Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кібербезпека
(повна назва кафедри)

ПОЯСНЮВАЛЬНА ЗАПИСКА
до дипломної роботи

магістр
(освітній рівень)

на тему: Методика безпечного зберігання інформації на цифрових носіях

Виконав: студент 6 курсу, групи СБмз-61
спеціальності 125 «Кібербезпека»
(шифр і назва спеціальності)

_____ Купчак Ю.А.
(підпис) (прізвище та ініціали)

Керівник _____ Муж В.В.
(підпис) (прізвище та ініціали)

Нормоконтроль _____ Кареліна О.В.
(підпис) (прізвище та ініціали)

Рецензент _____ Кунанець Н.Е.
(підпис) (прізвище та ініціали)

м. Тернопіль – 2019

АНОТАЦІЯ

Дипломна робота на тему «Методика безпечного зберігання інформації на цифрових носіях» на здобуття освітньо-кваліфікаційного рівня «Магістр» за спеціальністю «Кібербезпека».

Об'єктом дослідження є процес зберігання та захисту інформації на цифрових носіях інформації.

Предметом дослідження є методика безпечного захисту та зберігання інформації на цифрових носіях.

Мета роботи – запропонувати методику зберігання інформації на цифрових носіях.

Для досягнення цієї мети в роботі було вирішено ряд завдань:

1. Розглянуто ознаки ідентифікації інформації на цифрових носіях.
2. Вивчено аспекти захисту інформації на цифрових носіях.
3. Проаналізовано методики захисту інформації на спеціальних цифрових носіях.
4. Запропонована методика безпечного зберігання інформації на носіях інформації за допомогою програмного засобу шифрування - VersCrypt.

За результатами проведених досліджень методик безпечного захисту інформації на ЦНІ запропонована методика зберігання інформації на флеш-накопичувачах, реалізована за допомогою програмного засобу шифрування, що використовує різноманітні алгоритми шифрування.

Ключові слова: ЦИФРОВІ НОСІЇ ІНФОРМАЦІЇ, USB-ТОКЕН, ФЛЕШ-НАКОПИЧУВАЧ, НЕСАНКЦІОНОВАНИЙ ДОСТУП, ШИФРУВАННЯ.

ABSTRACT

Diploma thesis on "Methods of secure storage of information on digital media" for the acquisition of educational-qualification level "Master" in the specialty "Cybersecurity".

The object of the study is the process of storing and protecting information on digital media.

The subject of the study is the technique of secure protection and storage of information on digital media.

The purpose of the work is to offer a method of storing information on digital media.

To achieve this goal in the work has been solved a number of problems:

1. Signs of identification of information on digital are considered.

2. Aspects of information protection on digital media have been studied.

3. Methods of protection of information on special digital media are analyzed.

4. The proposed method of secure storage of information on storage media using the software encryption tool - VersCrypt.

According to the results of the researches of the methods of secure information security at the CNI, a method of storing information on flash drives is proposed, implemented with the help of an encryption software that uses various encryption algorithms.

Keywords: DIGITAL INFORMATION MEDIA, USB TOKEN, FLASH ACCESSORIES, UNAUTHORIZED ACCESS, ENCRYPTION.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

СЦНІ - спеціальні цифрові носії інформації

ЕЦП - електронний цифровий підпис

ЕОМ - електронно-обчислювальна машина

СЕД - система електронного документообігу

USB-токен - (Universal Serial Bus) виконаний у вигляді брелока

PIN - Private Identification Number — персональний ідентифікаційний номер

RSA - Rivest, Shamir, Adleman — криптосистема Райвеста, Шаміра, Адлмана

ПРД - правила розмежування доступу

НСД - несанкціонований доступ

КС - криптосистема

АС - автоматизована система

ПЕОМ - персональна електронна обчислювальна машина

РНБОУ - Рада національної безпеки та охорони України

ОП - оперативна пам’ять

ФП – флеш накопичувач

ФК – флеш-карта

ПЗП – постійний запам’ятовуючий пристрій

ІБ – інформаційна безпека

ПЗ – програмне забезпечення

НІ – носій інформації

ЗІ – захист інформації

СЗІ – служба захисту інформації

АНБ – Агентство національної безпеки

НДР – науково-дослідницька робота

ВСТУП

У наш час розвиток держави та суспільства напряму залежить від належного рівня комп’ютеризації та процесу розвитку цифрових технологій. У всіх країнах світу, а також в Україні, розвиваються інформаційно-телекомунікаційні системи, для державного управління та контролю у сфері інформатизації. Велику роль відіграє електронний документообіг. Обмін інформації здійснюється як відкритою, так і закритою мережею і відіграє особливо важливе значення в економіці, обороні, освіті, науці тощо. Для здійснення коректної роботи та самого процесу обміну інформації використовується інформаційно-телекомунікаційна мережа.

Основною вимогою для безпечного документообігу є безпека інформації, що передається, і полягає в її цілісності та підтвердженні авторства. Аналізуючи розвиток суспільства, а також ряд масових проблем із забезпеченням цілісності даних, розвивається стрімка модернізація засобів захисту інформації, реалізованих у програмному та апаратному забезпеченні. Ця обставина, обумовлена масовим застосуванням криптографічних методів і різноманітністю завдань, що розв'язуються з їх допомогою, приводить до істотного підвищення вимог до стійкості сучасних криптосистем, технологічності процесів їхньої розробки й проектування, економічності їхніх реалізацій. Одним із важливих та пріоритетних завдань у даній галузі залишається не тільки розробка нових національних криптографічних систем і алгоритмів, що задовольняють сучасним технологічним вимогам, але й підтримка криптосистем, що використовуються в цей час на відповідному рівні безпеки.

На сьогоднішній день, рішення проблеми інформаційної безпеки вже розглядаються на державному рівні, що підтверджується нормативно-правовими і організаційними документами. В Україні на цей час діє три Закони України: «Про електронні документи і електронний документообіг» , який встановлює основні організаційно-правові принципи електронного

документообігу і використання електронних документів; «Про електронні довірчі послуги», який визначає правовий статус електронного цифрового підпису та регулює взаємовідносини, які виникають при використанні електронного цифрового підпису та Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», що регулює взаємовідносини в області захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Одним із важливих аспектів сучасного інформаційного простору є спеціальні цифрові носії інформації, що широко використовуються в наш час.

Спеціальні цифрові носії інформації (СЦНІ) - це електронні документи, що мають містити інформацію, яка є основою для створення систем електронного документообігу, електронної торгівлі та електронного бізнесу, а також спеціалізовану інформацію для ідентифікації і автентифікації суб'єктів цих систем та спеціальну службову інформацію, яка повинна забезпечити захищену взаємодію з цими електронними документами.

За своєю природою спеціальні цифрові носії інформації є електронними документами спеціального типу з певним інтерфейсом доступу до них і тому можуть зберігатися на будь-яких носіях інформації.

Найбільш зручними є портативні інтелектуальні носії інформації, якими є: USB – токени, флеш-носії. В останній час як самостійні пристрої збереження СЦНІ можуть розглядатися засоби реалізації технології електронного паперу. Аналізу властивостей портативних інтелектуальних носіїв інформації присвячена численна література.

Метою даної магістерської роботи є впровадження нових підходів щодо безпечного зберігання інформації на цифрових носіях інформації. Об'єктом є суспільні відносини у сфері захисту інформації на цифрових носіях, а предметом – методика безпечного зберігання інформації на цифрових носіях інформації.

В рамках дослідження нами поставлено такі завдання: 1) дослідити ознаки ідентифікації інформації на цифрових носіях; 2) вивчити головні

аспекти захисту інформації на цифрових носіях; 3) проаналізувати методи, які входять до методики захисту інформації на спеціальних цифрових носіях; 4) запропонувати методику безпечного зберігання інформації на носіях інформації за допомогою програмного засобу шифрування - VeraCrypt.

РОЗДІЛ 1. ЦИФРОВІ НОСІЇ ІНФОРМАЦІЇ

1.1. Основні поняття та визначення

Для введення терміну «цифрові носії інформації» слід навести визначення, які встановлені діючим законодавством та нормативно-правовими актами Ради Євросоюзу.

«Електронний підпис – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов’язані та призначені для ідентифікації підписувача цих даних» [6].

«Удосконалений електронний підпис - електронний підпис, створений за результатом криптографічного перетворення електронних даних, з якими пов’язаний цей електронний підпис, з використанням засобу удосконаленого електронного підпису та особистого ключа, однозначно пов’язаного з підписувачем і який дає змогу здійснити електронну ідентифікацію підписувача та виявити порушення цілісності електронних даних, з якими пов’язаний цей електронний підпис» [7].

«Особа, що підписалась - має можливість володіти механізмом створення підпису та діє від свого імені чи від імені фізичної чи юридичної особи, чи організації, яку представляє» [1].

«Механізм перевірки підпису - пристосоване апаратне чи програмне забезпечення, що використовується для введення в дію даних для перевірки підпису» [1].

«Сертифікат - це електронна атестація, що пов'язує дані для перевірки підпису з особою. Підтверджує ідентичність особи» [1].

Наведемо терміни, які встановлені чинним законодавством України, зокрема Законом України «Про електронний документообіг» та Законом України «Про електронний цифровий підпис».

«Електронний документ — документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа» [2].

«Електронний цифровий підпис - сукупність даних, отримана за допомогою криптографічного перетворення вмісту електронного документа, яка дає змогу підтвердити його цілісність та ідентифікувати особу, яка його підписала» [3].

Електронний цифровий підпис є обов'язковим реквізитом електронного документа, який використовується для автентифікації автора та/або особи, яка підписала електронний документ, іншими суб'єктами електронного документообігу [2].

Накладанням ЕЦП завершується створенням документа в електронній формі.

Відносини, пов'язані з використанням ЕЦП, регулюються відповідним законом нашої держави [2].

Спеціальні цифрові носії інформації як електронні документи, які мають інформацію, що є основою для створення систем електронного документообігу, електронної торгівлі та електронного бізнесу, спеціалізовану інформацію для ідентифікації та автентифікації суб'єктів цих систем (наприклад, цифрові паспорти) та спеціальну службову інформацію, яка визначає захищену взаємодію з цим електронним документом [9].

За своєю природою спеціальні цифрові носії інформації є електронними документами спеціального типу з певним інтерфейсом доступу до них, і тому можуть зберігатися на будь-яких носіях інформації. Повністю розкривається потенціал ЦНІ, якщо засоби їх зберігання мають можливість організації спеціального захищеного інтерфейсу роботи з ЦНІ, тобто мають певні обчислювальні можливості [10].

Флеш-пам'ять (ФП) - являє собою різновид напівпровідникової незалежної пам'яті, що має здатність перезаписувати інформацію. ФП зберігає інформацію в масиві комірок, кожна з яких традиційно зберігає один (або більше) біт інформації. Кожний осередок є транзистор з двома ізольованими затворами, керуючим та плаваючий. Важливою особливістю є здатність

отримувати електрони, тобто заряджати. Крім того, комірка має електроди, так звані - стік та джерело.

Під час програмування між ними, завдяки впливу позитивного поля на контрольний затвор, створюється канал - потік електронів. Деякі електрони долають ізолюючий шар і потрапляють у плаваючі ворота завдяки більшій енергії і можуть зберігатися протягом багатьох років. Певний діапазон електронів на плаваючому затворі відповідає логічній одиниці і нічого більшого, ніж нулю. Під час читання ці стани розпізнаються за допомогою вимірювання межі напруги транзистора.

Для видалення інформації на контрольний затвор подається висока негативна напруга, а електрони з поплавкового затвора надсилаються до джерела. У сторонніх технологіях цей принцип роботи може відрізнятися з точки зору поточного потоку та зчитування даних комірок [11].

USB-токен - електронний пристрій збереження та обробки інформації, який конструктивно виконаний у вигляді брелка, що підключається до USB-порту безпосередньо чи за допомогою кабелю. USB-портом обладнана більшість комп'ютерів, а це зручно і надійно для користування. Фактично токен є ІК в іншому варіанті фізичного виконання (так званому форм-факторі) та з іншим інтерфейсом передачі даних.

Більша гнучкість у виборі форм-фактору токенів визначає потенційно більші технологічні можливості за рахунок використання більш продуктивних мікропроцесорів, більшого об'єму пам'яті та додаткових спеціалізованих мікросхем. Окрім переліченого, сам корпус токена може виготовлятись у варіанті, захищеному від механічних пошкоджень, випромінювань тощо.

1.2. Ознаки ідентифікації

Важливе місце в системах захисту інформації на портативних інтелектуальних носіях збереження цієї інформації (інтелектуальних картках, флеш накопичувачах, токенах, кишенькових комп'ютерах) посідають методи

перевірки ідентичності і встановлення справжності (автентифікації) інформації та її користувачів.

Ідентифікація - це з одного боку надання об'єкту (чи суб'єкту) інформаційного обміну унікального імені або числа - ідентифікатора, а з іншого операція розпізнавання суб'єктів та об'єктів доступу за ідентифікатором.

Ідентифікацію можна розглядати як перший крок до встановлення справжності: після ідентифікації проводиться автентифікація — перевірка відповідності суб'єкта доступу і пред'явленого ним ідентифікатора (тобто перевірка, чиє суб'єкт тим, за кого себе видає).

При встановленні справжності інформації розрізняють автентифікацію повідомлень - процедуру додавання до блоку даних контрольного поля для виявлення будь-якої зміни даних та автентифікацію даних - визначення джерела даних та встановлення того, що інформація не замінена і не спотворена.

Більш загально, автентифікація - це визначення уповноваженим одержувачем факту, що при існуючому протоколі автентифікації повідомлення, швидше за все, надсилаються авторизованим передавачем і не змінюються і не спотворюються. У проблемі встановлення справжності можна виділити такі групи питань:

- ознаки ідентифікації та автентифікації (розпізнавальні характеристики, ідентифікатори, автентифікатори, характерні ознаки, на основі яких ведеться розпізнавання людей та інформації);
- алгоритми встановлення справжності (на основі певних ознак);
- схеми реалізації цих алгоритмів та їх ефективність [12].

Далі розглянемо властивості ознак ідентифікації та автентифікації, добір певних ознак залежно від конкретної ситуації захисту інформації (частіше це компроміс між стійкістю системи захисту інформації, витратами на неї та складністю відповідного алгоритму).

Для зручності аналізу можна виділити за типом використання три групи ознак.

Пароль - цей тип ознаки (слово-пароль, фраза, PIN-код) який легко дешево реалізувати, зручний для автентифікації користувачів, які підключаються з непередбачуваних віддалених місць.

Паролі мають слабкі місця. їх розмір залежить від секретності, яку треба забезпечити, а зберегти їх користувачам важко. Існує дуже багато способів вивідати чи перехопити пароль, але, як правило, немає способу виявити активну розвідку до того, як втрати сталися, крім того, майстерність зловмисників досягла на сьогодні такого рівня, що викрадення пароля для них в багатьох ситуаціях є досить простою справою.

Пристрої автентифікації. Характерною ознакою є володіння авторизованим користувачем деяким конкретним предметом. Це може бути файл даних, у якому знаходиться певна ознака, картка з магнітною смужкою, смарт-картка, флеш накопичувач, USB-токен, обчислювач пароля та інше. Автентифікацію в такій формі важко обійти, тому що використовується унікальний фізичний об'єкт, яким має володіти людина для входу в систему. Власник швидше може помітити зникнення пристрою, ніж це буває при крадіжці пароля.

Пристрої автентифікації знімають труднощі, пов'язані із запам'ятовуванням паролів, можуть генерувати одноразові паролі, що важко піддаються перехопленню, можуть нести в собі значно складніший базовий секрет, ніж здатна запам'ятати людина.

Слабкі сторони: можлива висока вартість пристрою та відмова в роботі, ризик його загубити.

Біометричні ознаки. Характерною ознакою є якась фізична особливість, унікальна для особи, що проходить автентифікацію. У відомих методиках використовуються ознаки: голос людини, відбитки пальців, письмовий підпис, форма руки, особливості ока, риси обличчя. В більшості випадків добре спроектована біометрична система просто знімає ознаку і правильно автентифікує, природно вирішується питання транспортування ознаки [13].

Біометрична верифікація має свої вади:

- як правило, порівняно з іншими системами висока вартість придбання, установки, експлуатації цього обладнання;

- при дистанційному користуванні є ризик перехоплення інформації: зловмисник може відтворити запис ознак, щоб замаскувати себе під їх власника, або використати їх, щоб вистежити власника;

- якщо біометричними ознаками заволодіє зловмисник, то власник потрапляє в критичну ситуацію (біометричні ознаки неможливо змінити);

- сам процес автентифікації в загальному випадку досить складний;

- складно зробити систему досить чутливою і щоб вона не сприймала сторонніх користувачів і не «відверталась» від своїх;

- біометричні ознаки можуть бути непридатними у випадках біологічних змін та тілесних пошкоджень;

- є зауваження етичного характеру.

Незважаючи на згадані вади, біометричні методи вважають дуже перспективними.

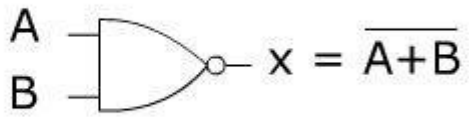
1.3. Флеш носії

Серед вище представлених видів ЦНІ, на мою думку флеш-носії зараз на піку своєї можливості, більшість людей надають перевагу зберіганню інформації на даних носіях, оскільки це практично та недорого.

Винайшов флеш-пам’ять японський інженер компанії Toshiba – доктор Фуджіо Масуока у 80-х роках XX століття, якщо вірити даним компанії, саме назва «Флеш» (з анг. «flash» - спалах) пішла від колеги по роботі – містера Шої Аріїзумі, через те, що при видаленні даних, нагадувало спалах фотокамер і представлена на Міжнародній нараді електронних пристроїв (International Electron Devices Meeting) у 1984 році у штаті Каліфорнія, місто Сан-Хосе.

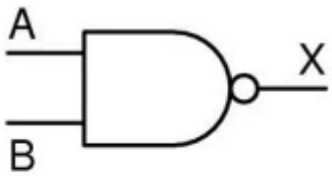
Компанія Intel зацікавившись цією технологією, в 1988 році випустила першу комерційну модель флеш-пам’яті на зразок «НЕ-АБО» наведено на

рисунку 1.1. Toshiba в гонці за інноваційними технологіями в 1989 році представила флеш-пам’ять типу «НЕ-І» наведено на рисунку 1.2.



A	B	$x=\overline{A+B}$
0	0	1
0	1	0
1	0	0
1	1	0

Рисунок 1.1 – Реалізація диз’юнкції з інверсією «НЕ-АБО»



A	B	X
0	0	1
0	1	1
1	0	1
1	1	0

$x = \overline{A \cdot B}$

Рисунок 1.2 - Реалізація кон’юнкції з інверсією «НЕ-І»

Флеш-пам’ять типу «НЕ-АБО» забезпечує високошвидкісний довільний доступ, тому можна отримати доступ до кожної з них окремо, також до них підключений окремий провідник, відповідно така архітектура здійснює обмеження на об'єм пам'яті на одиницю площі. Часто пам'ять «НЕ-АБО» використовується в мікросхемах BIOS, де дані випадково зчитуються і записуються.

Пам'ять типу «НЕ-І» записується і читається лише блоками, оскільки комірки згруповані в блочну систему. Доступ до цього типу пам'яті неможливо в довільному режимі, хоча на відміну від «НЕ-АБО», має більшу щільність запису, менші витрати на виробництво та набагато швидше зчитування та запис послідовних даних. Тому у поточній орієнтації на файли флешки використовують саме цей тип пам'яті.

В даний час архітектури «НЕ-АБО» та «НЕ-І» не можна розуміти паралельно, фрагменти мають інші зони застосування. «НЕ-АБО» - для накопичення невеликих об’ємів даних, «НЕ-І» - для великих розмірів інформації.

Типи пам'яті «НЕ-І»:

- Single Level - однорівнева секція, з низькою продуктивністю, енергоспоживанням та високою швидкість запису та з циклами дублювання, ціна такої пам’яті висока.

- Multi Level Cell - розділ з кількома рівнями, менша ціна, на відміну від SLC, менш міцніша і менше циклів перезапису, найкраще поєднання ціни та якості.

- Enterprise Multi Level Cell - розділ, схожий на MLC з набагато більшим циклом перезапису даних.

- Three Level Cell – трьохрівнева секція, з більшою щільність, меншою витривалістю, більшою швидкістю читання і запису та меншу кількість циклів перезапису в порівнянні з SLC та MLC.

- Quad-Level Cell (QLC) - елемент , здатний зберігати більше одного біта інформації, по порівнянні з однорівневою SLC, який може зберігати тільки один біт на елемент пам'яті. На рисунку 1.3 показано в графічному варіанті секцій «НЕ-І» [11].

Однією з головних проблем взаємодії з флеш-пам’яттю є обмін кількістю циклів перезапису. Наприклад, комутатори SLC можуть витримати 100 000 циклів перезапису, а MLC витримують лише 10 000, тому для оптимізації розміру пам'яті можна використовувати складні алгоритми. Крім того,

передбачена певна кількість запасних секцій, які замінюють інших, що вийшли з ладу [11].

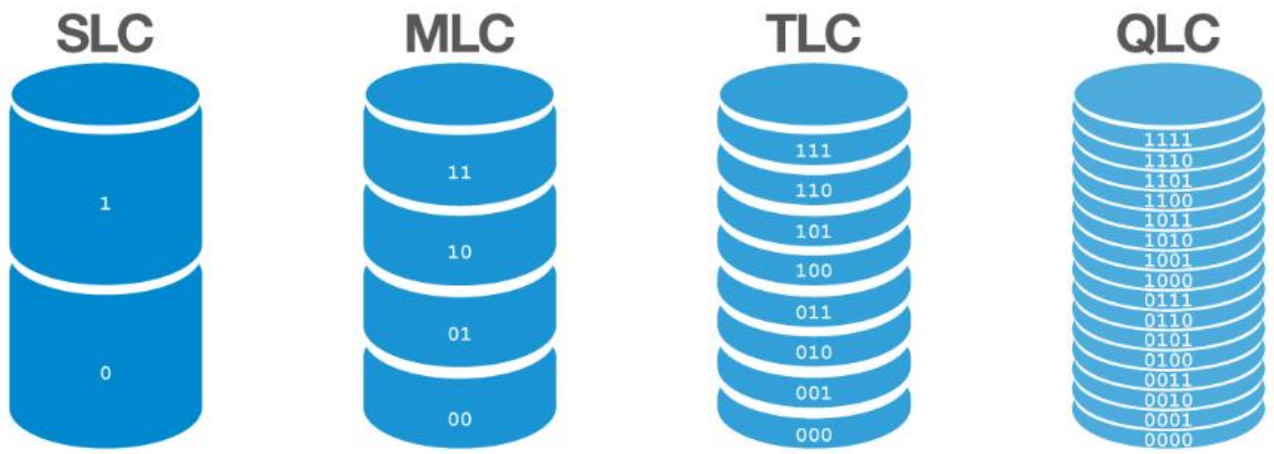


Рисунок 1.3 – типи секцій «HE-I»

Висновки до першого розділу

В першому розділі розглянуті основні поняття та визначення цифрового підпису, механізм перевірки підпису, спеціальні цифрові носії інформації, а саме:

1. USB-токени
2. Флеш накопичувачі

Також, розглянуто поняття ідентифікації інформації на спеціальних цифрових та портативних інтелектуальних носіях інформації, визначення ідентифікації та їх ознаки.

РОЗДІЛ 2. АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ІНФОРМАЦІЇ НА ЦИФРОВИХ НОСІЯХ ІНФОРМАЦІЇ

2.1. Аспекти захисту інформації на цифрових носіях інформації

У відповідно до складності умов і факторів, це загрози для ІБ, які створюють ризик для життєво важливих інтересів людини, суспільства і держави в інформаційному секторі. Основні загрози інформаційній безпеці діляться на наступні групи:

- загроза неправдивої інформації: погана, підозріла, дезінформація про людину, суспільство або державу;
- загрози розкриття спрямовані на зовнішні ресурси і створення інформації, на зовнішні джерела створення інформації, на те, як вони розроблені і застосовуються;
- загрози правам і свободам людей в області інформації, доступу до інформації, створення, пошуку, розповсюдження, одержання, поширення і експлуатацію права на інтелектуальну власність в матеріальній власності інформації та права на недоторканність приватного життя;
- право захищати честь і гідність [4] .

Одна з основних загроз інформаційній безпеці описана в Законі України Про національну безпеку України, описує і ідентифікує загрози, які поширені в кіберпросторі, встановлює пріоритети для безпечної роботи в цьому середовищі [3].

Інші загрози:

- демонстрація обмежень свободи слова та доступу до інформації для громадян;
- жорстокість ЗМІ, поширення жорстокі, насильства та порнографії.
- кіберзлочинність та залякування;
- таємниця та критична інформація, що належить державі або призначеної для задоволення потреб і національних інтересів громадськості та держави.

Загроза можливості розкриття інформаційних ресурсів і знання їх, полягає в тому, що інформація поширюються серед тих, хто не повинен мати доступ до цієї інформації. У контексті цієї роботи загроза розкриття передбачається, коли отриманий добровільний доступ до системних ресурсів. Ці ресурси повинні передаватися один одному і зберігатися в одній інформаційній системі, загроза порушення цілісності інформаційних ресурсів полягає в навмисному діянні людини: зміна даних, що зберігаються в інформаційній системі, в діяльності управління, видалення даних, а також моніторинг людської діяльності цієї інформаційної системи. Відмова устаткування відбувається автоматично, якщо один або декілька ресурсів інформаційної системи заблоковано [5].

2.2. Види смарт-карт, USB-токени

Флеш-накопичувач типу USB. ФН - це пристрій збереження даних, що включає флеш-пам’ять. Як правило він знімний, має здатність перезаписуватись та малий за розміром. Станом на 2019 рік, максимальна ємкість флеш-носія типу «А», становить 2 ТБ, наведено на рисунку 2.1. Деякі типи накопичувачів мають можливість здійснювати до 100 тисяч циклів запису та стирання, що забезпечує зберігання інформації на ньому до 100 років за звичних умов. Флеш-накопичувач має такий склад: невелика друкована плата, що містить елементи ланцюга, та роз'єму USB, електрично ізольований та захищений всередині пластиковим, металевим або прогумованим корпусом, який можна переміщувати ,наприклад, на брелку або у кишені. USB-роз'єм буває захищений ковпачком, що знімається або втягненим у корпус накопичувача, хоча при незахищеному компоненті він може не пошкодитися. Велика кількість флеш-накопичувачів застосовують стандартне USB-з'єднання типу «А», що дозволяє з'єднуватися з портом на персональному комп’ютері, але також існують накопичувачі для інших інтерфейсів.

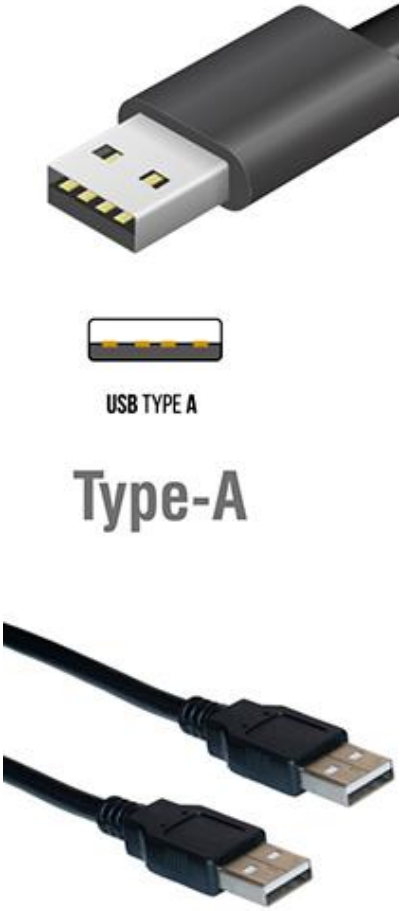


Рисунок 2.1 – USB типу «А»

USB флеш-накопичувачі черпають живлення від комп'ютера через USB-з'єднання. Деякі пристрої поєднують функціональність портативного медіаплеєра з флеш-накопичувачем USB; їм потрібен акумулятор лише при використанні та для відтворення музики.

Основні компоненти. Внутрішні механічні та електронні частини флеш-пам’яті зазвичай містять 5 частин. USB-роз'єм типу-«А» - надає фізичний інтерфейс комп'ютеру. У деяких флеш-накопичувачах USB використовується штекер USB, який не захищає 4 контакти, з можливістю підключення його до порту USB.

Контролер масового зберігання USB - мікроконтролер з вбудованим ПЗУ та ОЗУ.

Мікросхеми «НЕ-І» флеш-пам'яті - зберігають дані («НЕ-І» зазвичай використовується також у цифрових камерах) [11].

Кристалічний осцилятор - виробляє основний тактовий сигнал 12 МГц пристрою і керує виведенням даних пристрою через фазовий цикл.

Кришка - зазвичай виготовлена з пластику або металу, захищаючи електроніку від механічних пошкоджень і навіть можливих коротких замикань.

Додаткові компоненти. Типовий пристрій може також включати:

- перемички та тестові штифти - для тестування під час виготовлення флешки або завантаження коду в її мікроконтролер;

- світлодіоди - вказують на передачу даних чи зчитування та запис даних;

- перемикачі захисту від запису - увімкнення або вимкнення запису даних у пам'ять;

- вільний простір - забезпечує простір для включення другого чіпа пам'яті. Наявність другого простору дозволяє виробнику використовувати одну друковану плату для більш ніж одного пристрою розміру накопичувача.

Більшість флеш-накопичувачів поставляються з попередньо відформатованими файловими системами FAT32 або exFAT. Унікальність файлової системи FAT32 дозволяє отримати доступ до диску практично на будь-якому пристрої з підтримкою USB. Також для відновлення або отримання пошкоджених даних можна використовувати стандартні утиліти технічного обслуговування FAT (наприклад, ScanDisk). Однак, оскільки флешка з’являється як жорсткий диск, підключений USB до системи, диск можна переформатувати на будь-яку файлову систему, підтримувану операційною системою пристрою.

При широкому розгортанні флеш-накопичувачів, що використовуються в різних середовищах (захищених чи інших), питання безпеки даних та інформації залишається важливим. Використання біометричних даних та шифрування стає нормою з необхідністю підвищеної безпеки даних; в цьому відношенні особливо корисні системи шифрування, оскільки вони можуть прозоро шифрувати великі обсяги даних. У деяких випадках захищений USB-накопичувач може використовувати апаратний механізм шифрування, який використовує апаратний модуль замість програмного забезпечення для

сильного шифрування даних. IEEE 1667 - це спроба створити загальну платформу автентифікації для USB-накопичувачів.

Карти флеш-пам’яті, наприклад, карти Secure Digital (SD), доступні в різних форматах і ємностях і використовуються багатьма користувачами. SD - це галузева картка флеш-пам’яті; представлена в 1999 році і використовується практично в кожній категорії споживчих електронних пристроїв з моменту її створення. На сьогодні найбільша комерційна SD-карта - 1 ТБ. Стандарт miniSD був введений у 2003 році. Не користуючись особливою популярністю, було припинено підтримку виробником, приблизно через п’ять років після введення [14].

Також були розроблені менші варіанти карт SD. Стандарт miniSD був введений у 2003 році, хоча він користувався лише обмеженою підтримкою до припинення роботи через приблизно п’ять років.

MicroSD, який раніше називався TransFlash, був представлений у 2005 році. MicroSD-карти зазвичай зустрічаються в смартфонах та планшетах, ігрових системах та одноплановых комп'ютерах. Карту microSD можна використовувати як повнорозмірну SD-картки за допомогою пасивного адаптера. Типи флеш карток представлено на рисунку 2.1.

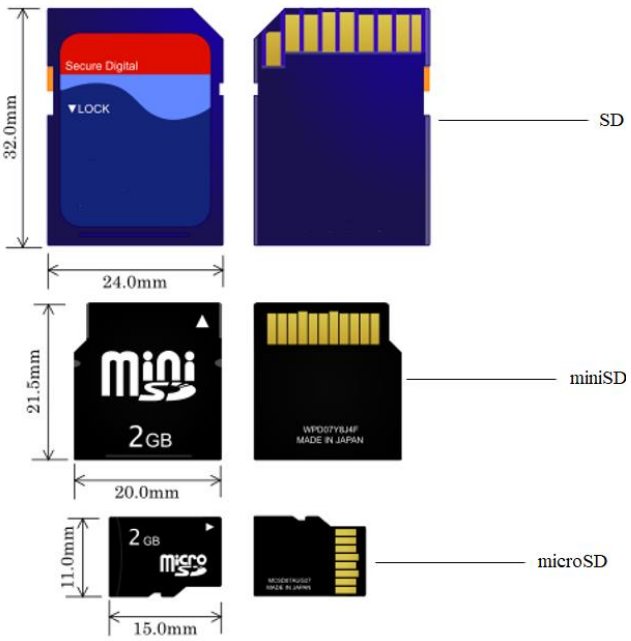


Рисунок 2.2 – Флеш носії типу SD, miniSD, microSD.

Однак, практично на всіх ПК є порти USB, що дозволяють використовувати USB флеш-накопичувачі. Для повноцінного використання флеш карт потрібний пристрій який буде зчитувати інформацію з даного типу ФН – так званий Card Reader (від анг. «Картко-зчитувач»). Зазвичай не постачається як стандартне обладнання (особливо для настільних комп'ютерів). Хоча доступні недорогі картко-зчитувачі - картрідери, які читають багато поширених форматів карток наедено на рисунку 2.3.

Рисунок 2.3 – картко-зчитувач

Додатковою перевагою карт пам'яті є те, що багато пристрої які підтримують дану технологію (наприклад, цифрові камери, портативні музичні плеєри) не можуть використовувати флешки USB (навіть якщо пристрій має порт USB), тоді як картки пам'яті, якими користуються пристрої, можна читати на комп'ютерах з карт-рідером.

USB –токени. Зовні це звичайний пристрій, схожий на флеш носій типу «А», але за своїми характеристиками в значній мірі схожий до смарт-карту. Ці пристрої дуже зручно використовувати, щоб не запам'ятовувати пароль, вся інформація зберігається на USB-токені. Також, носій може містити цифрові підписи, сертифікати та іншу інформацію, яку на звичайних носіях зберігати небезпечно .Двохфакторна автентифікація за допомогою USB-токенів відбувається в такі етап - підключення пристрою до порту USB комп'ютера,

після чого вводиться PIN-код. Перевага цього типу автентифікації полягає у високій мобільності, оскільки такі порти є на кожному робочому місці.

Відповідно, використання токену, який може безпечно зберігати конфіденційні дані: ключі шифрування, цифрові сертифікати тощо, забезпечує доступ до комп'ютерної мережі локально або віддалено.

USB-токени мають усі переваги безпечного зберігання конфіденційної інформації та здійснення криптографічної обробки інформації всередині пристрою. Багатофункціональність надає широкі можливості для їх застосування - форми суворої автентифікації і організації безпечного локального або віддаленого доступу до комп'ютерної мережі для побудови юридично значимих електронних систем управління документами, організації захищених каналів даних, керуванням інформацією користувачів, безпечних транзакцій і т.д.

Крім того, USB-токени можна носити разом із ключами у якості брелка, що мінімізує можливість втрати його та основним недоліком таких пристроїв - ціна.

Технологія одноразових паролів (OTP) передбачає при використанні паролю, згенерованого з використанням токена, використовується ключ, що одночасно генерується у користувача та на сервері автентифікації. Щоб отримати доступ до необхідної інформації, особа повинна ввести пароль, створений з використанням такого токена. Цей пароль порівнюється зі значенням, створеним на сервері, потім приймається вони порівнюються, при позитивному співпадінні цих паролів, доступ до даних дозволяється, якщо ж ні – блокується [15].

Змішані токени, так звані - гібридні, тому що поєднують в функціональність двох типів пристроїв - USB-токени з інтегральними схемами. За допомогою них, можна здійснювати двофакторну автентифікацію з підключенням через USB-порт, а також безконтактну у випадках, коли у немає доступу до USB-порту. Важливо зазначити, що гібридні носії інформації, з

маркерами USB і OTP з вбудованим чіпом, забезпечують високий рівень гнучкості та безпеки [16].

Токени у програмній реалізації - генерують одноразові паролі, які використовуються разом зі звичайними паролями для багатофакторної автентифікації. На основі секретного ключа програма-токен що генерує пароль, який відображається на екрані і використовується для автентифікації. [8].

2.3. Поняття загроз інформації

Зазвичай дослідники приділяють велику увагу поняттю інформаційної безпеки, тоді як небезпека та загроза, вважаються дещо спрощеними поняттями та зазвичай звужуються в контексті терміну інформаційної безпеки, тому необхідність розробки терміну загрози визначається:

- відсутністю одного підходу у вивченні поняття безпеки;
- недостатня розробка загальної концепції загрози та питань, що відрізняють від суміжних понять небезпеки та ризику, а отже, інформаційна загроза та її відмінність від понять інформаційної війни та інформаційного тероризму;
- проблеми невирішеної теорії безпеки інформації та наявність її виникнення;
- можливість створення відповідної системи, що здійснює моніторинг, керуванням небезпекою та загрозою в сфері інформації на основі теоретичних досягнень.

Найпоширенішими загрозами інформаційних ресурсів можна вважати потенційні події природного, технічного чи антропогенного характеру, що можуть мати небажані наслідки для інформаційної системи та інформації, що в ній зберігається.

Створення загрози, а саме пошук джерела загроз, характеризується елементом, як вразливість, загрози активізуються при наявності вразливості як

особливості системи. Безумовно, що самі загрози, згідно з усталеною теорією, є невичерпними, тому їх неможливо повністю описати [31].

Поєднуючи різні підходи та пропозиції щодо вирішення цієї проблеми, вважається, що доцільно виділити такі типи загроз інформаційної безпеки, розкриття інформаційних ресурсів; порушення їх цілісності; виходу з ладу самого обладнання.

Види загроз інформаційній безпеці:

- загроза розкриття інформаційних ресурсів;
- загроза порушення цілісності інформаційних ресурсів;
- загроза збою в роботі.

Загроза розкриттю інформаційних ресурсів полягає в інформації та знаннях, що стали відомими для тих хто не має доступу до такої інформації. В межах даної роботи загроза розкриття це стан, в якому отримується доступ до системних ресурсів, крім того, це як відкриті, так закриті джерела.

Ідеальною моделлю можна вважати середовище де обробляється інформація і вона не виходить за рамки даної мережі.

Порушення цілісності - це навмисний антропогенний вплив (зміна, видалення, зменшення) даних, що містяться в керованому середовищі [17].

При блокуванні доступу до одного або декількох ресурсів IT-системи може виникнути ризик несправності обладнання. Насправді, блокування може бути постійним, так що запитуваний ресурс ніколи не отримується або може спричинити затримки в отриманні ресурсу, задається питання, що достатньо, щоб зробити його марним [32].

Найпоширенішими і найбільш небезпечними помилками є навмисні, допущені користувачами, операторами, системними адміністраторами та іншими людьми, що працюють з IT-системами [15]. Зазвичай вони є загрозами (неправильні введені дані, програмні помилки, що спричиняють збій системи), що можуть спричинити непоправні наслідки, при втраті, викривленні чи розкритті інформації. Найкращий приклад - це введення невірно відомої інформації в ЕОМ, що спричинив зіткнення двох літаків у небі. Відповідно, в

наслідок даного випадку, загинуло чимало людей, а оператор через психічні розлади після нещасного випадку покінчив життя самогубством.

Загалом, згідно з дослідженнями експертів з ІБ, понад 65% шкоди інформаційним ресурсам було завдано ненавмисними помилками. Природні небезпечні явища трапляються набагато рідше, тому доцільно зосередитись на більш широкому впровадженні систем комп'ютерної безпеки [18].

За розміром шкоди також можна виділити крадіжку. У більшості випадків предметом цієї діяльності були штатні працівники організації, які добре розбираються в роботі ІТ-системи та заходах безпеки.

Взагалі, ображені працівники керуються спробою завдати шкоди структурі в якій вони працювали, через різного роду причин, включаючи упереджене ставлення до даної особи. Такі дії можуть супроводжувати:

- руйнування обладнання;
- шкідливе програмне забезпечення, яке за певний період руйнує програми та дані;
- заміна, знищення, модифікація даних;
- відкриття доступу до обмеженого середовища.

Такі працівники знайомі з процедурами установи і можуть завдати непоправної шкоди. Слід переконатися, що після звільнення працівника, доступ до критичної інформації та її середовища інформації для нього закритий, після чого у цілях політики безпеки, потрібно замінити усі паролі доступу.

Природні небезпеки характеризуються широким діапазоном. Перш за все, можна розрізнити перебої в інфраструктурі: відключення електроенергії, тимчасово недоступний доступ до інформаційних ресурсів, переривання водопостачання тощо.

Опираючись на статистику аналітиків, загальний відсоток інформаційних загроз, що становлять природну загрозу, становить близько 14 %.

Дії хакерів та хакерські атаки, зазвичай направленні для того, щоб примусово здійснити збій у програмному комплексі чи у середовищі, де виконуються функції обміну інформації, даних. Щодня, державні сервери

піддаються щоденним хакерським атакам, але в той же час їх загальний збиток дуже низький порівняно з іншими видами небезпек.

Шкідливі програми-віруси становлять серйозну загрозу зриву роботи ЕОМ та мережі. Банальне дотримання правил користування комп'ютерною технікою та наявність першокласного фахівця у сфері захисту інформації в органах управління значно полегшить вирішення цих завдань.

Тому крадіжці підлягають:

- обладнання (блоки, блоки та готові вироби), що використовуються для оснащення комп'ютерів та мереж;

- ПЗ та НІ;

- паперова інформація.

Джерела програмних помилок:

- помилка у програмному коді;

- форс-мажорні обставини, що можуть виникнути при заміні або додаванні нового обладнання, встановленні нових програм, введенні нових програмних режимів, виникненні раніше не збережених надзвичайних ситуацій;

- віруси, які заразили програму.

Сам вірус є небезпечним, враховуючи його можливості щодо збору інформації, особливо організаційних питань, вплив на відображення монітора користувачів, переміщення даних з однієї папки в іншу, множення таких файлів, видалення тощо. В кінцевому результаті, такі дії уповільнять ЕОМ, а в гіршому випадку збій цілої системи [19].

З огляду на компетенції органів державної влади, загрози, пов'язані з нападом на їхні інформаційні ресурси здійснювались з метою:

- доступу до інформації з обмеженим доступом;

- крадіжка службової інформації та ключових даних;

- здійснення керування алгоритмом роботи системи;

- виведення із ладу основної частини системи управління.

Тому існують також види загроз, завдяки їх кількості намагаються виявити загрози ІБ, враховуючи існуючі питання у сфері державної політики у сфері національної безпеки.

Поділяються за такими показниками:

- природного походження - катаклізми, повені, пожежі тощо;

- антропогенного -різного роду аварії, спричинені людиною;

Також, до антропогенного походження можна включити діяння людини у комп'ютерній сфері, а саме дії, що спрямовані на знищення ресурсів та інформаційної мережі тощо. До цієї групи видів діяльності належать: спричинені помилковою чи ненавмисною діяльністю, наприклад халатність особи чи необізнаність у користуванні програмними засобами чи прикладними програмами;

- навмисні дії, що загрожують стабільності роботи системи, або витоку важливої інформації, наприклад закладки, шкідливе програмне забезпечення тощо.

За ступенем гіпотетичного пошкодження:

- чіткі або потенційні загрози, які ускладнюють або перешкоджають реалізації національних інтересів, становлять загрозу керування державною системою, що підтримує життя її елементів, які формують систему;

-пряма дестабілізація функціонування системи державного управління.

По частоті повторень:

- які вже виникали;

- які постійно виникають;

За місцем виникнення:

- екзогенна - за межами;

- ендогенний - джерело, яке знаходиться в самій системі.

Відповідно до ймовірності реалізації:

- ймовірні небезпеки, які обов'язково виникнуть за певних умов. Наприклад, повідомлення про напад на інформаційні ресурси національної безпеки, яке передувало самій атаці;

- загрози, які за певних умов неможливі, як правило це залякування, що не виправдані фактичними чи навіть потенційними умовами намірів;

- випадкові небезпеки, коли досягаються певні умови, виникають щоразу по-різному.

Доцільно проаналізувати загрози на цьому рівні за допомогою оперативних методів дослідження, таких як теорія ймовірностей.

З точки зору детермінізму:

- загрози природного характеру, постійного повторюваного характеру, спричинені об'єктивними умовами існування та розвитку системи ІБ. Наприклад, кожен суб'єкт буде піддаватися інформаційним атакам, якщо він не працює або система захисту інформації не працює належним чином;

- випадкові небезпеки, які можуть виникнути чи ні. До таких загроз належить загроза хакерам з метою дестабілізації ІТ-систем суб'єктів РНБО.

За значенням:

- прийнятні небезпеки, які не можуть спричинити падіння системи. Приклади включають віруси, які не шкодять програмам, знищуючи їх;

- неприйнятні загрози, які: якщо вони будуть здійснені, можуть призвести до відмови системи та систематичної дестабілізації; може призвести до змін, несумісних із продовженням існування установи. Наприклад, вірус "я тебе люблю" пошкодив комп'ютерні системи у багатьох куточках світу, заподіявши загальний збиток у розмірі близько ста мільйонів доларів [19].

Поділяються за впливом:

- загрози системі, які впливають на всі компоненти пристрою і повинен відбуватися одночасно в кількох значущих і найважливіших точках. Щодо теми, це може бути навмисна дискредитація через телебачення, радіо, друковані ЗМІ та Інтернет;

- структурні загрози, що впливають на дану структуру системи.

Ці загрози також небезпечні і водночас впливають на структуру окремих державних органів або їх частин.

Елементарна загроза, яка охоплює окремі елементи структури, ці загрози є постійними та будуть небезпечними лише у тому випадку, якщо вони неефективні чи неконтрольовані.

Характер реалізації:

- реальні - з усіма гарантіями дестабілізації;

- потенціал - якщо алгоритм дестабілізації можна активувати за певних умов;

- реалізовані - реалізовані загрози;

- Уявна - псевдоактивація алгоритму чи подібного алгоритму без наслідків.

У зв'язку, щодо:

- об'єктивні та такі загрози, які підтверджуються сукупністю обставин та фактів, які об'єктивно характеризують довкілля. У той же час ставлення підрозділу управління не відіграє вирішальної ролі, оскільки існують об'єктивні загрози, незалежно від волі та обізнаності суб'єкта. Наприклад, хоча український законодавець у Законі України "Про основи національної безпеки України" не вказав пріоритетності захисту від інформаційних загроз, приділяючи їм найменшу увагу, оскільки їх значення є безпрецедентним, а тиск на інших загрози постійно ведуть і потрапляють у сферу інформації;

- суб'єктивна - сукупність факторів об'єктивної реальності, що вважається предметом управління ризиками безпеки і в даній ситуації вирішальну роль у визначенні конкретних обставин та факторів відіграє воля керівника, який приймає безпосереднє рішення про надання статусу або ідентифікує деякі події як загрозу [19].

За предметом впливу:

- державний;

- на людину;

- для суспільства.

Відповідно до форми вкладення:

- регуляторні – зазначаються у нормативних актах.

- ненормативні - не відображені належним чином, об'єктивно існуючі;.

Ця класифікація показує різноманітність та неоднорідність, багатошаровість та певну нескінченність загроз та загроз інформаційній безпеці, адекватних у часі та просторі, темпам суспільного розвитку.

Висновки до другого розділу

В даному розділі приділена увага щодо аспектів захисту інформації та встановлення можливих загроз, що спричиняють витоку, спотворення та втраті інформації. Розглянуті види загроз та в наслідок чого вони можуть бути спровоковані.

Також визначення поняття цілісності та проаналізувавши інформацію щодо ЦНІ можна визначити що основними загрозами є:

1. Загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформаційні ресурси.

2. Збій в роботі обладнання.

Розглянуті види флеш карток SD, miniSD, microSD.

РОЗДІЛ 3. АНАЛІЗ МЕТОДІВ ЗАХИСТУ ІНФОРМАЦІЇ НА ЦИФРОВИХ НОСІЯХ

3.1. Загрози безпеки флеш-накопичувачів

Як високо-портативний носій, ФН легко втрачаються або викрадаються, зважаючи на малі габарити. Це особлива проблема, якщо вони містять конфіденційні дані.

Як наслідок, деякі виробники додали до своїх накопичувачів апаратне забезпечення шифрування.

Апаратний – це метод, що здійснює шифрування за допомогою пристроїв, що безпосередньо інтегровані в обчислювальну техніку.

Деякі компанії випускають флеш-накопичувачі, які використовують апаратне шифрування як частину дизайну, для комерційних цілей, усуваючи потребу в сторонній програмі шифрування.

Деякі флеш накопичувачі підтримують біометричні відбитки пальців, щоб підтвердити особу користувача. Станом на 2005 рік - це була дорога альтернатива стандартному захисту паролем, запропонованому на багатьох нових ФН. Однак, USB-накопичувачі зі сканерами відбитків пальців, використовують контролери, що дозволяють отримати доступ до захищених даних без будь-якої автентифікації. Більшість із цих ФН покладаються на операційну систему для перевірки відбитків пальців через драйвер програмного забезпечення, обмежуючи коректну роботу диску на комп'ютерах з операційною системою - Microsoft Windows.

За деяких обставин, показано, що ці накопичувачі мають проблеми з безпекою і, як правило, дорожчі, ніж системи, засновані на програмному забезпеченні, які у вільному доступі.

Програмний – це метод шифрування за допомогою спеціальних програм та програмних систем, призначені для захисту інформації.

Щоб забезпечити цілісність та доступність інформації і не переживати, що інформацію дізнається третя особа, вміст ФН USB можна зашифрувати програмними засобами, наприклад «TrueCrypt», «VeraCrypt» чи «BitLocker». Окремо можна зашифрувати файл, попередньо створивши зашифрований архівний файл ZIP чи RAR.

Більшість флеш-накопичувачів USB не містять механізму захисту від запису. Ця функція, яка поступово стала менш поширеною, складається з перемикання на корпусі самого накопичувача наведено на рисунку 3.1, що заважає комп'ютеру писати або змінювати дані на накопичувачі. Наприклад, захист від запису дозволяє спокійно користуватись ФН без ризику зараження самої флеш-пам’яті USB різноманітними вірусами.

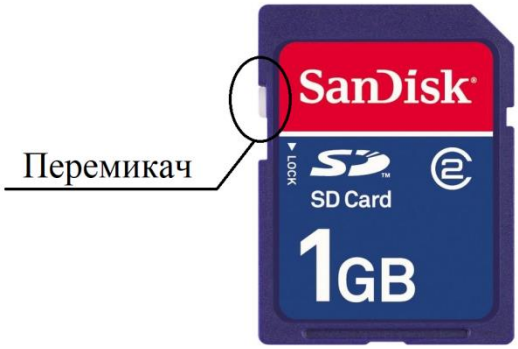


Рисунок 3.1 – SD – картка з перемикчем блокування запису

Флеш-накопичувачі можуть представляти собою значні проблеми безпеки для установ та організацій. Невеликий розмір і просте використання дозволяє користувачам зберігати та записувати конфіденційні дані з невеликими шансами на виявлення скоєного.

Як корпоративні, так і загальнодоступні комп’ютери уразливі до дій зловмисників, які підключають флешку до вільного USB-порту та використовують шкідливі програми, такі як реєстратори клавіатури або сніфери (від анг. «Sniff» -нюхати) пакетів даних.

Для завантаження комп'ютерів та здійснення несанкціонованого доступу в обліковий запис, створений USB-накопичувач, що містить завантажувальну

портативну операційну систему для доступу до файлів комп'ютера, навіть якщо комп'ютер захищений паролем. Таким чином, пароль можна змінити, або зламати за допомогою програми злому пароля та отримати повний контроль над комп'ютером.

Шифрування файлів забезпечує значний захист від цього типу атак. USB-флешки також можуть використовуватися навмисно або мимоволі для передачі зловмисних програм, вірусів та хробаків в мережі. Деякі організації, забороняють використовувати ФН, або ж використання лише облікованих USB носіїв, створивши відповідну комплексну систему захисту інформації, без виходу в інтернет. Попередньо, адміністратор безпеки повинен налаштувавши параметри комп’ютера та антивірусного забезпечення для відключення монтажу необлікованих ФН. Використання програмного забезпечення дозволяє адміністратору не тільки забезпечити блокування USB, але й контролювати використання SD-карт та інших пристроїв пам'яті.

Даний метод політики безпеки дає можливість компаніям використовувати USB-накопичувачі на робочих місцях без остраху умисної модифікації чи знищення інформації.

3.2. Алгоритми шифрування: AES, Serpent, Twofish, Camellia

Розширений стандарт шифрування або AES - це симетричний блок-шифр, для захисту секретної інформації та реалізований у програмному та апаратному забезпеченні у всьому світі для шифрування конфіденційних даних.

Національний інститут стандартів і технології (NIST) приступили до розробки AES в 1997 році , коли було оголошено про необхідність нового алгоритму для заміни стандарту шифрування даних (DES). Цей новий, вдосконалений алгоритм шифрування мав бути некласифікованим і здатним добре захищати важливу інформацію до наступного століття, згідно з повідомленням NIST про процес розробки вдосконаленого стандартного алгоритму шифрування . Він повинен був бути легким для впровадження в

апаратному та програмному забезпеченні, а також в смарт-картах та забезпечувати стійкість до різноманітних атак.

Процес вибору нового алгоритму симетричного ключа був повністю відкритий для публічного вивчення, це забезпечило ретельний, прозорий аналіз поданих конструкцій. NIST вказав, що новий розширений стандартний алгоритм шифрування повинен бути блоковим шифром, здатним обробляти 128-бітові блоки, використовуючи ключі розміром 128, 192 та 256 біт; інші критерії вибору в якості наступного розширеного стандартного алгоритму шифрування включали безпеку, вартість, можливість впровадження.

Вибір алгоритму AES. П'ятнадцять конкуруючих симетричних ключових алгоритмів були піддані попередньому аналізу світовою криптографічною спільнотою, включаючи Агентство національної безпеки (NSA) . У серпні 1999 року NIST обрав п'ять алгоритмів для більш широкого аналізу. Це були:
MARS, представлена великою командою IBM Research; RC6, представлений безпекою RSA;Rijndael, представлений двома бельгійськими криптографами, Джоаном Даменом та Вінсентом Ріджменом; Serpent, поданий Россом Андерсоном, Елі Біхам та Ларсом Кнудсеном; Twofish, представлений великою групою дослідників з Counterpane Internet Security, включаючи відомого криптографа Брюса Шнайєра [20].

Реалізація всього вищезазначеного була широко перевірена на мовах ANSI C та Java для швидкості та надійності шифрування та дешифрування, час налаштування ключа та алгоритму; стійкість до різних атак, як в апаратних, так і в програмно-орієнтованих системах. Члени світової криптографічної спільноти провели детальний аналіз (включаючи деякі команди, які намагалися зламати свої власні дані).

Після багатьох дискусій та аналізів, шифр Rijndael – поєднання двох прізвищ бельгійських творців Rijmen та Daemen - був обраний в якості запропонованого алгоритму для AES в жовтні 2000 року і опублікований NIST як «U.S. FIPS PUB 197». Стандарт шифрування набув чинності як стандарт федерального уряду у 2002 році. Він також включений до стандарту

Міжнародної організації зі стандартизації (ISO), Міжнародної електротехнічної комісії (IEC), який визначає блок-шифри з метою конфіденційності даних.

У червні 2003 року уряд США оголосив, що AES може бути використаний для захисту секретної інформації, і незабаром він став алгоритмом шифрування за замовчуванням для захисту класифікованої інформації, а також першим загальнодоступним та відкритим шифром, затвердженим NSA для суто секретної інформації. АНБ обрала AES як один із криптографічних алгоритмів, який буде використовуватися Управлінням інформаційного забезпечення для захисту систем національної безпеки.

Успішне використання урядом США призвело до широкого використання, AES став найпопулярнішим алгоритмом, що використовується в симетричній ключовій криптографії . Прозорий процес відбору допоміг створити високий рівень довіри до AES серед експертів із безпеки та криптографії. AES є більш безпечним, ніж його попередники - DES та 3DES - оскільки алгоритм є більш сильним і використовує більшу довжину ключів. Також дозволяє швидше шифрувати, ніж DES та 3DES, що робить його ідеальним для програмних програм, програмного забезпечення та апаратних засобів, які вимагають або низької затримки, або високої пропускної здатності, наприклад, брандмауерів та маршрутизаторів . Використовується в багатьох протоколах, таких як Layer Secure Sockets (SSL), Security Transport Layer (TLS) і його можна знайти в більшості сучасних програм та пристроїв, які потребують функцій шифрування.

Складається з трьох блокових шифрів: AES-128, AES-192 і AES-256. Кожен шифр шифрує та розшифровує дані в блоках по 128 біт, використовуючи криптографічні ключі 128-, 192- та 256-біт відповідно. Шифр Rijndael був розроблений для прийняття додаткових розмірів блоків та довжини ключів, але для AES ці функції не були прийняті.

Симетричні (також відомі як секретний ключ) шифри використовують один і той же ключ для шифрування та розшифрування, тому відправник і одержувач повинні знати і використовувати один і той же секретний ключ . Усі

довжини ключів вважаються достатніми для захисту класифікованої інформації, що вимагають або 192-, або 256-бітної довжини ключів. Існує 10 раундів для 128-бітних клавіш, 12 раундів для 192-бітних клавіш і 14 раундів для 256-бітних ключів - раунд складається з декількох етапів обробки, які включають підстановку, переміщення та змішування вхідного простого тексту та перетворення його на кінцевий вихід шифротексту наведено на рисунку 3.2.

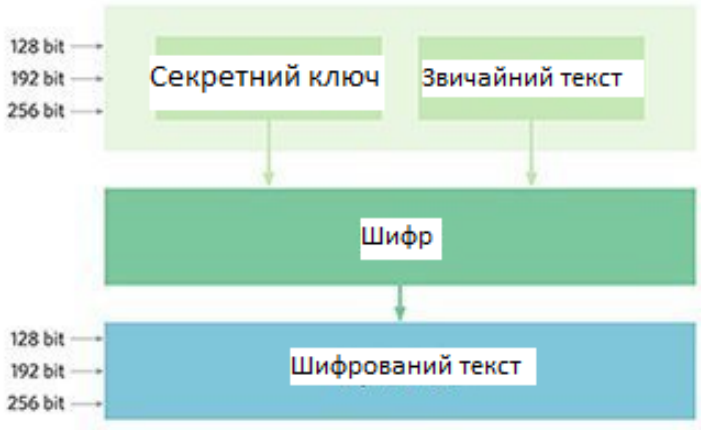


Рисунок 3.2 – Графічний принцип роботи AES

Алгоритм шифрування AES визначає ряд перетворень, які слід виконати для даних, що зберігаються в масиві. Перший крок шифру - це введення даних у масив; після чого перетворення шифрів повторюються протягом ряду раундів шифрування. Кількість раундів визначається довжиною ключа, при цьому 10 раундів для 128-бітних ключів, 12 раундів для 192-бітних ключів і 14 раундів для 256-бітних ключів.

Перше перетворення в шифрувальному шифрі AES - це підміна даних за допомогою таблиці заміщення; друге перетворення зміщує рядки даних, третє змішує стовпці. Останнє перетворення - це проста ексклюзивна або (XOR) операція, яка виконується на кожному стовпчику, використовуючи іншу частину ключа шифрування - довші ключі потребують більше раундів [20].

Шифрування AES перетворює дані масиву шляхом переміщення рядків та стовпців та підстановок на основі ключа шифрування наведено на рисунку 3.3.

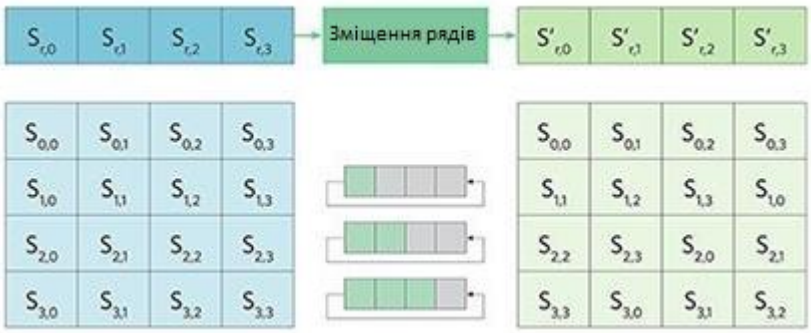


Рисунок 3.3 – Зміщення рядів алгоритму AES

Serpent (від лат. «Serpent» - змій) - алгоритм з відкритим кодом, який шифрується в блоки, так званим симетричним ключем. В основному лише один ключ використовується для шифрування та розшифрування. Алгоритм розроблений у 1998 році Россом Андерсоном, Ларсом Кнудсеном та Елі Біхам. Serpent був одним із остаточних виборів NIST, інституту стандартизації США, для захисту зв'язки федеральних агентств США, поступившись алгоритму AES і посів почесне друге місце. AES отримала загалом 86 голосів, Serpent - 59 та Twofish - 31.

Основна відмінність AES від Serpent полягає в тому, що AES має менше раундів і менше рівнів шифрування, що робить його швидшим у процесах шифрування та дешифрування. Натомість Serpent повільніший, але безпечніший.

Розробники алгоритму були зосереджені на отриманні максимально можливого рівня безпеки від будь-якого виду атак. Вони почали вивчати блокове шифрування на доступному обладнання, яке було в той період і для свого алгоритму вирішили використати вдвічі більше раундів, необхідних для блокування відомих атак. Метою було створення алгоритму, який міг би бути гарантовано стійким 100 років. Незважаючи на те, що вони використовували пруденційні критерії на етапі розробки, вони змогли отримати алгоритм, який був у два рази швидшим, ніж DES.

Перемога AES над Serpent під час процесу відбору стандартизації, проведеного NIST, викликала справжнє розчарування у розробників Serpent, до

того ж у березні 2000 року вони написали звіт про оцінювання свого алгоритму, повністю розкривши всі помилки, які, на їх думку, допущено NIST.

Процесор, який використовував NIST для обчислення першого раунду (перша фаза шифрування), за словами розробників Serpent, Pentium 200 МГц, виявився недостатньо потужним у порівнянні зі зростаючими можливостями обчислення процесорів 21 століття. Крім того, було сказано, що під час процесу відбору найважливішими критеріями оцінки алгоритму був рівень безпеки, який використовувався.

Розробники Serpent, були натхнені трьома наступними критеріями, що дало їм можливість створити алгоритм, який би мав бути максимально стійким.

Перше, код в блоках повинен бути максимально простий і простий для аналізу.

Друге, блок шифрування повинен мати кілька фаз кругового шифрування стосовно того, що потрібно для блокування нинішніх атак через те, що обчислювальні можливості постійно розвиваються і зазвичай логіка атаки безпосередньо пов'язана з тим, що збільшується кількість раундів.

Третє, код у блоках повинен використовувати лише добре відомі математичні операції, що використовуються в криптографії. З цієї причини розробники Serpent використовують мережу SP (заміна - перестановка), що використовується вже більше чверті століття, як базу для сучасних криптографічних систем, отже, зводячи до мінімуму можливість виявлення нових прийомів атаки.

Складні алгоритми важко правильно використовувати, натомість Serpent дуже простий і його можна оптимізувати за допомогою мов програмування, таких як «C» та «ADA».

Технічні розробки. Serpent - це 128-бітове блокове шифрування, яке використовує 32 раунда або 32 повторення того ж алгоритму з використанням математичних перестановок і підстановок. Фаза шифрування та дешифрування має однаковий рівень складності. Операції дешифрування - це саме перевернуті

перетворення, які використовуються для шифрування, але у зворотному порядку [20].

Serpent використовує різні математичні заміни "S-box" з 4-бітовим входом і 4-бітовим виходом. Кожна фаза шифрування використовує S-вікно, яке працює в сукупності 32 рази. Процес шифрування та розшифрування алгоритму Serpent показаний на рисунку 3.4.

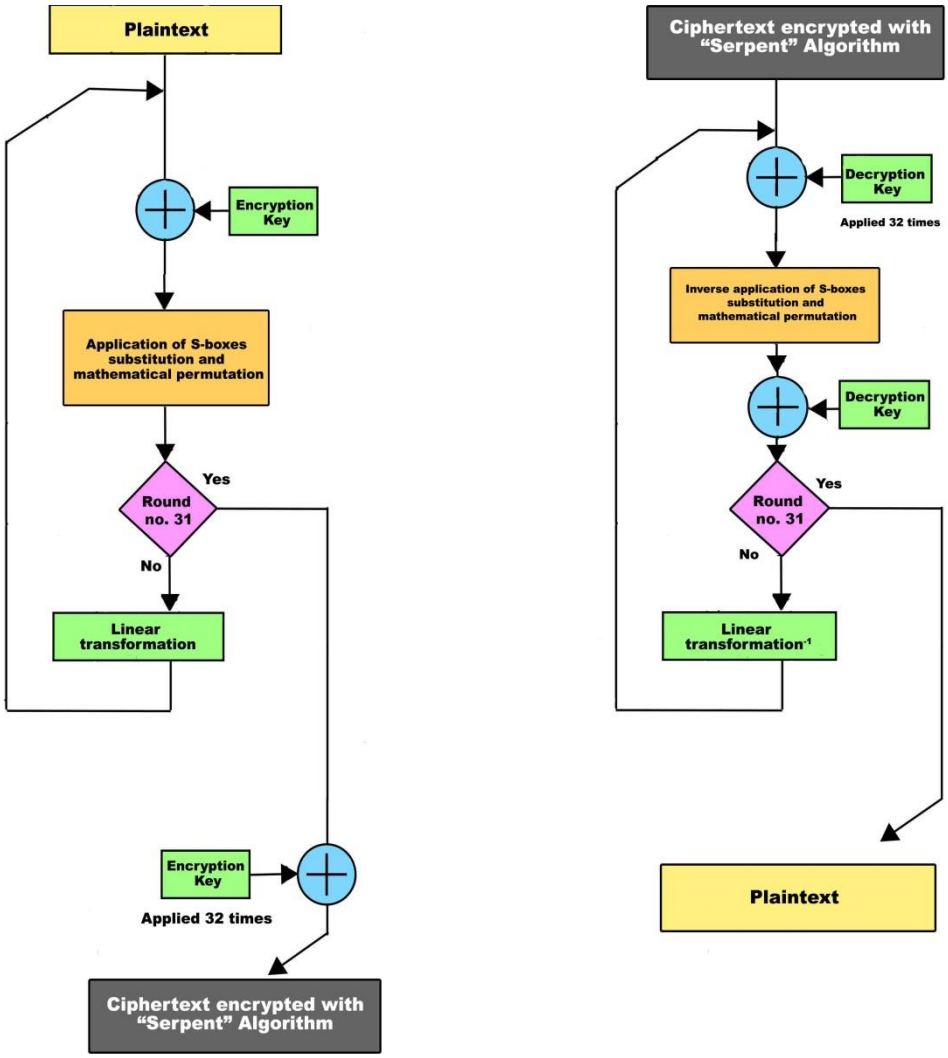


Рисунок 3.4 – Алгоритм розшифрування та шифрування Serpent

Twofish - алгоритм шифрування, розроблений Брюсом Шнейєром. Це симетричний шифр блоку ключів з розміром блоку 128 біт, з ключами до 256 біт. Він пов'язаний з AES і більш раннім блоковим шифром під назвою

Blowfish. Twofish має деякі відмінні риси, що відрізняють його від більшості інших криптографічних протоколів. Для одного з них використовується попередні обчислення, залежні від ключа S-боксу (S-box), є базовим компонентом будь-якого алгоритму симетричного ключа, який виконує підміну. У контексті блочного шифру Twofish S-бокс працює на скриття взаємозв'язку ключа до шифротексту. Twofish використовує попередньо обчислений, залежний від ключа S-бокс, що означає, що S-поле вже надано, але залежить від ключа шифру для розшифрування інформації наведено на рисунку 3.5.

Twofish розглядається як дуже безпечний варіант, що стосується протоколів шифрування.

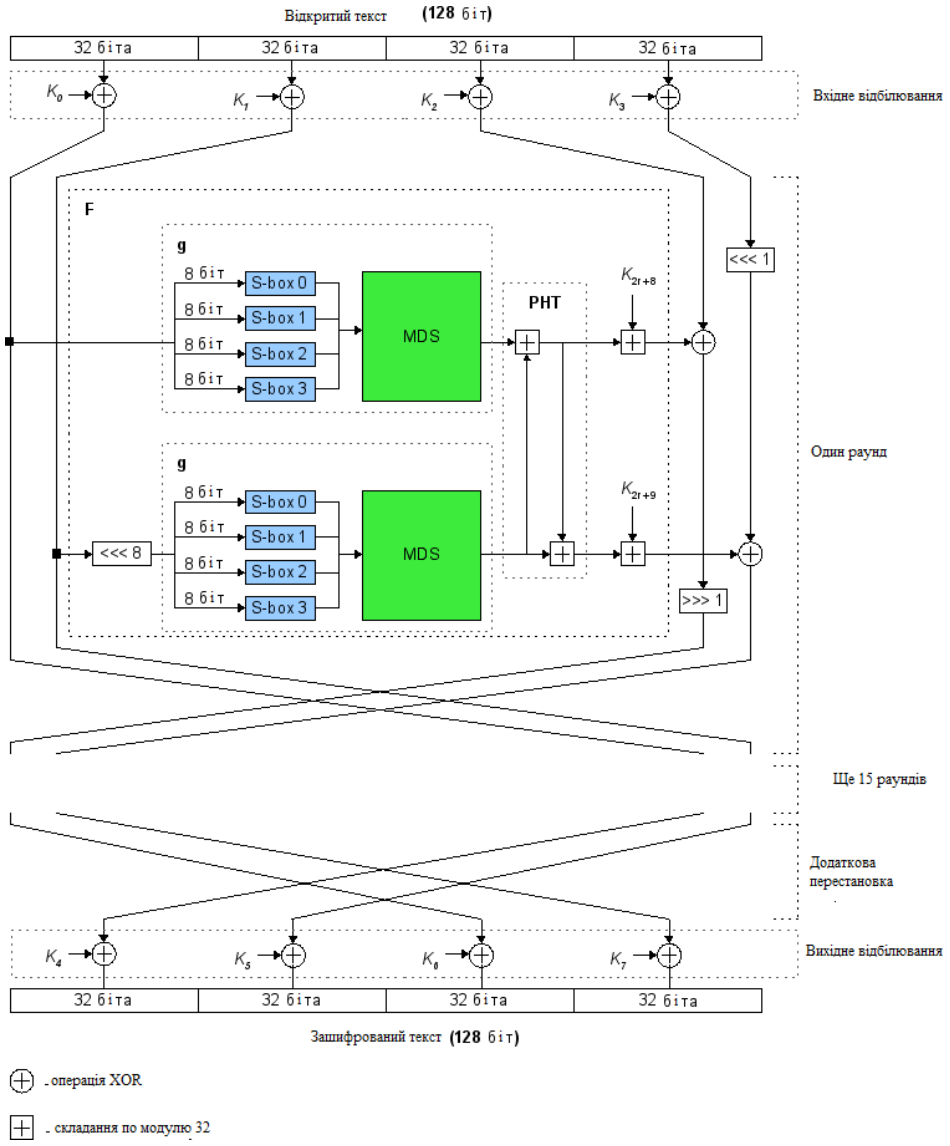


Рисунок 3.5 – Графічний алгоритм роботи Twofish

Однією з причин того, що він не був обраний як розширений стандарт шифрування - його менша швидкість. Будь-який стандарт шифрування, в якому використовується 128-розрядний або більший ключ, теоретично безпечний до брут форсу.

Оскільки Twofish використовує попередньо обчислені S-бокси, залежні від ключа, він може бути вразливим до атак бічних каналів. Це пов'язано з попереднім обчисленням таблиць. Однак, якщо ці таблиці залежать від ключів, це допоможе зменшити цей ризик. Було кілька нападів на Twofish, але, за словами її творця Брюса Шнайєра, це не являє собою справжнього криптоаналізу. Ці атаки не становлять загрози для шифру [28].

Camellia - симетричний алгоритм блочного шифру з розміром блоку 128 біт і ключовими розмірами 128, 192 і 256 біт. Його спільно розробили Mitsubishi Electric та Nippon Telegraph and Telephone Corporation (NTT) з Японії. Шифр був схвалений для використання в Міжнародній організації стандартизації (ISO/IEC), в Новій європейські схемі для підписів, цілісності та шифрування Європейського Союзу та в Комітеті з досліджень та оцінювання криптографії (CRYPTREC) в Японії.

Шифр був розроблений, щоб бути придатним для програмних і апаратних реалізацій, недорогих смарт – карт, для мережевих високошвидкісних систем. Він є частиною криптографічного протоколу безпеки транспортного рівня (TLS), призначеного для забезпечення захисту зв'язку через комп'ютерну мережу - Інтернет.

Camellia - це шифр Feistel з 18 раундами (при використанні 128-бітних ключів) або 24 раундами (при використанні 192- або 256-бітних кючів). Кожні шість раундів наноситься шар логічного перетворення: так звана "FL-функція" або її зворотна. Camellia використовує чотири 8 × 8-бітні S-бокси з вхідними та вихідними афінними перетвореннями (affine transformation) та логічними операціями наведено на рисунку3.6. Шифр також використовує відбілювання ключа вводу та виводу. Дифузійний шар використовує лінійне перетворення , засноване на матриці з відгалуженим числом 5.

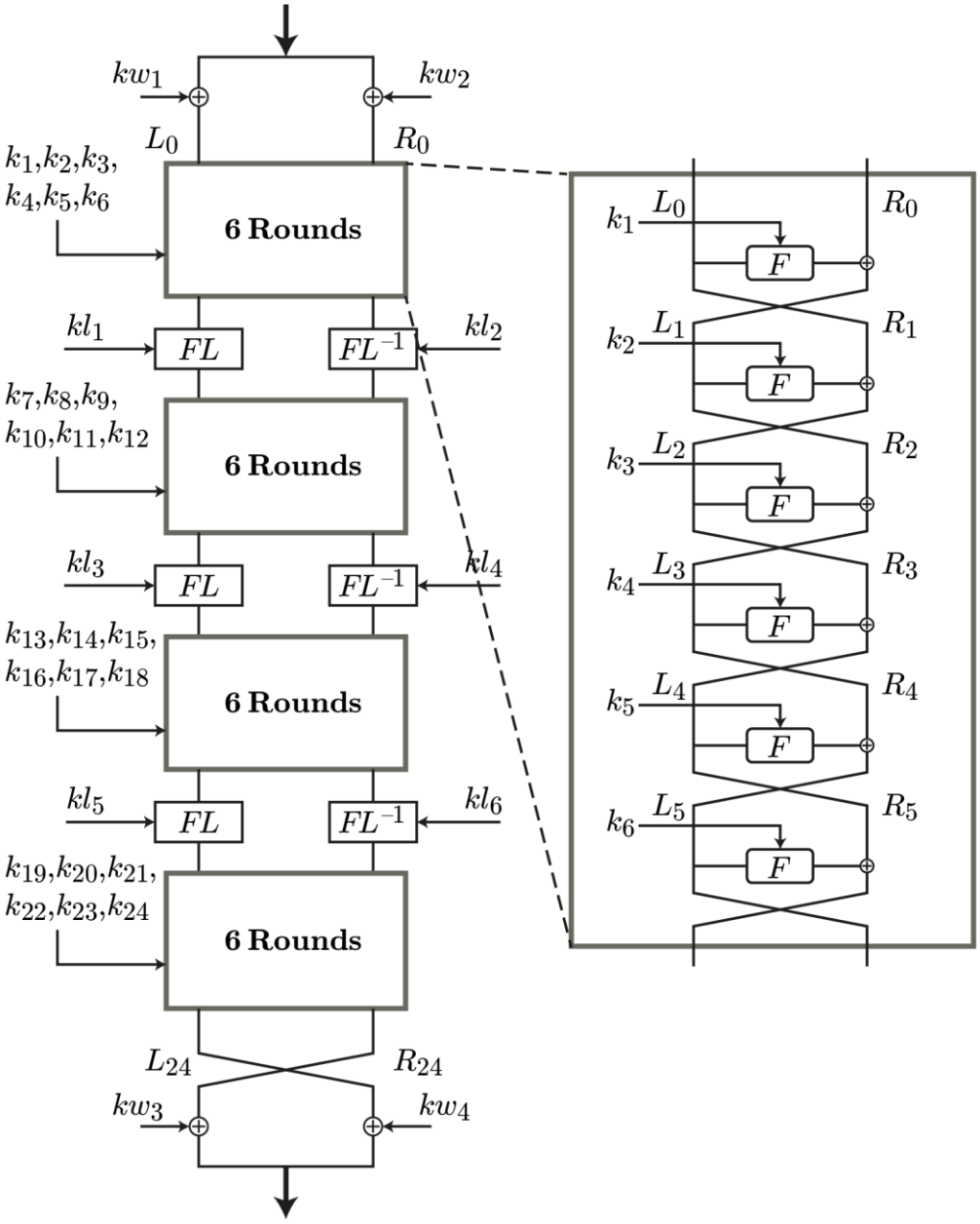


Рисунок 3.6 – Алгоритм роботи Camellia

Camellia вважається сучасним, безпечним алгоритмом шифрування. Навіть використовуючи менший варіант розміру ключа (128 біт), можна вважати, що за допомогою брут форсу, розшифрувати за допомогою сучасної технології неможливо. Немає відомих, успішних атак, які значно послаблюють шифр [23].

3.3. Приклад носія інформації, що використовується в системах захисту інформації від НСД

НСД - слід розуміти як доступ до інформації за допомогою засобів включених до складу комплексної системи, що порушує встановлені принципи обмеження доступу. Принципи обмеження доступу може бути реалізований або за допомогою стандартних інструментів, тобто набору вбудованого програмного забезпечення, включеного в комплексну систему розробником під час розробки, або системним адміністратором під час роботи, які включені до затвердженої конфігурації, та за допомогою програмного та апаратного забезпечення, що міститься в склад КСЗІ.

Під захистом слід розуміти як дії, спрямовані на забезпечення дотримання ПДР, шляхом встановлення та підтримки системи заходів щодо ЗІ [6].

Основні способи НСД включають:

- безпосереднє звернення до об'єктів для отримання конкретного типу доступу;

- створення програмних та апаратних засобів, які отримують доступ до об'єктів, минаючи функцію захисту;

- модифікація заходів безпеки, що дозволяє реалізувати НСД;

- реалізація в КС програмних або апаратних механізмів, що порушують структуру та функції КС і дозволяють реалізувати СУЗ [21].

Одним із прикладів систем захисту інформації, реалізованих за допомогою програмного та апаратного забезпечення, є система Лоза-1. Використовує ЦНІ як звичайний маркер USB наведено на рисунку 3.7.

Ця система безпеки зазвичай використовується в автоматизованих системах класу 1 для обробки секретної інформації, не вище "Цілком таємно".

Лоза-1 - це програмне забезпечення захисту інформації, яке працює разом з операційною системою Microsoft Windows, за винятком - Starter esition, Home

Edition. Забезпечує захист від НСД та реалізує всі стандартні функції, необхідні для надійної інформаційної безпеки.

Може бути використана для захисту інформації, яка буде становити державну таємницю, що підтверджено експертним висновком № 740, виданим Державною службою спеціального зв’язку та захисту інформації України 1 червня 2017 року[24].

Рисунок 3.7 - USB-токен

«Система Лоза-1 - це програмний засіб захисту інформації, що працює спільно з операційною системою Microsoft WindowsOC, окрім початкової та домашньої редакції (Starter edition, Home edition), забезпечує захист від НСД, реалізує всі стандартні функції, які необхідні для надійного захисту інформації» [25].

«Може використовуватись для захисту інформації, що встановить державну таємницю, це підтверджено експертним висновком № 740, виданий Державною службою спеціального зв'язку та захисту інформації України 01 червня 2017 року [24].

Слід звернути увагу на особливості цієї системи, постачається у двох конфігураціях:

1. «Підвищена безпека» - для захисту інформації, що становить державну таємницю.

2. «Стандартна безпека» - для захисту особистої та конфіденційної інформації (включаючи особисті дані).

Захист від несанкціонованого доступу до інформації:

- дозволяє захистити всі дані на знімних і твердих носіях; захист на рівні папок Windows та знімних дисків;

- забезпечує надійний захист документів Microsoft Word та Microsoft Excel завдяки тісній інтеграції з Microsoft Office (відключає небезпечні команди, макроси, шаблони тощо), підтримує версії Microsoft Office XP / 2003/2007/2010/2013/2016;

- дозволяє контролювати роботу знімних дисків: дискети, компакт-дисків та флеш-носіїв;

- дозволяє встановлювати дозволи або заборони на запущені процеси.

Контроль друку та експорту:

- система Vine-1 дозволяє встановлювати дозвіл / заборону друку / вивезення на рівні окремих документів;

- для посилення контролю система Vine-1 дозволяє присутнім адміністратора чи іншої уповноваженої особи під час друку та експорту (через необхідність введення пароля);

- контроль за входом користувача в систему;

- у конфігурації "Безпека" вхід можливий лише після введення пароля та встановлення ключового диска (можна використовувати звичайні дискети, «флеш-носій» або CD / DVD); застосовуються суворі правила щодо блокування паролів та користувачів, які перешкоджають вибору пароля в стандартній конфігурації безпеки вводити лише достатній пароль, політика щодо паролів менш сувора, ніж у конфігурації підвищеної безпеки [25].

Реєстрація події:

- веде безпечний журнал, в якому реєструються всі події, що стосуються захисту інформації;

- аналіз журналів та звітів про роботу не вимагає спеціальної кваліфікації;

- журнал подій ніколи не перезаписується: після досягнення межі журналу всі події зберігаються у файл на жорсткому диску;

- забезпечує детальну реєстрацію роздруківки та події експорту; разом із стандартною інформацією в журналі записуються штамп та обліковий номер документа, а також порядковий номер перевізника, на якому зберігається документ, та експортера; адміністратор може створити протокол друку документів [25].

Висновки до третього розділу

За результатами проведеного аналізу можна зробити висновок про загрози що можуть бути спричинені носіям інформації. Також розглянуто методи шифрування за допомогою алгоритмів AES, Serpent, Twofish, Camellia.

Із методів захисту інформації на ЦНІ слід зазначити використання алгоритмів шифрування і дешифрування даних.

Розглянуто засіб захисту інформації «Лоза-1, який спроможний забезпечувати захист інформації до рівня «Цілком таємно». Система «Лоза-1» реалізує всі стандартні функції, необхідні для надійного захисту інформації від НСД, але питання захисту інформації на USB-токенах, які використовуються в якості носіїв ключової інформації потребують подальших досліджень.

РОЗДІЛ 4 РОЗРОБКА МЕТОДИКИ БЕЗПЕЧНОГО ЗБЕРІГАННЯ ІНФОРМАЦІЇ ТА ЇЇ ВПРОВАДЖЕННЯ

4.1. Структурна і функціональна схеми методики

Для розробки методики безпечного зберігання інформації та дотримання комплексного порядку та правил, була складена структурна схема створення методики, представлена на рисунку 4.1.

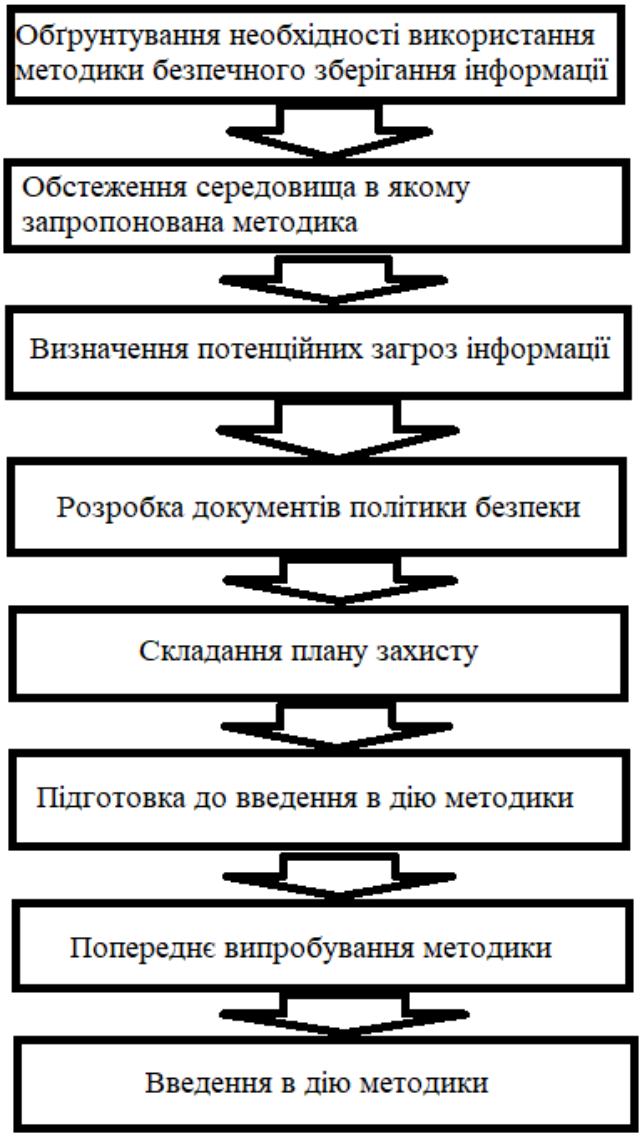


Рисунок 4.1– Структурна схема порядку створення методики

Структурно дана методика поділена на три основних напрямки:

організаційно-правове, інженерно-технічне і програмно-апаратне.

Організаційно-правовий напрямок містить роботу зі складанням нових і переробці існуючих організаційно-розпорядчих документів, що циркулюють у відповідній установі чи організації.

Інженерно-технічний напрям полягає в забезпеченні коректної роботи ЕОМ та ОС за допомогою якої буде реалізована дана методика.

Програмно-апаратний напрямок включає комплекс заходів, спрямований на захист інформаційних процесів на робочому місці персоналу засобами програмного захисту.

За основою структурної схеми, запропонована функціональна схема, вона відображає процес забезпечення інформаційної безпеки. Представлений на рисунку 4.2.

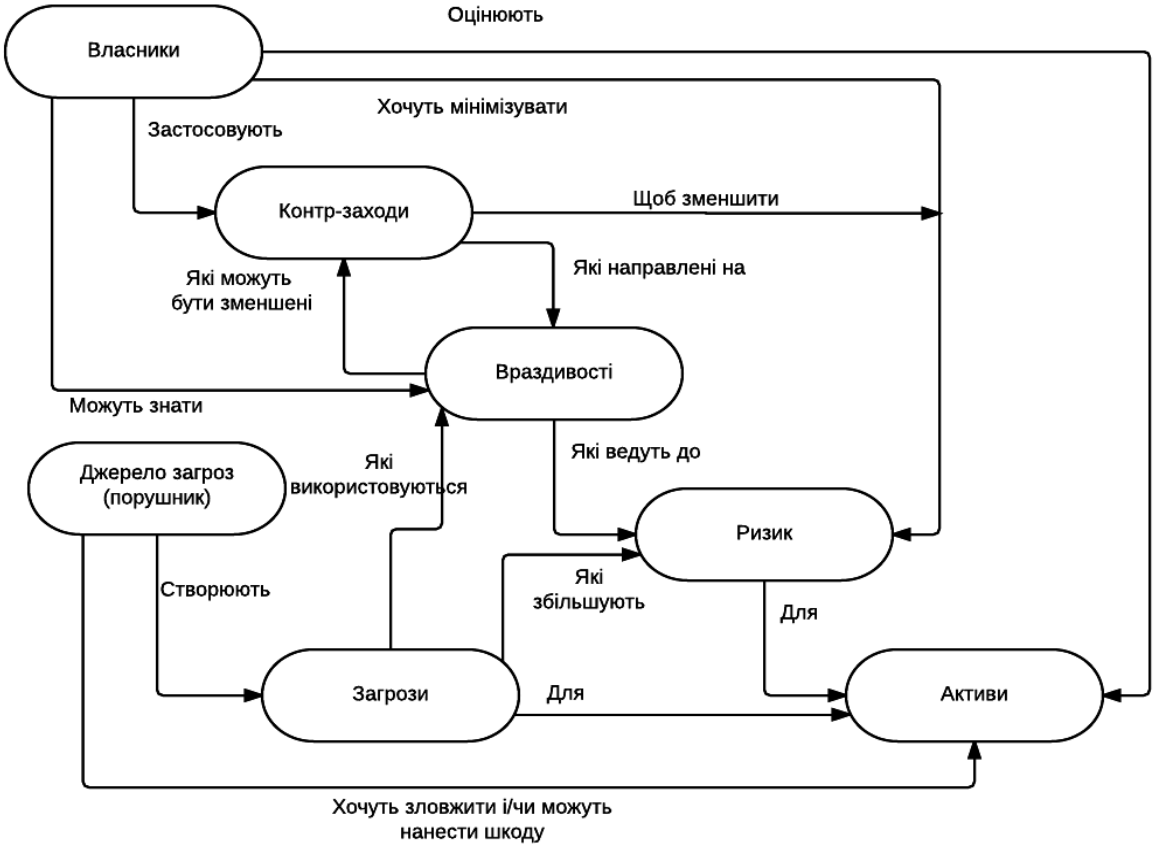


Рисунок 4.2 – Процесна схема методики

Функціональна схема відображає стадії забезпечення безпеки у виробничому процесі. Для забезпечення даного процесу, задіяні позаштатні

адміністратори служби захисту інформації (СЗІ). Кожен етап захисту інформаційної безпеки установи/організації, супроводжується організаційно-розпорядчою документацією, яка регламентує діяльність СЗІ і персоналу щодо конкретного захисного процесу.

Результатом такого підходу має бути безпечне та компетентне діловодство установи.

4.2. Організаційно-правові заходи

На підставі загроз, втрати чи витоку конфіденційної інформації, були обрані засоби для зменшення кількості вразливостей і зниження ступеня шкоди від загроз. Проаналізувавши статистику, зазвичай джерелом витоку інформації є персонал що працює з обмеженою інформацією по причині необізнаності чи випадковості.

Перш за все, будь-який працівник, який буде працювати з даною методикою, зобов’язаний теоретично ознайомитись з нею, слід провести інструктаж та всі інших заходів, спрямовані на захист інформації, щоб уникнути некоректного поводження з ним.

Слід створити відповідної документації, для закріплення за кожною людиною відповідного флеш-носія, надати право працювати за відповідним комп’ютером.

Проведення інструктажу персоналу після проведення всіх інших заходів, спрямованих на захист. Проведення обов'язкового навчання співробітників після установки нового обладнання або програмного забезпечення, щоб уникнути некоректного поводження з ним. Роз'яснення всім співробітникам їх дій в разі виникнення різного роду небезпек.

Вироблені додаткові заходи по відношенню до ІТ-фахівців, що працюють в установі. Основними завданнями ІТ-фахівця є: впровадження передових інформаційних технологій з метою автоматизації управління установою; використання мінімуму ІТ-засобів для досягнення цілей

автоматизації; формування культури корпоративної роботи користувачів.

Ця посада має дві основні складові – технологічну і соціально-керівну. З одного боку, необхідно впровадити інформаційну систему, максимально задовольняє запити користувачів, з іншого – пояснити її функції, навчити правилам користування, розподілити обов'язки та зони відповідальності серед персоналу з підтримки її працездатності.

При складанні нормативно-правових документів, слід звернути увагу на правила користування програмою. Інструкція з використання даної методики повинна включати наступні розділи:

- для чого і в якому порядку здійснюється шифрування;
- правила безпечного шифрування даних;
- правила створення паролю;
- шифрування томів;
- безпечне монтування та розмонтування томів для роботи;
- безпечне завершення роботи з зашифрованим носієм.

Після проведення інструктажу та попереднього навчання використання VeraCrypt за кожним працівником буде закріплено флеш-носій, та визначений список дозволених ЕОМ для використання. Попередньо з налаштованою політикою безпеки, та функціонуючим антивірусним програмним забезпеченням, виключаючи можливість під’єднання сторонніх носіїв до комп’ютерів, щоб мінімізувати негативний вплив на критичну інформацію.

Монтування тому флеш-носія виконуватиметься самою ж програмою VeraCrypt, приблизний час монтування від 5 до 10 секунд, для флеш носіїв з пам’яттю до 32 Гб. Завдяки конвеєрному руслу, зчитування, запис та видалення файлів здійснюється зі швидкістю, яка встановлена на заводі виробника флеш-носія.

Правила для паролю, який потрібно вводити під час розшифрування тому повинні включати наступі критерії:

- довжина паролю повинна бути мінімум 12 символів;

- поєднання різноманітних, незалежних між собою символів, включаючи строчні та прописні букви, цифри та знаки.

4.3. Програмно-апаратні засоби захисту інформації

Працівникам СЗІ, слід дотримуватись встановлених правил, які вказані у відповідній документації, а саме, одним із важливих моментів є щотижневе оновлення антивірусних баз для детектування та нейтралізації вірусів, чи шкідливих об’єктів де зберігається критична інформація.

Для обмеження доступу до USB-портів - налаштування шаблонів безпеки, для контролю флеш-носіїв, що будуть під’єднюватись до ЕОМ.

Оскільки методика безпечного зберігання інформації на цифрових носіях не передбачає використання локальної чи глобальної мережі, віддалене адміністрування неможливе. Тому за кожним позаштатним працівником СЗІ буде закріплена ЕОМ, за якою буде працювати працівник, який обробляє критичну інформацію.

4.4. Заходи захисту інформації

Для встановлення програми шифрування та розшифрування інформації VeraCrypt слід скачати з офіційного сайту відповідний інсталяційний файл.

Слід встановити даний програмний продукт на кожну машину, де на флеш-носіях буде оброблятись конфіденційна інформація.

Перед початком роботи, необхідно зашифрувати носій інформації, для цього потрібно вибрати один із багатьох варіантів алгоритмів та комбінацією даних алгоритмів шифрування, які пропонує програма, показано на рисунку 4.3.

Час зашифрування залежить від об’єму пам’яті, що буде зашифрована та від типу носія.

Для розшифрування, в програмі слід вказати зашифрований том, та

ввести пароль, який знає лише власник флеш-носія.

В користувацькій інструкції установи, повинна чітко вказуватись мінімальна довжина паролю, яку задає користувач, та термін, через який потрібно його змінити, в цілях політики безпеки.

AES-Twofish
AES-Twofish-Serpent
Camellia-Kuznyechik
Camellia-Serpent
Kuznyechik-AES
Kuznyechik-Serpent-Camellia
Kuznyechik-Twofish
Serpent-AES
Serpent-Twofish-AES
Twofish-Serpent

Рисунок 4.3 – Варіанти алгоритмів та їх комбінації шифрування VeraCrypt

Режими роботи програми:

- звичайний;
- скритий том.

В звичайному режимі, створюється лише один том, який розшифровується паролем, після вводу якого користувач має змогу читати, видаляти та записувати інформацію.

В скритому режимі, створюється два томи, тобто ще один том в зашифрованому томі. Встановлюється пароль на кожен том. Так звана методика

«Заперечення».

Для установи чи організації достатньо стандартного режиму шифрування.

При завершенні роботи, слід розмонтувати том, зашифрованого носія інформації, після чого, для забезпечення ще більш надійного зберігання даних, здійснити перезавантаження операційної системи ЕОМ.

4.5. Тестування програми шифрування службою захисту інформації

У функціонально надійному програмному проекті рекомендується використовувати широкий спектр добре перевірених правил та рекомендацій.

А саме: модульний підхід; програми, створений на основі існуючих стандартів дизайну та кодування; жорсткі типові мови програмування, структурні, а також об'єктно-орієнтовані технології програмування; реєстрація та аналіз даних тощо.

Метою тестування з виявленням помилок проекту є виявлення залишкових помилок проекту програмного забезпечення під час виконання дії програми з метою запобігання критично небезпечним збоям.

Суть методу полягає в наступному: перевіряється попередня умова (перш ніж буде виконана послідовність станів, перевіряються початкові умови на їх надійність) та поступова (результати перевіряються після послідовності станів). Якщо попередня умова не виконується, обробка припиняється з помилкою.

Перевірка програмного забезпечення проводиться послідовно на рівні окремих програм, програмних модулів та програмного забезпечення загалом. Одночасно аналізується програмна документація, перевіряється правильність вихідних та проміжних даних, правильність алгоритмів, тестування програми.

Програму можна протестувати повністю або вибірково в окремих точках простору даних джерела. За допомогою точкового тестування надійність програми не може бути повністю гарантована.

Повне тестування з усіма можливими вхідними наборами програми або тестування всієї структури програми неможливо, оскільки кількість тестів буде

неприпустимо великою. Тому часто застосовується структурно селективне тестування, засноване на поділі простору даних вихідних даних на класи і кожен клас дозволяє підтвердити певні властивості або продуктивність певних елементів програмної структури.

Тестування – це запущений процес виконання програми з наміром знайти помилки. Тестування є досить незвичним процесом, тому вважається важким, оскільки, мета особи, що тестує знайти слабкі сторони програми.

Якщо програма веде себе правильно, немає підстав говорити, що в ній немає помилок і з усією впевненістю можна сказати лише те, що невідомо, коли ця програма не спрацює, роль тестування полягає саме в пошуку помилок, які залишаються у добре розробленій програмі [26].

Метод виділення помилок, полягає у запобіганні витоку наслідків помилки за межі програмної системи, так що якщо помилка трапляється, то це може призвести то системного збою в роботі.

Програма не повинна мати можливості безпосередньо посилатися на інші програми або дані в іншій програмі та змінювати їх, не повинна мати можливість безпосередньо посилатися дані операційної системи та змінювати їх. Спілкування між двома програмами (або програмою та операційною системою) може бути дозволено лише в тому випадку, якщо використовуються чітко визначені комбінації, і лише якщо обидві програми згодні з цим.

Програма не повинна бути спроможною зупиняти систему та не змушувати змінювати її дані.

Коли програма звертається до операційної системи, всі параметри повинні бути перевірені. Програма не повинна мати змогу змінювати ці параметри між моментами перевірки та фактичним її використанням операційною системою.

Жодні системні дані, безпосередньо доступні програмі, не повинні впливати на функціонування операційної системи. Помилка програмного забезпечення, внаслідок якої вміст пам'яті може бути змінено, в кінцевому випадку призводить до збою системи.

Програми не повинні мати можливості обходити операційну систему безпосередньо за допомогою апаратних ресурсів, якими вона керує. Програма не повинна безпосередньо посилатися на компоненти операційної системи, призначені для використання лише її підсистемами.

Компоненти операційної системи повинні бути ізольовані один від одного, щоб помилка в одному з них не змінила інші компоненти або їх дані.

Якщо операційна система сама виявляє помилку, вона повинна спробувати обмежити вплив цієї помилки одним додатком і в крайньому випадку, припинити виконання тільки цієї програми.

Реалізація багатьох з цих принципів впливає на апаратну архітектуру. Хоча термін «операційна система» використовується в формулюваннях деяких з вищевказаних принципів, останній застосовується до будь-якій програмі (будь то операційна система, монітор або підсистема керування файлами), яка займається обслуговуванням інших програм.

4.6. Державна експертиза методики безпечного захисту інформації

Основними інструментами для перевірки відповідності програми є аналіз і тестування. Програма моделювання і симуляції може використовуватися як допоміжний інструмент в процесі відповідності.

Програма відповідності повинна бути розроблена і узгоджена заздалегідь з відповідними органами, які повинні визначити кроки, необхідні для демонстрації адекватності та відповідності специфікації програмного забезпечення:

- вимог до програмного забезпечення;
- архітектури програмного забезпечення;
- проекту програмного забезпечення;

Інструменти перевірки відповідності програмного забезпечення відповідають вимогам сучасних технологій сертифікаційного тестування за

якістю (включаючи надійність і функціональну безпеку) і інформаційної безпеки.

Сертифікаційні випробування на якість, функціональну надійність і вимоги функціональної безпеки проводяться відповідно до нормативних актів і стандартів.

Установа, як майбутній користувач програми шифрування VeraCrypt, провівши внутрішній аналіз та тестування даної програми і вважає, що є доцільним впровадити дану методику. Відповідно до Постанови Кабінету Міністрів України «Про затвердження Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України», має право звернутись до Адміністрації Держспецзв'язку із заявою на проходження державної експертизи, для отримання експертного висновку щодо використання (застосування) об'єкта за призначенням [27].

Завданням даної комісії: дати об'єктивну експертну оцінку щодо затвердження та погодження методик, що пропонуються [19].

Вимоги до функціональної надійності програми засновані на умовах, що дозволяють програмі виконувати намічені функції в реальних умовах експлуатації. Програмне забезпечення в інформаційних систем широко використовується для обробки інформації. Помилки в роботі цих програмних засобів можуть призвести до небезпечних помилок, матеріального і морального збитку.

4.7. Втрата чи пошкодження флеш носія інформації

Після втрати чи виведення з ладу носія інформації, буде проведене службове розслідування, після якого позаштатні працівники служби захисту інформації зобов'язані скласти акт розслідування, в якому повинен бути встановлений факт втрати чи пошкодження носія інформації, та вияснення чи інформація була скомпрометована чи ні.

Враховуючи метод та відповідність до світових стандартів шифрування, при втраті флеш-носія, доступ до даних без паролю зведена до мінімуму,

враховуючи метод перебору паролю – брутфорс, при дотриманні правил правильного створення паролю, з сучасними можливостями, знадобиться велика кількість часу для його вгадування, відповідно інформація, яка можливо стане доступна, вже буде не актуальна.

Для того щоб підібрати та встановити надійність паролю, позаштатним адміністраторам безпеки слід провести навчання, та періодичні інструктажі, з правил використання, зберігання та створення паролю.

У разі пошкодження флеш носія, або виведення його із ладу, що не уможливлює його подальшого використання, слід знищити його. Знищення здійснюється попередньо затвердженою комісією у складі позаштатних адміністраторів ЗСІ, шляхом механічного руйнування.

4.8. Принцип шифрування програми VeraCrypt

Режими шифрування томів забезпечує метод XTS (анг. XEX-based tweaked-codebook mode with ciphertext stealing – режим з шифрованою книгою на основі крадіжки шифротексту), затвердженим міжнародним стандартом NITS - IEEE P1619.

$$C = E_{K1}\left(P_j \wedge (E_{K2}(\mathrm{n}) \otimes a^i)\right) \wedge (E_{K2}(\mathrm{n}) \otimes a^i) \quad (1)$$

С – блок шифротексту;

Р – блок відкритого тексту;

К – криптографічний ключ;

К1 – ключ шифрування, 256-розрядний для кожного підтримуваного шифру;

К2 - вторинний ключ, 256 біт для кожного підтримуваного шифру;

∧ - побітова операція АБО (XOR);

⊗- модульне множення двох многочленів над бінарним полем Галуа по модулю x128+x7+x2+x+1;

a – примітивний елемент поля Галуа (2^{128}), який відповідає поліному X (тобто 2);

j – індекс блоку для n-бітових блоків;

i- індекс блоку шифру в блоці даних (для першого блоку шифру вблоці даних i=0) [22].

Розмір кожного блоку даних завжди становить 512 байт, незалежно від розміру сектора.

Під час шифрування або дешифрування даних, VeraCrypt використовує так зване конвеєрне русло (асинхронна обробка). Поки програма завантажує частину файлу з зашифрованого тому, VeraCrypt автоматично розшифровує його (в оперативній пам'яті). Завдяки конвеєрному виконанню, додатку не доводиться чекати, коли будь-яка частина файлу буде розшифрована, і він може розпочати завантаження інших частин файлу відразу. Це ж стосується шифрування під час запису даних на зашифрований носій. Конвеєрна передача дозволяє зчитувати дані та записувати їх на зашифрований том так само швидко, як і на звичайний носій, що не зашифрований.

Генератор випадкових чисел VeraCrypt (RNG) використовується для генерації головного ключа шифрування, вторинного ключа (режим XTS), та ключових файлів. Він створює pool (анг.- басейн) випадкових значень в оперативній пам'яті. Басейн довжиною 320 байт, заповнений даними з таких джерел як:

- рухи миші;
- натискання клавіш;
- Windows CryptoAPI (збирається регулярно з інтервалом 500 мс);
- статистика мережевого інтерфейсу (NETAPI32);
- різні дискриптори Win32, змінні часу та лічильники (регулярно збираються з інтервалом 500 мс).

Перед тим, як значення, отримане з будь-якого з вищезазначених джерел, записується в басейн, воно ділиться на окремі байти (наприклад, 32-бітове

число ділиться на чотири байти). Потім ці байти індивідуально записуються в басейн за допомогою операції додавання по модулю 2^8 (не замінюючи старих значень у басейні) у позиції курсору басейна. Після записуя байту, позиція курсору висувається на один байт. Коли курсор доходить до кінця, його положення встановлюється на початок басейну. Після кожного 16-го байта, записаного в басейн, функція змішування автоматично застосовується до всього басейну [5].

Висновки до четвертого розділу

Враховуючи все, що було вище сказано, можна зробити висновок, що програма шифрування VeraCrypt виконує свої функції у повному обсязі, щоб забезпечити користувачів надійним зберіганням критичної інформації. Проста у використанні та зрозуміла на інтуїтивному рівні програма, дозволить з легкістю зашифрувати та розшифрувати томи з інформацією.

Програма шифрування у поєднанні із налагодженою політикою безпеки, та правильною експлуатацією дозволить побудувати комплексну систему захисту інформації в якій зможе циркулювати конфіденційна інформація.

Зважаючи на те, що програма відповідає стандартам, технічним умовам та рекомендаціям: ISO / IEC 10118-3: 2004, FIPS 197, FIPS 198, FIPS 180-2, FIPS 140-2 (XTS-AES, SHA-256, SHA-512, HMAC), NIST SP 800-38E, PKCS №5 v2.0 та PKCS №11 v2.20, необхідний більш глибокий аналіз програми VeraCrypt, щоб отримати державну сертифікацію на її використання.

РОЗДІЛ 5. СПЕЦІАЛЬНА ЧАСТИНА

5.1. Переваги та недоліки програм шифрування

TrueCrypt – з 2014 року офіційно не підтримується його виробниками, і при встановленні чи використанні вибиває помилку-попередження, що дана програма не гарантує 100% безпечності інформації, що буде зашифрована. З неофіційних джерел це пояснено тим, що на розробників був не аби який тиск зі сторони АНБ та інших структурних підрозділів розвідки. Хоча, після проведення аудиту у 2015 році, значних недоліків в архітектурі даної програми.

На заміну пропонується VeraCrypt, програма шифрування, написана на мовах: асемблер, C та C++. Удосконалена, виправлено ряд важливих моментів в області захисту інформації.

Великою перевагою VeraCrypt є відкритий код у вільному доступі, таким чином, використання «підступної» програми, яка була модифікована зловмисниками – мінімізується. Спроможна працювати спільно з ОС XP, Vista, 7, 8, 8.1, 10.

BitLocker, також використовується спільно з ОС MS Windows, хоча є обмеження, працює лише з Vista, 7, 8, 8.1, 10 - Ultimate, Enterprise, Pro та Professional.

І це є першим недоліком, тому що не всі користувачі мають відповідні версії операційної системи. Зважаючи на статистику 2019 року, 1.81 % користувачів ще досі використовує MS Windows XP, тоді як на версію 10 перейшло вже 45,79%. Також, редакція Home ОС Windows, не підтримує технологію шифрування.

Нажаль, основним недоліком є закритий код, який являється частиною самої операційної системи. Тому проведення державного аудиту неможливо, або є ризик, що корпорація Майкрософт юридично може вимагати розмістити у своєму продукті бекдори (анг. Back door – «чорний хід»), без відома користувачів.

Методика безпечного зберігання інформації за допомогою програми шифрування VeraCrypt є більш доцільною, безплатною, постійно розвивається та систематично випускає нові оновлення, також проводилось декілька аудитів, які мали позитивний результат.

5.2. Принцип роботи програмного забезпечення VeraCrypt

Перед тим як користувач зможе повноцінно використовувати зашифровану флешку, потрібно запусти застосунок програми шифрування, створити новий том наведено на рисунку5.1.

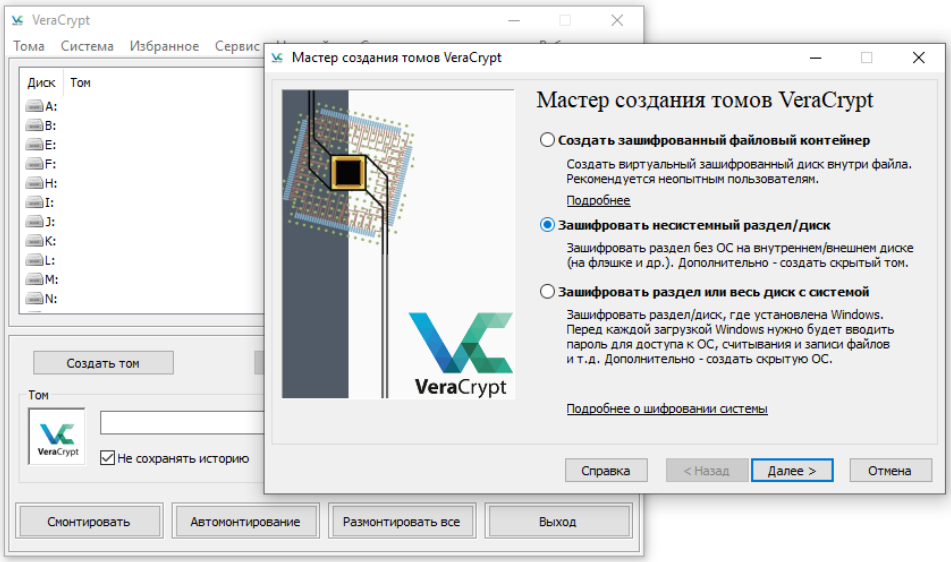


Рисунок 5.1 – Створення зашифрованого тому на носії інформації

Після чого обираємо один із двох варіантів, а саме «Звичайний» чи «Скритий режим», як зазначалось у роботі, для установи достатньо використовувати звичайний режим. Після чого, ми вибираємо флеш носій інформації наведено на рисунку5.2.

Програма відразу ж запропонує форматувати том, чи зашифрувати його з файлами, які знаходяться в середині розділу. Рекомендується зашифровувати пустий розділ. Далі, проводяться налаштування шифрування, а саме вибір алгоритмів наведено на рисунку5.3.

Розробники даної програми рекомендують усі з перелічених алгоритмів, як надійні та стійкі, але виходячи із даних дипломної роботи, надійним буде поєднання двох алгоритмів – Serpent та AES. Наступним кроком є задавання паролю, за допомогою якого, можна буде розшифрувати том наведено на рисунку 5.4. Рекомендації щодо створення надійного паролю розглянуті у розділі четвертому даної роботи.

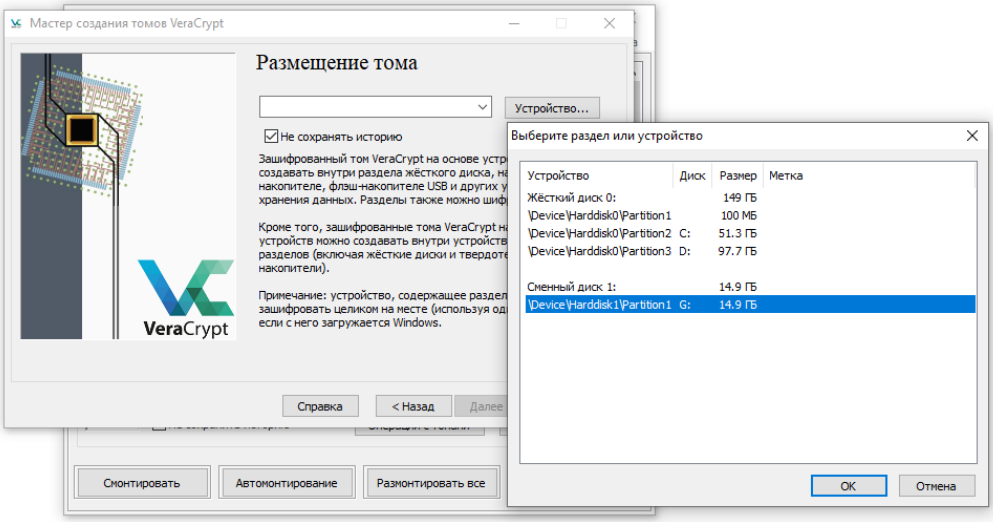


Рисунок 5.2 – Вибір носія інформації

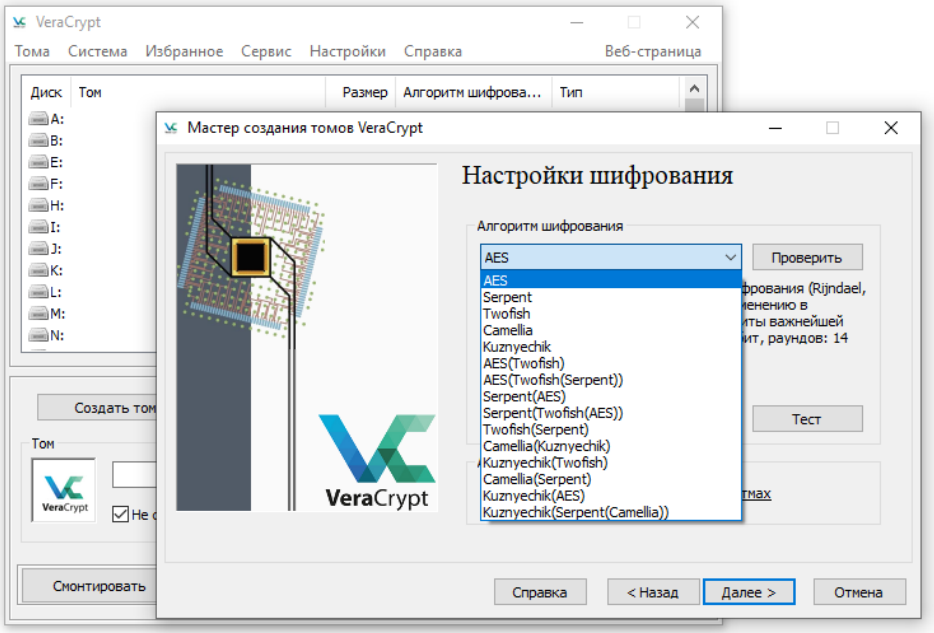


Рисунок 5.3 – Вибір алгоритмів шифрування

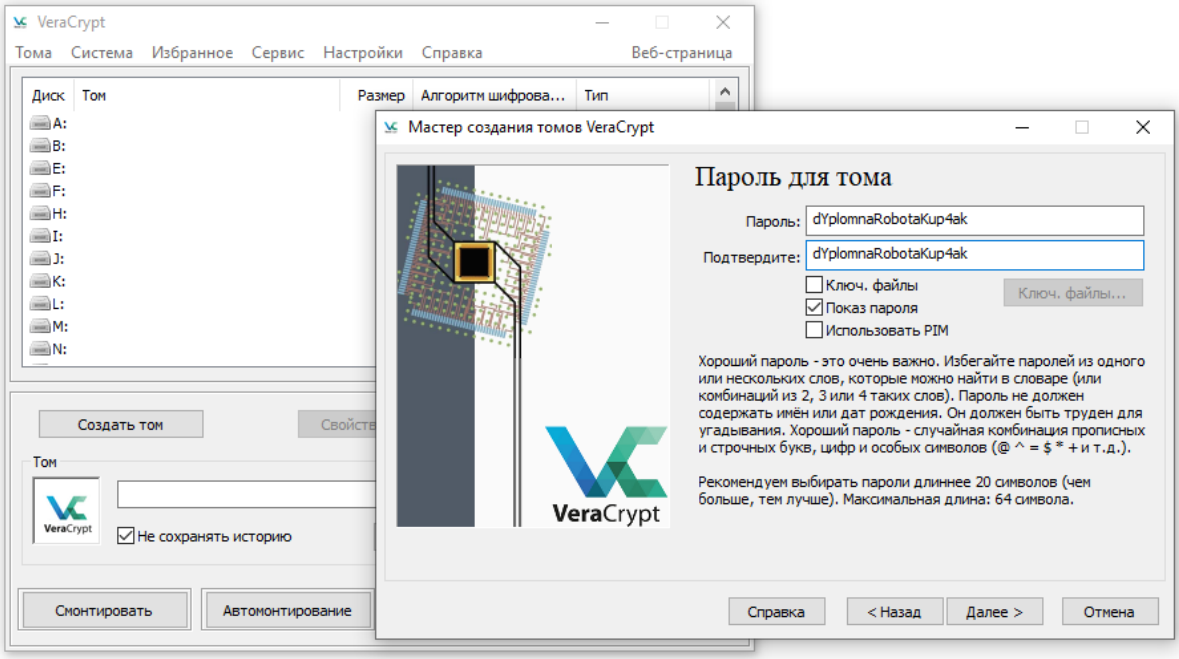


Рисунок 5.4 – Створення паролю для тому

На рисунку 5.5 показано, як за допомогою миші керування випадково генеруються числа, які використовуються для генерації головного ключа. Створюється басейн з випадковими значеннями в оперативній пам’яті.

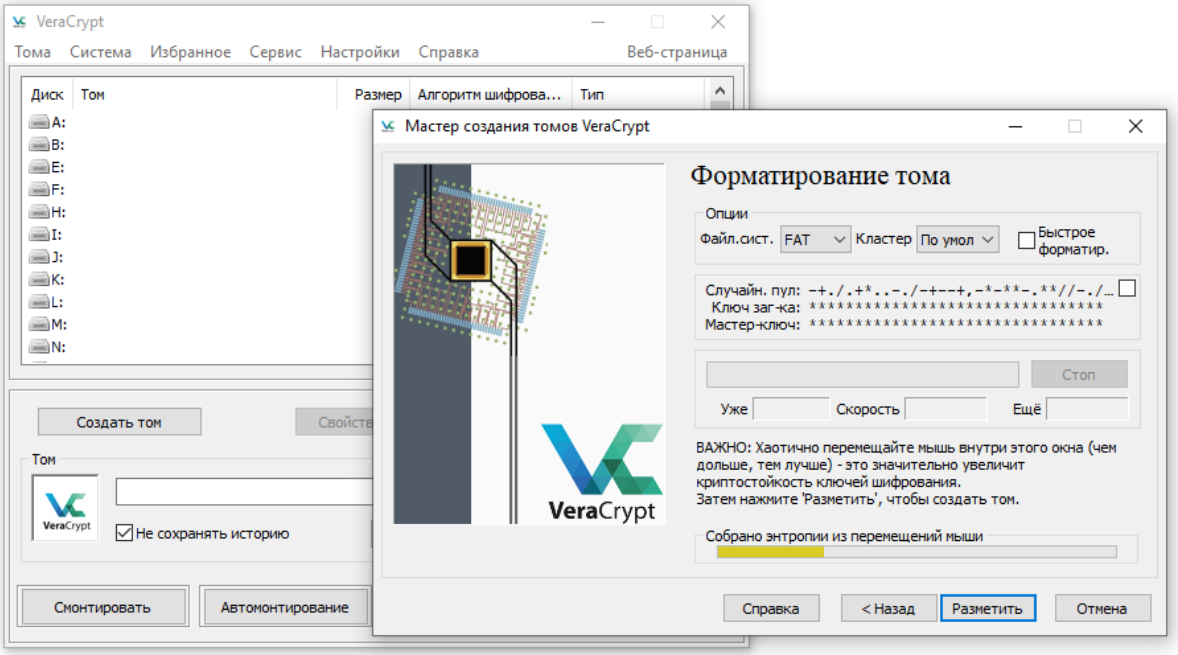


Рисунок 5.5 – Генерування випадкових чисел

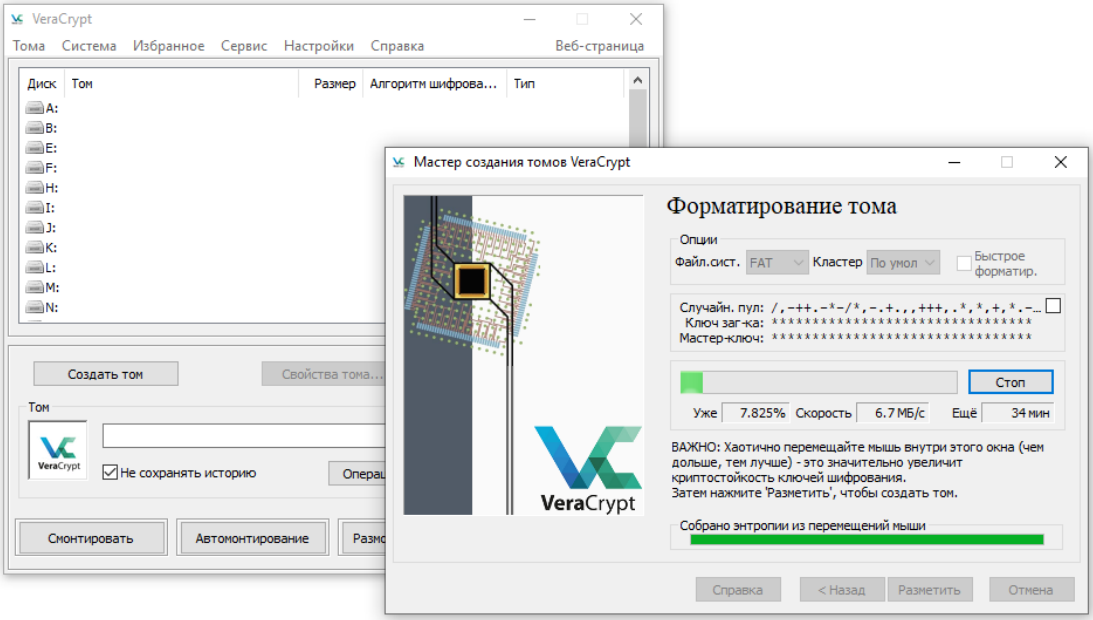


Рисунок 5.6 - Форматування та шифрування тому

На рисунку 5.6 показана швидкість та час до закінчення шифрування логічного тому, для флеш носія з роз’ємом 2.0 типу «А» зі швидкістю 5.0 – 7.0 МБ/с, приблизний час до повного шифрування носія інформації такого формату на 16 Гб, займає від 35 до 40 хв. Після завершення шифрування, вікно сповіщення повідомляє користувача про успішне виконання процесу наведено на рисунку 5.7.

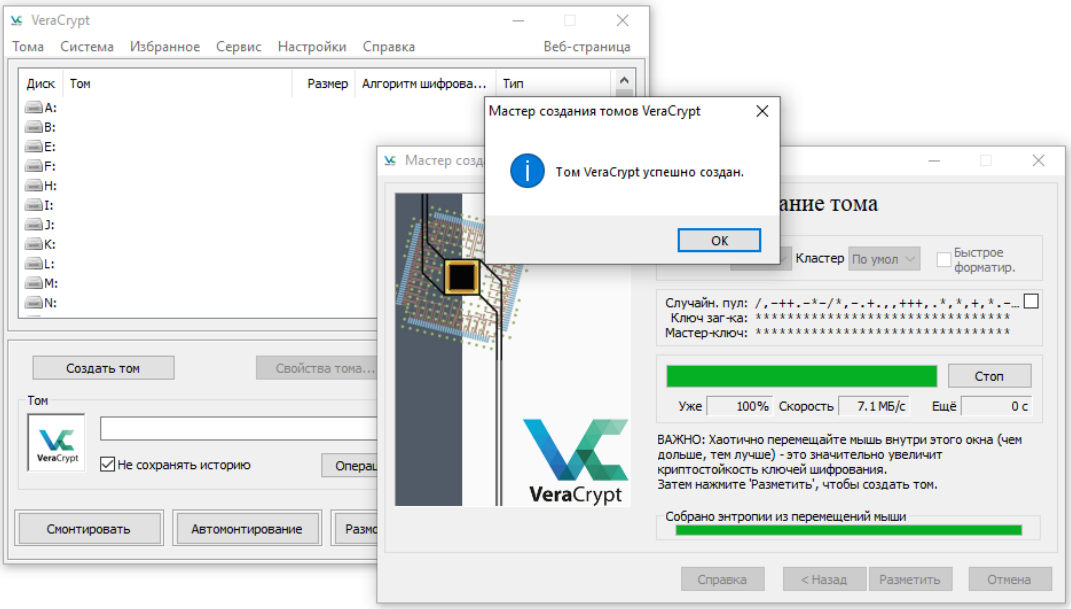


Рисунок 5.7 – Успішне завершення шифрування носія інформації

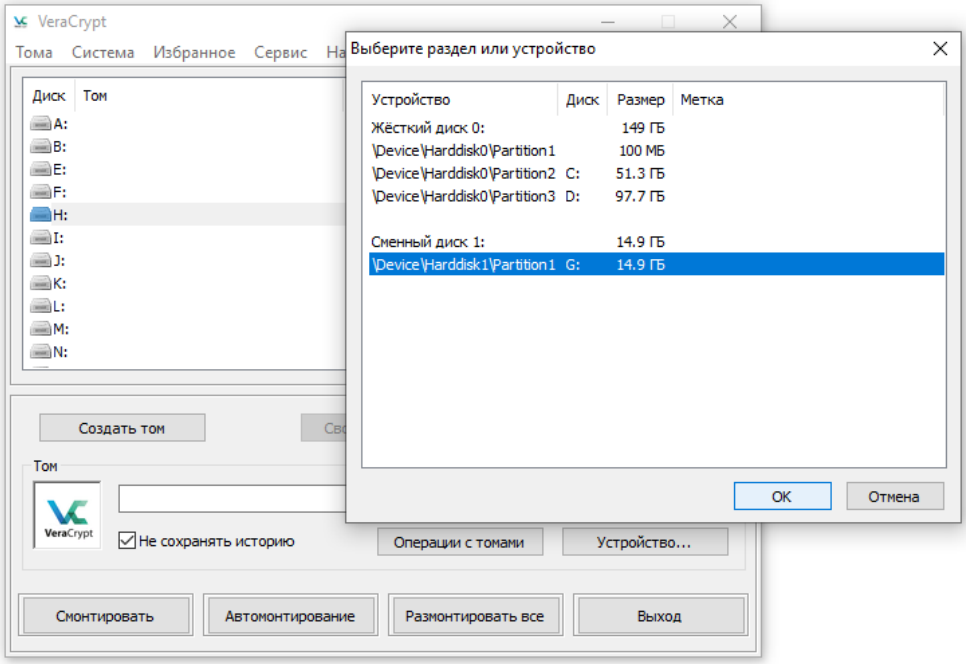


Рисунок 5.8 – Вибір розділу зашифрованого носія

Для початку використання зашифрованого тому слід вибираючи вкладку «Пристрої», вибрати розділ носія інформації та присвоїти йому ідентифікатор, після чого змонтувати його. На рисунку 5.9 показано автентифікацію методом вводу паролю, який був заданим перед початком шифрування.

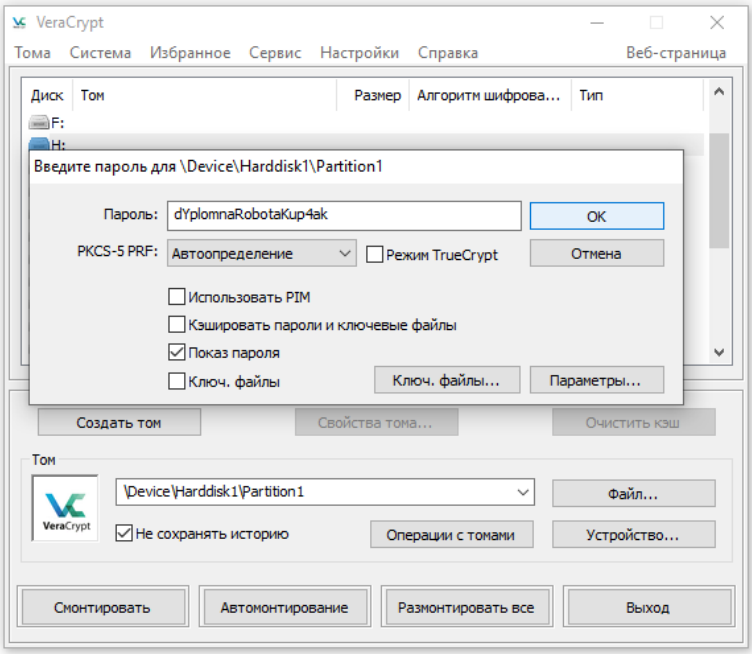


Рисунок 5.9 – Ввід паролю для монтування розділу

При успішній автентифікації, появляється том під індексом, який був присвоєний перед монтуванням, в даному випадку це «H», том «USB - дисковод» з індексом «G» це і є сам зашифрований розділ, який без монтування відкрити неможливо, наведено на рисунку 5.10

Рисунок 5.10 – Змонтований зашифрований том

Користувач може використовувати даний розділ для записування, змінення та видалення даних. Після закінчення роботи, слід відмонтувати даний розділ, нажавши у програмному вікні вкладу «Розмонтувати».

Висновки до п’ятого розділу

Проаналізуваши можливість шифрування даних на носії інформації, для безпечного зберігання даних, а також проілюстровано порядок дій при зашифрувані розділу флеш носія 2.0 стандарту «А» можна вважати що програма дійсно є легкою і зрозумілою у користуванні. Великий вибір алгоритмів шифрування та їх поєднання, гарантує стійкість інформації від загрози несанкціонованого доступу.

VeraCrypt на відміну від BitLocker має відкритий програмний код, що забезпечує відкритість та прозорість методу шифрування, без можливості зміни алгоритму структурного коду.

РОЗДІЛ 6. ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ

6.1. Приклади компонентів для використання системи захисту інформації

Для кожної сфери діяльності людини, особливо робота з автоматизованими системами, безпека інформації завжди на першому місці. Для захисту якої витрачаються колосальні затрати грошових коштів. Одним із прикладів є програмний пристрій «Лоза – 1», який спроможний захистити критичну інформацію користувача.

Станом на 2019 рік, ринкова вартість системи захисту інформації «Лоза - 1» версії 4, науково-дослідницького інституту «Автопром» за одиницю клієнтської ліцензії становить 6000 грн. без ПДВ.

Враховуючи вартість даної системи, слід не забувати про програмне забезпечення (ПЗ), з яким воно працює.

Ліцензоване ПЗ Microsoft Windows 10 Pro для комерційного використання вартує 3500 грн., або ж Microsoft Windows 10 Professional для дому та малих організацій ціна 1093 грн..

Методика зберігання інформації, яка запропонована у науково-дослідницькій роботі - VeraCrypt є безплатною, оскільки офіційні представники та винахідники, презентують її як відкриту та для вільного доступу програму.

6.2. Розрахунок матеріальних витрат

Матеріальні витрати визначаються як добуток кількості витрачених матеріалів та їх ціни:

$$M_{вi} = q_{\text{i}} \cdot p_{\text{i}} , \qquad (6.1)$$

де: q_{i} – кількість витраченого матеріалу і–го виду; p_{i} – ціна матеріалу і–го виду.

Звідси, загальні матеріальні витрати можна визначити:

$$З_{м.в.} = \sum M_{вi} . \qquad (6.2)$$

Проведені розрахунки занесено у таблицю 6.1. та 6.2.

Таблиця 6.1 – Зведені розрахунки матеріальних витрат для «Лоза-1»

Найменування матеріальних ресурсів	Один. виміру	Норма витрат	Ціна за один., грн.	Затрати матер., грн.	Транс-портно-заготівель-ні витрати, грн.	Загальна сума витрат на матер., грн.
1	2	3	4	5	6	7
Ліцензія на Microsoft Windows 10 Pro для комерційного використання	штук	20	6000	-	-	120000
системи захисту інформації «Лоза - 1»	штук	20	3500	-	-	70000
					Разом:	190000

Таблиця 6.2 – Зведені розрахунки матеріальних витрат для методики захисту інформації за допомогою VeraCrypt

Найменування матеріальних ресурсів	Один. виміру	Норма витрат	Ціна за один., грн.	Затрати матер., грн.	Транс-портно-заготівель-ні витрати, грн.	Загальна сума витрат на матер., грн.
1	2	3	4	5	6	7
Ліцензія на Microsoft Windows 10 Pro для комерційного використання	штук	20	6000	-	-	120000
програма шифрування VeraCrypt	штук	20	-	-	-	-
Флеш носій інформації Kingston DataTraveler Mini RX 16GB USB 3.0 (DTMRX/16G)	штук	20	-	-	-	-
					Разом:	122000

Як ми бачимо із порівняльних таблиць, використання методики безпечного зберігання інформації на носіях цифрових носіях за допомогою програми шифрування VeraCrypt є фінансово доцільнішою.

6.3. Розрахунок норм часу на виконання науково-дослідної роботи

Ефективне використання часу має надзвичайно важливе значення, оскільки ефективність залежить від оптимального використання часу.
Розробка поділяється на кілька етапів, що сприятиме та структуруватиме впровадження розробки методології.

Основними етапами розробки методології є:

1. Обґрунтування необхідності використання методики безпечного зберігання інформації.
2. Обстеження середовища в якому запропонована методика.
3. Визначення потенційних загроз інформації.
4. Розробка документів політики безпеки.
5. Складання плану захисту.
6. Підготовка до введення в дію методики.
7. Попереднє випробування методики.
8. Введення в дію методики.

Для оцінки тривалості виконання окремих робіт використовують нормативи часу або попередній досвід. До таких відносять і тривалість встановлення програмного забезпечення та програм шифрування . Виконавцем усіх операцій по розробці методики безпечного зберігання інформації на носіях являються позаштатні працівники служби захисту інформації. Витрати часу по окремих операціях технологічного процесу відображені в таблиці 6.3.

Таблиця 6.3 – Операції технологічного процесу та час їх виконання

№ п/п	Назва операції (стадії)	Виконавець	Середній час виконання операції, год.
1	2	3	4

Продовження таблиці 6.3

1	2	3	4
1.	Обґрунтування необхідності використання методики безпечного зберігання інформації	Інженер	8
2.	Обстеження середовища в якому запропонована методика.	Інженер	16
3.	Визначення потенційних загроз інформації.	Інженер	8
4.	Розробка документів політики безпеки.	Інженер	16
5.	Складання плану захисту.	Інженер	12
6.	Підготовка до введення в дію методики.	Інженер	24
7.	Попереднє випробування методики.	Інженер	24
8.	Введення в дію методики.	Інженер	36
Разом			144

6.4. Розрахунок витрат на електроенергію

Затрати на електроенергію 1–ці обладнання визначаються за формулою:

$$З_в = W \cdot T \cdot S\,, \qquad (6.3)$$

де W – необхідна потужність, кВт; T – кількість годин роботи обладнання; S – вартість кіловат-години електроенергії.

Вартість кіловат-години електроенергії слід приймати згідно існуючих на даний час тарифів (1,40 грн. + 20% ПДВ за 1 кВт). Отже, 1 кВт з ПДВ коштує 1,68 грн.

Потужність комп’ютера для створення проекту – 400 Вт, кількість годин роботи обладнання згідно таблиці 3.1 –144 години.

Тоді,

$$З_в = 0{,}4 \cdot 144\ 1{,}68 = 96{,}76 \text{ грн.}$$

6.5. Розрахунок суми амортизаційних відрахувань

Характерною особливістю використання основних фондів у виробничому процесі є їх відновлення, для засобів праці у натуральному виразі необхідне для відшкодування у вартісній формі, що виконується за рахунок амортизації. Амортизація - це процес перенесення вартості на вартість нової продукції з метою повного відновлення витрачених коштів [28].

Для визначення амортизації використовується формула:

$$A = \frac{Б_В \cdot Н_А}{100\%}, \tag{6.4}$$

де A – амортизаційні відрахування за звітний період, грн.; $Б_В$ – балансова вартість групи основних фондів на початок звітного періоду, грн.; $Н_А$ – норма амортизації.

Комп’ютерні програми, ЕОМ для обробки інформації належать до четвертої групи основних фондів. Для цієї групи річна норма амортизації дорівнює 60 % (квартальна – 15 %) [29].

Для даного проекту засобом є методика безпечного зберігання інформації на флеш-носіях інформації, програмою шифрування VeraCrypt, керуючись операційною системою Microsoft Windows 10 Pro для комерційного використання . Сума становить 3600 грн. Отже, амортизаційні відрахування будуть рівні:

$$A = 3600 \cdot 5\% / 100\% = 180{,}00 \text{ грн.}$$

Оскільки робота виконувалась 144 години, то амортизаційні відрахування будуть становити:

$$A = 180{,}0 \cdot 144 / 144 = 180{,}0 \text{ грн.}$$

6.6. Складання кошторису витрат та визначення собівартості науково-дослідної роботи

Результати проведених вище розрахунків зведено у таблицю 6.4.

Таблиця 6.4 – Кошторис витрат на НДР

Зміст витрат	Сума, грн.	В % до загальної суми
1	2	3
Матеріальні витрати	122000	99,77
Витрати на електроенергію	96,76	0,08
Амортизаційні відрахування	180,00	0,15
Собівартість	122276,76	100,00

Собівартість ($C_в$) програмного продукту розрахуємо за формулою:

$$C_в = З_{м.в.} + З_в + A \ . \qquad (6.5)$$

Отже, собівартість програмного продукту дорівнює:

$$C_в = 122000{,}00 + 180{,}00 + 96{,}76 = 122276{,}76 \text{ грн.}$$

6.7. Розрахунок ціни програмного продукту

Ціну науково-дослідної роботи можна визначити за формулою:

$$Ц = \frac{C_В \cdot (1 + P_{рен}) + K \cdot B_{н.і.}}{K} \cdot (1 + ПДВ) \ , \qquad (6.6)$$

де $P_{рен.}$ – рівень рентабельності, 30 %; K – кількість замовлень, од. (встановлюється лише при розробці програмного продукту та мікропроцесорних систем); $B_{н.і.}$ – вартість носія інформації, грн. (встановлюється лише при розробці програмного продукту); *ПДВ* – ставка податку на додану вартість, (20 %).

Оскільки розробка є прикладною, і використовуватиметься тільки для одного підприємства, то для розрахунку ціни не потрібно вказувати коефіцієнти К та Ві.н , оскільки їх в даному випадку не потрібно [30].

Тоді, формула для обчислення ціни розробки буде мати вигляд:

$$Ц = C_B \cdot (1 + P_{рен}) \cdot (1 + ПДВ) \tag{6.7}$$

Звідси ціна на проект складе:

$$Ц = 122276{,}76 \cdot (1 + 0{,}3) \cdot (1 + 0{,}2) = 190751{,}75 \text{ грн.}$$

6.8 Визначення економічної ефективності і терміну окупності капітальних вкладень

Ефективність виробництва – це узагальнене і повне відображення кінцевих результатів використання робочої сили, засобів та предметів праці на підприємстві за певний проміжок часу.

Економічна ефективність (E_p) полягає у відношенні результату виробництва до затрачених ресурсів:

$$E_p = \frac{П}{C_B}, \tag{6.8}$$

де $П$ – прибуток; C_B – собівартість.

Плановий прибуток ($П_{пл}$) знаходимо за формулою:

$$П_{пл} = Ц - C_в . \tag{6.9}$$

Розраховуємо плановий прибуток:

$П_{пл}$ = 190751,75 – 122276,76 = 68474,99 грн.

Отже, формула для визначення економічної ефективності набуде вигляду:

$$E_p = \frac{П_{пл}}{C_в}. \quad (6.10)$$

Тоді,

$$E_p = 68474{,}99 / 122276{,}76 = 0{,}56.$$

Поряд із економічною ефективністю розраховують термін окупності капітальних вкладень (T_p):

$$T_p = \frac{1}{E_p}, \quad (6.11)$$

Термін окупності дорівнює:

$$T_p = 1 / 0{,}56 = 1{,}8 \text{ роки}$$

Висновки до шостого розділу

В організаційно-економічній частині дипломного проекту були розраховані основні техніко-економічні показники розвитку безпечного методу захисту інформації (табл. 6.5).

Розраховане значення економічної ефективності становить 0,56.

Не менш нормальним є термін окупності, який повинен становити від 1 до 3 років, відповідно розвиток вважається можливим і прибутковим, а для даної методики це 1,8 року.

Підбиваючи підсумки, можна вважати, що проект даної методики є фінансово доцільним та може впроваджуватись з подальшим розвитком.

Таблиця 6.5 – Техніко-економічні показники науково-дослідної роботи

№ п/п	Показник	Значення
1	2	3

Продовження таблиці 6.5

1	2	3
1.	Собівартість, грн.	122276,76
2.	Плановий прибуток, грн..	68474,99
3.	Ціна, грн.	190751,75
4.	Економічна ефективність	0,56
5.	Термін окупності, рік	1,8

РОЗДІЛ 7 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

7.1. Охорона праці

Для реалізації методики що запропонована у даній роботі ніяк не обійтись без електронно-обчислювальної машини. Оскільки вона дозволяє записувати, видаляти та читати інформацію що циркулює на цифрових носіях.

Однак, разом з позитивною стороною, людство при використанні комп'ютерних технологій піддається цілого ряду негативних факторів, які істотно позначаються на його життєздатності.

Робота з комп'ютером характеризується значною розумовою напругою і нервово-емоційним навантаженням користувача, високою напруженістю зорової роботи і достатньо великим навантаженням на м'язи рук при роботі з клавіатурою ПЕОМ.

Щоб зменшити до мінімуму шкідливі чинники та запобігти негативним наслідкам, слід дотримуватись різного роду рекомендацій та інструкцій.

До роботи на персональних ЕОМ допускаються особи не молодші 18 років, що не мають протипоказань за результатами попереднього і періодичного медичних оглядів і які пройшли інструктаж, навчання і перевірку знань по охороні праці і мають I кваліфікаційну групу по електробезпеці

Допуск до роботи на персональних ЕОМ осіб молодших 18 років (практиканти, учні) здійснюється під керівництвом досвідчених робітників, що мають кваліфікаційну групу по електробезпеці не нижче III.

Робота на робочих місцях, оснащених дисплеями, супроводжується дією таких небезпечних і шкідливих чинників: напруга зору, гіподинамія, монотонність праці, підвищений рівень статичної електрики, відбитий блиск екрана дисплея, емоційні перевантаження, можливість ураження електричним струмом.

Для зниження і попередження шкідливого впливу вищевказаних чинників необхідно:

- для зниження рівня статичної електрики розташовувати екран дисплея на відстані не ближче 550 - 700 мм від очей оператора;

-для зниження відбитого блиску екран дисплея повинний розташовуватися перпендикулярно світловому потоку від віконних прорізів або від електросвітильників;

- для зниження втомлюваності очей освітленість робочого місця повинна бути не менше 300 - 500 Люкс; яскравість світіння екрана - не менше 100 кл / кв.м.; контрастність зображення знаку - не менше 0,8; частота регенерації - не менше 72 Гц;

- для зниження впливу гіподинамії й емоційних перевантажень варто використовувати технологічні перерви і виконувати комплекс фізичних вправ[34].

Режим праці і відпочинку операторів, що працюють з ЕОМ, повинен бути наступним: через кожну годину інтенсивної роботи необхідно влаштовувати 15-хвилинну перерву, при менш інтенсивної через кожні 2 години.

Ефективність перерв підвищується при поєднанні з виробничою гімнастикою або організації спеціального приміщення для відпочинку персоналу із зручними м'якими меблями, акваріумом, зеленою зоною тощо.

Важливе місце в комплексі заходів по створенню умов праці, які працюють з ПЕОМ, займає створення оптимальної світловий середовища, тобто раціональна організація природного та штучного освітлення приміщення і робочих місць. Правильно спроектоване і виконане виробниче освітлення покращує умови зорової роботи, знижує стомлюваність, сприяє підвищенню продуктивності праці, благотворно впливає на виробниче середовище, надаючи позитивну психологічну дію на працюючого, підвищує безпеку праці і знижує травматизм. Недостатність освітлення призводить до напруги зору, послаблює увагу, приводить до настання передчасної стомленості. Надмірно яскраве освітлення викликає осліплення, роздратування і різь в очах. Неправильний

напрямок світла на робочому місці може створювати різкі тіні, відблиски, дезорієнтувати працюючого. Всі ці причини можуть призвести до нещасного випадку або профзахворювань, тому настільки важливий правильний розрахунок освітленості.

Місцеве освітлення на робочих місцях забезпечується світильниками, що встановлюються безпосередньо на робочому столі або на вертикальних панелях спеціального обладнання. Вони повинні мати відбивач і розташовуватися нижче або на рівні лінії зору операторів, щоб не викликати засліплення.

7.2. Безпека в надзвичайних ситуаціях

При забезпеченні безпеки життєдіяльності при роботі з ПК, слід дотримуватись правил, а саме: залишити в гардеробі вуличний одяг, особисті речі, прибрати з робочого місця предмети, що не будуть використовуватися в роботі, забороняється класти на блоки ПЕОМ папір, книги, документи й інші предмети, забороняється підключати комп’ютер через трійники разом з іншими електроприладами, щоб уникнути перевантаження мережі.

Включити, при необхідності, штучне освітлення, настільний світильник. Зовнішнім оглядом переконатися в справності з’єднувальних проводів, штепсельних вилок, шин заземлення і вимикачів, у надійності кріплення захисних кожухів і кришок блоків ПЕОМ. Перевірити відсутність пилюки на екрані дисплея і наявність паперу в приймальному лотку принтера. Не допускати забивання пилюкою і сторонніми предметами вентиляційних отворів для відводу тепла з блоків ПЕОМ.

При виявленні пошкоджень, які створюють небезпеку або значні незручності в роботі, негайно повідомити позаштатного адміністратора СЗІ.

При вмиканні персональної ЕОМ в електромережу, братися тільки за ізольовані частини штепсельних вилок. Дотримуватися послідовності вмикання блоків ПЕОМ. Щоб уникнути розрядів статичної електрики забороняється доторкатися до екрана дисплея. При введенні даних, редагуванні програм,

читанні інформації з екрана, безперервна тривалість роботи перед екраном не повинна перевищувати 4 години. Впродовж двох регламентованих перерв по 10 хвилин, через 2 години від початку робочої зміни і через 2 години після обідньої перерви, виконувати комплекс фізичних вправ, релаксаційної гімнастики.

Забороняється при включеному електроживленні ПЕОМ:

- розкривати захисні кожухи і кришки блоків ПЕОМ, робити регулювання і чищення внутрішніх деталей, замінювати запобіжники;

- переключати сполучні шнури блоків ПЕОМ;

- змінювати встановлену конфігурацію робочого місця, переставляти блоки ПЕОМ;

- робити вологе прибирання поверхні комп'ютера;

- приймати їжу безпосередньо за клавіатурою комп'ютера.

Категорично забороняється на робочому місці користувача ПЕОМ:

- палити, користуватися відкритим вогнем;

- зберігати легкозаймисті, вибухонебезпечні і хімічно активні речовини, що руйнують ізоляцію.

Після закінчення роботи, потрібно закрити програми з якими працювали, закрити всі каталоги, підготувати комп'ютер до виключення. Відключити ПЕОМ і місцеве електроосвітлення від мережі. Впорядкувати робоче місце, прибрати документи, якими користувались Переконатися у відсутності пожежної небезпеки. У разі неполадок або збоїв в роботі, повідомити про це людину, яка відповідальна за ПЕОМ [35].

Дії при аварійній ситуації. Ознаками аварійної ситуації на робочому місці користувача ПЕОМ є:

- виявлення збоїв у роботі ПЕОМ, затискання паперу в принтері, зникання зображення на екрані дисплея;

- коротке замикання, іскріння, появи запаху горілого, підвищене нагрівання корпусу, штепсельних роз’ємів, з’єднувальних шнурів, зниження або зникнення напруги в мережі тощо.

У аварійній ситуації необхідно:

- роботу припинити, ПЕОМ відключити від мережі;

- при загорянні використовувати вуглекислотний або порошковий вогнегасник;

- вжити заходів по евакуації людей і наданню першої допомоги потерпілим;

- доповісти про те, що трапилося, керівнику. При необхідності викликати швидку допомогу, пожежну команду.

Висновки до сьомого розділу

До розділу з охорони праці та безпеки в надзвичайних ситуаціях при роботі за комп’ютером можна також добавити так загальні вимоги безпеки:

- при роботі з ПК необхідно бути уважним, дотримуватись вимог Правил внутрішнього розпорядку і виробничої санітарії;

- кількість символів при обробці текстового та цифрового матеріалу не повинно перевищувати 30 тисяч за 4 години роботи;

- при виникненні нещасного випадку з працюючим на ЕОМ ПК, потерпілий або свідок нещасного випадку повинен негайно повідомити керівника підрозділу для проведення розслідування і усунення причин нещасного випадку, надати першу допомогу;

- порушення вимог даних рекомендацій тягне за собою відповідальність порушника згідно з чинним законодавством.

РОЗДІЛ 8. ЕКОЛОГІЯ

8.1. Статистичне групування в екології

У системі статистичних методів, групування займає особливе місце. Це пояснюється тим, що на відміну від інших методів групування виконує дві функції: по-перше, розподіляє сукупності на однорідні групи, а по-друге, визначає межі і можливості застосування інших статистичних методів (середніх величин, кореляційно-регресійного тощо).

Статистичне групування - це розподіл сукупності досліджуваних екологічних явищ на групи із характерними для них ознаками задля дослідження: стохастичного взаємозв' язку між ознаками, закономірностей всієї сукупності, структури та структурних зрушень.

Метою статистичного групування є поділ сукупностей на однорідні типові групи за існуючими для них кількісними ознаками з метою всебічної характеристики їхнього стану, розвитку і взаємодії, їх характеристика; дослідження структури масової сукупності; вивчення взаємодії між окремими ознаками сукупності.

Суть методу статистичних групувань полягає у тому, що складне масове явище розглядається не як єдине нероздільне ціле, а в ньому виділяються окремі групи одиниць із статистичними показниками, які дають кількісну характеристику якісно-своєрідній частині одиниць усієї сукупності. Тобто кожна з одержаних груп об'єднує однорідні одиниці сукупності.

Статистичні групування поділяються на види за декількома ознаками, залежно від мети та завдань дослідження:

- на типологічні; структурні; аналітичні, залежно від кількості групувальних ознак, покладених в основу групування;
- на прості та комбінаційні; залежно від виду групувальної ознаки;
- на факторні і результативні; залежно від способу побудови групувань;
- на первинне і вторинне.

Типологічні групування - це такі групування, які приводять до виділення у складі масових явищ їх соціально-екологічних типів (тобто однорідних частин за якістю та умовами розвитку, в яких діють одні ї теж закономірності факторів). їх застосовують при вивченні стану забруднення природних сфер за видами типів і класів забруднювачів, за джерелами забруднень тощо.

Структурні групування характеризують склад однорідної сукупності за будь-якою ознакою. З допомогою таких групувань аналізують структуру сукупності і структурні зрушення в розвитку екологічних явищ і процесів.

Аналітичні групування спрямовані на виявлення зв'язку між окремими ознаками явища, що вивчається. Вони проводяться за факторною ознакою і в кожній групі визначається середня величина результативної ознаки, зазначено у таблиці 8.1.

Таблиця 8.1 – Вплив викидів шкідливих речовин в атмосферне повітря на екологічні збори і витрати

Показники	Групи, об'єктів за обсягом викидів, тис. т					Всього
	I <0,6	II 0,6-1,2	III 1,2-2,4	IV 2,4-4,8	V >4,8	
Кількість об'єктів	14,3	21,4	35,7	17,9	10,7	100,0
Обсяг викидів	2,8	7,4	22,6	21,9	45,2	100,0
Екологічні збори за забруднення навколишнього. середовища	0,2	19,4	14,8	28,3	37,4	100,0
Витрати підприємств на природоохоронні заходи	0,1	2,7	44,4	16,3	36,4	100,0

Тут викиди виступають в якості факторної ознаки, оскільки від їх обсягу залежить сума екологічних зборів. Останні, є результативною ознакою, тобто наслідком викидів. Із зростанням обсягу викидів від групи до групи зростають суми зборів, а також зростають витрати на природоохоронні заходи. При цьому зростання останніх показників не є прямо пропорційним.

Факторне групування - це групування, яке проводиться за факторною ознакою, тобто ознакою, яка впливає на інші ознаки. Факторні ознаки мають важливіше аналітичне значення, даючи можливість кількісно оцінити вплив окремих факторів на досліджувані явища.

Результативне групування - це групування, яке проводиться за результативною ознакою, тобто ознакою, яка є залежною від факторних ознак.

Комбінаційне групування - це групування, яке проводиться за двома і більше групувальними ознаками. У комбінаційних групуваннях групи з однією ознакою поділяються на підгрупи за іншою ознакою. Поряд з комбінаційним групуванням найбільш часто використовують просте групування, групування, яке проводиться за однією ознакою [37].

8.2. Методологія моделювання екологічних проблем

Методологія — це система принципів наукового дослідження, вчення про науковий метод пізнання законів природи за допомогою сукупності методів дослідження, що застосовуються в будь-якій науці відповідно до специфіки об'єкта її пізнання. Існує два універсальні підходи щодо методології пізнання: мерологічний та холістичний.

Моделювання та прогнозування стану довкілля являє собою систему понять і методів, націлених на відтворення, аналіз та прогноз розвитку різноманітних природних та техногенних екологічних систем на різних рівнях їх ієрархічної організації – від окремої екосистеми до національних і глобальних екосистем планети Земля. Моделювання є одним з головних засобів пізнання в екології. На цей час широко використовуються такі методи, як:

- натурно-експериментальне моделювання;
- математичне (у тому числі числове) моделювання;
- системне моделювання.

Основні фактори, що враховуються при моделюванні екологічних систем, можна розділити на такі дві групи:

1) фактори зовнішнього впливу:

- кліматичні зміни (температура, опали тощо);

- антропогенне втручання тощо;

2) внутрішні фактори:

- конкуренція;

- паразитизм;

- хижацтво;

- захворюваність та її поширення;

- трофічні ланцюги.

При ньому потрібно враховувати, що вплив таких факторів характеризується наявністю:

- ефекту запізнення;

- кумулятивного ефекту;

- граничних ефектів.

Як правило, математичний опис впливу факторів зв'язаний і великою кількістю взаємозалежних змінних, зв'язаних між собою нелінійними співвідношеннями, що сильно ускладнює задачу і вимагає застосування ЕОМ.

При побудові моделей екологічних процесів застосовують наступні основні принципи.

1) Принцип системності.

Внаслідок пересиченості екосистем зв'язками екологічні об'єкти являють собою єдину систему. З цієї причини в екології виявилося необхідним злиття методів системного аналізу і математичного моделювання. Це призвело до створення інтегрального методу системного моделювання - вищого етапу в розвитку екологічного моделювання.

Принцип системності полягає в усвідомленні цілісності об'єктів світу, їхньої стійкості і взаємозв’язку зі зовнішнім світом тощо; інший аспект цього принципу - динамічна багатогранність, єдність якості її кількості, теорії та практики.

2) Принцип єдності структурності та ієрархічності.

Фундаментальна риса екосистем - наявність у них складних ієрархічних структур. Звідси випливає вимога єдності структурності й ієрархічності системних екологічних моделей. Відповідно виникає проблема структурування моделі, тобто виділення істотних підсистем і елементів із сукупності всіх зв'язків і компонентів.

Звичайно систему організують найбільш залежні одне від одного елементи (підсистеми). Інші впливають на поводження системи слабко, а через їхню велику кількість - не узгоджено, отже їх можна розглядати як інтегровані зовнішні чи внутрішні фактори впливу.

3) Принцип багатомодельного опису.

Через динамізм і складність екологічних об'єктів, що виникають у результаті множинності мети антропогенного втручання, на сьогодні немає можливості побудови єдиної теорії сонціоекосистеми в класичному розумінні, тобто як дедуктивної моделі, з якої можна вивести всі можливі наслідки. Тому наука йде по шляху створення множинних взаємодоповнюючих моделей.

4) Принцип єдності формалізованою і неформалізованого опису.

Досвід перших глобальних моделей розвитку світової соціоекосистеми, побудованих за замовленням Римського клуба, показав: єдиного формалізованого (математичного) опису недостатньо для адекватного моделювання соціоекосистеми. Для цього необхідно враховувати неформальні факторії і доповнювати формалізований опис (з позицій Історичного, психологічного та ні. підходів) неформалізованим описом.

5) Принцип визнання фундаментальності екологічних процесів.

Екологічні процеси неможливо звести до простої сукупності біологічних, фізичних, економічних процесів, оскільки всі вони тісно переплетені між собою. У цьому переплетенні виникають нові, екологічні закономірності. Звідси випливає самостійна значимість екологічних цінностей.

6) Принцип єдності теорії та практики.

Благополуччя соціоекосистеми, частиною якої є людина, має для неї найважливіше значення. Тому екологія є не тільки фундаментальною, але і прикладною наукою, що поєднує пізнання екологічних закономірностей із практичним їхнім застосуванням у повсякденній діяльності людини. Ця єдність виражається у вигляді принципу: "Не тільки дивися і думай — роби".

Значення моделювання в екології. За допомогою моделювання одержують можливість оцінювання потенційних наслідків застосування різних стратегій оперативного керування впливу на екосистему, користування природними ресурсами (біотичними й абіотичними), оптимізації екосистем. Моделювання дозволяє глибоко проникнути в сутність явищ, зрозуміти їхню справжню природу [38].

Висновки до восьмого розділу

Зважаючи на колосальні проблеми навколишнього середовища, пов’язані з діяльністю людини, слід зауважити, що моделювання екологічних проблем та статистичне групування, дозволяє виявити суть проблематики, причини їх виникнення, визначити обсяг та методи їх вирішення.

ВИСНОВКИ

В даній роботі було проаналізовано загрози та методи зберігання інформації на цифрових носіях. Використання систем електронного документообігу дає можливість оптимізувати документообіг та скоротити як витрати часу, так і матеріальні витрати на забезпечення процесу документообігу цілому.

За результатами дослідження поставлених завдань ми прийшли до наступних висновків.

Аналіз показав, що серед багатьох організаційних, програмних та технічних заходів криптографія є одним з основних інструментів забезпечення конфіденційності та цілісності інформації, авторизації, оперативного контролю управління та обробки даних.

Було проаналізовано ряд методів захисту властивостей інформації на ЦНІ. Можна зазначити що основними загрозами для ЦНІ є загрози несанкціонованого і неправомірного впливу сторонніх осіб на інформаційні ресурси, збій в роботі обладнання наслідком якого може бути втрата, модифікація і витік інформації.

Запропонована методика, одна із найбільш доступних та легких у використанні, що забезпечує своєю стійкістю та прозорим шифруванням даних, програма шифрування даних – VeraCrypt.

Якщо виконувати вимоги даної методики, то крадіжка інформації з носія інформації, захищеного за допомогою програми шифрування VeraCrypt, потребуватиме надзвичайно великих ресурсів, як і фінансових так і часових. Цю методику можна використовувати як на державних об’єктах для підвищення захисту інформації так і на цивільних підприємствах. Відповідно, підрахувавши фінансові витрати, та амортизацію даного проекту, можна вважати, що проект фінансово доцільний.

Відповідно до поставлених завдань, було визначено ознаки ідентифікації у першому розділі, за допомогою яких визначається поняття справжності особи, що має право використовувати носій для обробки інформації.

Вивчено головні аспекти захисту інформації на цифрових носіях, та загрози відповідно яким є загроза втрати даних.

Проаналізовано методи, які входять до методики захисту інформації на її носіях і можна вважати, що дотримання комплексних методів з поєднанням даної методики, надійно забезпечить збереженість інформації від витоку та несанкціонованому доступу.

Також, найбільшим аргументом, щодо впровадження даної методики є відкритий код програмного продукту написаний на мовах програмування «C», «C++» та «Assembly», що мінімізує можливість умисного втручання, для зміни у вандальських цілях.

БІБЛІОГРАФІЯ

1. Директива 1999/93/ЕС Європейського Парламенту та Ради від 13 грудня 1999 року “Про систему електронних підписів, що застосовується в межах Співтовариства” (DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures, Офіційний журнал L 013, 19/01/2000 p. 0012 – 0020. Переклад здійснено Центром перекладів актів Європейського права при міністерстві юстиції України): [Електронний ресурс] – Режим доступу: http://uazakon.com/document/spart50/inx50337.htm -Дата доступу: 20.11.2019 – Назва з екрана.

2. Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 року № 851- IV,зі змінами від 07 листопада 2018 року [Електронний ресурс] Офіційний веб-портал Верховної Ради України. – Режим доступу : https://zakon.rada.gov.ua/laws/show/851-15/ed20030522 - Дата доступу: 20.11.2019 – Назва з екрана.

3. Закон України «Про національну безпеку України» від 21 червня 2018 року № 2469- VIII [Електронний ресурс] Офіційний веб-портал Верховної Ради України. – Режим доступу : http://zakon.rada.gov.ua/laws/show/2469-19 - Дата доступу: 20.11.2019 – Назва з екрана.

4. Присяжнюк М.М. Дезінформація та її роль у інформаційно-психологічних операціях [Електронний ресурс] М.М.Присяжнюк, О.П.Параніч. – Режим доступу : http://defpol.org.ua/site/index.php/en/arhiv/kolonkaavt_ora/106-2009-09-09-18-06-14 Дата доступу: 22.11.2019 – Назва з екрана.

5. Навчальні матеріали онлайн [Електронний ресурс] Поняття загроз інформаційній безпеці. – Режим доступу: https://pidruchniki.com/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsii - Дата доступу: 15.11.2019 – Назва з екрана.

6. Закон України «Про електронний цифровий підпис» від 22 травня 2003 року № 852- IV [Електронний ресурс] Офіційний веб-портал Верховної

Ради України – Режим доступу : http://zakon.rada.gov.ua/laws/show/ 852-15/ed20030522 - Дата доступу: 10.11.2019 – Назва з екрана.

7. Закон України «Про електронні довірчі послуги» від 05 жовтня 2017 року № 2155- VIII [Електронний ресурс] Офіційний веб-портал Верховної Ради України – Режим доступу : http://zakon.rada.gov.ua/laws/show/2155-19#n534 - Дата доступу: 22.11.2019 – Назва з екрана.

8. Компанія «Інфобезпека» [Електронний ресурс] Захист інформації в портативному ПК – Режим доступу: http://www.infobezpeka.com/news/?id=118 - Дата доступу: 25.11.2019 – Назва з екрана.

9. Каминская Л. Электронная бумага: из мира научной фантастики – в реальность – Режим доступу: http://itc.ua - Дата доступу: 22.11.2019 – Назва з екрана.

10. Спеціальні цифрові носії інформації – теорія, технології, застосування УДК 621.391.7:336.71(075.8) В.К. Задірака, А.М. Кудін, В.О. Людвиченко, О.С. Олексюк Інститут кібернетики ім. В.М. Глушкова, м. Київ, Україна zvk140@ukr.net

11. Черточка [Електронний ресурс] Флеш-пам’ять – Режим доступу: http://cherto4ka.xyz/2018/03/18/флеш-память - Дата доступу: 20.11.2019 – Назва з екрана.

12. Нормативний документ [Електронний ресурс] Системи технічного захисту інформації затверджений наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22, із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 – Режим доступу: https://archives.gov.ua/Archives/Info/ND_TZI_2.5-004-99.pdf - Дата доступу: 20.11.2019 – Назва з екрана.

13. Олешко І. В. Порівняльний аналіз методів біометричної автентифікації на основі критерію відносної ентропії. Вісник Національного університету "Львівська політехніка" – 2012 – № 741 : Автоматика, вимірювання та керування. – С. 170–175.

14. Сьогодні Life Style [Електронний ресурс] Евгений Опанасенко: Карти пам'яті подолали недосяжний об'єм в 1 ТБ – Режим доступу: https://www.segodnya.ua/ua/lifestyle/science/karty-pamyati-preodoleli-nedostizhimyy-obem-v-1-tb-1227096.html – Дата доступу: 09.11.2019 – Назва з екрану.

15. Piraeus Online Banking Интерактивная система фронт-офисного обслуживания клиентов банка [Електронний ресурс] Инструкция по роботе с OTP-паролями в Web-приложении системы – Режим доступу: https://www.piraeusbank.ua/i_upload/(Piraeus_OTPConfirmationCorporate)UserManual%20(web).pdf – Дата доступу: 09.11.2019 – Назва з екрану.

16. Aladdin [Електронний ресурс] eToken. Руководство администратора Версия 3.66 02.04.2008 – Режим доступу: https://www.aladdin-rd.ru 79ст. 02.04.2008 – Дата доступу: 15.11.2019 – Назва з екрану.

17. Навчальні матеріали онлайн [Електронний ресурс] Інформаційна безпека України в умовах євроінтеграції – Режим доступу: https://pidruchniki.com/1584072028356/politologiya/informatsiyna_bezpeka_ukrayini_v_umovah_yevrointegratsiyi - Дата доступу: 15.11.2019 – Назва з екрана.

18. В.К. Задірака, О.С. Олексюк, М.О. Недашковський, Методи захисту банківської інформації. Навчальний посібник: Вища школа. Київ ,1999. 261 с.

19. Навчальні матеріали онлайн [Електронний ресурс] Поняття загроз інформаційній безпеці – Режим доступу: https://pidruchniki.com/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi - Дата доступу: 25.11.2019 – Назва з екрана.

20. Н. Р. Спиричева, Алгоритмы блочной криптографии. Навчальний посібник: Уральський університет. Єкатеринбург, 2013. 77с.

21. Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін, Комплексні системи захисту інформації. Навчальний посібник [Електронний ресурс] Розділ 7 Захист інформації в комп'ютерній системі підприємства – Режим доступу: https://web.posibnyky.vntu.edu.ua/fmib/41yaremchuk_kompleksni_systemy_zahtstu

_informaciyi/rozdil7.html - Дата доступу: 22.11.2019 – Назва з екрана.

22. Офіційний сайт програмного забезпечення VeraCrypt [Електронний ресурс] - Режим доступу: https://www.veracrypt.fr/en/Home.html - Дата доступу: 01.11.2019 – Назва з екрана.

23. Б. А. Ахметов, А. Г. Корченко, В. П. Сиденко, Ю. А. Дрейс, Н. А. Сейлова, Прикладная криптология: методы шифрования. Навчальний посібник: (КазНИТУ) имени К.И. Алмати, 2015. 496 с.

24. Державна служба спеціального зв'язку та захисту інформації України [Електронний ресурс] Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом (станом на 21.11.2019 року) – Режим доступу: http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=288071 Дата доступу: 15.11.2019 – Назва з екрана.

25. ТОВ НДІ «АВТОПРОМ» [Електронний ресурс] Засоби захисту від несанкціонованого доступу – Режим доступу: http://avtoprom.kiev.ua/avtoprom/ua/ - Дата доступу: 10.11.2019 – Назва з екрана.

26. [Електронний ресурс] Тестування програмних продуктів – Режим доступу: http://ua-referat.com/Тестування_програмних_продуктів - Дата доступу: 10.11.2019 – Назва з екрана.

27. Постанова Кабінету Міністрів України [Електронний ресурс] Положення про Адміністрацію Державної служби спеціального зв'язку та захисту інформації України від 3 вересня 2014 року №411 зі змінами від 7 листопада 2018 року – Режим доступу: https://zakon.rada.gov.ua/laws/show/411-2014-%D0%BF?lang=ru - Дата доступу: 10.11.2019 – Назва з екрана.

28. Економіка [Електронний ресурс] Зношення, амортизація та відновлення основних фондів підприємства – Режим доступу: https://referat.me/economy/380702-znoshennya-amortizac-ya-ta-v-dnovlennya-osnovnih-fond-v-p-dpriyemstva - Дата доступу: 10.11.2019 – Назва з екрана.

29. Податки та бухгалтерський облік 2017/№ 94 [Електронний ресурс] Амортизація основних засобів – Режим доступу: https://i.actor.ua/ukr/journals/nibu/2017/november/issue-94/article-32188.html - Дата доступу: 10.11.2019 – Назва з екрана.

30. Економічне обгрунтування коштоису витрат [Електронний ресурс] Складання кошторису витрат та призначення собівартості НДР - Режим доступу - https://studwood.ru/1511724/ekonomika/skladannya_koshtorisu_vitrat_viznachennya_sobivartosti - Дата доступу: 22.11.2019 – Назва з екрана.

31. Навчальні матеріали онлайн [Електронний ресурс] Поняття та види загроз національним інтересам та національній безпеці в інформаційній сфері – Режим доступу: https://pidruchniki.com/15341220/politologiya/ponyattya_vidi_zagroz_natsionalnim_interesam_natsionalniy_bezpetsi_informatsiyniy_sferi - Дата доступу: 25.11.2019 – Назва з екрана.

32. Лекции.Нет [Електронний ресурс] Види загроз інформаційній безпеці– Режим доступу: https://lektsii.net/1-73125.html - Дата доступу: 12.11.2019 – Назва з екрана.

33. Ю. Є. Яремчук, П. В. Павловський, В. С. Катаєв, В. В. Сінюгін, Комплексні системи захисту інформації. Навчальний посібник: ІРВЦ. Вінниця, 2018. 120 с.

34. Березнівська районна рада [Електронний ресурс] Розпорядження «Про затвердження програми вступного інструктажу, інструкцій з охорони праці та пожежної безпеки» – Режим доступу: http://berezne-rada.rv.ua/ - Дата доступу: 13.11.2019 – Назва з екрана.

35. ДНАОП Законодавча база [Електронний ресурс] Інструкція з охорони праці для працівників, зайнятих на роботах із персональними ЕОМ– Режим доступу: https://dnaop.com/ - Дата доступу: 13.11.2019 – Назва з екрана.

36. Буковинська бібліотека [Електронний ресурс] Групування статистичних даних – Режим доступу: https://buklib.net/books/35946/- Дата доступу: 14.11.2019 – Назва з екрана.

37. Навчальні матеріали онлайн [Електронний ресурс] Статистичне групування, його суть, завдання і види. – Режим доступу: https://pidruchniki.com/15800119/statistika/statistichne_grupuvannya_yogo_sut_zavdannya_vidi - Дата доступу: 25.11.2019 – Назва з екрана.

38. [Електронний ресурс] Моделювання і прогнозування стану водного об’єкта внаслідок антропогенного впливу – Режим доступу: https://www.bestreferat.ru/referat-121163.html - Дата доступу: 20.11.2019 – Назва з екрана.

ДОДАТКИ

Додаток А

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ

М А Т Е Р І А Л И

VII НАУКОВО-ТЕХНІЧНОЇ КОНФЕРЕНЦІЇ

«ІНФОРМАЦІЙНІ МОДЕЛІ, СИСТЕМИ ТА ТЕХНОЛОГІЇ »

11–12 грудня 2019 року

ТЕРНОПІЛЬ
2019

УДК 004.56.5

Ю. Купчак, В. Муж

Тернопільський національний технічний університет імені Івана Пулюя

МЕТОДИКА БЕЗПЕЧНОГО ЗБЕРІГАННЯ ІНФОРМАЦІЇ НА ЦИФРОВИХ НОСІЯХ

На сучасному етапі розвитку людства, неабияким питанням є реалізація можливості безпечного зберігання інформації будь-якої важливості, без великих затрат коштів та часу. Питання захисту інформації з використанням цифрових носіїв визначається поширенням видів контролю доступу, інформаційних, ідентифікаційних, біометричних та інших систем, а також окремих прикладних програм, які використовують цифрові носії як засіб зберігання і обробки персональних даних користувачів комп'ютерних систем.

Виходячи з вищесказаного, для усіх сфер діяльності людини, методика безпечного зберігання та використання інформації, що належить до державних інформацій ресурсів чи інформації з обмеженим доступом, на цифрових носіях є актуальним питання, вирішення якої дозволить підвищити безпеку інформації від несанкціонованого доступу та дій, що можуть призвести до її випадкової або умисної модифікації чи знищення, унеможливити передачу та/або розголошення конфіденційної інформації шляхом неконтрольованого ознайомлення чи копіювання. В той же час, забезпечити безвідмовний доступ до інформації особам, які мають на це право[1].

З цього приводу варто звернути увагу на способи безпечного зберігання інформації на цифрових носіях та впровадження методики безпечного зберігання критичної інформації на цифрових носіях, а саме на флеш-накопичувачах (типу USB, SD, SSD та ін.). За результатами неодноразових експерементальних досліджень виявлено актуальність використання програмних засобів шифрування, а саме: «TrueCrypt», «VeraCrypt» та «BitLocker», які можуть працювати спільно з 32-х і 64-х розрядною операційною системою із закритим вихідним кодом - Microsoft Windows[3].

Шифрування може здійснюватися за такими алгоритмами як: AES, Serpent, Twofish, Camellia, а також комбінацією даних алгоритмів. Використовуються криптографічні геш-функції «RIPEMD-160», «SHA-256», «SHA-512» та «Whirlpool». Можливості даних програм дозволяють легко працювати із зашифрованими віртуальними дисками, видаляти, створювати, записувати дані, а також створювати окремі розділи, що сприяє безпечній роботі з інформацією [2].

Запропонована методика зберігання та використання критичної інформації на носіях інформації, за допомогою шифрування програмним засобом, дозволить:

1 забезпечити цілісність, доступність та конфіденційність інформації;
2 унеможливити (значно ускладнити) несанкціонований доступ до критичної інформації;
3 зменшити економічні та часові витрати.

Висновком даної роботи є те, що на сьогоднішній день є доволі значна кількість програмних засобів, які дозволяють забезпечити конфіденційність, цілісність та доступність інформації, однак залишаються проблеми ліцензування, експертизи та сертифікації таких програмних засобів в Україні.

Література:

1. https://zakon.rada.gov.ua
2. https://habr.com/en/