = 14248 + 1449 = 15697 \text{ грн.}$$

Капітальні (фіксовані) витрати на проектування та впровадження проектного рішення методики захисту інформації розраховується за формулою:

$$K = K_{\text{пр}} + K_{\text{зпз}} + K_{\text{пз}} + K_{\text{аз}} + K_{\text{н}}, \quad (3.15)$$

у якій $К_{\text{пр}}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, 10000 тис. грн;

$К_{\text{зпз}}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), 316000 тис. грн;

$К_{\text{пз}}$ – вартість створення основного й додаткового програмного забезпечення, 15697 тис. грн;

$К_{\text{аз}}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, 1116000 млн. грн;

$К_{\text{н}}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, 30000 тис. грн.

Таким чином, капітальні витрати складатимуть:

$$К = 10000 + 316000 + 15697 + 1116000 + 30000 = 1487697 \text{ млн.грн.}$$

3.3 Розрахунок експлуатаційних витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період, що виражені у грошовій формі.

Річні експлуатаційні витрати на функціонування методики складають:

$$С = С_в + С_к + С_{ак}\text{ , грн.} \quad (3.16)$$

у якій $С_в$ - витрати на оновлення ПЗ;

$С_к$ - витрати на керування системою;

$С_{ак}$ – витрати, викликані активністю користувачів методики захисту.

Витрати на керування системою ($С_к$) складають:

$$С_к = С_а + С_з + С_{єв} + С_{ел} + С_{тос}\text{ , грн.} \quad (3.17)$$

у якій:

$С_а$ - річний фонд амортизаційних відрахувань;

$С_з$ - річний фонд заробітної плати інженерно-технічного персоналу;

$С_{ел}$ - вартість електроенергії, що споживається апаратурою;

$С_{тос}$ - витрати на технічне й організаційне адміністрування;

$С_{єв}$ – єдиний внесок соціального страхування.

Річний фонд амортизаційних відрахувань визначається у відсотках від суми капітальних інвестицій, і дорівнює:

$$С_а = С_{а.аз} + С_{а.пз} = \frac{К_{аз}}{Та} + \frac{К_{зпз}}{Та} \quad (3.18)$$

$$С_{а,аз} = \frac{1116000}{5} = 223200 \text{ грн.}$$

$$С_{а,пз} = \frac{316000}{5} = 63200 \text{ грн.}$$

$$С_а = 223200 + 63200 = 286400 \text{ грн.}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод}\text{ , грн} \quad (3.19)$$

де $З_{осн}$, $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн на рік.

Основна заробітна плата визначається, виходячи з місячного посадового окладу $З_{зп}$, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

$$С_з = 14248 * 12 + (14248 * 0,1) * 12 = 188074 \text{ , грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_е$), визначається за формулою:

$$С_{ел} = Р * F_р * Ц_е \text{, грн.} \quad (3.20)$$

у якій Р – встановлена потужність апаратури; 1,5 кВт·годину;

$F_р$ – річний фонд робочого часу системи 1993;

$Ц_е$ – тариф на електроенергію - 1,68 грн/кВт·годину.

$$С_{ел} = 1,5 * 1993 * 1,68 = 5022, \text{ грн.}$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначається за даними організації або у відсотках від вартості капітальних витрат (1-3%).

$$С_{тос} = К * 0,02, \text{ грн.} \quad (3.21)$$

$$С_{тос} = 1487697 * 0,02 = 29754, \text{ грн.}$$

Єдиний внесок $С_{єв}$ згідно із Законом для платників, зазначених у підпункті 1 пункту 1 розділу II «Інструкції про порядок нарахування і сплати єдиного внеску на загальнообов'язкове державне соціальне страхування» [27], щодо кожної застрахованої особи встановлюється в розмірі 22 відсотків на суму нарахованої заробітної плати.

$$С_{єв} = С_з * 0,22, \text{ грн.} \quad (3.22)$$

$$С_{єв} = 188074 * 0,22 = 41376, \text{ грн.}$$

Розрахуємо витрати на керування системою за формулою 3.17:

$$С_к = 286400 + 188074 + 41376 + 5022 + 29754 = 550626 \text{ , грн.}$$

За статистичними даними моделі Gartner Group, наведеними в таблиці 1 [26], експлуатаційні витрати складають 79%, з яких 12% виділяється на керування системою $С_к$, 21% - на оновлення ПЗ $С_в$, 46% - на активність користувачів $С_{ак}$. Враховуючи ці дані отримуємо $С_в$ = 963596 грн., $С_{ак}$ = 2110733 грн.

Тоді експлуатаційні витрати складають:

$$С = 963595 + 550625 + 2110733 = 3624953 \text{ , грн.}$$

3.4 Оцінка величини можливого збитку

Для того, щоб оцінити величину збитку від витоку інформації, необхідно розглянути, через які види порушень можуть бути нанесені збитки. Оскільки методика спрямована на протидію внутрішнім порушенням, збитки можуть бути нанесені наступними порушеннями:

- порушення конфіденційності інформації за рахунок її копіювання на зовнішні носії та подальшого продажу або розповсюдження;
- порушення цілісності та доступності інформації через впровадження до системи шкідливого ПЗ, який може бути завантажений з незареєстрованого носія;
- порушення автентичності даних за рахунок підміни файлів на ті, які можна скопіювати з незареєстрованного зовнішнього носія.

Для розрахунку вартості збитку, що понесе типова компанія, при реалізації внутрішніх несанкціонованих дій, необхідно враховувати наступні дані:

tп – час простою вузла корпоративної мережі, у годинах;

tв – час, необхідний для відновлення системи, у годинах;

tві – час відновлення інформації, у годинах;

$З_0$ – заробітна платня обслуговуючого персоналу;

$З_с$ – заробітна платня співробітників атакованого вузла;

$Ч_0$ – чисельність обслуговуючого персоналу;

$Ч_с$ – чисельність співробітників атакованого вузла;

О – обсяг продажів атакованого вузла, у грн.;

П – вартість доопрацювання, модифікації програмного забезпечення чи апаратного устаткування;

І – число атакованих вузлів;

N – середнє число атак на рік.

Втрати від простою атакованого сегменту можна визначити за формулою:

$$U = П_П + П_В + V \quad (3.23)$$

де $П_п$ – оплачувані втрати робочого часу при простоях системи, у грн.;

$П_в$ – вартість відновлення системи (переустановлення, зміна налаштувань);

V – втрати від зниження обсягу продажів за час простою системи, у грн..

Для розрахунку витрат на оплату робочого часу при простоях системи використовується наступна формула:

$$П_п = \frac{\sum З_с}{F} * t_п \quad (3.24)$$

де F – місячний фонд робочого часу, що становить 176 год..

При кількості працівників атакованої системи, що становить 5 осіб, та середній заробітній платні у 15000 грн., маємо число витрат на оплату робочого часу при простоях системи складатимуть:

$$П_п = \frac{15000*5}{176} * 9 = 3835 \text{ , грн.}$$

Для розрахунку вартості відновлення системи використовується наступна формула:

$$П_в = П_{ві} + П_{пв} + П_{зч} \quad (3.25)$$

де $П_{ві}$ – витрати на повторне уведення інформації у систему, у грн.;

$П_{пв}$ – витрати на відновлення вузла системи, у грн.;

$П_{зч}$ – вартість доопрацювання та зміни в коді системи.

Витрати на повторне уведення інформації у систему розраховуються наступним чином:

$$П_{ві} = \frac{\sum З_с}{F} * t_{ві} \quad (3.26)$$

$$П_{ві} = \frac{15000*5}{176} * 8 = 3410 \text{ , грн.}$$

Витрати на відновлення вузла системи визначаються за формулою 3.27:

$$П_{пв} = \frac{\sum З_о}{F} * t_в \quad (3.27)$$

де $З_о$ – заробітна плата адміністратора, у грн.;

$t_в$ – час на відновлення системи.

$$П_{пв} = \frac{15000*5}{176} * 10 = 4262 \text{ , грн.}$$

Тоді вартість відновлення системи становить:

$$П_в = 3410 + 4262 + 5000 = 12672 \text{ , грн.}$$

Розрахуємо втрати від зниження обсягу продажів під час простою:

$$V = \frac{О}{F_г} * (t_п + t_в + t_{ві}) \quad (3.28)$$

де $F_г$ - річний фонд робочого часу роботи організації, $F_г$ = 2080 год..

$$V = \frac{4500000}{2080} * (9 + 10 + 8) = 58414, \text{ грн.}$$

Розрахуємо число упущеної вигоди внаслідок здійснення несанкціонованих дій за формулою 3.23:

$$U = 3835 + 12672 + 58414 = 74921 \text{ , грн.}$$

Розрахуємо загальний збиток від атаки на вузол або сегмент корпоративної мережі:

$$B = \sum i * \sum n * U \quad (3.29)$$

$$B = 12 * 10 * 74921 = 8990520 \text{ , грн.}$$

3.5 Розрахунок економічної ефективності

Термін окупності капітальних інвестицій $Т_о$ показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження підсистеми розмежування доступу:

$$Т_о = \frac{К}{Е} = \frac{1}{ROSI}, \text{ років} \quad (3.30)$$

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \quad (3.31)$$

у якій Е – загальний ефект від впровадження підсистеми

К – капітальні інвестиції за варіантами, що забезпечили цей ефект.

Загальний ефект від впровадження методики визначається з урахуванням ризиків порушення інформаційної безпеки и становить:

$$E = B * R - C \quad (3.32)$$

у якій В – загальний збиток від атаки на вузол або сегмент корпоративної мережі;

R – очікувана імовірність атаки на вузол або сегмент корпоративної мережі, частки одиниці;

С – щорічні витрати на експлуатацію підсистеми.

$$E = 8990520 * 0{,}51 - 3624953 = 960212$$

$$ROSI = \frac{852652}{1487697} = 0{,}65 \text{ частки одиниці}$$

Термін окупності капітальних інвестицій:

$$T_o = \frac{1}{0{,}65} = 1{,}5 \text{ років}$$

3.6 Висновки до економічного розділу

В результаті проведеного економічного аналізу, розробка та впровадження в існуючі комплекси систем захисту апаратного пристрою для посиленої ідентифікації USB-flash-носіїв дозволить зберегти кошти організації, в яких циркулює інформація з обмеженим доступом від збитків, які понесе організація у випадку витоку даних.

Отриманий термін окупності розробки пристроїв дорівнює 1,5 роки демонструє доцільність розробки такого рішення. Капітальні затрати дорівнюють 1489286 грн., а загальна трудоємкість дорівнює 94 години. Саме цих витрат необхідно для досягнення загального економічного ефекту у 65%.

ВИСНОВКИ

У ході виконання дипломної роботи був проведений аналіз інцидентів витоків інформації від несанкціонованих дії внутрішніх порушників при використанні зовнішніх знімних flash-носіїв інформації. Оскільки в організаціях циркулює інформація з обмеженим доступом, її витік за межі організації наносить великі збитки. На базі цих даних був зроблений висновок, що для посилення захисту інформації від витоку через зовнішні знімні носії необхідно розробити методику, яка поліпшить стан захищеності інформації.

Також були проаналізовані існуючі методи захисту від такого виду загрози, такі як, наприклад, використання програмних комплексів засобів захисту та доведено, що такі методи не є ідеальними та потребують доповнення додатковими засобами захисту.

У якості додаткового засобу захисту ІзОД була запропонована методика захисту інформації від несанкціонованих дій при використанні зовнішніх flash-носіїв за рахунок посиленої ідентифікації flash-носіїв. Для цього був розроблений пристрій, який забезпечує доступ до системі тільки того пристрою, який в ньому ініціалізовано. Таке рішення забезпечує однозначність використання тільки легітимного носія.

В економічному розділі були проведені розрахунки витрат на розробку та впровадження запропонованого рішення та обґрунтована доцільність розробки методики. У зв’язку з тим, що в автоматизованих системах обробляються дані з обмеженим доступом, втрати від витоку або спотворенню їх можуть бути нанести великі збитки. Розроблена методика частково вирішує проблему здійснення несанкціонованих дій користувачами та потребує небагато витрат на її реалізацію. Проте одержуваний економічний ефект позитивно позначається на безпеці даних.

ПЕРЕЛІК ПОСИЛАНЬ

1. «Утечки данных», стаття на www.tadviser.ru від 27.08.2020, (Електрон. ресурс) / Спосіб доступу: URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%A3%D1%82%D0%B5%D1%87%D0%BA%D0%B8_%D0%B4%D0%B0%D0%BD%D0%BD%D1%8B%D1%85
2. «Флэшка как угроза», стаття на nestor.minsk.by від 22.05.2008, (Електрон. ресурс) / Спосіб доступу: URL: https://nestor.minsk.by/kg/2008/20/kg82003.html
3. «Флешки - переваги і недоліки», стаття на usb-fleshki.com.ua, (Електрон. ресурс) / Спосіб доступу: URL: http://www.usb-fleshki.com.ua/chto-takoe-fleshki_uk
4. «Види знімних носіїв інформації», стаття на ukr.kagutech.com від 01.12.2020, (Електрон. ресурс) / Спосіб доступу: URL: https://ukr.kagutech.com/4214424-types-of-removable-media
5. «USB Flash drive», стаття на datarecovery.org.ua, (Електрон. ресурс) / Спосіб доступу: URL: https://datarecovery.org.ua/2018/05/06/about_usb_flash_drive/
6. «USB-флеш-накопичувач», стаття на Wikipedia, (Електрон. ресурс) / Спосіб доступу: URL: https://uk.wikipedia.org/wiki/USB-%D1%84%D0%BB%D0%B5%D1%88-%D0%BD%D0%B0%D0%BA%D0%BE%D0%BF%D0%B8%D1%87%D1%83%D0%B2%D0%B0%D1%87
7. «USB флеш-накопитель», стаття на procomputer.su, (Електрон. ресурс) / Спосіб доступу: URL: http://procomputer.su/pereferiya-pc/134-chto-takoe-fleshka-usb-nakopitel
8. «Що таке токен для КЕП (ЕЦП)», стаття на uakey.com.ua, (Електрон. ресурс) / Спосіб доступу: URL: https://uakey.com.ua/news/blog/shho-take-token-dlja-kep-ecp#:~:text=%D0%9D%D0%B0%D0%B9%D0%BF%D0%BE%D1%88%D0%B8%D1%80%D0%B5%D0%BD%D1%96%D1%88%D0%B8%D0%B9%

20%D1%82%D0%B8%D0%BF%20%D0%B7%D0%B0%D1%85%D0%B8%D1%89%D0%B5%D0%BD%D0%B8%D1%85%20%D0%BD%D0%BE%D1%81%D1%96%D1%97%D0%B2%20%D0%B2,)%20206%2D72%2D15.

9. «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу», НД ТЗІ 2.5-005-99, ДСТСЗІ СБ України, Київ
10. «Методи та засоби захисту комп'ютерної інформації. Інформація як об'єкт захисту», стаття на pmf.uad.lviv.ua, (Електрон. ресурс) / Спосіб доступу: URL: http://pmf.uad.lviv.ua/storage/uploads/%D0%BB%D0%B5%D0%BA%D1%86%D1%96%D1%8F%20%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D0%B9%D0%BD%D0%B0%20%D0%B1%D0%B5%D0%B7%D0%BF%D0%B5%D0%BA%D0%B0.pdf
11. «Хранение данных в компьютерных системах», стаття на www.dropbox.com, (Електрон. ресурс) / Спосіб доступу: URL: https://www.dropbox.com/ru/business/resources/storage-devices
12. «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», НОРМАТИВНИЙ ДОКУМЕНТ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ ТЗІ 1.1-003-99
13. «Умышленные утечки информации», стаття на www.anti-malware.ru, (Електрон. ресурс) / Спосіб доступу: URL: https://www.anti-malware.ru/threats/intentional-information-leaks
14. «Типове положення про службу захисту інформації в автоматизованій системі», НД ТЗІ 1.4-001-2000, ДСТСЗІ СБ України, Київ
15. «ПРОТИДІЯ ВИТОКУ ІНФОРМАЦІЇ ЧЕРЕЗ ЗНІМНІ НОСІЇ», Національний авіаційний університет, DOI: 10.18372/2310-5461.15.5125, А. Петренко, Є. Бєтанов

16. «Засоби захисту інформації», стаття на ssbb.com.ua, (Електрон. ресурс) / Спосіб доступу: URL: https://ssbb.com.ua/uk/poshuk-i-vyyavlennya-proslyshky/poshuk-zakladnykh-ustrojstv/sredstva-zashity-informacii/
17. «Запобігання витоків даних - DLP. Що таке DLP системи і особливості їх використання на підприємстві? Як працює dlp», стаття на skillmaker.ru, (Електрон. ресурс) / Спосіб доступу: URL: https://skillmaker.ru/uk/bezopasnost/predotvrashchenie-utechek-dannyh-dlp-chto-takoe-dlp-sistemy-i-osobennosti-ih/
18. Засіб технічного захисту інформації від несанкціонованого доступу (НСД) «Комплекс «Гриф» версії 4, Інститут комп'ютерних технологій, (Електрон. ресурс) / Спосіб доступу: URL: http://www.ict.com.ua/?lng=1&sec=8&art=41
19. СИСТЕМА ЗАХИСТУ ІНФОРМАЦІЇ ЛОЗА™-1, ВЕРСІЯ 4, ТОВ НДІ АВТОПРОМ, (Електрон. ресурс) / Спосіб доступу: URL: http://avtoprom.kiev.ua/avtoprom/ua/content/%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D0%B0-%D0%B7%D0%B0%D1%85%D0%B8%D1%81%D1%82%D1%83-%D1%96%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D1%96%D1%97-%D0%9B%D0%9E%D0%97%D0%90%E2%84%A2-1-%D0%B2%D0%B5%D1%80%D1%81%D1%96%D1%8F-4
20. «История использования USB», стаття на datadump.ru від 19.04.2017, (Електрон. ресурс) / Спосіб доступу: URL: http://datadump.ru/usb-usage-history/
21. Руководство администратора КСЗ по комплексу средств защиты информации от несанкционированного доступа «Гриф» версии 3, Киев 2011
22. «Протоколы аутентификации», стаття на bytemag.ru, (Електрон. ресурс) / Спосіб доступу: URL: https://www.bytemag.ru/articles/detail.php?ID=9059
23. «Современные алгоритмы шифрования», стаття на bytemag.ru, (Електрон. ресурс) / Спосіб доступу: URL: https://www.bytemag.ru/articles/detail.php?ID=6645&sphrase_id=6930398

24. «Arduino», (Електрон. ресурс) / Спосіб доступу: URL: https://uk.wikipedia.org/wiki/Arduino

25. «Аппаратная часть платформы Arduino», (Електрон. ресурс) / Спосіб доступу: URL: http://arduino.ru/Hardware

26. Методичні вказівки до виконання економічної частини дипломного проекту зі спеціальності 125 Кібербезпека / Упорядники: І.В. Шереметьєва, Д.П. Пілова, Н.М. Романюк. – Дніпро: Національний технічний університет «Дніпровська політехніка», 2017. – 17с.

27. «Інструкція про порядок нарахування і сплати єдиного внеску на загальнообов'язкове державне соціальне страхування», (Електрон. ресурс) / Спосіб доступу: URL: https://zakon.rada.gov.ua/laws/show/z0508-15#Text

ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ ДИПЛОМНОЇ РОБОТИ

Таблиця А.1 – Перелік матеріалів дипломної роботи

№	Формат	Найменування	Кількість листів	Примітки
1	А4	Реферат	3	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	Стан питання. Постановка задачі	40	
6	А4	Спеціальна частина	28	
7	А4	Економічний розділ	16	
8	А4	Висновки	1	
9	А4	Перелік посилань	4	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	14	
14	А4	Додаток Д	2	
15	А4	Додаток Е	1	
16	А4	Додаток Ж	1	
17	А4	Додаток З	2	

ДОДАТОК Б. ОСНОВНІ ДЕСКРИПТОРИ USB

Назва поля	Умов. скор.	Розмір (байт)	Комментар
idVendor	VID	2	Ідентифікатор виробника пристрою. При присвоєнні ідентифікатора виробника, відповідне числове значення вноситься до реєстру виробників.
idProduct	PID	2	Ідентифікатор продукту. Призначається виробником пристрою. Product ID використовується для диференціації продуктів в рамках одного виробника.
bcdDevice	REV	2	Ідентифікатор ревізії. Використовується для диференціації різних апаратних модифікацій в рамках однієї моделі пристрою.
bDeviceClass, bFunctionClass, bInterfaceClass	Class	1	Клас пристрою. Використовується для завдання класу схожих пристроїв із загальним набором ідентичних властивостей.
bDeviceSubclass, bFunctionSubClass, bInterfaceSubclass	SubClass (SUB)	1	Підклас пристрою. Використовується для завдання підкласу схожих пристроїв в рамках класу.
bDeviceProtocol, bFunctionProtocol, bInterfaceProtocol	Protocol (Prot, PROTO)	1	Протокол пристрою. Використовується для завдання протоколу для пристроїв в рамках класу і підкласу.
iProduct	Product	-	Текстовий рядок-описувач продукту.
iSerialNumber	Serial	-	Серійний номер. Використовується для унікалізації абсолютно однакових пристроїв, наприклад дві однакових флешки. Призначається і підтримується виробником пристрою. Пов'язаний механізм носить ім'я Серіалізация. Серіалізация так само бере участь в унікальній ідентифікації пристрою, оскільки додає ще один рівень унікальності.

ДОДАТОК В. ХАРАКТЕРИСТИКИ МІКРОКОНТРОЛЕРУ ATMEGA2560

Модуль	Кількість
EEPROM (ППЗП)	4 Kb
SRAM (ОЗП)	8 Kb
FLASH ROM	256 Kb
Циклів перезапису EEPROM	100 000
Циклів перезапису FLASH ROM	10 000
Кількість режимів очикування	6
Таймери	
8bit	2
16bit	4
RTC\Real Time Clock	1
PWM (ШИМ-перетворювачі 8bit, вихід)	4
Порти	
Порти вводу-виводу (загальна кількість)	86
Аналогові, по 10bit (вхід)	16
Послідовні USART	4
Послідовні SPI, працюючий (master/slave)	1
Послідовний, побайтний	1
Цифрові входи\виходы	54
Частота процесору AVR	16Мгц
Живлення платы Arduino Mega 2560	
стартове	1,8В
рабочє	5В
максимальне	7-12В
Вихідні токи портів 5В	800мА
Вихідні токи портів 3,3В	150 мА
Температурний режим	-40°С — +85°С

ДОДАТОК Г. ЛИСТІНГ ПРОГРАМИ НА МОВІ ПРОГРАМУВАННЯ С ДЛЯ ПРОТОТИПУ ППКЗН НА ARDUINO MEGA ADK

```
#define WANT_HUB_TEST 1

// this is for XMEM2
#define EXT_RAM_STACK 1
#define EXT_RAM_HEAP 1
#define LOAD_XMEM

#if defined(__AVR__)
#include <xmem.h>
#elif defined(ARDUINO_ARCH_SAM)
#include <SPI.h>
#endif

#if WANT_HUB_TEST
#include <usbhub.h>
#endif
#include <Wire.h>
#define LOAD_RTCLIB
#include <RTClib.h>
#include <masstorage.h>
#include <Storage.h>
#include <PCpartition/PCPartition.h>
#include <avr/interrupt.h>
#include <FAT/FAT.h>
#include <stdio.h>
#if defined(__AVR__)
static FILE tty_stdio;
static FILE tty_stderr;
volatile uint32_t LEDnext_time; // fade timeout
volatile uint32_t HEAPnext_time; // when to print out next heap report
volatile int brightness = 0; // how bright the LED is
volatile int fadeAmount = 80; // how many points to fade the LED by
#endif

USB Usb;
USB_DEVICE_DESCRIPTOR buf;
```

```
volatile uint8_t current_state = 1;
volatile uint8_t last_state = 0;
volatile bool fatready = false;
volatile bool partsready = false;
volatile bool notified = false;
volatile bool runtest = false;
volatile bool usbon = false;
volatile uint32_t usbon_time;
volatile bool change = false;
volatile bool reportlvl = false;
int cpart = 0;
PCPartition *PT;

#if WANT_HUB_TEST
#define MAX_HUBS 1
USBHub *Hubs[MAX_HUBS];
#endif

static PFAT *Fats[_VOLUMES];
static part_t parts[_VOLUMES];
static storage_t sto[_VOLUMES];

/*make sure this is a power of two. */
#define mbxs 128
static uint8_t My_Buff_x[mbxs]; /* File read buffer */

#if defined(__AVR__)

#define prescale1       ((1 << WGM12) | (1 << CS10))
#define prescale8       ((1 << WGM12) | (1 << CS11))
#define prescale64      ((1 << WGM12) | (1 << CS10) | (1 << CS11))
#define prescale256     ((1 << WGM12) | (1 << CS12))
#define prescale1024    ((1 << WGM12) | (1 << CS12) | (1 << CS10))

extern "C" {
        extern unsigned int freeHeap();
}
static int tty_stderr_putc(char c, FILE *t) {
       USB_HOST_SERIAL.write(c);
       return 0;
}
```

```
static int __attribute__((unused)) tty_stderr_flush(FILE *t) {
	USB_HOST_SERIAL.flush();
	return 0;
}

static int tty_std_putc(char c, FILE *t) {
	Serial.write(c);
	return 0;
}

static int tty_std_getc(FILE *t) {
	while(!Serial.available());
	return Serial.read();
}

static int __attribute__((unused)) tty_std_flush(FILE *t) {
	Serial.flush();
	return 0;
}

#else
// Supposedly the DUE has stdio already pointing to serial...
#if !defined(ARDUINO_ARCH_SAM)
// But newlib needs this...
extern "C" {
	int _write(int fd, const char *ptr, int len) {
		int j;
		for(j = 0; j < len; j++) {
			if(fd == 1)
				Serial.write(*ptr++);
			else if(fd == 2)
				USB_HOST_SERIAL.write(*ptr++);
		}
		return len;
	}

	int _read(int fd, char *ptr, int len) {
		if(len > 0 && fd == 0) {
			while(!Serial.available());
			*ptr = Serial.read();
			return 1;
		}
```

```
        return 0;
    }

#include <sys/stat.h>

    int _fstat(int fd, struct stat *st) {
        memset(st, 0, sizeof (*st));
        st->st_mode = S_IFCHR;
        st->st_blksize = 1024;
        return 0;
    }

    int _isatty(int fd) {
        return (fd < 3) ? 1 : 0;
    }
}
#endif // !defined(ARDUINO_ARCH_SAM)
#endif

//////////GENIOUS CODE//////////

#include <MD5.h>;

const int PIN_BUTTON = 6;
const int PIN_ADMIN_LED = 7;
const int PIN_RGB_RED = 5;
const int PIN_RGB_GREEN = 4;
const int PIN_RGB_BLUE = 3;

const int MODE_NONE = 0;
const int MODE_PROCESSING = 1;
const int MODE_SUCCESS = 2;
const int MODE_ERROR = -1;

String hash = "";
String correctHash = "";
String logProto = "";
bool showlog = false;

bool isAdmin = false;
int mainMode = 0;
```

```
void logWrite(String dateTime, String hash, String logStatus)
{
 logProto = dateTime + "    " + hash + "    " + logStatus + "\n\r" + logProto + "\n\r";
}

void rgbLight(int red, int green, int blue)
 {
 analogWrite(PIN_RGB_RED, red);
 analogWrite(PIN_RGB_GREEN, green);
 analogWrite(PIN_RGB_BLUE, blue);
}

void showMode()
{
 switch(mainMode) {
   case MODE_NONE:
     rgbLight(0, 0, 0);
     break;
   case MODE_PROCESSING:
     rgbLight(255, 0, 255);
     break;
   case MODE_SUCCESS:
     rgbLight(0, 255, 0);
     break;
   case MODE_ERROR:
     rgbLight(255, 0, 0);
     break;
   }
}


String PrintDescriptors(uint8_t addr)
{
 uint8_t num_conf = 0;
 String vidpid = getdevdescr( (uint8_t)addr, num_conf );
 return vidpid;
}

void PrintAllDescriptors(UsbDevice *pdev)
{
 String serial = getallstrdescr(pdev->address.devAddress);
 String vidpid = PrintDescriptors( pdev->address.devAddress );
```

```
  hash = serial + vidpid;
  Serial.println("hash:\t\t\t");
  Serial.print(hash);
}

String getdevdescr( uint8_t addr, uint8_t &num_conf )
{
  USB_DEVICE_DESCRIPTOR buf;
  uint8_t rcode;
  rcode = Usb.getDevDescr( addr, 0, DEV_DESCR_LEN, ( uint8_t *)&buf );
  if ( rcode ) {
    return "error";
  }
  String string = "";
  return string + buf.idVendor + buf.idProduct;
}

// function to get all string descriptors
String getallstrdescr(uint8_t addr)
{
  uint8_t rcode = 0;
  String string = "";
  Usb.Task();
  if ( Usb.getUsbTaskState() >= USB_STATE_CONFIGURING ) { // state configuring
or higher
    USB_DEVICE_DESCRIPTOR buf;
    rcode = Usb.getDevDescr( addr, 0, DEV_DESCR_LEN, ( uint8_t *)&buf );
    if ( rcode ) {
      return string;
    }
    if ( buf.iSerialNumber > 0 ) {
      string = getstrdescr( addr, buf.iSerialNumber );
    }
  }
  return string;
}

//  function to get single string description
String getstrdescr( uint8_t addr, uint8_t idx )
{
  uint8_t buf[ 256 ];
  uint8_t rcode;
```

```
  uint8_t length;
  uint8_t i;
  uint16_t langid;
  String string = "";
  rcode = Usb.getStrDescr( addr, 0, 1, 0, 0, buf );  //get language table length
  if ( rcode ) {
    Serial.println("Error retrieving LangID table length");
    return string;
  }
  length = buf[ 0 ];      //length is the first byte
  rcode = Usb.getStrDescr( addr, 0, length, 0, 0, buf );  //get language table
  if ( rcode ) {
    Serial.print("Error retrieving LangID table ");
    return string;
  }
  langid = (buf[3] << 8) | buf[2];
  rcode = Usb.getStrDescr( addr, 0, 1, idx, langid, buf );
  if ( rcode ) {
    Serial.print("Error retrieving string length ");
    return string;
  }
  length = buf[ 0 ];
  rcode = Usb.getStrDescr( addr, 0, length, idx, langid, buf );
  if ( rcode ) {
    Serial.print("Error retrieving string ");
    return string;
  }
  for ( i = 2; i < length; i += 2 ) {   //string is UTF-16LE encoded
    string += (char) buf[i];
  }
  return string;
}

void setup() {
        bool serr = false;
        for(int i = 0; i < _VOLUMES; i++) {
                Fats[i] = NULL;
                sto[i].private_data = new pvt_t;
                ((pvt_t *)sto[i].private_data)->B = 255; // impossible
        }
        // Set this to higher values to enable more debug information
        // minimum 0x00, maximum 0xff
```

```
        UsbDEBUGlvl = 0x81;

#if !defined(CORE_TEENSY) && defined(__AVR__)
        // make LED pin as an output:
        pinMode(LED_BUILTIN, OUTPUT);
//        pinMode(2, OUTPUT);
        // Ensure TX is off
        _SFR_BYTE(UCSR0B) &= ~_BV(TXEN0);
        // Initialize 'debug' serial port
        USB_HOST_SERIAL.begin(115200);
        // Do not start primary Serial port if already started.
        if(bit_is_clear(UCSR0B, TXEN0)) {
                Serial.begin(115200);
                serr = true;
        }


        // Blink LED
        delay(500);
        analogWrite(LED_BUILTIN, 255);
        delay(500);
        analogWrite(LED_BUILTIN, 0);
        delay(500);
#else
        while(!Serial);
        Serial.begin(115200); // On the Teensy 3.x we get a delay at least!
#endif
#if defined(__AVR__)
        // Set up stdio/stderr
        tty_stdio.put = tty_std_putc;
        tty_stdio.get = tty_std_getc;
        tty_stdio.flags = _FDEV_SETUP_RW;
        tty_stdio.udata = 0;

        tty_stderr.put = tty_stderr_putc;
        tty_stderr.get = NULL;
        tty_stderr.flags = _FDEV_SETUP_WRITE;
        tty_stderr.udata = 0;

        stdout = &tty_stdio;
        stdin = &tty_stdio;
        stderr = &tty_stderr;
```

```
#endif
        if(serr) {
                fprintf_P(stderr, PSTR("\r\n\n\n\n\n\n\n\n\n\n\n\n\n\n\nStart\r\n"));
                fprintf_P(stderr,       PSTR("Current       UsbDEBUGlvl       %02x\r\n"),
UsbDEBUGlvl);
                fprintf_P(stderr, PSTR("Long filename support: "
#if _USE_LFN
                        "Enabled"
#else
                        "Disabled"
#endif
                        "\r\n"));
        }

#if !defined(CORE_TEENSY) && defined(__AVR__)
        analogWrite(LED_BUILTIN, 255);
        delay(500);
        analogWrite(LED_BUILTIN, 0);
        delay(500);
        analogWrite(LED_BUILTIN, 255);
        delay(500);
        analogWrite(LED_BUILTIN, 0);
        delay(500);
        analogWrite(LED_BUILTIN, 255);
        delay(500);
        analogWrite(LED_BUILTIN, 0);
        delay(500);

        LEDnext_time = (uint32_t)millis() + 1;
#if EXT_RAM
        printf_P(PSTR("Total EXT RAM banks %i\r\n"), xmem::getTotalBanks());
#endif
        printf_P(PSTR("Available heap: %u Bytes\r\n"), freeHeap());
        printf_P(PSTR("SP %x\r\n"), (uint8_t *)(SP));
#endif

#if WANT_HUB_TEST
        for(int i = 0; i < MAX_HUBS; i++) {
                Hubs[i] = new USBHub(&Usb);
#if defined(__AVR__)
                printf_P(PSTR("Available heap: %u Bytes\r\n"), freeHeap());
#endif
```

```
        }
#endif
        // Initialize generic storage. This must be done before USB starts.
        Init_Generic_Storage();

        while(Usb.Init(1000) == -1) {
                printf_P(PSTR("No USB HOST Shield?\r\n"));
                Notify(PSTR("OSC did not start."), 0x40);
        }

#if !defined(CORE_TEENSY) && defined(__AVR__)
        cli();
        TCCR3A = 0;
        TCCR3B = 0;
        // (0.01/(1/((16 *(10^6)) / 8))) - 1 = 19999
        OCR3A = 19999;
        TCCR3B |= prescale8;
        TIMSK3 |= (1 << OCIE1A);
        sei();

        HEAPnext_time = (uint32_t)millis() + 10000;
#endif
#if defined(__AVR__)
        HEAPnext_time = (uint32_t)millis() + 10000;
#endif
}


#if !defined(CORE_TEENSY) && defined(__AVR__)
// ALL teensy versions LACK PWM ON LED

ISR(TIMER3_COMPA_vect) {
        if((int32_t)((uint32_t)millis() - LEDnext_time) >= 0L) {
                LEDnext_time = (uint32_t)millis() + 30;

                // set the brightness of LED
                analogWrite(LED_BUILTIN, brightness);

                // change the brightness for next time through the loop:
                brightness = brightness + fadeAmount;

                // reverse the direction of the fading at the ends of the fade:
```

```
            if(brightness <= 0) {
                brightness = 0;
                fadeAmount = -fadeAmount;
            }
            if(brightness >= 255) {
                brightness = 255;
                fadeAmount = -fadeAmount;
            }
        }
}
#endif

bool isfat(uint8_t t) {
        return (t == 0x01 || t == 0x04 || t == 0x06 || t == 0x0b || t == 0x0c || t == 0x0e || t
== 0x1);
}

void die(FRESULT rc) {
        printf_P(PSTR("Failed with rc=%u.\r\n"), rc);
        //for (;;);
}

void loop() {
  if (Serial.available() > 0) {
    Serial.println(logProto);
    showlog = false;
    }
  if (digitalRead(PIN_BUTTON) == HIGH) {
    delay(200);
    isAdmin = !isAdmin;
  }

  showMode();

    if (isAdmin) {
      digitalWrite(PIN_ADMIN_LED, HIGH);
    } else {
      digitalWrite(PIN_ADMIN_LED, LOW);
    }

        FIL My_File_Object_x; /* File object */
```

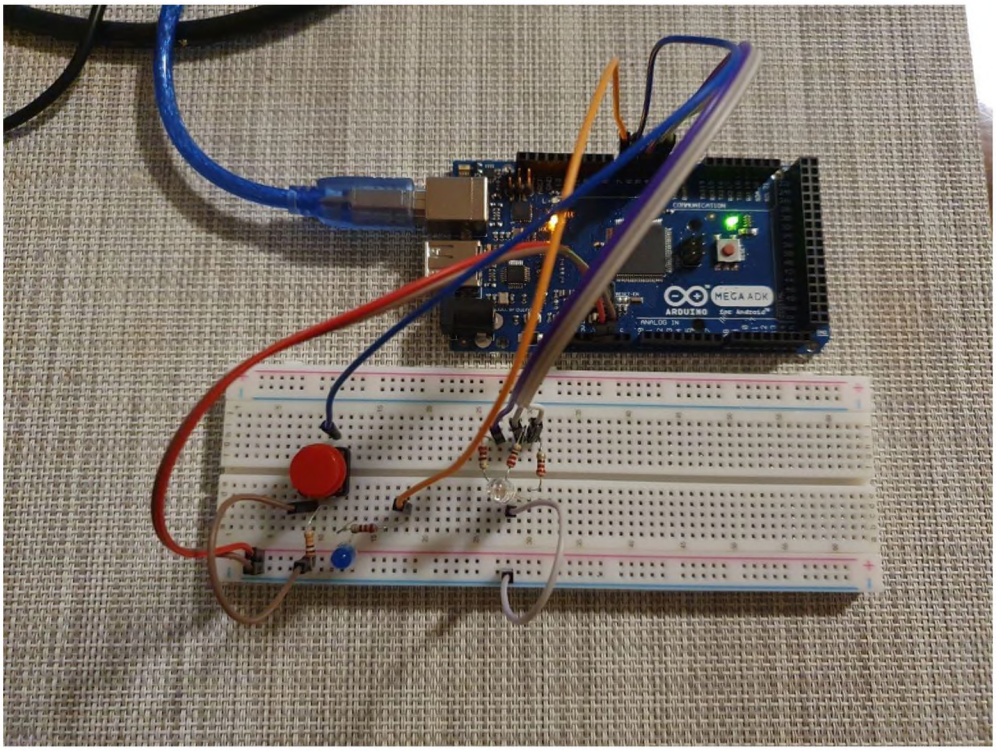
```
#if defined(__AVR__)
        // Print a heap status report about every 10 seconds.
        if((int32_t)((uint32_t)millis() - HEAPnext_time) >= 0L) {
                if(UsbDEBUGlvl > 0x50) {
                        printf_P(PSTR("Available heap: %u Bytes\r\n"), freeHeap());
                }
                HEAPnext_time = (uint32_t)millis() + 10000;
        }
        TCCR3B = 0;
#endif

        if(!change && !usbon && (int32_t)((uint32_t)millis() - usbon_time) >= 0L) {
                change = true;
                usbon = true;
        }

        if(change) {
                change = false;
                if(usbon) {
                        Usb.vbusPower(vbus_on);
                        printf_P(PSTR("VBUS on\r\n"));
                } else {
                        Usb.vbusPower(vbus_off);
                        usbon_time = (uint32_t)millis() + 2000;
                }
        }
        Usb.Task();
        current_state = Usb.getUsbTaskState();

        if (current_state < 20) {
          mainMode = MODE_NONE;
          } else if(current_state < 90) {
            mainMode = MODE_PROCESSING;
            }

        if(current_state != last_state) {
                if(UsbDEBUGlvl > 0x50)
                        printf_P(PSTR("USB state = %x\r\n"), current_state);
#if !defined(CORE_TEENSY) && defined(__AVR__)
                if(current_state == USB_STATE_RUNNING) {
                        fadeAmount = 30;
                }
```

```
#endif
        if(current_state ==
USB_DETACHED_SUBSTATE_WAIT_FOR_DEVICE) {
#if !defined(CORE_TEENSY) && defined(__AVR__)
            fadeAmount = 80;
#endif
            partsready = false;
            for(int i = 0; i < cpart; i++) {
                if(Fats[i] != NULL)
                    delete Fats[i];
                Fats[i] = NULL;
            }
            fatready = false;
            notified = false;
            cpart = 0;
        }
        last_state = current_state;
    }

    // only do any of this if usb is on
    if(usbon) {
        if(partsready && !fatready) {
            if(cpart > 0) fatready = true;
        }

        for(int B = 0; B < MAX_USB_MS_DRIVERS; B++) {
            if((!partsready) && (UHS_USB_BulkOnly[B]->GetAddress())) {

                int i = 0;
                partsready = true;
                    ((pvt_t *)(sto[i].private_data))->lun = i;
                    ((pvt_t *)(sto[i].private_data))->B = B;
                    sto[i].Reads = *UHS_USB_BulkOnly_Read;
                    sto[i].Writes = *UHS_USB_BulkOnly_Write;
                    sto[i].Status = *UHS_USB_BulkOnly_Status;
                    sto[i].Initialize = *UHS_USB_BulkOnly_Initialize;
                    sto[i].Commit = *UHS_USB_BulkOnly_Commit;
                    sto[i].TotalSectors = UHS_USB_BulkOnly[B]-
>GetCapacity(i);
                    sto[i].SectorSize = UHS_USB_BulkOnly[B]-
>GetSectorSize(i);
```

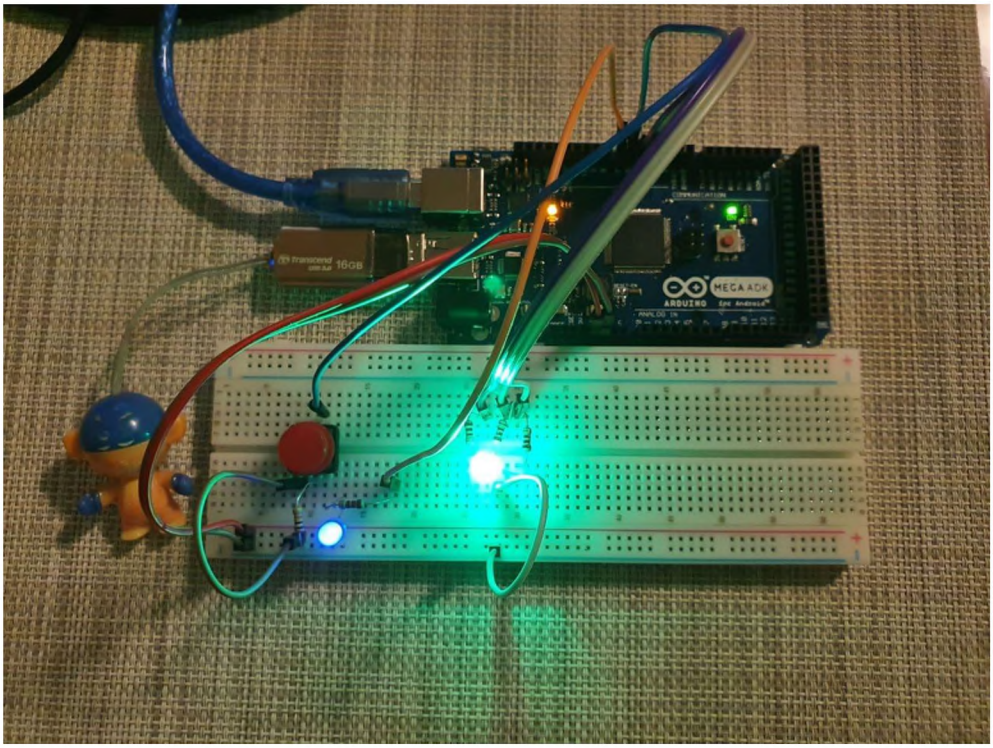
```
                                printf_P(PSTR("Total          Sectors:\t%08lx\t%lu\r\n"),
sto[i].TotalSectors, sto[i].TotalSectors);
                                Usb.ForEachUsbDevice(&PrintAllDescriptors);
                                Serial.println(hash + sto[i].TotalSectors);
                                String fullHash = hash + sto[i].TotalSectors;

                                char *md5str = MD5::make_digest(fullHash.c_str(), 16);
                                String strHash = md5str;
                                if (isAdmin) {
                                  correctHash = strHash;
                                  mainMode = MODE_SUCCESS;
                                  logWrite("3", strHash, "admin success");
                                  } else {
                                    if (correctHash == strHash) {
                                      mainMode = MODE_SUCCESS;
                                      logWrite("1", strHash, "read success");
                                      } else {
                                        mainMode = MODE_ERROR;
                                        logWrite("2", strHash, "read error");
                                        }
                                    }
                        }
                }
        }
}
```

ДОДАТОК Д. ФОТОГРАФІЇ РОБОТИ ППКЗН

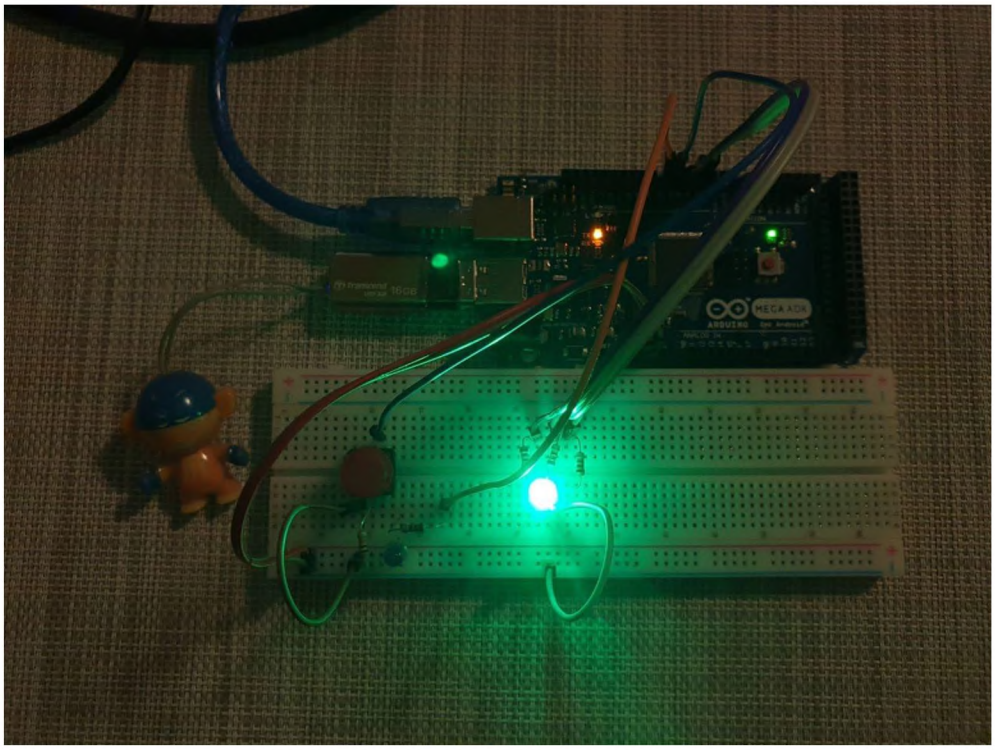
Схема прототипу пристрою



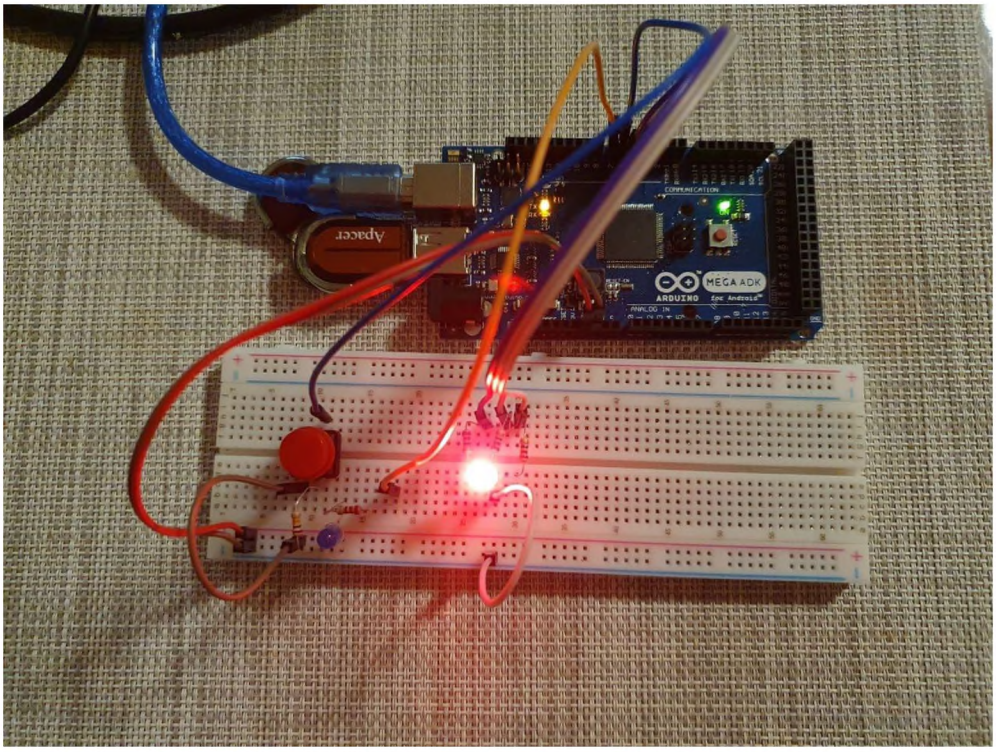
Реєстрація flash-носія у технологічному режимі



Перевірка зареєстрованого flash-носія в робочому режимі



Перевірка незареєстрованого flash-носія в робочому режимі



ДОДАТОК Е. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

1. Пояснювальна записка Кузьмінова М.С.pdf
2. Презентація Кузьмінова М.С.pptx

ДОДАТОК Ж. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Відгук керівника економічного розділу:

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)

ДОДАТОК З. ВІДГУК КЕРІВНИКА ДИПЛОМНОЇ РОБОТИ

Відгук

на кваліфікаційну роботу магістра на тему:
«Методика захисту інформації з обмеженим доступом від несанкціонованих дій при використанні зовнішніх flash-носіїв»
студента групи 125м-19-1
Кузьмінової Марії Сергіївни

Мета роботи – забезпечення спостереженості використання зовнішніх flash-носіїв.

Тема роботи безпосередньо пов'язана з об'єктом діяльності фахівця за спеціальністю 125 Кібербезпека – розвиток методик контролю за обігом зовнішніх носіїв інформації.

Задачі роботи (аналіз особливостей використання зовнішніх носіїв при реалізації технології обробки інформації, аналіз стану контролю за обігом зовнішніх носіїв інформації, аналіз актуальних загроз, формування та формалізація вимог до розробки, обґрунтування вибору протоколу автентифікації, розробка алгоритму функціонування, структурної та функціональної схеми пристрою підвищеного контрою зовнішніх носіїв, обґрунтування вибору елементної бази, розробка програмної реалізації базових функцій) віднесені в освітньо-кваліфікаційній характеристиці магістра до класу евристичних, вирішення яких основане на знаково-розумових уміннях фахівця.

Оригінальність технічних рішень полягає у розробці уніфікованого підходу, з мінімальними змінами вже існуючих комплексів засобів захисту.

Практичне значення результатів проектування полягає в можливості забезпечення додаткового контролю за обігом зовнішніх носіїв інформації та в створені прототипу пристрою.

До недоліків дипломної роботи відносяться:

- недостатньо обґрунтовано вибір протоколу взаємної автентифікації;

- недостатньо обґрунтовано структура та формат записів локального журналу подій;
- недостатньо обґрунтовано алгоритми функціонування пристрою;
- програмне забезпечення пристрою реалізоване не в повному обсязі.

Оформлення пояснювальної записки до кваліфікаційної роботи виконано з деякими відхиленнями від стандартів. Робота виконувалась із незначним відставанням від графіку.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог положення про систему виявлення та запобіганню плагіату.

Ступінь самостійності виконання дипломної роботи висока.

За час дипломування Кузьмінова М.С. виявила себе фахівцем, здатним самостійно, на високому рівні вирішувати поставлені задачі.

В цілому кваліфікаційна робота виконана у відповідності до вимог, що ставляться до кваліфікаційної роботи магістра, заслуговує оцінки “відмінно”, а Кузьмінова М.С. присвоєння їй кваліфікації магістр з кібербезпеки, освітньо-професійна програма «Кібербезпека».

Керівник спеціальної частини
дипломної роботи магістра,
старший викладач _____ О.В. Кручінін

Керівник дипломної
роботи магістра,
д.т.н., професор _____ В.І. Корнієнко