Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
дипломної роботи

магістра
(ступінь підготовки)

галузь знань *12 Інформаційні технології*
(шифр і назва галузі знань)
напрям підготовки *125 Кібербезпека*
(код і назва напряму підготовки)
спеціальність *Кібербезпека*
(код і назва спеціальності)
ступінь підготовки *магістр*
(назва освітнього рівня)
кваліфікація *професіонал із організації інформаційної безпеки*
(код і назва кваліфікації)

на тему: ***Засіб захисту від несанкціонованого завантаження операційної системи для АС класа «1»***

Виконавець: студент ***6*** **курсу, групи** ***125м-16-1***

(підпис) ***Кучер Ростислав Юрійович*** (прізвище ім'я по-батькові)

Керівники	Прізвище, ініціали	Оцінка	Підпис
роботи	д.ф.-м.н., проф. Кагадій Т.С.		
розділів:			
спеціальний	ст. викл. Кручінін О. В.		
економічний	к. е. н., доц. Волотковська Ю. О.		

Рецензент			

Нормоконтроль	к.ф.-м.н., доц. Гусєв О.Ю.		

Дніпро
2018

Міністерство освіти і науки України
Державний вищий навчальний заклад
«Національний гірничий університет»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

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

«_____»_____20___року

ЗАВДАННЯ
на виконання кваліфікаційної роботи магістра

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

студенту **125м-16-1** **Кучер Ростислав Юрійович**
(група) (прізвище ім'я по-батькові)

Тема дипломної роботи ***Засіб захисту від несанкціонованого завантаження операційної системи для АС класа «1»***

1 ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Наказ ректора Державного ВНЗ «НГУ» від _____№_____.

2 МЕТА ТА ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Об'єкт досліджень ***Способи захисту від несанкціонованого завантаження операційної системи в автоматизованій системі класа «1»***

Предмет досліджень ***Процес захисту від несанкціонованого завантаження операційної системи в автоматизованій системі***

Мета НДР ***Розробити надійний та ефективний засіб захисту від несанкціонованого завантаження операційної системи в автоматизованій системі***

Вихідні дані для проведення роботи ***Матеріали науково-дослідної та переддипломної практики***

3 ОЧІКУВАНІ НАУКОВІ РЕЗУЛЬТАТИ

Наукова новизна ***Розробка алгоритму роботи, який є практичнішим, ефективнішим та з низькою собівартістю, та адаптованого до умов функціонування в сучасних автоматизованих системах***

Практична цінність ***Уніфікованість засобу захисту, що був розроблений***

.

.

4 ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Відповідність методичним рекомендація до підготовки та захисту дипломної роботи (проекту) для студентів галузі знань «Кібербезпека»

.

5 ЕТАПИ ВИКОНАННЯ РОБІТ

Найменування етапів робіт	**Строки виконання робіт (початок-кінець)**
Аналіз існуючих способів захисту від несанкціонованого завантаження завантаження операційної системи в АС	1.10.2017 – 30.10.2017
Розробка структурної схеми, функціональної схеми та алгоритму роботи засобу захисту від несанкціонованого завантаження ОС	31.10.2017 – 30.11.2017
Економічне обґрунтування доцільності розробки пристрою захисту від завантаження ОС зі зйомного носія в АС українських підприємств	1.12.2017 – 5.01.2018
Оформлення результатів роботи	6.01.2018 – 20.01.2018

6 РЕАЛІЗАЦІЯ РЕЗУЛЬТАТІВ ТА ЕФЕКТИВНІСТЬ

Економічний ефект ***Знижуються витрати підприємства на експлуатацію КСЗІ***

Соціальний ефект ***Створення умов для більш доцільного використання робочого часу***

7 ДОДАТКОВІ ВИМОГИ

Відповідність вимогам українського законодавства та відомчих нормативно-правових актів

Завдання видав _____ Кагадій Т.С.
(підпис) (прізвище, ініціали)

Завдання прийняв до виконання _____ Кучер Р.Ю.
(підпис) (прізвище, ініціали)

Дата видачі завдання: _____

Термін подання дипломної роботи до ДЕК _____.

РЕФЕРАТ

Пояснювальна записка _ с., ___ рис., ___ табл., ___ додатка, ___ джерела.

Об’єкт дослідження: способи захисту від несанкціонованого завантаження операційної системи.

Мета роботи: розробка альтернативного пристрою захисту інформації від несанкціонованого завантаження операційної системи, що адаптована до умов функціонування сучасних АС.

Методи дослідження: аналіз, синтез, індукція, дедукція, системний аналіз, структурний аналіз, методи порівняння та спостереження.

Виконуючи аналіз існуючих способів захисту ОС від несанкціонованої завантаження зі стороннього носія, був проведений порівняльний аналіз ефективності їхньої системи захисту.

У спеціальній частині був розроблений альтернативний пристрій захисту від несанкціонованого завантаження операційної системи та методика роботи цього пристрою, який є доцільним для використання в АС класа «1».

В економічному розділі наведено економічне обґрунтування доцільності використання розробленого пристрою захисту.

Практичне значення роботи полягає в створенні пристрою захисту від несанкціонованого завантаження операційної системи, адаптованого до умов функціонування в сучасних АС.

Наукова новизна роботи полягає в розробці способу та алгоритму роботи, який є практичнішим, ефективнішим та з низькою собівартістю, а також адаптованим до умов функціонування в сучасних АС.

ЗАХИСТ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНІЙ СИСТЕМІ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, НЕСАНКЦІОНОВАНЕ ЗАВАНТАЖЕННЯ, КРИТЕРІЇ ОЦІНКИ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ.

Реферат

Пояснительная записка ___ с., ___ рис., ___ табл., ___ прилож., ___ ист.

Объект исследования: способы защиты от несанкционированной загрузки операционной системы.

Цель работы: разработка альтернативного устройства защиты от несанкционированной загрузки операционной системы, которая адаптирована к условиям функционирования современных АС.

Методы исследования: анализ, синтез, индукция, дедукция, системный анализ, структурный анализ, методы сравнения и наблюдения.

Выполняя анализ существующих способов защиты ОС от несанкционированной загрузки со стороннего носителя был проведен сравнительный анализ эффективности их системы защиты.

В специальной части было разработано альтернативное устройство защиты от несанкционированной загрузки операционной системы и методика работы устройства, использование которого является целесообразным для использования в АС класса «1».

В экономическом разделе приведено экономическое обоснование целесообразности использования разработанного устройства защиты.

Практическое значение работы состоит в создании устройства защиты от несанкционированной загрузки операционной системы, адаптированного к условиям функционирования в АС класса «1».

Научная новизна работы заключается в разработке способа и алгоритма работы, который является практичным, эффективным и с низкой себестоимостью, а также адаптированным к условиям функционирования в АС класса «1».

ЗАЩИТЫ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ, НЕСАНКЦИОНИРОВАННЫЙ ДОСТУП, НЕСАНКЦИОНИРОВАННАЯ ЗАГРУЗКА, КРИТЕРИИ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ.

ABSTRACT

Explanatory note ___ p., ___ pic., ___ tables, ___ applications, ___ sources.

Object of research: ways to protect against unauthorized booting of the operating system.

Objective: development of an alternative device to protect against unauthorized booting of the operating system, which is adapted to the operating conditions of modern AS.

Research methods: analysis, synthesis, induction, deduction, system analysis, structural analysis, methods of comparison and observation.

Performing an analysis of the existing methods of protecting the OS from unauthorized booting from a third-party carrier was carried out a comparative analysis of the effectiveness of their system of protection.

In the special part, an alternative device was developed to protect against unauthorized booting of the operating system and the method of operation of the device, the use of which is appropriate for use in AS class "1".

The economic section provides an economic justification for the use of the developed security device.

The practical importance of the work is to create a device to protect against unauthorized loading of the operating system, adapted to the operating conditions in AS class «1».

The scientific novelty of the work is to develop a method and algorithm of operation that is practical, efficient and of low cost, and also adapted to the conditions of operation in AS class «1».

PROTECTION OF INFORMATION IN AUTOMATED SYSTEMS, UNAUTHORIZED ACCESS, UNAUTHORIZED BOOTING, CRITERIA FOR ESTIMATION OF INFORMATION PROTECTION.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

ПК – персональний комп’ютер;

ОС – операційна система;

АС – автоматизована система;

HTTP (Hyper text transfer protocol) – протокол передачі гіпертекстових документів;

MBR (Main Boot Record) – головний завантажувальний запис;

GPO (Group Policy Object) – набір правил, відповідно до яких відбувається налаштування робочого середовища Windows;

GPT (Guid Partition Table) – стандарт формату розміщення таблиць розділів на фізичному жорсткому диску;

ПЗП – постійний запам’ятовуючий пристрій;

CMOS (Complimentary Matal-Oxide-Semiconductor) – технологія побудови логічних електронних схем;

CSM (Compatibility Support Module) – модуль підтримки сумісності;

UDP (User Datagram Protocol) – один із протоколів в стеку TCP/IP;

TFTP (Trivial File Transfer Protocol) – тривіальний протокол передачі файлів;

IPv4 (Internet Protocol version 4) – четверта версія мережевого протоколу IP;

IPv6 (Internet Protocol version 6) – шоста версія мережевого протоколу IP;

DHCP (Dynamic Host Configuration Protocol) — протокол динамічної конфігурації вузла;

МДЗ – модуль довіреного завантаження;

АПМДЗ – апаратно-програмний модуль довіреного завантаження;

КЗЗ – комплекс засобів захисту;

ІзОД – інформація з обмеженим доступом;

КСЗІ – комплексна система захисту інформації;

АМДЗ – апаратний модуль довіреного завантаження «Аккорд» ;

НД ТЗІ – нормативний документ системи технічного захисту інформації;

ПЗ – програмне забезпечення;

НСД – несанкціонований доступ;

СЗІ – служба захисту інформації.

ЗМІСТ

ВСТУП

У сучасному світі цінність інформації зросла як ніколи, кількість користувачів, засобів передачі та зберігання даних неухильно зростає з кожним роком. Слід зазначити, що задача захисту інформації є актуальною для підприємств та установ всіх форм власності, у тому числі комерційних. Ця задача згідно вимог нормативних документів може бути вирішена шляхом створення комплексних систем захисту інформації, які розробляються для автоматизованих систем. Безумовно, при розробці та впровадженні комплексної системи захисту інформації (КСЗІ) одним з основних факторів є мінімізація витрат на створення та експлуатацію систем.

Захист інформації в автоматизованій системі повинен забезпечуватися згідно політики безпеки, яка представляє собою сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації. Реалізацію політики безпеки забезпечує комплекс засобів захисту (КЗЗ), який представляє собою сукупність програмно-апаратних засобів.

Як відомо КСЗІ – це сукупність програмно-апаратних засобів, які забезпечують реалізацію політики безпеки інформації. При розробці КСЗІ слід ретельно обирати та чітко визначати взаємодію між цими заходами та засобами. Вимоги щодо КСЗІ визначаються профілем захищеності, який містить послуги безпеки. Згідно НД ТЗІ 2.5-004-99, послуги безпеки об’єднані в групи: критерії конфіденційності, критерії цілісності, критерії доступності, критерії спостереженості, критерії спостереженості. Послуга спотережності відноситься у тому числі і до КЗЗ. Однією з таких послуг є цілісність комплексу засобів захисту (НЦ), яка визначає міру здатності КЗЗ захищати себе і гарантувати свою спроможність керувати захищеними об'єктами.

В загальному випадку вимоги цієї послуги можуть бути порушені у випадках:

- некоректного налаштування системи;

- впливу шкідливого програмного забезпечення;
- помилок під час експлуатації;
- порушень під час експлуатації.

Все частіше підприємцям, і не тільки їм, доводиться стикатися з тим, як захищати АС, доцільність використаної системи захисту, а також вивчати співвідношення ціни до якості.

Необхідність захисту комп'ютерної системи від несанкціонованого втручання зумовлена бажанням користувача приховати від загального доступу інформацію, що зберігається в пам'яті комп'ютера. Крім того, виявлено порушення захисту комп'ютерної системи може призвести до її роботі поза заданого режиму. Це може бути викликано заміною або зміною відомої програми, або виконанням її в стані, в якому її поведінка не погоджено.

Таким чином, одним з найважливіших аспектів забезпечення захисту комп'ютерної системи в процесі завантаження, коли система найбільш вразлива, є перевірка цілісності операційної системи і програмного середовища, тобто здатність КЗЗ захищати себе та гарантувати свою спроможність керувати захищеними об'єктами до початку її роботи, відповідно до НД ТЗІ 2.5-004-99.

З питання захисту від несанкціонованого завантаження в АС, на даний момент, в Україні існує не так багато інформації у відкритому доступі, а також немає єдиних узгоджених способів захисту або засобів їх реалізації. У зв'язку з цим виникає необхідність переглянути базу вже існуючих систем захисту, відповідно до критерію НЦ-2, впроваджені обмеження, дотримання яких дозволяє гарантувати, що послуги безпеки доступні тільки через інтерфейс КЗЗ и всі пропозиції на доступ до захищених об'єктів контролюються КЗЗ.

Одним із важливих етапів огляду існуючих засобів захисту є аналіз ефективності їх системи захисту від несанкціонованого завантаження в ОС. Потрібно розуміти, що засоби захисту не є повністю адаптовані до сучасних потреб функціонування АС в українських підприємствах. На сьогоднішній день існує достатньо відкритих способів захисту від несанкціонованого доступу, що по-різному підходять до цього процесу реалізації захисту.

РОЗДІЛ 1
АНАЛІЗ ІСНУЮЧИХ СПОСОБІВ ТА ЗАСОБІВ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ЗАВАНТАЖЕННЯ ОПЕРАЦІЙНОЇ СИСТЕМИ В АС

В сучасних автоматизованих системах актуальним питанням є можливість КЗЗ протидіяти реалізації несанкціонованого завантаження ОС. В зв'язку з цим необхідно розглянути, яким чином відбувається процес несанкціонованого доступу.

При ввімкненні АС відбувається виконання певних команд, записаних в базовій системі вводу-виводу BIOS. BIOS послідовно визначає та перевіряє всі компоненти, такі як процесор, оперативну пам'ять, відеокартку, після чого відбувається запит до постійного запам'ятовуючого пристрою (ПЗП). Саме з пристрою ПЗП буде відбуватися пошук завантажувача ОС. І лише після цього почнеться завантаження комплексу засобів захисту (КЗЗ) операційної системи. У випадку завантаження зі стороннього носія, використовується файл автоматичного запуску програм Autorun.inf. Цей файл повинен знаходитись в кореневому каталозі файлової системи пристрою, для якого здійснюється автозапуск. З допомогою цього файлу завантаження КЗЗ автоматизованої системи не відбувається. В такому випадку це не призводить до порушення КЗЗ, однак доступ до вже незахищеної АС залишається (рис. 1.1).

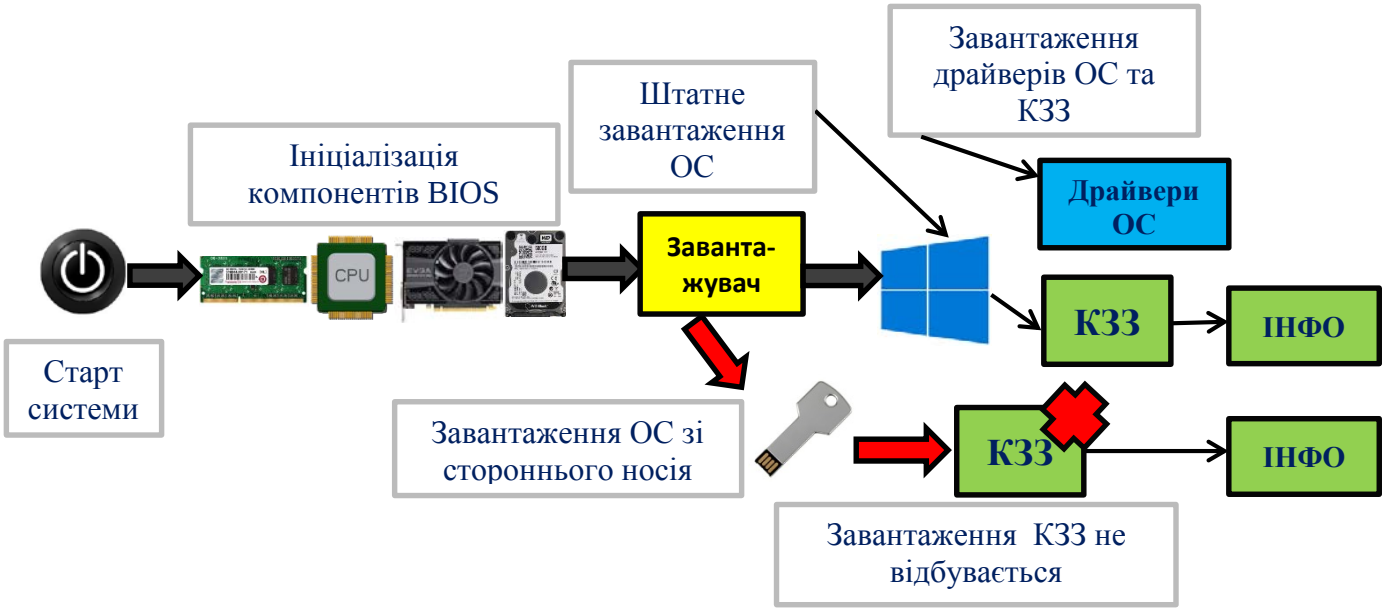


Рисунок 1.1 - Схема завантаження штатної ОС та ОС зі стороннього носія

На сьогоднішній день можна виділити три основні способи реалізації захисту:

- використання програмно-апаратного засобу захисту материнської плати;
- організаційний метод контролю за діями користувача;
- використання додаткових програмно-апаратних засобів довіреного завантаження.

1.1 Аналіз захисних механізмів інтерфейсу BIOS

BIOS - набір мікропрограм, які забезпечують початковий запуск комп'ютера і ініціалізацію обладнання, записаний в спеціальній мікросхемі на материнській платі. Він надає операційній системі API для доступу до всього наявного обладнання та під'єднаних пристроїв (рис. 1.2).

Під час запуску комп'ютера BIOS проводить перевірку критично важливих компонентів системи - POST, тобто Power-on Self-test. Окрім цього, метою процедури POST є робота з програмними ресурсами персональної платформи: обчислення обсягу оперативної пам'яті, пошук та ініціалізація відео системи, послідовних та паралельних портів, накопичувачів на гнучких та жорстких дисках, додаткових пристроїв, що підключені до PCI та USB шин абощо.

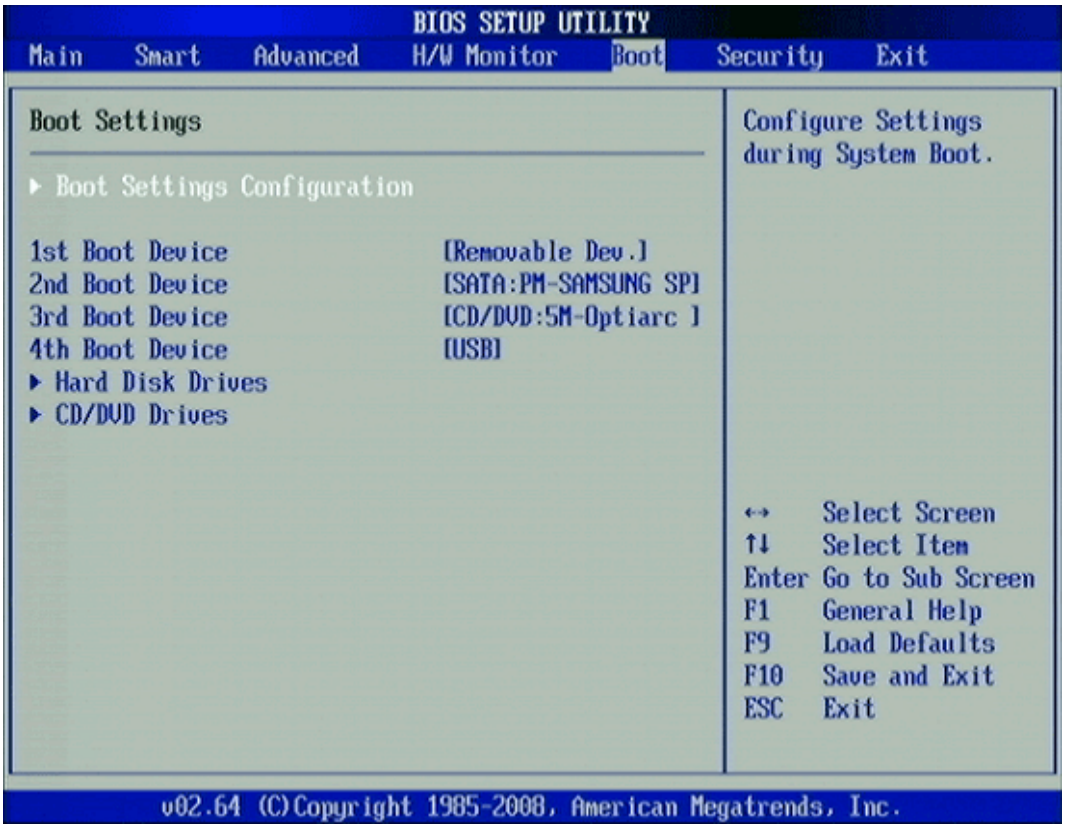


Рисунок 1.2 - Розділ управління порядком завантаження з накопичувачів в BIOS

Етапи ініціалізації та перевірки працездатності відстежуються засобами діагностики BIOS. Для цього процедури POST при переході від одного до іншого пристрою щоразу посилають у діагностичний порт (Manufacturing Test Port) спеціальні сигнали, що називаються POST-кодами. Деякі з них дублюються відповідними звуковими сигналами.

Якщо буде виявлена несправність або будь-яка проблема, BIOS видасть інформацію у вигляді повідомлення або, що частіше, подасть звуковий сигнал. Якщо все в порядку, швидше за все, прозвучить 1 короткий сигнал, і завантаження продовжиться.

Існує сучасна версія системи BIOS під назвою UEFI. Це стандартизований розширюваний інтерфейс програмно-апаратних засобів. UEFI - інтерфейс-підкладка між компонентами комп'ютера і операційною системою. По суті той же BIOS, але має ряд покращень. Виконує такі ж функції, що і стандартний BIOS, тобто проводить перевірку, ініціалізує обладнання, шукає завантажувач і передає управління ОС.

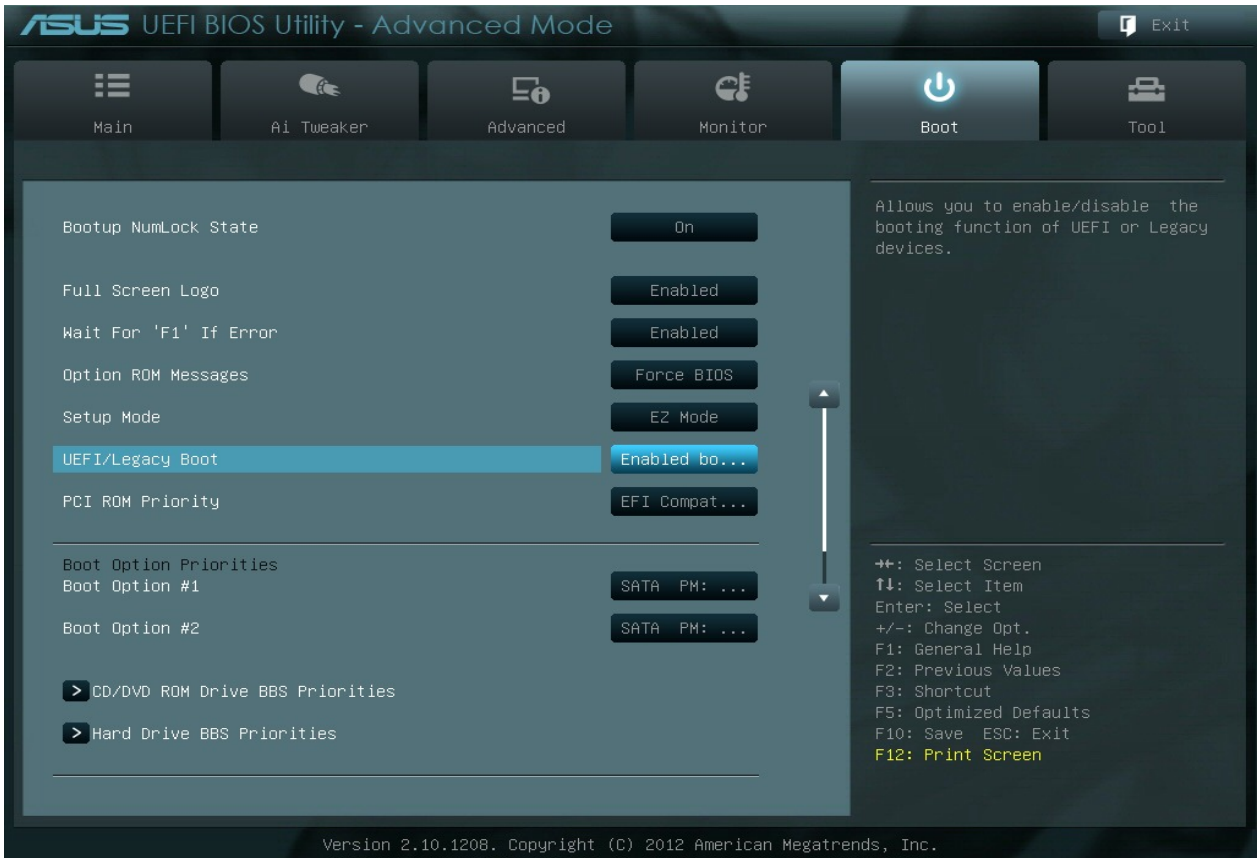


Рисунок 1.3 – Розділ управління порядком завантаження з накопичувачів в UEFI

Основні переваги UEFI перед BIOS:

1 Часу на завантаження йде набагато менше, що досягається за допомогою паралельної ініціалізації, на відміну від BIOS, який ініціалізує всі компоненти послідовно. Операційна система може використовувати драйвера UEFI, а не завантажувати свої власні, а також користувач може обмежитися пропонованими UEFI драйверами, в разі відсутності потреби роботи з графічною підсистемою.

2 Доступна функція робити завантаження з дисків об'ємом більше 2 Тб. Справа в тому, що BIOS для завантаження використовував MBR - головний завантажувальний запис, який може адресувати тільки 2 Тб простору. UEFI ж використовує GPT - інший стандарт формату розміщення розділів на фізичному жорсткому диску, який дозволяє адресувати цілих 9 ЗБ (зеттабайт)(рис. 1.3).

3 UEFI використовує графічний інтерфейс з підтримкою миші, для спрощення роботи з рядовим користувачем. З'явилися деякі вбудовані програми, наприклад, браузер. Таким чином, UEFI став представляти не тільки інтерфейс

між операційною системою і апаратними компонентами, але й щось на кшталт Live CD.

4 Підтримка мережевого завантаження. UEFI може здійснювати завантаження через мережу за допомогою технології Preboot eXecution Environment (PXE). Ця технологія підтримує основні мережеві протоколи, такі, як IPv4 і IPv6, UDP, DHCP і TFTP. Також підтримується можливість використання завантажувальних образів, що зберігаються в мережевих сховищах даних.

5 Зворотна сумісність. Для забезпечення сумісності більшість реалізацій UEFI на комп'ютерах архітектури PC також підтримують режим Legacy BIOS для дисків з MBR. Для цього в UEFI існує функція CSM. У разі використання диска з MBR завантаження виконується в тому ж режимі, що і в системах на основі BIOS. Також можливе завантаження систем на основі BIOS з дисків, що мають GPT.

Також можна скористатися стороннім програмним забезпеченням. Наприклад, в програмі Disk Password Protection пропонується можливість встановити захист завантаження на диск з операційною системою. Зняти захист не вдасться навіть у випадках вилучення батарейки, видалення програми або підключення диска до іншого комп'ютера. Все одно при завантаженні системи буде запитуватися пароль безпеки. Після проведення налаштувань системним адміністратором, кінцевому користувачеві відразу після ініціалізації BIOS, а також UEFI, на екрані буде показано запрошення до введення пароля.

Якщо пароль вірний, то почнеться запуск операційної системи. Таким чином, при кожному завантаженні операційної системи буде запитуватися встановлений пароль, поки захист не буде відключено.

Існує ще і режим прихованого захисту завантаження. Якщо при установці захисту завантаження вибрати опцію "Режим прихованого захисту завантаження", то запрошення до введення паролю не буде виводитися, а введення з клавіатури залишиться, буде дублюватися на екран. Буде складатися враження, що комп'ютер завис. Однак, якщо ввести вірний пароль і натиснути Enter, то почнеться завантаження операційної системи. Це може бути корисним, якщо користувач хоче приховати факт наявності захисту завантаження.

Користувачі, які бажають максимально захистити свої дані, ставлять паролі на всьому, на чому тільки можна, але нерідко ці паролі ними забуваються. Такі дії призводять до покупки нової материнської плати або її перепрограмування, однак цього можна уникнути, скориставшись слабкістю архітектури побудови ЕОМ і навмисно залишеними розробниками «чорними ходами». Слід розуміти, що пароль в BIOS зупинять тільки рядового користувача.

Проаналізувавши дані про захист BIOS приходимо до висновку, що існує 3 основних напрямки злому в цій системі.

1 Маніпуляція з живленням CMOS

Так як CMOS вимагає постійного підживлення для збереження даних, то з цього випливає, що прибравши батарейку на деякий час, приблизно пару хвилин, добиваємося очищення BIOS. Після необхідно знову вставити батарейку на потрібне місце і при запуску ЕОМ задати потрібні параметри часу, нового пароля, якщо необхідно та інші потрібні вам налаштування.

На більшій частині материнських плат існують спеціальні роз'єми для очищення пам'яті CMOS, які зазвичай розташовані в безпосередній близькості від батарейки, дізнатися місце розташування такого роз'єму можна зі схеми материнської плати, наведеної в інструкції до неї або на сайті компанії-виробника. Для очищення пам'яті CMOS необхідно замкнути ці роз'єми, після чого включити ПК і заново виставити настройки BIOS.

Спосіб ефективний, але довгий і не завжди надійний. Часу на непомітне проникнення до корпусу може бути мало і така маніпуляція може спрацювати не завжди. Ці особливості роблять цей спосіб не дуже практичним і швидше крайнім засобом, ніж реальною практикою. До того ж батарейку на деяких моделях материнських плат буває вкрай складно вилучити без використання додаткових інструментів.

2 Використання інженерного пароля

Якщо можливості відкрити корпус не було, то нам доводилося підбирати інженерний пароль. Даний пароль знаходиться у відкритому доступі і загальний у

всіх материнських платах однієї серії. Спосіб полягає у введенні замість забутого пароля BIOS інженерного пароля для даної системної плати.

Таблиця 1.1 – Приклади інженерних паролів для AWARD і AMI BIOS

Тип материнської плати	Паролі
AWARD BIOS v4.5x	AWARD_SW, AWARD_PW, 589589, PASSWORD, SKY_FOX, AWARD SW, award.sw, AWARD?SW, award_?, award_ps, ZAAADA.
AMI BIOS	AMI, AMI_SW, A.M.I., aammii, ami.kez, ami°, amiami, AMI!SW, AMI.KEY, AMI?SW

Однак варто пам'ятати, що дані паролі працюють тільки на BIOS версії 4,55G і нижче, тобто клас системних плат до i845P чіпсета.

3 Маніпуляції в середовищі DOS.

Цей спосіб скидання пароля полягає у використанні середовища DOS. Для цього необхідно завантажитися в середу DOS, оригінальна версія DOS без емулювання з-під ОС Windows. Після чого потрібно ввести команди наведені в таблиці 1.2.

Таблиця 1.2 – Приклад інженерних паролів для середовища DOS

Тип материнської плати	Команди
AWARD и AMI BIOS:	DEBUG -O 70 17 -O 71 17 Q
Phoenix BIOS:	DEBUG -O 70 FF -O 71 FF Q

Крім цього методу існують програми визначення або скидання пароля BIOS із середовища ОС. Наприклад: amikrack.exe і awardcrack.exe і інші, але для їх

використання необхідно мати доступ до ОС, що проблематично, якщо стоїть пароль на подальше завантаження після тестування компонентів робочої станції.

Але ці способи дієві для старих материнських плат, ближче до моменту появи UEFI. Не кожен роботодавець готовий пожертвувати значною сумою на вдосконалення захисту або удосконалення неможливо через ряд причин. Більшість з них намагаються значно зменшити свої втрати на користь прибутку, що залишає питання захисту інформації на старому обладнанні актуальним. На сучасних ноутбуках та ПК тимчасове знеструмлення CMOS не приводить до скидання пароля входу в BIOS / UEFI, оскільки він зберігається в окремій мікросхемі незалежної пам'яті. Сучасні виробники вказують, що їх материнські плати стійкі до злому CMOS інженерним паролем і не тільки.

Однак ніяких експертних висновків з цього приводу у відкритому доступі немає. Повністю довіряти виробнику, без наявності відповідних сертифікатів, не варто. Наприклад, можна відновити пароль за кодом помилки. Цей код відображається після триразового введення неправильного пароля і являє собою хеш від збереженого пароля. Оскільки хеш-функції незворотні, то обчислити пароль безпосередньо не можна. Однак існують програми, що підбирають пароль з таким самим значенням згортки. Це може бути, як заданий пароль, так і інша комбінація символів, що дає такий же хеш при перевірці. Зайти в налаштування можна за допомогою одного з них, так як перевіряється саме хеш. Даний пароль також можна підібрати в онлайн-сервісах.

1.2 Організаційний спосіб контролю за діями користувача

Організаційний спосіб контролю за діями користувача дозволяє захистити комп'ютерну систему від несанкціонованого завантаження ОС, контролюючи всі дії користувача системи за допомогою співробітника служби захисту інформації. Співробітник СЗІ забезпечує керування комплексної системи захисту інформації (КСЗІ) в АС та здійснює контроль за її функціонуванням, відповідно до Типового положення про службу захисту інформації в автоматизованій системі НД ТЗІ 1.4-

001-2000. На працівника СЗІ покладається виконання робіт з видачі доступу до системи, процес авторизації користувачів, перевірка зовнішніх носіїв інформації, логування всіх дій в системі, огляд робочого місця після сеансу, контроль за станом захищеності інформації в АС. Цей спосіб є досить простим в реалізації, має високий рівень захисту, відсутня необхідність придбання і впровадження дорогого технічного забезпечення.

Але треба зазначити, що співробітник служби захисту інформації може охопити за раз до 2-х користувачів. Якщо ж таких користувачів стає більше, то потрібно наймати нових співробітників, а їм також потрібно платити зарплатню. Як підсумок - це може призвести до зайвих витрат підприємства, оскільки не на кожному підприємстві використання даного способу є доцільним. АС в середньому може використовуватися 4-5 год на день, а платити працівнику, чи працівникам, доведеться за весь робочий день, тобто система простоюватиме досить значний період, оскільки виявиться надлишковою або носитиме збитковий характер.

В такому випадку краще розглянути можливість використання автоматизованих засобів захисту. Таке рішення в деяких ситуаціях стане більш доцільним.

1.3 Способи з використанням програмно-апаратних рішень довіреного завантаження

В даний час високий попит має використання єдиного засобу захисту довіреного завантаження, що здатен вирішити цілу низки завдань, спрямованих на захист системи. До таких завдань відносяться:

- захист від несанкціонованого доступу;
- розмежування доступу користувачів і процесів до інформації;
- криптографічний захист файлів за допомогою механізмів шифрування та електронного цифрового підпису.

Власники багатьох компаній хочуть використовувати пристрої, що одночасно реалізують всі перераховані функції захисту інформації в силу того, що

частина функцій в їх системах вже реалізована за допомогою інших пристроїв, або ж, в силу особливостей функціонування їх системи, в цих функціях взагалі немає необхідності. У цьому випадку компанії вважають за краще купувати засоби захисту інформації, що реалізують тільки необхідні їм функції захисту інформації і не переплачувати за наявність інших. Необхідно зазначити, що за можливості така система захисту має бути універсальною, в разі зміни компонентів АС.

Для того щоб засоби захисту інформації задовольняло всім сучасним вимогам, воно повинно дозволяти вирішувати всі вищеназвані завдання, але саме в тій комбінації, яка потрібна даній конкретній компанії. Для початку треба розібратися з поняттям довіреного завантаження.

Довірене завантаження - це завантаження різних операційних систем тільки з заздалегідь визначених постійних носіїв, наприклад лише з жорсткого диску, після успішного завершення спеціальних процедур: перевірки цілісності технічних і програмних засобів ПК, використовуючи механізм покрокового контролю цілісності, і апаратної ідентифікації, аутентифікації користувача. Завантаження з інших носіїв повинно блокуватися. Причому вона відбувається тільки після виконання ідентифікації, аутентифікації користувача, а також перевірки цілісності програмного і апаратного забезпечення комп'ютера. Тим самим забезпечується захист комп'ютера від несанкціонованого доступу на найважливішій фазі його функціонування - етапі завантаження операційної системи.

1.3.1 Комплекс засобів захисту інформації «Гриф-2000»

КЗЗ «Гриф-2000» призначений для забезпечення захисту ІзОД при її обробці в автоматизованих системах класу «1» на базі персональних комп'ютерів під управлінням операційної системи (ОС) MS Windows 2000 Professional і старших версій. Комплекс дозволяє створити на базі персонального комп'ютера спеціалізоване робоче місце з обмеженим колом користувачів і забезпечити

захист оброблюваної ІзОД від загроз цілісності, конфіденційності та доступності при реалізації політики адміністративного управління доступом до інформації, тобто захистити інформацію від несанкціонованого ознайомлення, модифікації, видалення. Розробка виконана відповідно до вимог НД ТЗІ 2.5-007-2001 «Вимоги до комплексу засобів захисту інформації, що становить державну таємницю, від несанкціонованого доступу при її обробці в автоматизованих системах класу «1».

Існує Гриф версії 3, яка вирішує завдання забезпечення захисту інформації тільки з використанням програмних засобів. Таке рішення дозволяє полегшити введення в експлуатацію засобів захисту, але жертвує його надійністю за рахунок відсутності в ній апаратних рішень, які розширюють список вразливостей яким може протистояти. Розробка комплексу Гриф версії 3 виконана у відповідності до вимог НД ТЗІ 2.5-012-2015 і НД ТЗІ 2.5-008-2002.

Можливості КЗЗ «Гриф-2000»:

- розмежування доступу користувачів до обраних каталогів (папок) і файлів, які в них перебувають, відповідно до принципів адміністративного управління доступом, що дозволяє організувати спільну роботу на ПЕОМ декількох користувачів, що мають різні службові обов'язки і права щодо доступу до ІзОД;
- управління потоками інформації і блокування потоків інформації, що призводять до зниження її конфіденційності;
- контроль виведеної друкованої інформації;
- гарантоване видалення інформації шляхом затирання вмісту файлів, що містять ІзОД, при їх видаленні;
- відновлення функціонування КЗЗ після збоїв, що гарантує доступність інформації при дотриманні правил доступу до неї.

Недоліки даної платформи:

- КЗЗ Гриф-2000 реалізований на базі незначного списку підтримуваних материнських плат;
- КЗЗ Гриф версії 3 має тільки програмний комплекс заходів щодо захисту системи і не забезпечує захист від несанкціонованого завантаження.

1.3.2 Апаратно-програмний модуль довіреного завантаження «Соболь»

АПМДЗ «Соболь» - засіб захисту комп'ютера від несанкціонованого доступу, що забезпечує довірене завантаження (рис. 1.4). «Соболь» може застосовуватися для захисту автономного комп'ютера, а також робочої станції або сервера, що входять до складу локальної обчислювальної мережі. Найбільш важливою особливістю комплексу є можливість модуля довіреного завантаження, далі МДЗ, проводити ідентифікацію і аутентифікацію користувачів до завантаження операційної системи за допомогою персональних електронних ідентифікаторів, таких як USB-ключі, смарт-карти, ідентифікатори iButton і ін., а також контроль цілісності програмного і апаратного забезпечення комп'ютера до завантаження операційної системи. Також комплекс може проводити блокування несанкціонованого завантаження операційної системи з зовнішніх носіїв.

АПМДЗ «Соболь» має сторожовий таймер, що дозволяє блокувати роботу комп'ютера. Працює дана функція за умови, що після його включення і після закінчення певного часу, управління не було передано платі МДЗ і контролюється працездатність основних компонентів МДЗ. Компонентами можуть виступати датчики випадкових чисел, незалежна пам'ять або ідентифікатори. Виконується реєстрація дій користувачів, і спільна робота з зовнішніми додатками, таких як датчики випадкових чисел, засоби ідентифікації і аутентифікації, програмні засоби захисту інформації та інші. АПМДЗ «Соболь» дозволяє контролювати незмінність конфігурації комп'ютера - PCI-пристроїв, ACPI, SMBIOS і оперативної пам'яті. Дана можливість істотно підвищує захист робочої станції.

Рисунок 1.4 – АПМДЗ «Соболь»

Для установки комплексу потрібен вільний роз'єм материнської плати, для сучасних комп'ютерів - стандарти PCI, PCI-X, PCI Express, mini-PCI, mini-PCI Express, і незначний обсяг пам'яті жорсткого диска комп'ютера, що захищається. Можливості даного засобу від несанкціонованого доступу:

- можливість захисту сучасних персональних комп'ютерів і серверів, в тому числі підтримка АПМДЗ нової плати Mini PCI Express Half для захисту ноутбуків і моноблоків;
- простота установки, настройки і адміністрування;
- можливість програмної ініціалізації без розтину системного блоку;
- широкий вибір форматів виконання;
- контроль цілісності системного реєстру Windows.

На даний момент комплекс АМДЗ «Соболь» неможливо завезти на територію Україну і сертифікувати даний продукт.

1.3.3 Система захисту інформації «ЛОЗА-1»

Система «ЛОЗА-1» — це програмний засіб захисту інформації від НСД в автоматизованих системах класу «1», зазвичай це автономний комп’ютер. Комплекс може працювати під керуванням операційних систем Microsoft Windows починаючи з версії XP Professional і закінчуючи версією Server 2012 R2.

Система «ЛОЗА-1» може використовуватись для захисту інформації, що становить державну таємницю, — це підтверджено експертним висновком №740, виданим Державною службою спеціального зв'язку та захисту інформації України 01 червня 2017 р.

СЗІ «ЛОЗА-1» забезпечує:

- захист від несанкціонованого доступу до інформації;
- контроль друку та експорту;
- контроль входу користувачів до системи;
- реєстрація подій в системі;
- моніторинг мережі.

Переваги вибору даного захисту від НСД:

- 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;
- 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;
- 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 «флешок» дозволи на доступ до диска можуть встановлюватись для окремих носіїв (вони ідентифікуються за «залізним» серійним номером), «флешки», зареєстровані на сервері, можуть використовуватись і на робочих станціях (при встановленні

відповідної настройки), для «флешок» також передбачена система опису, що настроюється користувачем;

- система «ЛОЗА-1» дозволяє встановлювати дозволи або заборони на запуск процесів.

Недоліки даної платформи:

- Даний засіб захисту має лише програмну реалізацію та не захищає від несанкціонованого завантаження АС.

1.3.4 Апаратний модуль довіреного завантаження «Аккорд»

Комплекс «Аккорд» - це апаратний модуль довіреного завантаження для IBM-сумісних ПК - серверів і робочих станцій локальної мережі, що забезпечує захист пристроїв і інформаційних ресурсів від НСД. Комплект засобу складається з: 1) знімача інформації з контактним пристроєм, що забезпечує інтерфейс між контролером комплексу і персональним ідентифікатором користувача; 2) платою розширення, яка встановлюється в материнську плату ПК; 3) персональний ідентифікатор користувача-спеціальний пристрій, що містить унікальну ознаку користувача, з яким зареєстрований користувач входить в систему і який використовується системою для визначення його прав, а також для реєстрації факту доступу і характеру виконуваних ним робіт, або наданих йому послуг. Комплекс починає працювати відразу після виконання штатного BIOS комп'ютера - до завантаження операційної системи. Контролери сімейства «Аккорд» забезпечують довірене завантаження ОС, що підтримують найбільш поширені файлові системи, включаючи: FAT12, FAT16, FAT32, NTFS, HPFS, Ext2, Ext3, Ext4, ReiserFS, FreeBSD UFS / UFS2, Solaris UFS, QNX4, MINIX.
Комплекс «Аккорд » може бути реалізованим на базі різних контролерів:

- PCI или PCI–X ;
- PCI-express ;
- Mini PCI-express ;
- Mini PCI-express half card ;

- M.2 з ключами A а/або E (інтерфейс PCI-express).

На даний момент комплекс АМДЗ «Аккорд» неможливо завезти на територію Україну і сертифікувати даний продукт.

1.4 Висновки до першого розділу

Всі вище описані способи захисту від несанкціонованого завантаження в ОС мають певний ряд недоліків. Виникає необхідність в пошуку інших засобів захисту. Необхідно розглянути можливість реалізації захисту інформації за допомогою вбудованих засобів ОС, маніпулюючи з налаштуванням USB-портів. В разі недостатнього захисту чи неможливості реалізації захисту, маніпулюючи з налаштуваннями USB інтерфейсу, виникає необхідність розробки власного пристрою чи способу захисту інформації.

РОЗДІЛ 2
РОЗРОБКА ЗАСОБУ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ЗАВАНТАЖЕННЯ ОПЕРАЦІЙНОЇ СИСТЕМИ

2.1 Формування завдання

Створення ефективного засобу захисту від несанкціонованого завантаження, що запобігає можливості реалізації несанкціонованого завантаження в АС зі стороннього носія, необхідно:

- розглянути можливі шляхи реалізації засобу;
- розробити методику роботи та загальну схему роботи;
- економічно обґрунтувати доцільність створення засобу.

2.2 Аналіз способів захисту від завантаження зі стороннього носія по USB інтерфейсу

У сучасних комп'ютерах універсальна шина USB замінила собою практично всі інші види портів для підключення периферійних пристроїв. На цей інтерфейс перейшли принтери і сканери, фото- і відеокамери, клавіатури і маніпулятори і маса інших периферійних пристроїв. Зрозуміло, найпопулярнішими USB-пристроями є мобільні накопичувачі - флешки і портативні жорсткі диски.

Шина USB — це послідовний інтерфейс передавання даних для середньо- та низько швидкісних периферійних пристроїв обчислювальної техніки. З'єднання USB-кабелями формує інтерфейс між USB-пристроями та USB-хостом. Як хост використовується керований з операційної системи USB-контролер, до складу якого входить USB-концентратор, або ж хаб. Розподіл пропускної здатності шини між периферійними пристроями планується хостом і реалізується ним за допомогою посилки маркерів. Шина дозволяє підключати, конфігурувати, використовувати і відключати пристрої під час роботи хоста і самих пристроїв (рис. 2.1).

Повсемісне поширення USB-інтерфейсу призводить, з одного боку, до зростання ризиків витоку інформації, а з іншого - до неможливості відмовитися від використання USB-пристроїв в організаціях. Повністю заблокувати USB зазвичай практично неможливо: не тільки тому, що в рамках бізнес-процесів потрібно використовувати мобільні накопичувачі і гаджети, але з тих міркувань, що через USB-інтерфейс підключається переважна більшість сучасних клавіатур, мишок і інших необхідних в повсякденній роботі пристроїв.

Рисунок 2.1 – Схема розпаювання контактів USB

В деяких ситуаціях обмеження доступу підключення флешок, переносних жорстких дисків і інших пристроїв можливо тільки за умови відключення USB портів на комп'ютері або ноутбуці. Відключення портів USB допоможе запобігти підключення будь-яких накопичувачів, які можуть бути використані для крадіжки важливої інформації або стати причиною зараження комп'ютера вірусом і поширення шкідливого програмного забезпечення по локальній мережі. Зробити це можна декількома способами, що мають різну ефективність і складність реалізації.

В системах Windows існує можливість автоматичного запуску програми. За цю функціональність відповідальний файл autorun.inf, за допомогою якого користувач без прав доступу досить ефективно обходить захист системи. Компанії Microsoft довелося позбутися цього функціоналу та вже через 3 місяці після відключення Autorun, кількість атак, які використовували його в Windows XP і Vista, знизилася на 1.3 мільйона. Починаючи з Windows 7, цей функціонал відключений за замовчуванням.

Але це не означає, що вразливість була повністю закрита. Умілі хакери знаходили нові способи обходу безпеки. Однією з таких стала вразливість при обробці ярликів. Цей баг у захисті експлуатував вірус-черв'як Stuxnet, а також різноманітні бібліотеки створення ескізів, які вступають в дію при простому перегляді вмісту флешки в «Провіднику».

Аналогічна функціональність існує в ОС UNIX-типу. Наприклад, оточення робочого столу GNOME і KDE, допускають наявність спеціальних файлів автозапуску на знімному накопичувачі: .autorun, autorun або autorun.sh. Якщо на флешці присутні два або всі три з перерахованих типів файлів, то оброблятися буде тільки один. Пріоритет буде відданий файлу .autorun, а далі в порядку черги за списком вище. Можна сказати, що це аналог autorun.inf в Windows, тільки з меншим функціоналом. Тут необхідно прописувати шлях до виконуваного файлу, але не можна - одразу до кількох, а також не можна виходити за межі файлової системи флешки за допомогою посилання на каталог, що стоїть вище в ієрархії.

Однією із стандартних систем в UNIX системах є механізм захисту AppArmor. Це програмний інструмент попереджувального захисту, заснований на політиках безпеки, які визначають, до яких системних ресурсів і з якими привілеями може отримати доступ той чи інший додаток. У AppArmor включено також інструменти статистичного аналізу та інструменти, засновані на навчанні, що дозволяє прискорити і спростити побудову нових профілів. Такий механізм захисту ненадійний, оскільки захищає лише настільки, наскільки здатні його профілі, розташовані в /etc/apparmor.d. Наприклад, в Ubuntu 10.10 профіль для evince-thumbnailer дозволяє запис в ~ / .config / autostart - місце, яке може бути використане розробниками шкідливого ПО для автоматичного завантаження їх вірусного коду, а також довільних скриптів, при вході користувача в систему. Від деяких речей AppArmor не здатний захистити в принципі, оскільки такий захист може порушити стабільність роботи системи:

- виклики бібліотеки X11 (може бути порушений доступ до мережі);
- завершення процесу скрінсейвера, перехоплення натиснутих клавіш, емуляція натискань клавіш і так далі.

Крім того, для виконуваних файлів, таких як документи pdf, теж існує можливість автовідкриття. Потрібно створити файл .autoopen або autoopen в корінній директорії переносного пристрою і прописати туди шлях до потрібного файлу, при цьому коренем є зйомний пристрій, а не корінь системи. Наприклад в файловому менеджері Nautilus ця функціональність поки не реалізована. Впевненість деяких користувачів в тому, що під ОС UNIX-типу немає або майже немає вірусів, призводить до сумних наслідків. В результаті користувач, не замислюючись, підтверджує автозапуск файлів - єдиний спосіб вірусу почати свою роботу в таких системах. На даний момент UNIX системи модернізуються для більш широкого кола користувача, використовуючи для цього бібліотеки ОС Windows або розроблять власні аналоги. Такі дії призводить до появи нових вразливостей і не завжди бувають вчасно закриті.

Розглянемо 8 способів, за допомогою яких можна заблокувати доступ до USB портів.

2.2.1 Відключення USB в налаштуваннях BIOS

Перед тим як ввійти до налаштувань, необхідно дізнатися виробника материнської плати та клавіші для завантаження. Далі потрібно провести наступні маніпуляції:

1 Входимо до налаштувань BIOS.

2 Вимикаємо всі пункти, пов'язані з контролером USB (наприклад, USB Controller або Legacy USB Support).

3 Після того, як були проведені зміни, потрібно зберегти налаштування та вийти з BIOS. Зазвичай це робиться за допомогою клавіші F10.

4 Робоча станція перезавантажується, перевіряється відключення USB портів.

Однак такий спосіб позбавляє нас можливості використовувати USB - пристрої або будь-які інші, налаштування яких були змінені. Для роботи системи можна залишити порти (або порт) PS / 2 для контролерів, однак в такому випадку необхідно використовувати привід для дисків. Даний спосіб вирішує проблему роботи з USB, але створює нові проблеми захисту від завантажувальних дисків.

2.2.2 Зміна параметрів реєстру для USB-пристроїв

Другим способом є відключення USB-накопичувачів через BIOS в ОС Windows за допомогою реєстру. Дана маніпуляція дозволяє закрити доступ для різних USB-накопичувачів, але при цьому інші пристрої, такі як клавіатури, миші, принтери, сканери все одно будуть працювати.

1. Спершу необхідно відкрити меню Пуск -> Виконати, далі ввести команду «regedit», щоб відкрити редактор реєстру.

2. Перейшовши в розділ HKEY_LOCAL_MACHINE \ SYSTEM \ CurrentControlSet \ Services \ USBSTOR

3. У правій частині вікна знаходиться пункт «Start», що потрібно відредагувати. Вводиться значення «4» для блокування доступу до USB-накопичувачів. Відповідно, якщо знову ввести значення «3», доступ буде відкритий (рис. 2.2).

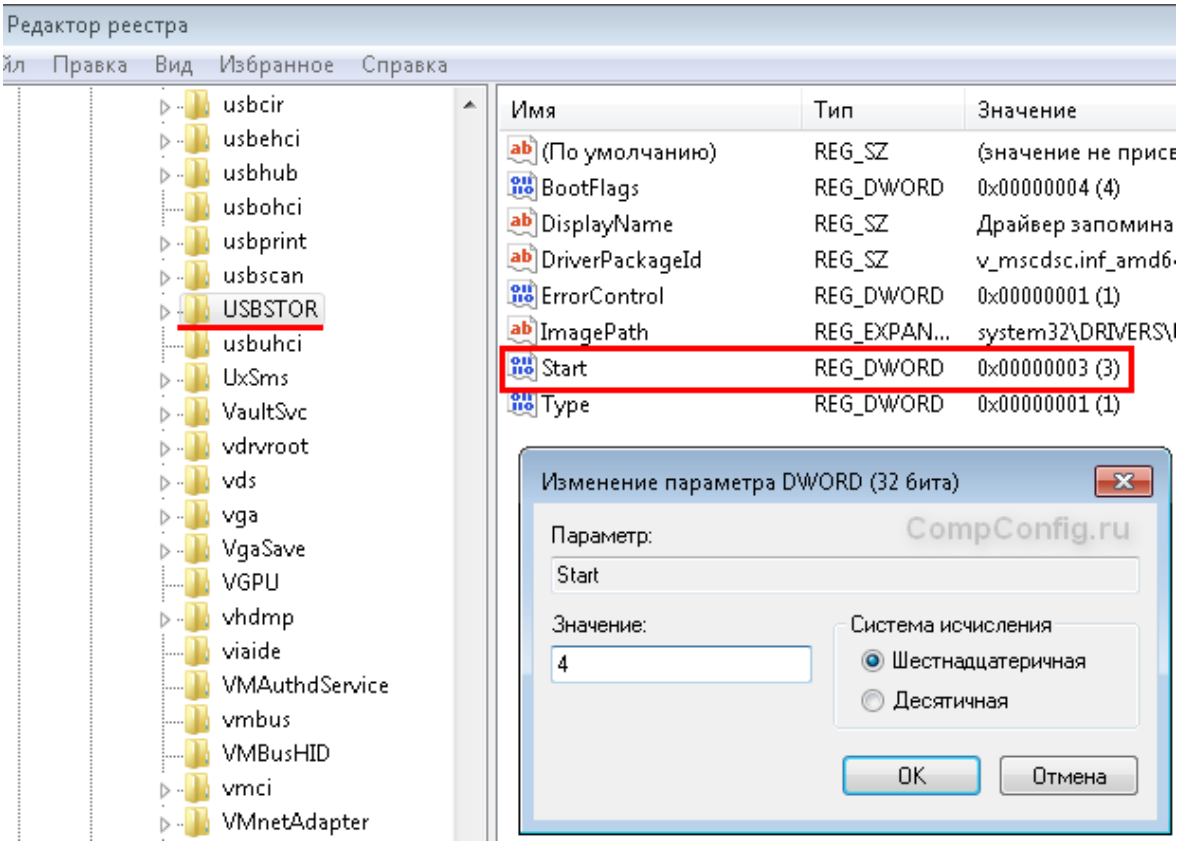


Рисунок 2.2 – Налаштування USBSTOR в редакторі реєстра

Після редагування реєстру потрібно перезавантажити комп'ютер. Але даний спосіб працює тільки при встановленому драйвері USB контролера. Якщо з міркувань безпеки драйвер не був встановлений, значення параметра «Start» може бути автоматично скинуто на значення «3», коли користувач підключить накопичувач USB, ОС Windows спробує встановить власний драйвер. Також даний спосіб захисту можна подолати за допомогою завантажувальної флешки і офлайн-редактор реєстру, змінюючи значення Start в початкове положення.

2.2.3 Відключення USB портів в диспетчері пристроїв

1. Для початку треба зайти до контекстному меню «Комп'ютер» і вибрати в ньому підрозділ «Властивості». Відкриється вікно в лівій частині якого потрібно натиснути на посилання «Диспетчер пристроїв».

2. У дереві диспетчера пристроїв знаходимо пункт «Контролери USB» та відкриваємо його (рис. 2.3).

3. Вимикаємо контролери шляхом натискання правої кнопки миші і вибору пункту меню «Відключити».

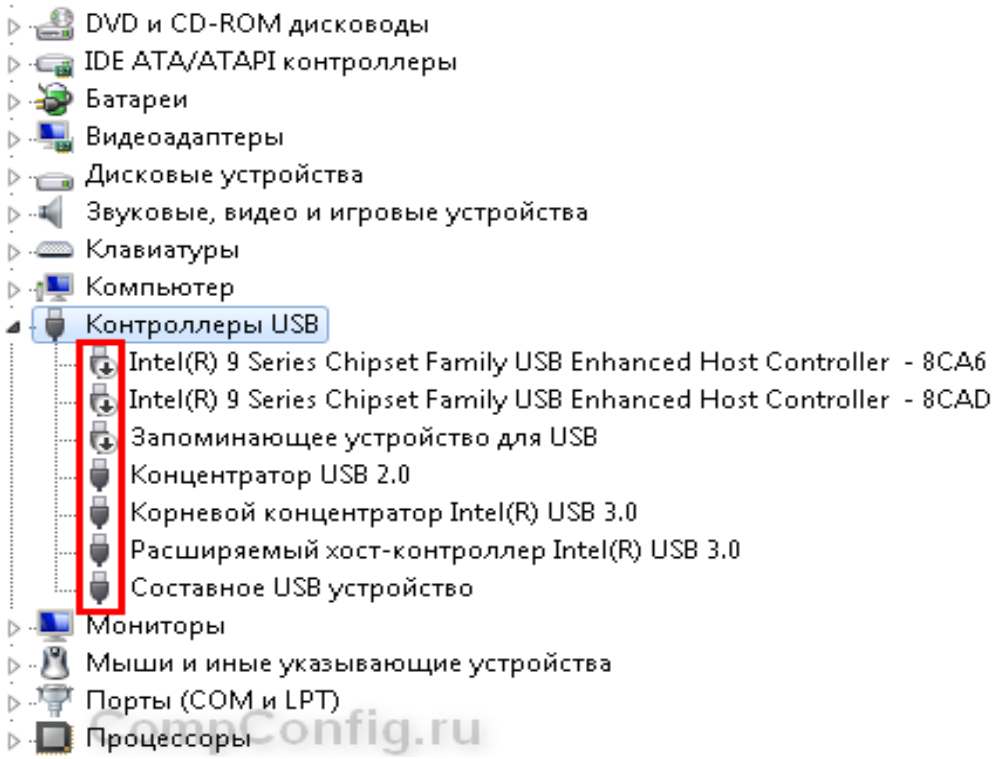


Рисунок 2.3 – Доступні USB-контролери в операційній системі

Цей спосіб не завжди працює. У прикладі, наведеному на малюнку вище, відключення контролерів (2 перших пункту) не привело до бажаного результату. Відключення 3-го пункту (Оперативна пам'ять для USB) спрацювало, але це дає можливість відключити лише окремий екземпляр USB-накопичувача.

2.2.4 Управління деінсталяцією драйверів контролера USB

Для видалення USB драйверу з ОС можна скористатися вбудованими засобами. Для цього необхідно:

1 Відкрити меню «Пуск».

2 З переліку команд меню «Комп'ютер» обрати вкладку «Властивості».

3 Перейти до «Диспетчер пристроїв».

4 У вікні диспетчера, в горизонтальному меню, відкрити розділ «Вид» і натиснути «Показати приховані пристрої» (рис. 2.4).

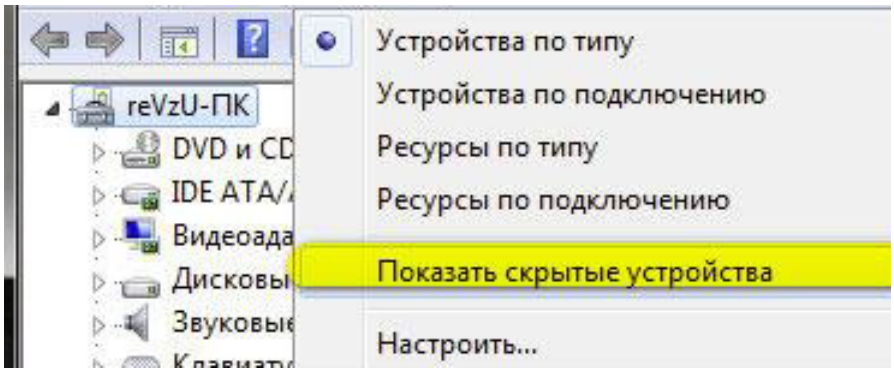


Рисунок 2.4 – Використання системних команд для пошуку серійного номеру

5 Відкривши директорію «Контролери USB», видаляємо старі або невикористовуванні драйвери (рис. 2.5).

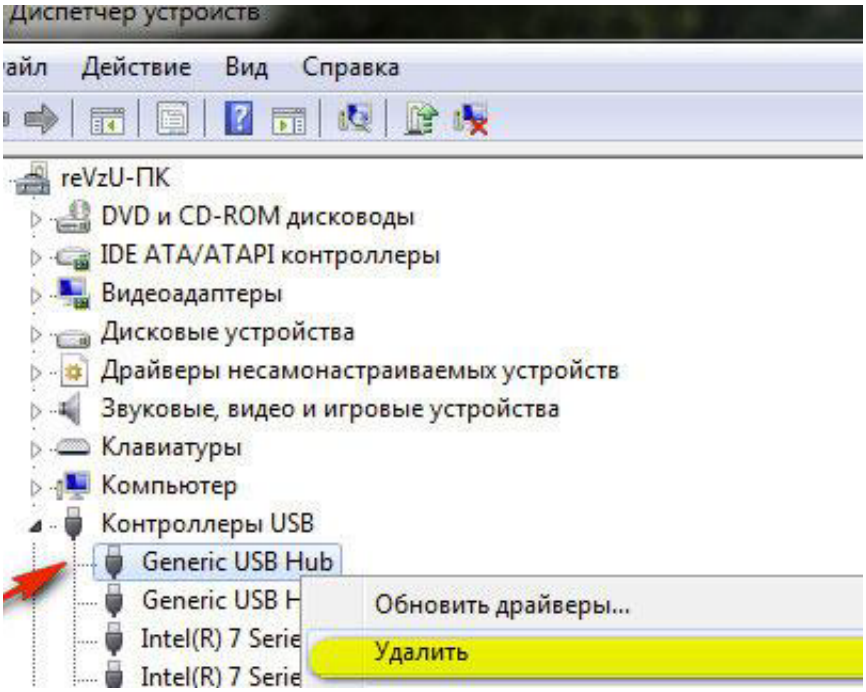


Рисунок 2.5 – Видалення драйверу пристрою в диспетчері пристроїв

Але недоліком цього способу є те, що при підключенні користувачем USB-накопичувача, Windows буде перевіряти наявність драйверів і при їх відсутності запропонує встановити драйвер.

В такому разі можна спробувати детальне видалення драйверу USB:

1 Утримуючи клавішу «Win», натискаємо клавішу «Pause / Break». Існує інший спосіб: Пуск → правою кнопкою «Комп'ютер» → Властивості.

2 У вікні, в лівій панелі, переходимо «Додаткові параметри системи».

3 На вкладці «Додатково» натискаємо кнопку «Змінні середовища».

4 У верхньому блоці клацніть «Створити»(рис. 2.6).

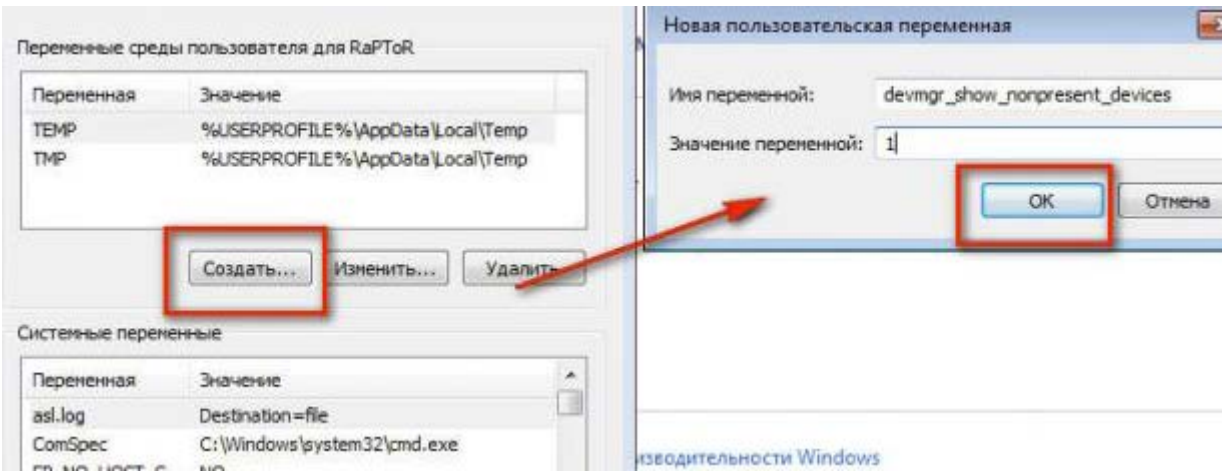


Рисунок 2.6 – Створення нової користувацької змінної

5 У вікні «Нова призначена для користувача змінна»:

- в рядку «Ім'я змінної» введіть - devmgr_show_nonpresent_devices;
- в «Значення змінної» - 1.

6 Натисніть «ОК» в панелі змінної і у вікні «Змінні середовища».

7 Поверніться у вікно властивостей системи (Win + Break) і клацніте «Диспетчер пристроїв».

8 У диспетчері відкрийте: Вид → Показати приховані ...

9 Натисніть кнопку «Оновити конфігурацію ...» (остання в панелі).

10. Іконки не використовуваних драйверів в диспетчері пофарбовані в сірий колір, тобто можна видалити цей драйвер. По черзі відкриваємо наступні директорії і прибираємо USB драйвери (рис. 2.7).

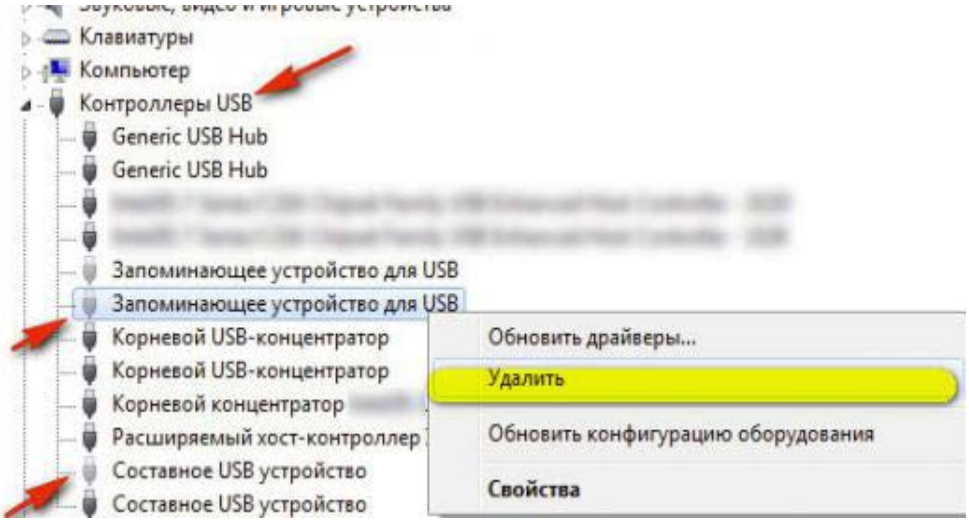


Рисунок 2.7 – Видалення використовуваних та замаскованих драйверів

11. По завершенні очищення перезавантажуємо ПК.

Але порушник КЗЗ може завантажити драйвер з іншого типу носіїв даних, що передбачені для робити з такою АС. Наприклад наявність дисководу вирішує проблему відновлення драйверу.

2.2.5 Використання програми Microsoft Fix It (50061)

Ще один спосіб заборони доступу до USB-накопичувачів - це використання Microsoft Fix It 50061.

Ідея цього способу полягає в тому, що розглядаються 2 умови вирішення задачі:

- USB-накопичувач ще не був встановлений до комп'ютера
- USB-пристрій підключено до комп'ютера

Пакет Microsoft easy fix може бути реалізованим одним з наступних типів файлів на основі технології, яка використовується для створення простого пакету виправлень .msi або .diagcab, але рішення diagcab призначені тільки для Windows 7 і пізніших версій Windows. Windows Vista і Windows XP не можуть запускати рішення .diagcab. Ще слід врахувати, що даний спосіб підходить не для всіх версій ОС Windows.

2.2.6 Використання додаткового програмного забезпечення для блокування доступу до USB-накопичувачів інформації

В робочому процесі системні адміністратори часто використовують утиліти для обмеження використання флеш-накопичувачів и зовнішніх дисків. Більшість таких програм просто змінює значення згаданої вище гілки реєстру, але існують просунуті варіанти. Такі вміють запам'ятовувати дозволені флешки за номером томи (VSN - Volume Serial Number) и блокуваті інші.

Однак такий захист не надійний, оскільки можна спробувати просто вивантажити процеси цих програм з пам'яті або підмінити VSN, оскільки це 32-бітове значення, що надається розділу при його форматуванні за значенням поточної дати і часу.

Дізнатися VSN довіреної флешки можна командою vol або dir. Використовуючи програму Volume Serial Number Changer, флеш-накопичувач отримує такий же номер і не має обмежень у користуванні. До захисту VSN довіреного флеш-накопичувача додають використання лише певної мітки тому (рис. 2.8). Це захист слабкий, але він може затримати особу без прав доступу на вхід до системи на певний час.

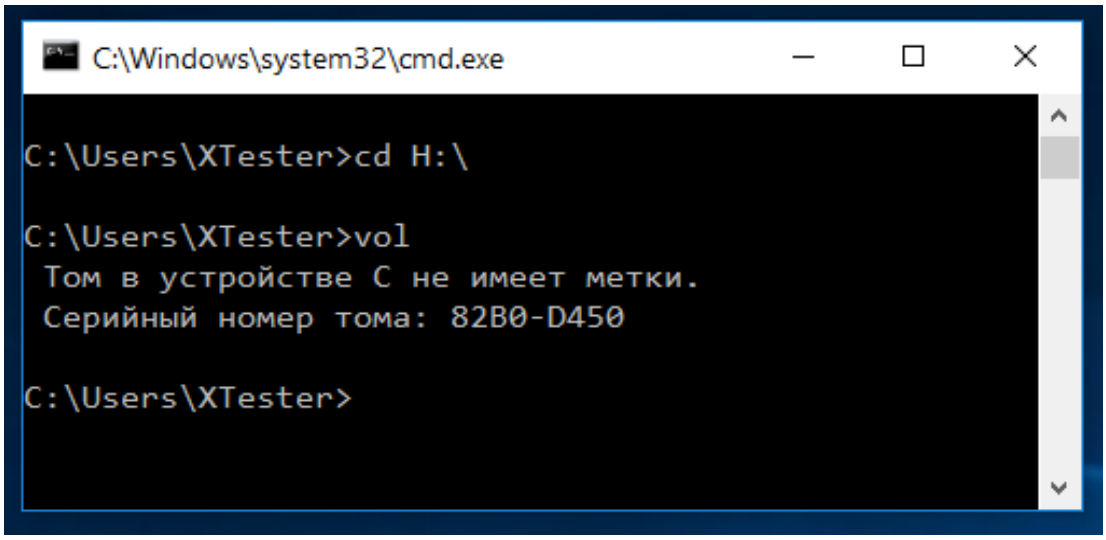


Рисунок 2.8 – Використання системних команд для пошуку серійного номеру

Інший варіант отримання доступу до системи, спробувати порушувати роботу програм контролю, часом завантажуючись з флешки і змінюючи назви її робочих файлів, в разі необхідності, видаляючи з автозавантаження. Адміністратор АС вважатиме програму забагованою і можливо видалить її.

Несподіваним захистом від несанкціонованого завантаження з використання флешок виникає на комп'ютерах з поганим дешевим блоком живлення, на більшості дешевих офісних робочих станціях. Справа в тому, що шина 5 В виснажується настільки, що флешці не вистачає живлення. В такому випадку потрібно відключити інший пристрій з парного USB-порту або використовувати активний хаб з власним блоком живлення.

Значно надійнішою програмою для встановлення заборони доступу до USB портів є USB Drive Disabler. Дана програма відповідає за работу служби usbstor. Налаштувань USB Ports Disabler не має, установка пароля для самозахисту, на жаль, не передбачена, через що програму доводиться ховати в файловій системі. Але утиліта має свої плюси, наприклад, вибірковість дії, що виявляється у відключенні тільки носіїв інформації, тоді як підключені по USB-інтерфейсу периферійні контролери будуть визначатися і працювати в звичайному режимі.

2.2.7 Фізичне відключення USB портів

Хоча фізичне відключення USB портів на материнській платі є практично нездійсненним завданням, можна відключити порти, що знаходяться на передній або верхньої частини корпусу комп'ютера, від'єднавши кабель, що йде до материнської плати. Цей спосіб повністю не закриє доступ до USB портів, але зменшить ймовірність використання накопичувачів недосвідченими користувачами і тими, хто просто полінується підключати пристрої до задньої частини системного блоку. Але задні порти розпаяні на самій материнській платі, котрих мінімально два. У сучасних материнських платах дуже часто є тільки 1 порт PS / 2 і друге периферійний пристрій підключається до порту USB. Тому можна спробувати підключити USB-хаб, приєднати його замість мишки або клавіатури і підключити всю штатну периферію через нього. Другий залишити для завантажувальної флешки.

2.2.8 Управління груповими політиками ОС

В домені комп'ютери керуються централізовано через групові політики, однак і цей захист можливо подолати. При підключенні нового USB пристрою до комп'ютера, система автоматично визначає пристрій і встановлює відповідний драйвер, в результаті чого користувач практично відразу може використовувати підключений USB пристрій або накопичувач. У деяких організаціях для запобігання витоку конфіденційних даних і проникнення в мережу вірусів, можливість використання USB накопичувачів (флешки, USB HDD, SD-карти і т.п) відключають з міркувань безпеки. Політика блокування USB пристроїв буде працювати, якщо інфраструктура відповідає вимогам: Версія схеми Active Directory - Windows Server 2008 і вище. Необхідно розуміти, що набір політик, що дозволяє управляти установкою і використанням зйомних носіїв, з'явився тільки в ОС Windows Vista, Windows 7 і вище.

Симулюючи ситуацію з обмеженням використання USB накопичувачів для всіх комп'ютерів в певному контейнері (OU). Припустимо, відбувається поширення дій політики на OU з ім'ям Workstations. Для цього, відкривається консоль управління GPO (gpmc.msc) і, натиснувши ПКМ по OU Workstations, створимо нову політику (Create a GPO in this domain and Link it here) (рис. 2.9).

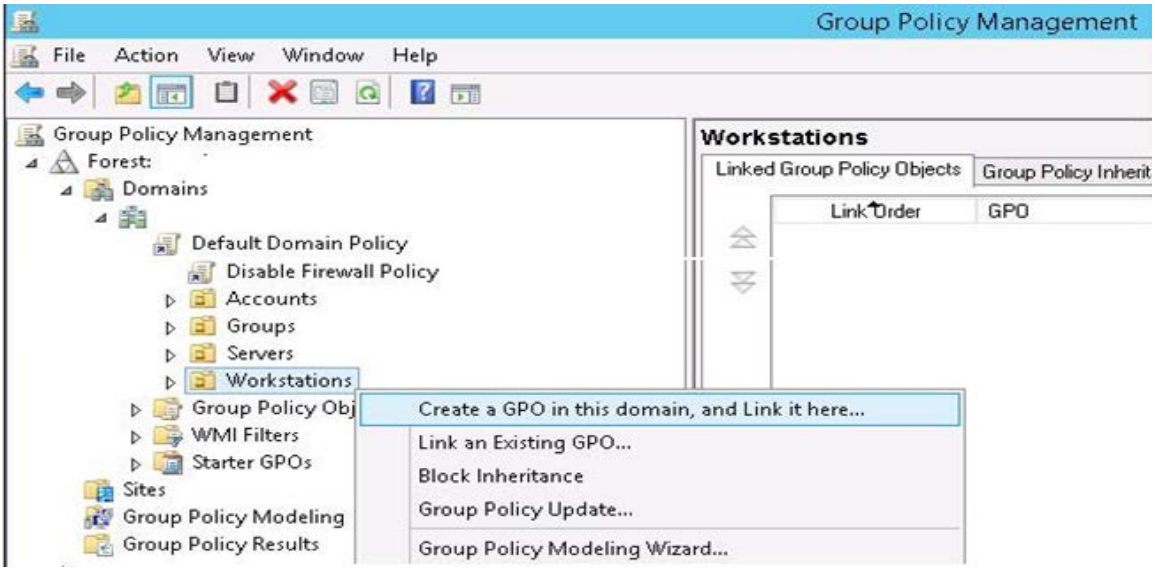


Рисунок 2.9 – Створення нової групової політики

У разі використання окремого комп'ютера, політика обмеження використання USB портів може бути відредагована за допомогою локального редактора групових політик - gpedit.msc. Назвемо політику Disable USB Access (рис. 2.10).

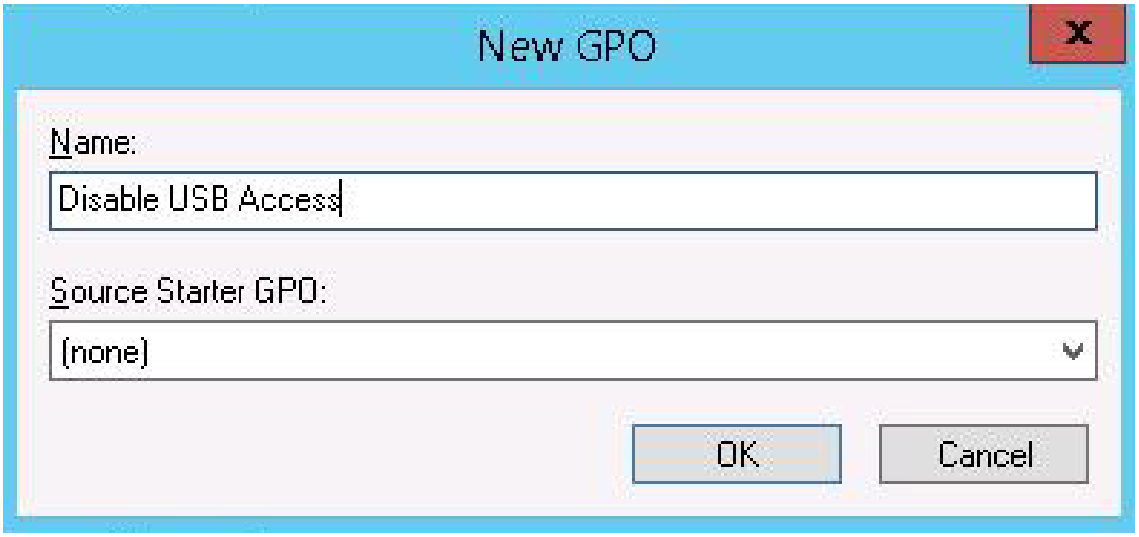


Рисунок 2.10 – Створення нової групової політики в локальному редакторі

Тепер необхідно відредагувати її параметри (Edit) (рис. 2.11).

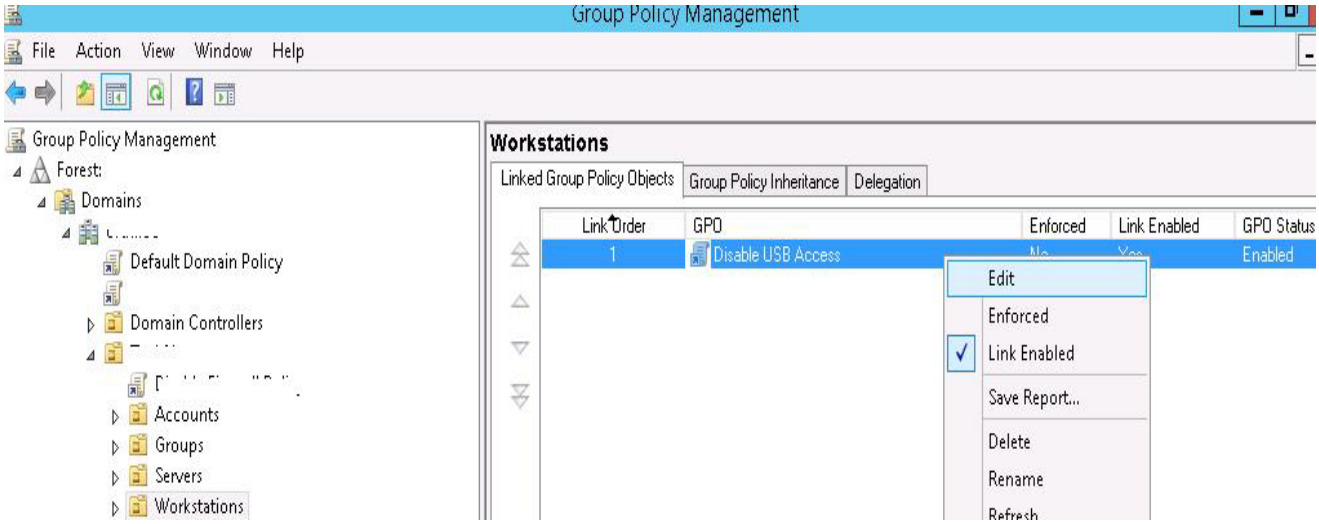


Рисунок 2.11 – Редагування створеної політики Disable USB Access

Налаштування блокування зовнішніх носіїв присутні в призначеному для користувача і комп'ютерних розділах GPO:

User Configuration-> Policies-> Administrative Templates-> System-> Removable Storage Access (Конфігурація користувача -> Адміністративні шаблони -> Система -> Доступ до зйомних запам'ятовуючих пристроїв)

Computer Configuration-> Policies-> Administrative Templates-> System-> Removable Storage Access (Конфігурація комп'ютера-> Адміністративні шаблони -> Система -> Доступ до зйомних запам'ятовуючих пристроїв)

Блокуються USB накопичувачі на рівні комп'ютера і далі проводяться дії з розділом Removable Storage Access.

У розділі Removable Storage Access є кілька політик, що дозволяють відключити можливість використання різних класів пристроїв зберігання: CD / DVD диски, флоппі диски (FDD), USB пристрої і інші пристрої.

Політика з найбільшими обмеженнями - All Removable Storage Classes: Deny All Access (Зйомні пристрої всіх класів: Заборонити будь-який доступ) - дозволяє повністю відключити доступ до будь-яких типів зовнішніх пристроїв зберігання даних. Щоб включити цю політику, треба перевести стан параметру в Enable (рис. 2.12).

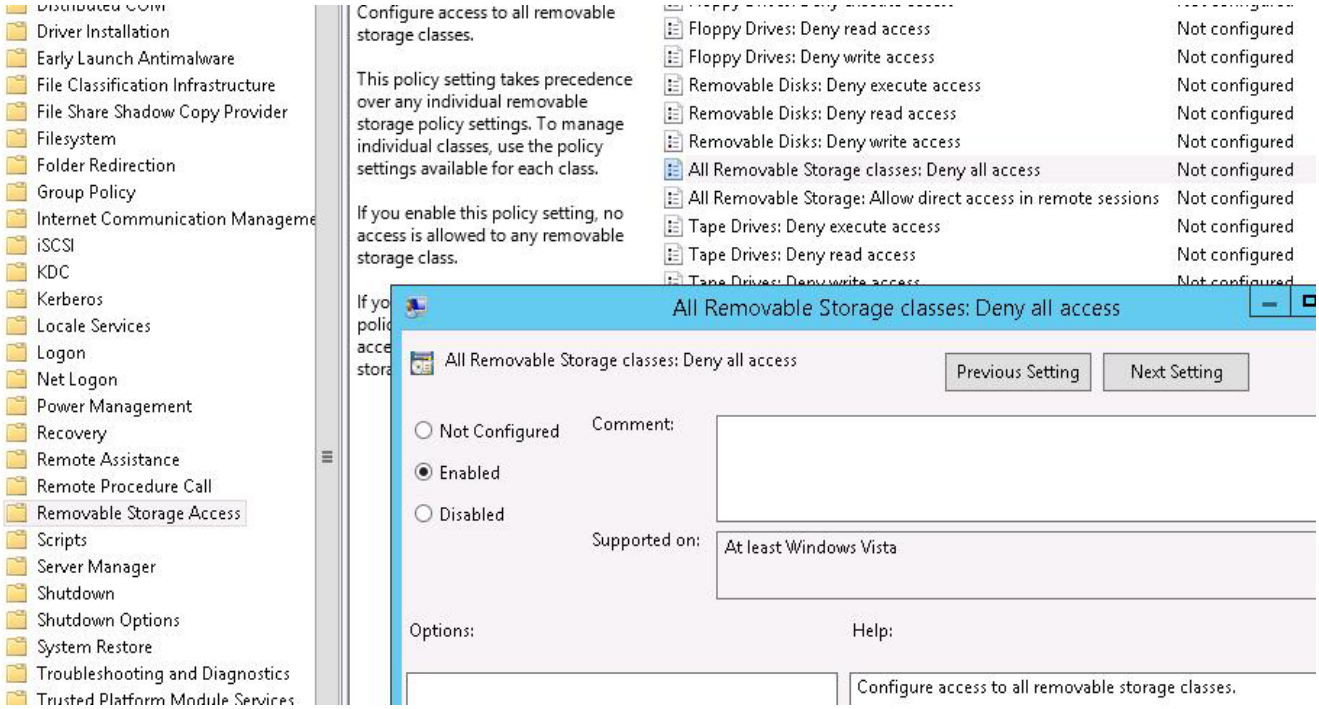


Рисунок 2.12 – Редагування параметру Enable в груповій політиці All Removable Storage Classes: Deny All Access

Після активації політики та поновлення її на клієнтах (gpupdate / force) зовнішні пристрої визначаються системою, але при спробі їх відкрити з'являється помилка: Location is not available, Drive is not accessible. Access is denied (рис. 2.13)

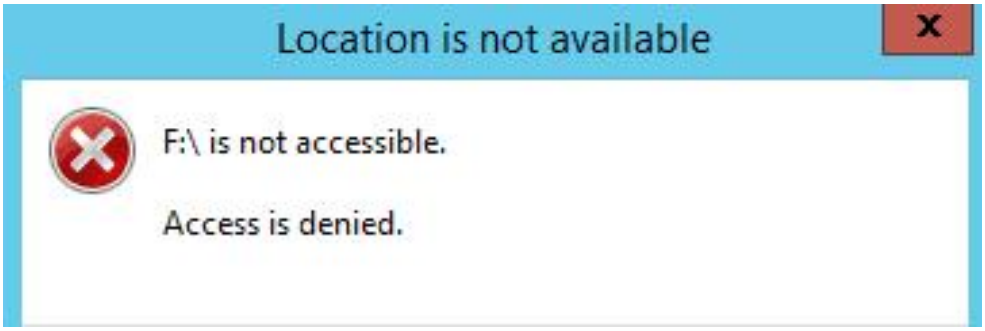


Рисунок 2.13 – Системне сповіщення системи про відмову у доступі

У разі необхідності, аналогічне обмеження можна задати, через реєстр, створивши в гілці HKEY_CURRENT_USER \ Software \ Policies \ Microsoft \ Windows \ RemovableStorageDevices ключ Deny_All типу Dword зі значенням 00000001.

У цьому ж розділі політик можна налаштувати більш гнучкі обмеження на використання зовнішніх USB накопичувачів.

Наприклад, щоб заборонити запис даних на USB флешки і диски, досить включити політику Removable Disk: Deny write access (Зйомні диски: Заборонити запис) (рис. 2.14).

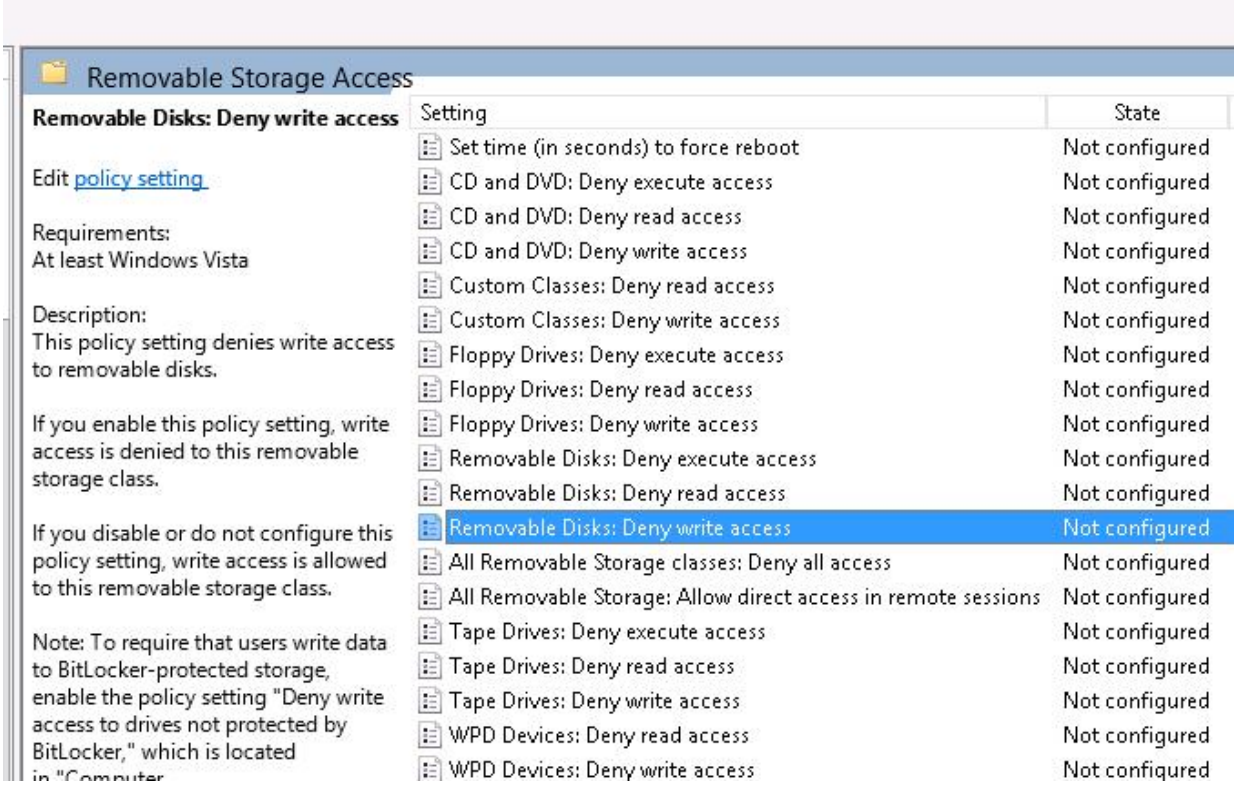


Рисунок 2.14 – Встановлення заборони на запис зі зйомних носіїв

У такому випадку користувачі зможуть читати дані з флешки, але при спробі записати на неї інформацію, отримають помилку (рис. 2.15):

Destination Folder Access Denied

You need permission to perform this action

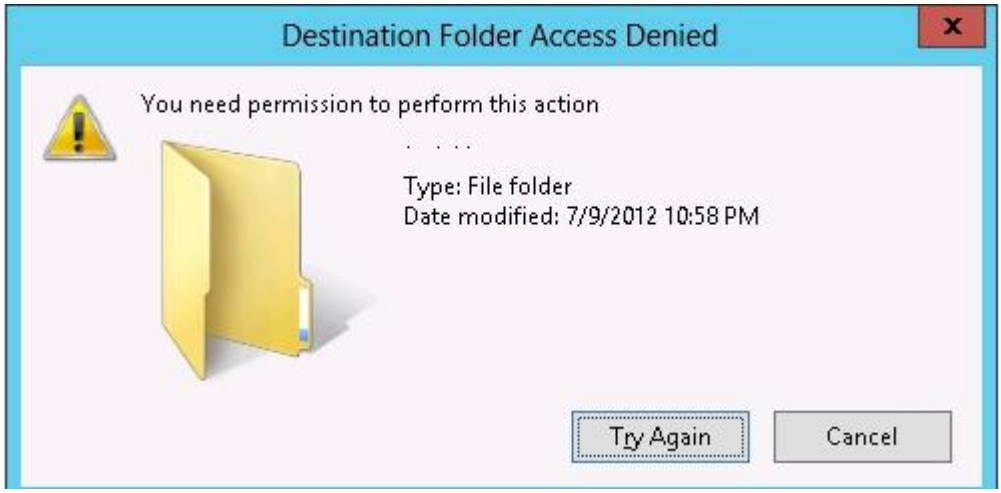


Рисунок 2.15 – Системне сповіщення про заборону запису на носій

За допомогою політики Removable Disks: Deny execute access (Зйомні диски: Заборонити виконання) можна заборонити запуск з USB дисків виконуваних файлів і файлів сценаріїв (рис. 2.16).

Рисунок 2.16 – Заборона запуску виконуваних файлів зі зйомник носіїв

Але в домені комп'ютери керуються централізовано через групові політики, однак і цей заслін можна подолати. Найпростіший спосіб - не дати політикам завантажитися. Для цього запускаєш Windows в безпечному режимі або просто відключаєш машину від локальної мережі при включенні. У другому випадку можна залогінитися в домен навіть без фізичного підключення до нього, оскільки Windows кешує дані попереднього входу і при втраті зв'язку з контролером домену виконує перевірку локально.

Після входу можна знову підключитися до локальної мережі і працювати як зазвичай, тільки вже без активних політик. Мінус цього способу полягає в не вибіркову підході. В політиках записані не тільки обмеження, але і додаткові ресурси, на зразок виділеної мережевої папки.

Окремо варто виділити файл налаштувань групових політик gpedit.msc, що дозволяє задати адміністративний шаблон, який забороняє доступ до знімних запам'ятовуючих пристроїв. Одне з найбільш важливих налаштувань в ньому називається «Виконувати тільки зазначені додатки Windows». Зазвичай за допомогою цього інструменту офісний працівник отримує доступ тільки до додатків з білого списку. В ньому знаходяться Word, Excel, калькулятор та інші необхідне ПЗ. Всі інші «імена» виконуваних файлів автоматично потрапляють під

заборону. Але досить перейменувати cmd.exe або totalcmd.exe в winword.exe і можна використовувати. Змінити обмеження можна через редактор віддаленого реєстру в WinPE. Вони записані в наступній гілці:

HKEY_CURRENT_USER \ SOFTWARE \ Microsoft \ Windows \ CurrentVersion \ Policies \ Explorer \ RestrictRun.

Для цього потрібно завантажитися з флешки, дізнатися пароль локального адміністратора або скинути його, якщо не вдалося дізнатися. Паралельно з тим активуємо потрібний обліковий запис, в разі необхідності. Далі запускається gpedit.msc та відключається заборону (рис. 2.17).

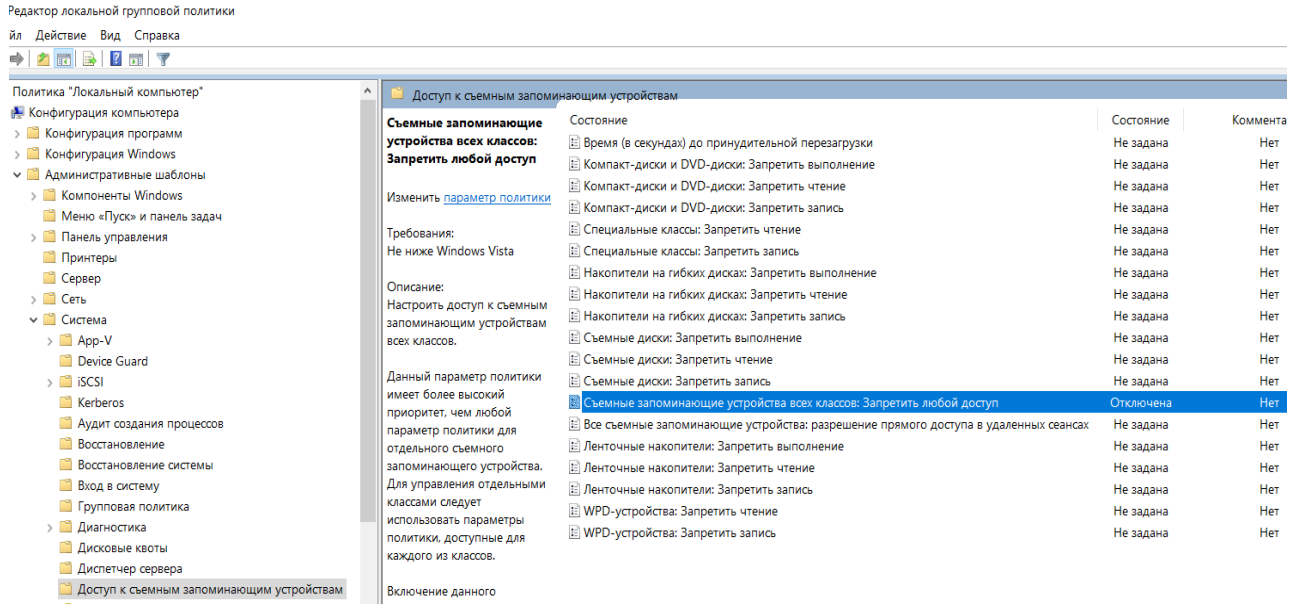


Рисунок 2.17 – Відключення заборони на використання USB-накопичувачів

Проаналізувавши вище описану інформацію, отримано всі необхідні дані для розробки можливих варіантів реалізації пристрою захисту від несанкціонованого доступу та принципу роботи.

2.3 Розробка пристрою захисту АС від несанкціонованого завантаження ОС зі стороннього носія

Розробка пристрою з функцією контролю активності USB-порта. Вимоги до пристрою, що захищає АС від можливості реалізації несанкціонованого завантаження ОС:

1 Пристрій має активувати USB-порт тільки після завантаження штатної ОС та КЗЗ. Для цього потрібно, щоб пристрій отримував команду від ОС, тобто між операційною системою та пристроєм має бути налагоджений обмін даними.

1.1 Виходячи с цього обмін буде налагоджений за допомогою USB каналу, що знаходиться на материнській платі.

1.2 Для цього необхідно, щоб пристрій мав контролер. Так як немає необхідності аналізу трафіку даних, то контролер повинен виконувати функцію управління комутатором USB. Якщо часові параметри опрацювання команд, такі як ввімкнути чи вимкнути пристрій, відбуваються з затримкою від 1 мс до 100 мкс, то вони не є критичними. В зв'язку з цим, високих вимог до продуктивності контролера не висувається**.** В такому випадку великої кількості пам'ять даних для програм непотрібно.

Для оперативної запам'ятовуючої пам'яті потрібна незначна кількість місця, оскільки не має потреби в обробці пакетів та великого об'єму даних, також немає таблиць. В ній зберігатиметься приблизно від 20 до 30 змінних, тому вистачить обсягу в кілобайту. Даний пристрій повинен мати USB інтерфейс для підключення до материнської плати, тобто низьке живлення для роботи з USB.

1.3 Має бути передбачено наявність комутуючого пристрою USB, що забезпечить комутацію USB портів, тобто N- кількість входів комутуємо на один.

Треба зазначити, що повинен бути керуючий сигнал для його блокування від контролера. Можливо буде потрібен стабілізатор живлення з 5 вольт на 3,3 вольта, а також перетворювачі рівня для узгодження рівнів сигналу.

1.4 Контролер має активуватися при ввімкненні живлення ПК.

1.5 До надходження команди від ОС – порти USB мають бути заблоковані.

Також пристрій обов'язково має виконувати блокування USB портів на задній панелі в АС.

Розглянемо декілька варіантів розроблюваного засобу, щоб обрати найбільш ефективний з них.

2.3.1 Зовнішній пристрій захисту від несанкціонованого завантаження

Зовнішній пристрій захисту, виконаний у вигляді моноблока, підключається до передніх портів USB на корпусі АС.

Така система захисту стає неефективна в зв'язку з тим, що досить витягнути прилади з порту USB і можливості запобігання несанкціонованого завантаження нічого не завадить (рис. 2.18).

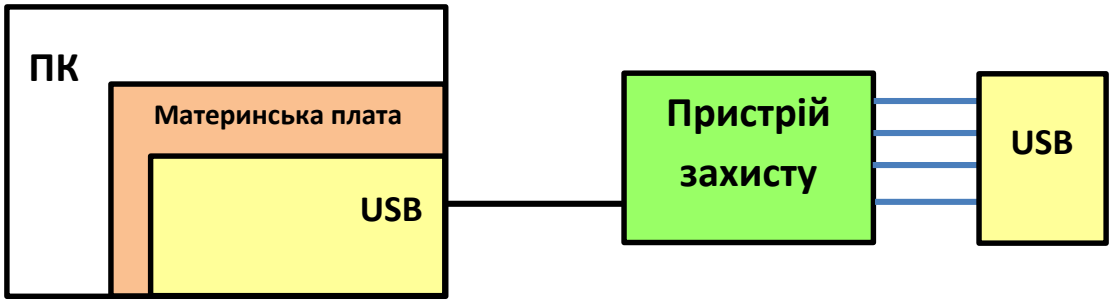


Рисунок 2.18 – Функціональна схема роботи зовнішнього пристрою

2.3.2 Внутрішній пристрій захисту від несанкціонованого завантаження

Внутрішній пристрій можна розробити з використанням мікропроцесорів чи без них. У такому вигляді виконання, не виникає небезпека простого фізичного доступу до пристрою, при цьому використовується живлення з материнської плати. Пристрій підключається до кабелю, що проходить від материнської плати до передніх портів USB, в середині корпуса АС, тобто є проміжною ланкою. В кожній з реалізацій відбувається блокування задньої панелі USB-інтерфейсу на корпусі АС, з використання одного чи декількох способів блокування USB, розглянутих раніше.

1 Реалізація пристрою захисту з використанням таймеру.

Такий пристрій досить дешевий розробці. Він не керує USB-інтерфейсом, а лише блокує активність його на час завантаження операційної системи та КЗЗ (рис. 2.20).

Однак це не надійний спосіб. Існує можливість того, що порушник перезапустить АС без знеструмлення. В такому випадку, ОС може знадобитися

додатковий час на завантаження і ліміт встановленого таймеру закінчиться раніше, залишивши систему без захисту. Також можлива ситуація, що повторна генерація сигналу RESET не відбудеться. У такому випадку, після закінчення тимчасової затримки, порти розблокуються. АС більше не зможе блокувати USB-інтерфейс та втрачає захист від несанкціонованого завантаження зі стороннього носія (рис. 2.19). На рисунку нижче, наведено можливу структуру роботи пристрою, де $\overline{CS}$ – сигнал блокування, VDD – плюс.

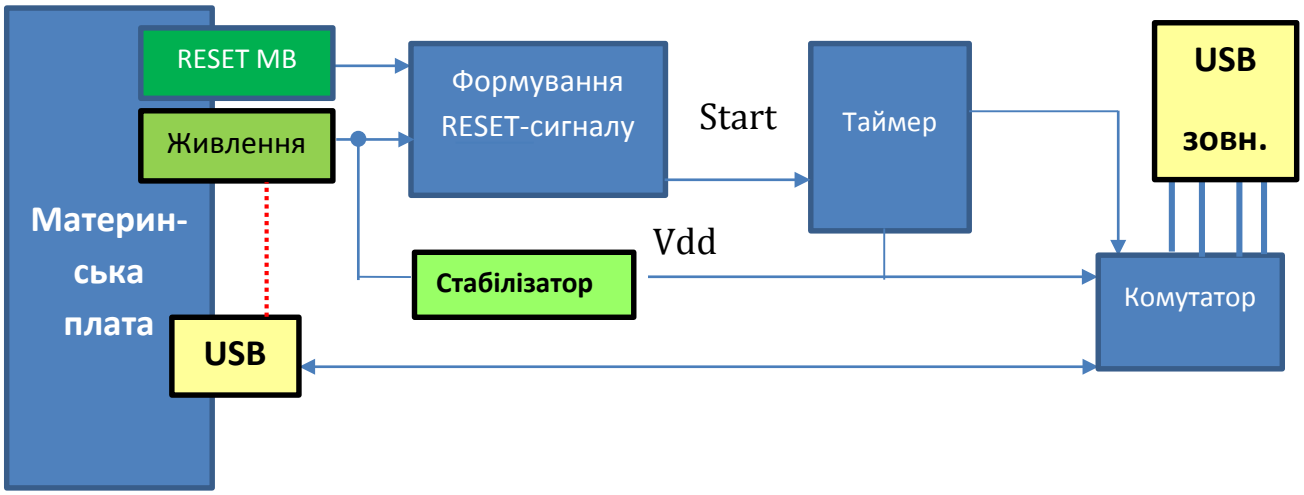


Рисунок 2.19 – Структурна схема роботи зовнішнього пристрою з таймером

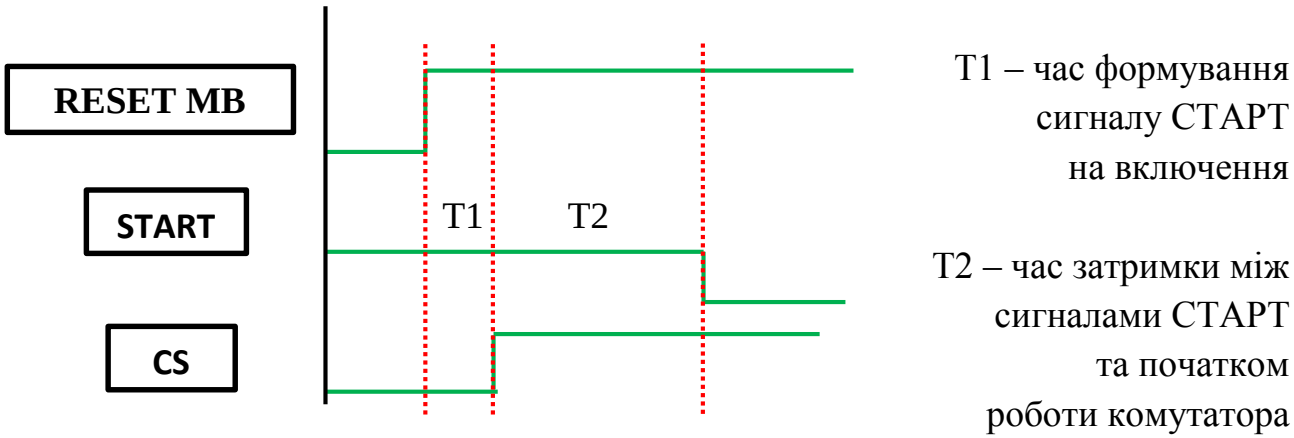


Рисунок 2.20 – Графік формування сигналу доступу до комутатора

2 Реалізація пристрою з використанням мікроконтролеру

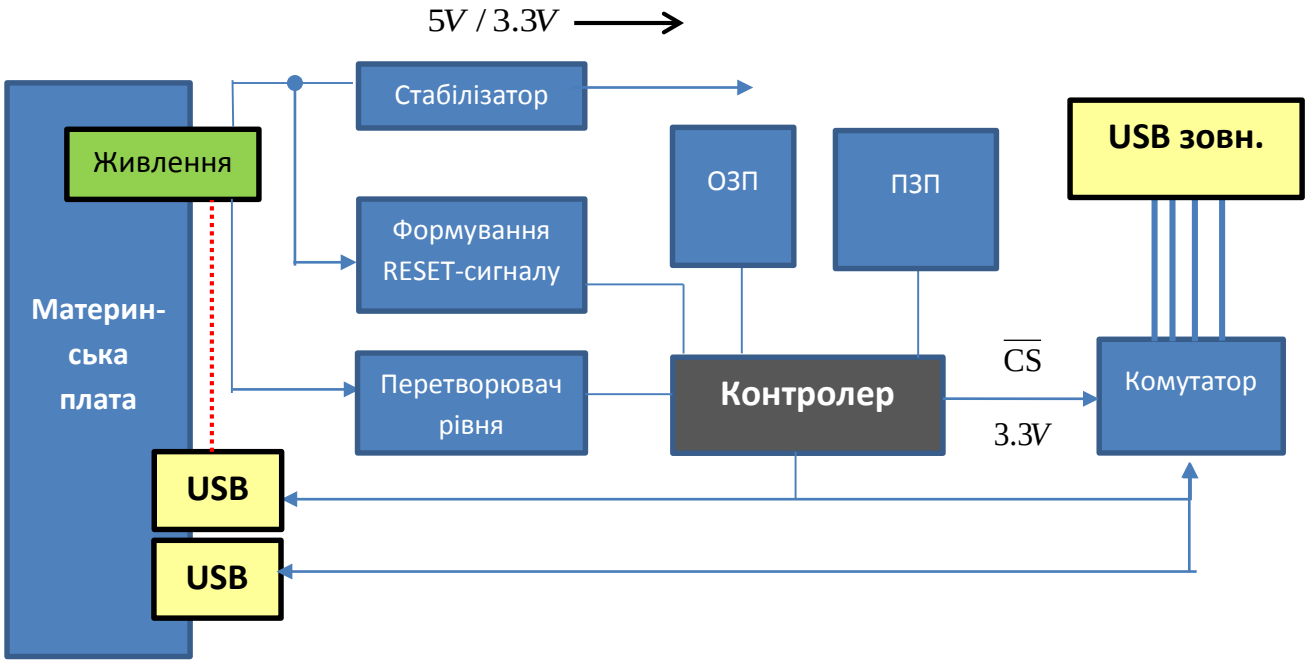


Рисунок 2.21 – Структурна схема роботи зовнішнього пристрою на базі PIC-мікроконтролеру

При включенні живлення на нього буде сформований сигнал скидання, буде запущена програма управління пристроєм. За замовчуванням комутатор має бути заблокований. Через порт USB надійде команда на ввімкнення USB портів, контролер сформує сигнал управління, котрий розблокує комутатор. Після комутатор буде комутуватися на внутрішньому порту материнської плати – тим самим забезпечуючи підключення пристрою. У випадку загрози КЗЗ здійснює формування сигналу блокування портів. Схема алгоритму роботи пристрою зображена в Додатку Б.

Опираючись на вимоги до пристрою та реалізацію на базі мікроконтролеру, можна сказати, що пристрій складається з наступних частин: контролера, ОЗП (пам’ять даних) та ПЗП (пам'ять програм), перетворювача рівня (ПУ), стабілізатора. Комутатор має підключення до живлення з материнської плати.

Вимоги до контролера:

- низьке енергоспоживання;
- невеликий об’єм ОЗП та ПЗП;
- низька швидкодія;

- наявність портів USB;
- наявність керованих виходів.

Виходячи з вимог до контролеру, найкращим вибором є PIC16F628A:

- тактова частота від DC до 20МГц;
- підтримка переривань;
- 35 однослівних команд, всі команди виконуються за один машинний цикл, крім команд розгалуження і умови з істинним результатом/
- Генератор таймеру TMR1: - 1.2мкА, 32кГц, 2.0В (тип.)
- Широкий діапазон напруги живлення від 2.0В до 5.5В
- Режим низьковольтного програмування
- Програмування на платі через послідовний порт (ICSP) (з використанням двох виводів)
- Захист коду програми
- Скидання по зниженню напруги живлення BOR
- Скидання по включенню живлення POR
- Висока витривалість комірок FLASH / EEPROM: 125 байт, 100 000 циклів стирання / запису FLASH пам'яті програм, 1 000 000 циклів стирання / запису EEPROM пам'яті даних
- наявність послідовного інтерфейсу
- наявність програм керованого виходу USART.
- Пам'ять програм (слів): 2048;
- ОЗП (байт): 224

Комутатор: на даний момент в робочих станціях зазвичай використовується USB 2.0 та 3.0. Враховуючи, що розроблюваний пристрій не опрацьовує велику кількість даних, то вистачить USB 2.0. На висновку цього обираємо FE1.1S, що має:

- повністю відповідає специфікації універсальної послідовної шини Revision 2.0 (USB 2.0);
- вбудовані регулятори від 5 до 3,3 В і 1,8 В;
- можливість налаштування EEPROM;

- інтегровані USB 2 приймально-передавальні пристрої;
- автоматичний контроль стану автономного живлення;
- вбудована схема включення живлення;
- вбудовані трансивери USB 2.0

Дозволяє комутувати порти, при подачі сигнал низького рівня USB блокуються, при подачі високого рівня - розблоковуються. FE1.1S підходить в якості комутатора для керування портами.

В схему пристрою було додано стабілізатор ADP1710AUJZ для коректної роботи комутатора.

Пристрій для формування сигналу скидання може бути сформований на пасивних елементах, резистор та конденсатор. Також треба врахувати необхідність використання перетворювача рівня. Обрано PL 2303, оскільки: 2 контакти виведення живлення: 3.3 і 5.5 В, контакти: TX, RX, GND, 3.3V, 5.5V (рис. 2.21).

3 Реалізація пристрою з використанням ЦПОС.

Для деяких систем, крім задачі виконання критерію НЦ-2, є необхідність вести журнал подій, дій пов’язаних з безпекою. Якщо політикою безпеки передбачено протоколювання спроб підключення, то ця функція перекладається на розроблюваний пристрій, оскільки до завантаження штатної ОС та КЗЗ не можливо провести таку операцію. Журнал реєстрації повинен містити інформацію, достатню для встановлення користувача, процесу і/або об'єкта, що мали відношення до кожної зареєстрованої події. Протокол взаємодії журналу з КЗЗ складається з наступних команд: запит журналу, видалення журналу, запис до журналу. Можливі варіації цих команд.

За один запис в журнал подій має бути занесено наступну інформацію: дату в форматі рік\місяць\день, час з точність до секунди, код події, ідентифікатор пристрою, успішність чи неуспішність кожної зареєстрованої події, перші декілька байт обміну даних. Мінімально вистачить 32 кілобайт пам’яті. Можливі наступні варіації коду подій, що будуть логуватися:

- 00-підключення;
- 01-файли;
- 02-папки;
- 03-автозапуск;
- 04-збереження інформації;
- 05-видалення.

В такому випадку розроблюваний засіб захисту має додатково відповідати критерію реєстрації подій під час завантаження НР-1, відповідно до НД ТЗІ 2.5-004-99. КЗЗ має можливість в будь-який момент перевірити журнал підключень пристрою та проводить очищення по певному алгоритму чи вручну (рис. 2.22).

Основний алгоритм роботи. При включенні живлення, формується сигнал скидання, що блокує USB порти. Якщо відбувається підключення до АС, то відбувається протоколювання подію в зовнішню ПЗП. Якщо під'єднався відомий пристрій до системи, тобто із «білого» списку пристроїв, що пройшли перевірку СЗІ, то журнал отримає штатний лог та можливість роботи з АС. В разі під'єднання невідомого пристрою, система заблокує доступ та запише відповідний лог до журналу.

Якщо підключень не відбувалось, то перевіряється наявність підключень на даний момент. Якщо нічого немає, починається розблокування портів. Після завантаження ОС та КЗЗ, відбувається розблокування портів та зчитується протокол подій. КЗЗ має можливість посилати команди на зчитування, видалення запис подій. В разі переповнення журналу або заповнення його до половини, система може просигналізувати про це користувачу, що має доступ до неї. Варто зазначити, що команд видалення може бути запрограмовано досить багато і з різним функціоналом. Наприклад видалення лише 10 перших, коли буфер журналу даних стане переповненим. Схема алгоритму роботи пристрою наведена в Додатку В.

Таким чином формуються наступні вимоги до пристрою:

- Підвищені вимоги по продуктивності. Контролер, крім комутації портів, повинен проводити аналіз трафіку.

- Низьке енергоспоживання контролеру;
- Мінімум 3 порти USB 2.0;
- Підвищені вимоги до об’єму пам’яті програм. Алгоритму необхідно оброблювати пакети середнього рівня складності.
- Пам’ять даних (ОЗП) необхідно хоча б 100 кілобайт.
- Збереження протокольованих даних в ПЗП, окремо від контролера. Мінімум має бути 32 кілобайт пам’яті для запису. До цієї зовнішньої пам'яті немає вимог до швидкості обміну.
- В пристрої має бути достатня кількість USB портів, для під’єднання материнської плати та зовнішніх пристроїв.
- Потрібен годинник реального часу (RT), для ведення протоколювання.
- Невисокий струм споживання для контролеру, через використання живлення з USB материнської плати.

Виходячи з вимог до пристрою, воно складається з: контролеру (процесор), ОЗП (пам’ять даних) та ПЗП (пам'ять програм), перетворювача рівня (ПУ), стабілізатора, окремого ПЗУ для збереження журналу підключень, перетворювача рівня, годинника реального часу. Комутатор має підключення до живлення на з материнської плати. Процесор працює на 3.3 В, а значить для підключення USB портів доведеться використовувати перетворювач рівня.

Виходячи з вимог до пристрою, найкращим вибором контролеру є TMS320VC5509A:

- три внутрішніх шини читання даних / операндів;
- дві внутрішніх шини записи даних / операндів;
- вбудоване ОЗУ 128К х 16 біт;
- на базі контролеру вже є годинник реального часу реалізований всередині;
- програмний контроль енергоспоживання шести функціональних блоків з внутрішніх пристроїв.

Для зовнішнього ПЗП підходить флеш-пам'ять M25P10-AVMN6P:

- напруга живлення від 2,7 до 3,6В;

- сумісний з послідовним інтерфейсом шина SPI;
- частота тактової частоти 40 МГц (максимум) ;
- низьке енергоспоживання;
- займає мало місця на платі;
- об’єм пам’яті 1 Мбіт.

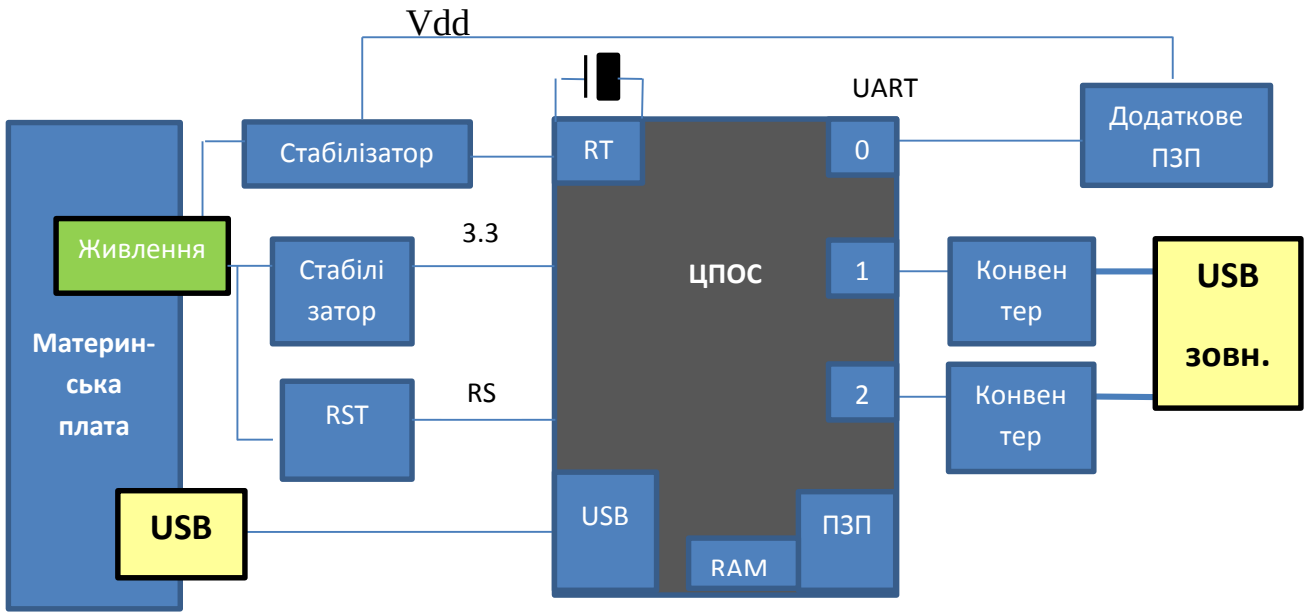


Рисунок 2.22 – Структурна схема роботи зовнішнього пристрою на базі ЦПОС

2.4 Висновки до другого розділу

У результаті проведеної роботи, було:

- проаналізовано можливість протидії завантаженню зі стороннього носія штатними засобами захисту операційної системи;
- розглянуто вимоги до створення засобів захисту від несанкціонованого завантаження;
- визначено комплектну базу та побудовану схему алгоритму роботи перспективних рішень роботи;
- проаналізовано можлива ефективність розроблюваних пристроїв та сформована методика їх роботи;

- встановлено, що реалізацій пристрою на базі ЦПОС найкраще відповідає всім запитам з захисту від несанкціонованого завантаження.

РОЗДІЛ 3

ЕКОНОМІЧНЕ ОБҐРУНТУВАННЯ ДОЦІЛЬНОСТІ ВИКОРИСТАННЯ РОЗРОБЛЕНОГО ЗАСОБУ ЗАХИСТУ В АС

3.1 Техніко-економічне обґрунтування доцільності створення пристрою захисту від несанкціонованого завантаження операційної системи

У дипломній роботі проаналізовано способи та засоби захисту від несанкціонованого завантаження зі стороннього носія до автоматизованої системи. У спеціальній частині розглянуто можливі способи реалізації засобу, структура роботи та елементна база пристрою захисту від несанкціонованого доступу до АС.

Передбачається, що запропонований пристрій з використанням ЦПОС зможе суттєво зменшити витрати на захист автоматизованих систем українських підприємств. Порівнюються економічна ефективність організаційного способу контролю за діями користувача та пристрій захисту від несанкціонованого завантаження з використанням ЦПОС.

Середня заробітна плата по Дніпропетровській обл. складає 7479 грн. на місяць, опираючись на дані Міністерства фінансів України за 2017 рік. Для зручності розрахунків вважатимемо, що заробітна плата працівника СЗІ та розробників пристрою захисту однакова та округлена до 7480 грн/місяць.

Кошторисна вартість проектування та впровадження програми ($С_{Свир}$) включає в себе наступні витрати, що визначаються за формулою:

$$С_{Свир} = С_{ЗПр.} + С_{ЕСВ} + C_{М.ч..} + C_{З\text{-}в.Н.} + C_{М.}, \quad (3.1)$$

де $С_{ЗПр.}$ – заробітна плата розробників ПП, грн.;

$С_{ЕСВ}$ – відрахування на соціальне страхування, грн.;

$C_{М.ч..}$ – вартість машинного часу, необхідного для розробки та налаштування ПП, грн.;

$C_{З\text{-}в.Н.}$ – загальновиробничі (накладні) витрати (витрати на оплату праці управлінського персоналу, оплату службових відряджень, консультаційно-інформаційні витрати, ремонт і технічне обслуговування інших основних фондів, окрім ПК, оренда приміщення тощо);

$C_{М.}$ – вартість матеріалів, комплектуючих, грн.

До заробітної плати розробників програмного продукту ($С_{ЗПр.}$) належать витрати на виплату основної та додаткової зарплати виконавців, обчислені згідно із системою оплати праці, прийнятими в організації, включаючи будь-які види матеріальних та грошових доплат. Визначається за формулою:

$$C_{ЗПр.} = C_{ЗПосн.} + C_{ЗПдод.}, \quad (3.2)$$

Основна заробітна плата розробників ПП визначається за формулою:

$$C_{ЗПосн.} = C_{ЗПдень.} \times T_{заг.}, \quad (3.3)$$

де $C_{ЗПдень}$ – денна зарплата програміста (340 грн. / люд-дн.);

$T_{заг.}$ – загальна трудомісткість розробки ПП (комп'ютерної системи), 6 людино-днів .

$$С_{ЗПосн.} = 340 \times 6 = 2040 \; грн.$$

Додаткова заробітна плата (премії, одноразові заохочення тощо) розраховується згідно з нормативом, який установлює підприємство і який складає 10 – 20 % від основної зарплати. Витрати на додаткову заробітну плату визначаються за формулою:

$$C_{ЗПдод.} = k_{ЗПдод.} \times C_{ЗПосн.} \quad (3.4)$$

де $k_{ЗПдод.}$ – нормативний коефіцієнт додаткової заробітної плати = 0,3 част. од;

$C_{ЗПосн}$ – витрати на основну заробітну плату, 2040 грн.

$$C_{ЗПдод.} = 0{,}3 \times 2040 = 612\ грн.$$

Визначимо заробітну плату розробників ПП:

$$C_{ЗПр.} = 2040 + 612 = 2652\ грн.$$

До витрат на сплату єдиного соціального внеску ($С_{ЄСВ}$) належать витрати, що здійснюються у порядку та розмірах, передбачених чинним законодавством України (тобто це нарахування від суми основної та додаткової зарплати, які беруться з підприємства; згідно з нормативами і які складають 22%).

Витрати на сплату єдиного соціального внеску визначаються за формулою:

$$C_{ЕСВ.} = k_{ЕСВ} \times (C_{ЗПосн.} + C_{ЗПдод}), \quad (3.5)$$

де $k_{ЕСВ}$ – коефіцієнт витрат на сплату ЄСВ.

$$C_{ЕСВ.} = 0{,}22 \times (2040 + 612) = 583 \text{ грн.}$$

Для розрахунку заробітної плати, що отримає програміст, за виконання програмування пристрою окрім своїх основних службових обов'язків, слід визначити час, що буде витрачений ним на опрацювання технічного завдання, підготовку робочої станції та виконання програмування.

Тривалість вивчення технічного завдання, опрацювання довідкової літератури з урахуванням уточнення ТЗ і кваліфікації програміста можливо оцінити за формулою[27]:

$$t_в = \frac{B}{(0{,}7...0{,}8) \cdot k}\ , \text{люд-год}, \quad (3.6)$$

де В – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання, В = 1,2...1,5;

k – коефіцієнт, що враховує кваліфікацію програміста і визначається стажем роботи за фахом:

- до 2 років – 0,8;
- від 2 до 3 років – 1,0;
- від 3 до 5 років – 1,1...1,2;

- від 5 до 7 років – 1,3...1,4;
- понад 7 років – 1,5...1,6.

Таким чином, тривалість вивчення методики буде складати:

$$t_в = \frac{1 \cdot 1,2}{0,7 \cdot 0,8} = 2,14 \text{ люд-год.}$$

Тривалість підготовки робочої станції можливо оцінити за формулою[27]:

$$t_{пр} = \frac{1}{(0,2...0,3) \cdot k}, \text{ люд-год,} \quad (3.7)$$

де k – коефіцієнт, що враховує кваліфікацію програміста і визначається стажем роботи за фахом:

- до 2 років – 0,8;
- від 2 до 3 років – 1,0;
- від 3 до 5 років – 1,1...1,2;
- від 5 до 7 років – 1,3...1,4;
- понад 7 років – 1,5...1,6.

Тривалість підготовки робочої станції буде складати

$$t_{пр} = \frac{1}{0,3 \cdot 0,8} = 4,17 \text{ люд-год.}$$

Враховуючи особливості побудови методики, виконання усіх її пунктів буде займати приблизно $t_м$ =40 годин робочого часу.

Загальний час, що має бути витрачений на виконання тестування, розраховується за формулою:

$$t_з = t_в + t_{пр} + t_м, \text{ люд-год.} \quad (3.8)$$

Загальний час, що має бути витрачений на виконання програмування, складатиме:

$$t_з = 2,14 + 4,17 + 40 = 46,31 \text{ люд-год.}$$

Оскільки 1 година робочого часу програміста складає 42,5 грн., то одна година понаднормової роботи складає 63,75 грн.

Оскільки для виконання процесу налагодження програмного забезпечення необхідно використовувати ПК, то потрібно розрахувати вартість використання машинного часу, що включає в себе амортизаційні відрахування та вартість електроенергії за період використання ПК.

Для створення моделі пристрою був придбаний комп’ютер, сума комплектуючих якого коштувала у 2017 році 8 тис грн.

Комп’ютери відносяться до четвертої групи «машини та обладнання» об’єктів основних засобів та інших необоротних активів, термін корисного використання в цій групі дорівнює мінімум 2 роки, виберемо мінімальний термін 2 роки. Щорічні амортизаційні відрахування розраховано за прямолінійним методом:

$$A = 8000 \div 2 = 4000 \text{ грн/рік}$$

Таблиця 3.1 – Компоненти для розробки пристрою

№ п\п	Найменування комплектуючих засобу захисту	Ціна комплектуючої засобу захисту, грн.
1	TMS320VC5509A PGE	80
2	PL 2303	50
3	TPS767D301PWP	100
4	M25P10-AVMN6P	80
Сумарна ціна комплектуючих		310

Таблиця 3.2 – Програмне забезпечення, що використовується у розробці ПО для пристрою

Найменування ПЗ	Тип ліцензії	Строки використання
ОС Windows 7 Professional	Платна, 1500 грн.	Не обмежені, оновлення безкоштовні
Icarus Verilog	Freeware (Безкоштовна)	Не обмежені, оновлення безкоштовні
Libreoffice	Freeware (Безкоштовна)	Не обмежені, оновлення безкоштовні
OpenMP	Freeware (Безкоштовна)	Не обмежені, оновлення безкоштовні

Треба зауважити, що данні наведені в таблицях є приблизними для обчислення і носять демонстраційний характер.

$$C_{м.} = 1500 + 310 = 1810 \; грн.$$

Амортизаційні відрахування за час проведення тестування на проникнення розраховуються за формулою:

$$A_{\text{Т}} = ((A + A_{пз}) \div 2020) \cdot tз \text{, грн.,} \qquad (3.8)$$

де 2020 – річна норма робочих годин;

$t_з$ – кількість понаднормових годин, під час яких має проводитись розробка.

Амортизаційні відрахування за час проведення програмування становитимуть:

$$A_{\text{Т}} = ((1500 + 4000) \div 2020) \cdot 46.31 = 126 \text{ грн.} \qquad (3.9)$$

Проектна потужність закуплених комп'ютерів складає:

$$P = 0{,}4 \text{, кВт/год.}$$

Оскільки дана модель розраховується не для конкретного підприємства, то розрахунок тарифів за електроенергію ведеться по максимальним тарифам енергоспоживання. Згідно з існуючою тарифною сіткою для підприємств першого класу за денним тарифом вартість одного кВт/год. складає 1,68 грн.

Вартість електроенергії під час проведення програмування розраховується як:

$$R = P \cdot 1{,}68 \cdot 63.75 \text{, грн,} \qquad (3.10)$$

де 63,75 – кількість понаднормових годин, під час яких має проводиться тестування.

Вартість електроенергії під час проведення тестування буде становити:

$$R = 0{,}4 \cdot 1{,}68 \cdot 63.75 = 43 \text{ грн.}$$

Загальна вартість використання машинного часу для тестування може бути розрахована за формулою:

$$\text{С}_{\text{мч}} = A_{\text{Т}} + R \text{, грн.} \qquad (3.11)$$

Загальна вартість використання машинного часу для програмування буде становити:

$$С_{МЧ} = 126 + 43 = 169 \text{ грн.}$$

До статті «Накладні витрати» відносять витрати, пов'язані з управлінням і організацією робіт. Накладні витрати розраховуються відносно основної заробітної плати. Величина накладних витрат приймається рівною 85% від основної зарплати виконавців.

Формула розрахунку:

$$C_{З\text{-}в.Н.} = C_{ЗПосн} \times k_{НАКЛ.} \quad (3.12)$$

де $C_{З\text{-}в.Н.}$ — накладні витрати, грн.;

$C_{ЗПосн.}$, — основна заробітна плата виконавців, грн.;

$k_{накл.}$ — коефіцієнт обліку накладних витрат ($k_{накл.}$ = 0,85).

$$C_{З\text{-}в.Н.} = 2040 \times 0{,}85 = 1734 грн.$$

Результати розрахунку витрат на проектування програмного забезпечення зведені у таблиці 3.3.

Таблиця 3.3 – Кошторис витрат на розробку і впровадження програми

Найменування статей	Позначення	Сума, грн.
Основна заробітна плата	$C_{ЗПосн.}$	2040
Додаткова заробітна плата	$C_{ЗПдод}$	612
Відрахування на соціальні потреби	$С_{ЕСВ}$	583
Матеріали	$C_{М}$	1810
Амортизація ПК та ПО	$C_{М.ч..}$	169
Накладні витрати	$C_{З\text{-}в.Н.}$	1734
Разом	$С_{Свир}$	10183

Таким чином загальні витрати на розробку пристрою складають 10183 грн.

Оскільки планується випускати 30 пристроїв, ціна собівартості пристрою складає 340 грн. Витрати на виробництво одиниці продукту складають 100% від собівартості пристрою – 340 грн. З урахуванням надбавки на додану вартість в розмірі 20%, ціни упаковки пристрою – 100 грн., ціна реалізації одного пристрою складає 936 грн.

При використанні організаційного способу контролю за діями користувача слід враховувати, що для підтримки функціонування КЗЗ співробітнику СЗІ потрібно щомісячно платити зарплатню. Користуючись попередніми розрахунками, вважатимемо, що вартість однієї години роботи працівника СЗІ складає 42,5 грн. Враховуючи, що денне навантаження працівника становить 4 години, то місячна зарплатня становить 3740 грн. Виходячи з того, що в день підприємству треба виплатити співробітнику 170 грн., окупний термін розробленого пристрою складає 6 днів.

Найближчим пристроєм, що реалізує аналогічні функції безпеки, на ринку апаратно-програмних комплексів захисту від несанкціонованого завантаження є АПМДЗ «Соболь». Ціна такого комплексу складає приблизно 5250 грн.

Таким чином річна економія після впровадження засобу захисту на базі ЦПОС розраховується за формулою:

$$E = B - J, \text{ грн.}, \tag{3.13}$$

де B — ціна комплекса з аналогічними функціями, грн.;

J — ціна реалізації запропонованого пристрою, грн.

Річна економія від впровадження методики становить:

$$E = 5250 - 936 = 4247 \text{ грн.}$$

$$Еф = 4247 \cdot 100 \div 5250 = 81\%$$

3.2 Висновки за третім розділом

В виконаному економічному розділі було розраховано необхідні витрати на розробку пристрою, що включають заробітну плату виконавців, ціну

комплектуючих, амортизацію програмного забезпечення та вартість робочої станції, що є необхідним для проведення процесу розробки. В результаті було визначено ціну собівартості та ціну реалізації пристрою, що на 81% дешевше від аналогічного за функціоналом комплексу довіреного завантаження. Таким чином, розробка та створення засобу захисту від несанкціонованого завантаження ОС в АС є доцільним та економічно вигідним.

ВИСНОВКИ

У дипломній роботі було розроблено засіб захисту від несанкціонованого завантаження операційної системи в АС класа «1».

Розглянуто існуючі способи захисту ОС від несанкціонованої завантаження зі стороннього носія та проведено порівняльний аналіз ефективності їх системи захисту. В результаті проведеної роботи було визначено, що існуючі засоби захисту не є досконалими.

Розглянуто можливість реалізації захисту АС за допомогою вбудованих засобів ОС, маніпулюючи з налаштуванням USB-портів. Визначено, що в разі

недостатнього захисту чи неможливості реалізації з використанням USB, виникає необхідність розробки власного пристрою чи способу захисту інформації.

У спеціальній частині були сформульовані вимоги до створення альтернативного засобу захисту від несанкціонованого завантаження, проаналізовано можливу ефективність пристроїв та сформована методика їх роботи, визначено комплектну базу та схему алгоритму роботи перспективних рішень роботи. Розроблений альтернативний пристрій захисту від несанкціонованого завантаження є доцільним для використання в АС класа «1».

В економічному розділі наведено економічне обґрунтування доцільності використання розробленого пристрою захисту.

Практичне значення роботи полягає в створенні пристрою захисту від несанкціонованого завантаження операційної системи, адаптованого до умов функціонування в сучасних АС.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1 НД ТЗІ 2.5-004-99 - Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу

2 НД ТЗІ 2.5-004-99 - Типове положення про службу захисту інформації в автоматизованій системі .

3 О.Г. Вагонова, Ю.О. Волотковська, Н.М. Романюк. Методичні вказівки до виконання економічної частини дипломного проекту (для студентів напряму підготовки 1701 Інформаційна безпека) – Дніпропетровськ: ДВНЗ "Національний гірничий університет", 2013. – 17 с.

4 ДТЕК Дніпрообленерго. Тарифи на електроенергію на 2017 рік. [Електронний ресурс]. – Режим доступу: http://doe.com.ua/tarif_prom/2017.
5 Порочна спадщина Windows: концептуальні методи взлому (Електрон. Ресурс) / Спосіб доступу: URL: https://xakep.ru/2011/07/19/56270/
6 розкриваємо Windows. Легкі способи отримати права адміністратора на робочому комп'ютері (Електрон. Ресурс) / Спосіб доступу: URL: https://xakep.ru/2016/09/29/bypassing-office-pc-restrictions/
7 Кількість вірусів, використовуючих Windows Autorun , стрімголов падає (Електрон. Ресурс) / Спосіб доступу: URL: https://xakep.ru/2011/06/15/55950/
8 How to use Microsoft easy fix solutions (Електрон. Ресурс) / Спосіб доступу: URL: https://support.microsoft.com/en-us/help/2970908/how-to-use-microsoft-easy-fix-solutions
9 Бездисковая загрузка по технологии iSCSI на базе ОС Windows (Електрон. Ресурс) / Спосіб доступу: URL: https://habrahabr.ru/post/244661/
10 LAN Boot ROM (Електрон. Ресурс) / Спосіб доступу: URL: http://www.probios.ru/options/lan/integrated/lan-boot-rom.html
11 Робимо скидання пароля bios (Електрон. Ресурс) / Спосіб доступу: URL: http://pyatilistnik.org/delaem-sbros-parolya-bios/
12 Аккорд-У: универсальное средство защиты информации (Електрон. Ресурс) / Спосіб доступу: URL: https://www.linux.org.ru/forum/general/9266034
13 Обозначение цепей питания в иностранных материалах (Електрон. Ресурс) / Спосіб доступу: URL: http://radiokot.ru/articles/49/
14 Как удалить старые драйвера usb-устройств из Windows? (Електрон. Ресурс) / Спосіб доступу: URL: http://izbavsa.ru/tehnika/kak-udalit-starye-drayvera-usb-ustroystv-windows
15 PIC16F628A - Основные характеристики (Електрон. Ресурс) / Спосіб доступу: URL: http://www.microchip.ru/d-sheets/40044.htm:PIC16F628A:1x1
16 Налаштування BIOS через ОС (Електрон. Ресурс) / Спосіб доступу: URL: https://www.linux.org.ru/forum/general/9266034

17 Система захисту інформації ЛОЗА™-1, версія 2 (Електрон. Ресурс) / Спосіб доступу: URL: http://avtoprom.kiev.ua/product.html
18 Программный комплекс средств защиты информации от несанкционированного доступа «Гриф» (Електрон. Ресурс) / Спосіб доступу: URL: http://ict.com.ua/?lng=1&sec=8&art=51
19 Комплекс средств защиты информации «Гриф-2000» (Електрон. Ресурс) / Спосіб доступу: URL: http://ict.com.ua/?lng=1&sec=8&art=31
20 Средства защиты информации от несанкционированного доступа (Електрон. Ресурс) / Спосіб доступу: URL: https://www.y-center.ru/corporate/zaschita-informatsii/sredstva-zaschity-informatsii/ot-nesanktsionirovannogo-dostupa/
21 Про Intel vPro або як віддалено зайти в чужий BIOS (Електрон. Ресурс) / Спосіб доступу: URL: https://habrahabr.ru/company/intel/blog/138377/
22 Опції BIOS USB Mouse Support - Legacy USB Support (Електрон. Ресурс) / Спосіб доступу: URL: http://www.nastrojkabios.ru/klaviatura-i-mish/legacy-usb-support.html
23 Блокувальник USB портів - USB Security Lock (Електрон. Ресурс) / Спосіб доступу: URL: https://faqhard.ru/articles/13/35.php
24 Швидко і просто відключити USB-порти на Win7 2 частина (Електрон. Ресурс) / Спосіб доступу: URL: https://habrahabr.ru/sandbox/59259/
25 Защита компьютеров от нежелательных USB устройств (Електрон. Ресурс) / Спосіб доступу: URL: http://www.everstrike.ru/blockingusb/
26 БЛОКИРОВКА USB-НАКОПИТЕЛЕЙ ПРИ ПОМОЩИ ВОЗМОЖНОСТЕЙ ГРУППОВОЙ ПОЛИТИКИ (Електрон. Ресурс) / Спосіб доступу: URL: http://gpo-planet.com/?p=3218
27 FE1.1, FE2.1 или что нам стоит USB HUB построить (Електрон. Ресурс) / Спосіб доступу: URL: http://we.easyelectronics.ru/electro-and-pc/fe11-fe21-ili-chto-nam-stoit-usb-hub-postroit.html
28 Як перевірити проходженя reset-a? (Електрон. Ресурс) / Спосіб доступу: URL: http://vlab.su/viewtopic.php?t=1130

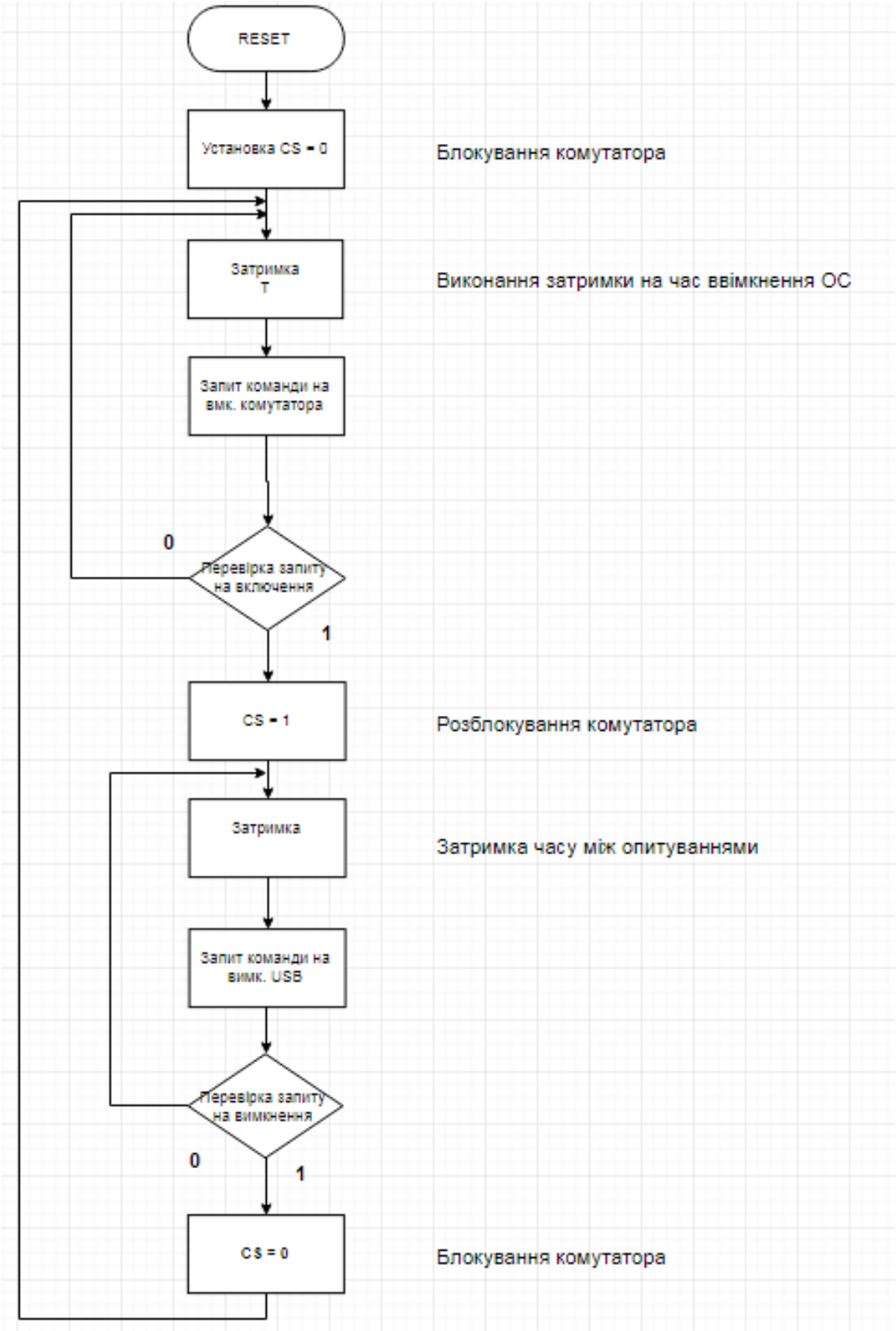
29 ПЛИС (FPGA) и микроконтроллер. В чем разница? (Електрон. Ресурс) / Спосіб доступу: URL: http://micro-proger.ru/2016/03/17/plis-fpga-i-mikrokontroller-v-chem-raznica/
30 Взлом Linux за допомогою підключення USB-пристроїв стає реальністю (Електрон. Ресурс) / Спосіб доступу: URL: https://xakep.ru/2011/03/08/54991/
31 Процесор цифрових сигналів (Електрон. Ресурс) / Спосіб доступу: URL: https://uk.wikipedia.org/wiki/%D0%9F%D1%80%D0%BE%D1%86%D0%B5%D1%81%D0%BE%D1%80_%D1%86%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%B8%D1%85_%D1%81%D0%B8%D0%B3%D0%BD%D0%B0%D0%BB%D1%96%D0%B2

ДОДАТОК А
ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

1. Дипломний проект Кучер Р.Ю. 125м–16–1.docx – Пояснювальна записка.
2. КучерР.Ю.pttx – Презентація.

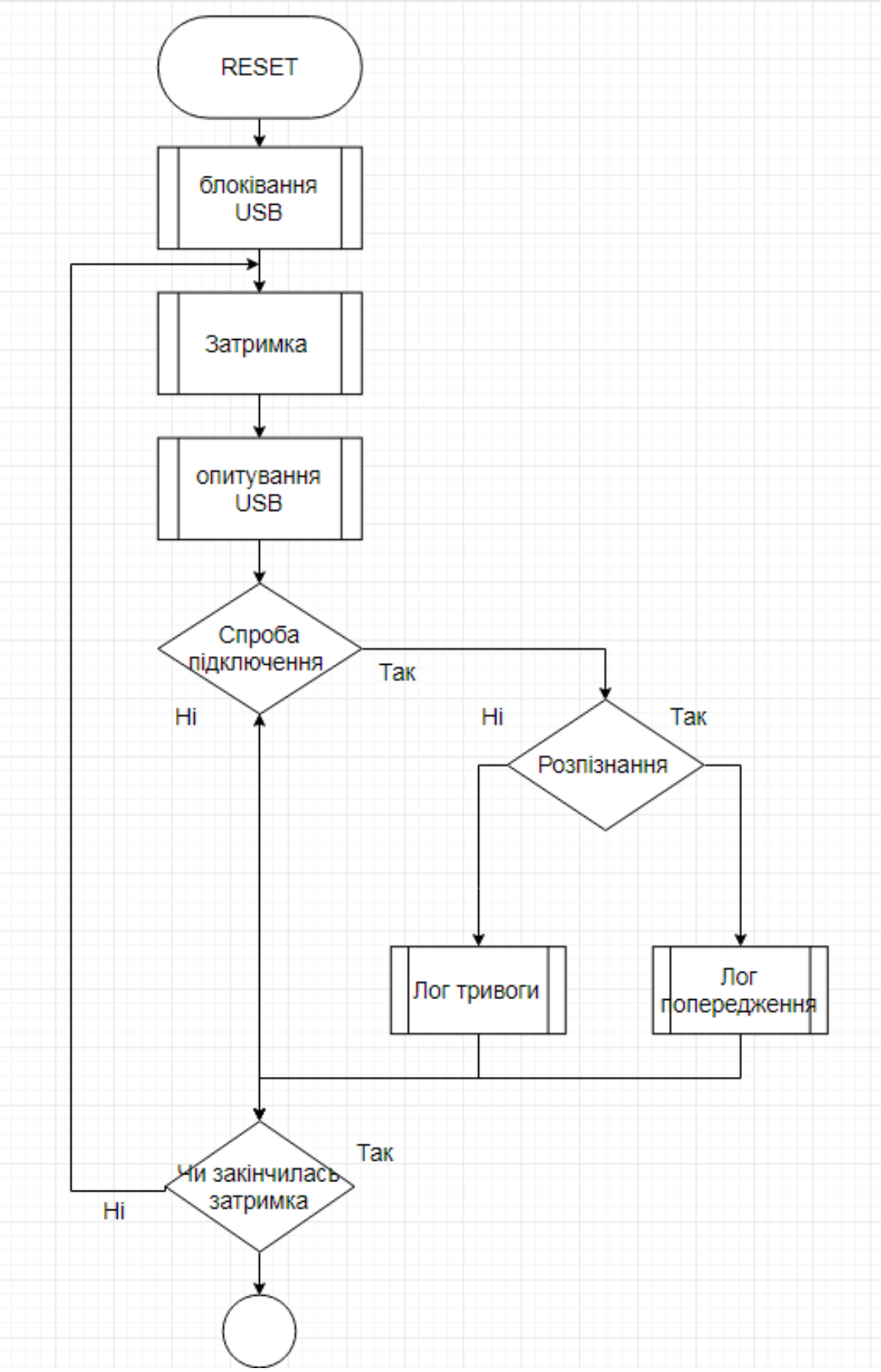
ДОДАТОК Б

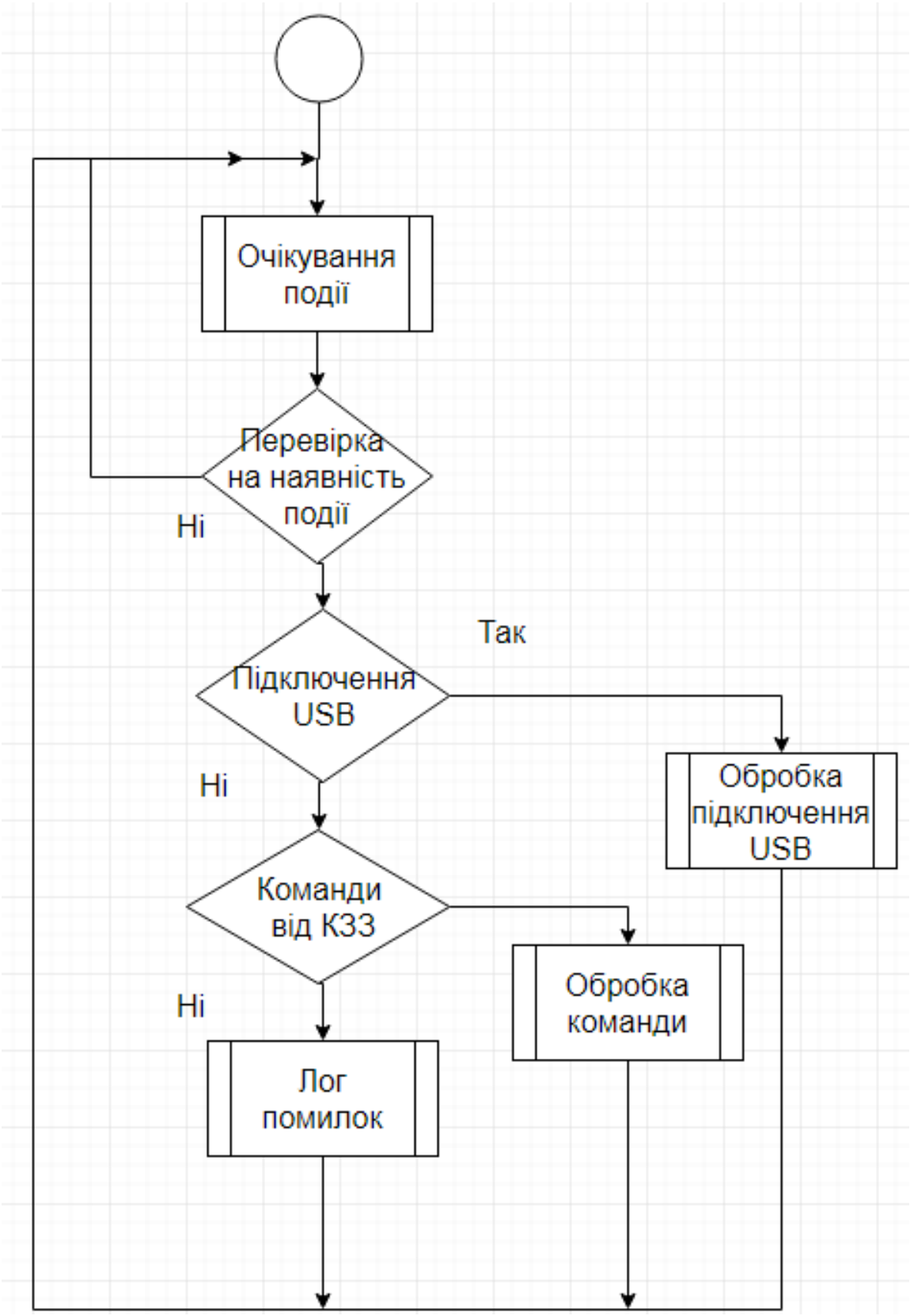
Схема алгоритму роботи розроблюваного засобу захисту на базі мікроконтролеру



ДОДАТОК В

Схема алгоритму роботи розроблюваного засобу захисту на базі ЦПОС


RESET
блокування USB
Затримка
опитування USB
Спроба підключення
Так
Ні
Ні
Розпізнання
Так
Лог тривоги
Лог попередження
Так
Чи закінчилась затримка
Ні


Очікування події
Перевірка на наявність події
Ні
Так
Підключення USB
Ні
Обробка підключення USB
Команди від КЗЗ
Ні
Обробка команди
Лог помилок

ДОДАТОК Г

ВІДГУК

на дипломну роботу магістра на тему:

«Засіб захисту від несанкціонованого завантаження операційної системи для АС класа «1»

студента групи 125м–16–1 *Кучера Ростислава Юрійовича*

Мета дипломної роботи – розробка ефективного засобу захисту від несанкціонованого завантаження операційної системи для АС класа «1».

Тема дипломної роботи безпосередньо пов'язана з об'єктом діяльності фахівця за спеціальністю 125 Кібербезпека – розвиток способів та засобів забезпечення цілісності комплексів засобів захисту.

Задачі дипломної роботи (аналіз вразливостей обчислювальних систем на етапі завантаження штатної операційної системи, аналіз методів та засобів захисту від несанкціонованого завантаження операційної системи, розробка вимог, до засобу, що розробляється, обґрунтування принципів побудови, розробка структурної та функціональної схем, алгоритмів функціонування обґрунтування елементної бази засобу захисту від несанкціонованого завантаження операційної) віднесені в освітньо-кваліфікаційній характеристиці магістра до класу евристичних, вирішення яких основане на знаково-розумових уміннях фахівця.

Оригінальність технічних рішень полягає у їх гнучкості та можливості вибору ефективного вибору засобу в залежності від вимог політики безпеки .

Практичне значення результатів проектування полягає у можливості використання запропонованих рішень для більшості материнських плат, що використовуються на сьогодні.

До недоліків дипломної роботи відносяться:

– незначні помилки в описі схем, що були розроблені;

– недостатній рівень опрацювання алгоритмів роботи засобів;

– недостатньо обґрунтовано вибір елементної бази.

Оформлення пояснювальної записки до дипломного проекту виконано з деякими відхиленнями від стандартів.

Ступінь самостійності виконання дипломної роботи достатня.

За час дипломування Кучер Р.Ю. виявив себе фахівцем, здатним вирішувати поставлені задачі.

В цілому дипломна робота виконана у відповідності до вимог, що ставляться до дипломної роботи магістра, заслуговує оцінки “_____”, а Кучер Р.Ю. присвоєння йому кваліфікації професіонал із організації інформаційної безпеки.

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

Керівник дипломної
роботи магістра,
д.ф-м.н., професор _____ Т.С. Кагадій

ДОДАТОК Д

ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Керівник розділу доц. Волотковська Ю.О.

(підпис) (ініціали, прізвище)