МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ
ТЕХНІЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ІВАНА ПУЛЮЯ
ФАКУЛЬТЕТ КОМП'ЮТЕРНО-
ІНФОРМАЦІЙНИХ СИСТЕМ І ПРОГРАМНОЇ
ІНЖЕНЕРІЇ
КАФЕДРА КІБЕРБЕЗПЕКИ

КУПЧАК ЮРІЙ АНДРІЙОВИЧ

УДК 004.56.5

МЕТОДИКА БЕЗПЕЧНОГО ЗБЕРІГАННЯ ІНФОРМАЦІЇ НА ЦИФРОВИХ НОСІЯХ

125 – «Кібербезпека»

Автореферат
дипломної роботи на здобуття освітнього ступеня
«магістр»

Тернопіль 2019

Роботу виконано на кафедрі кібербезпеки, Тернопільського національного технічного університету імені Івана Пулюя Міністерства освіти і науки України

Керівник роботи: к.ю.н., доцент кафедри кібербезпеки
Муж Валерій Вікторович,
Тернопільський національний технічний університет імені Івана Пулюя.

Рецензент: д.к.н., професор кафедри комп'ютерних наук
Кунанець Наталія Едуардівна
Тернопільський національний технічний університет імені Івана Пулюя.

Захист відбудеться 24 грудня 2019 р. о 09:00 годині на засіданні екзаменаційної комісії №____ у Тернопільському національному технічному університеті імені Івана Пулюя за адресою: 46001, м. Тернопіль, вул. Руська, 56, навчальний корпус №___, ауд. ____

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми роботи. Безпека інформації має велике значення для забезпечення життєво-важливих інтересів будь-якої держави. Створення розвиненого і захищеного середовища є неодмінною умовою розвитку суспільства та держави, в основі якого мають бути найновіші автоматизовані технічні засоби. Однією з потенційних загроз для інформації слід вважати цілеспрямовані або випадкові деструктивні дії персоналу (людський фактор), оскільки вони становлять 75 % усіх випадків.

Для виконання важливих дій, а саме контролю та управління державними чи приватними інформаційними ресурсами, використовується електронний документообіг. Вимогою такого методу управління є безпека та цілісність інформації що циркулює в інформаційній системі. Основним та найголовнішим завданням є забезпечення стійкості та унеможливлення компроментації, модефікації чи спотворення критично важливих даних .

Методика безпечного зберігання даних повинна опиратися комплекс заходів, що спрямовані на унеможливлення розкриття інформації стороннім особам, а також бути здатною реалізувати своє функціонування не

тільки в повсякденних умовах, але і в критичних ситуаціях.

Мета роботи: полягає у впровадженні методики безпечного зберігання інформації на цифрових носіях, як і для державних, так і для приватних організацій.

Об'єкт, методи та джерела дослідження. Об'єктом дослідження є суспільні відносини у сфері захисту цифрових даних. Основним методом дослідження є аналіз програмних і апаратних засобів захисту інформації від витоку каналами зв'язку. Методи, які застосовано у дослідженні: економіко-статистичний, графічний, порівняльний.

Наукова новизна отриманих результатів:

- проаналізовано нормативно-правову базу та сучасні підходи в галузі криптографічного захисту інформації;
- запропоновано підхід щодо впровадження методики безпечного зберігання критичної інформації на цифрових носіях;
- проведений тестовий аналіз ефективності захисних заходів;
- запропоновано шляхи покращення захисту від НСД;

– розроблені рекомендації щодо методів організаційного та інженерного захисту інформації в автоматизованих системах;
– виконано техніко-економічне обґрунтування прийнятих рішень;
– розглянуто питання застосування інформаційних технологій, охорони праці, безпеки в надзвичайних ситуаціях те екології;
– розроблено план захисту інформації.

Практичне значення отриманих результатів.

Запропоновано методику безпечного зберігання інформації за допомогою програми шифрування VeraCrypt. У ході тестування, та опрацьованих матеріалів, використання програми шифрування, що працює відповідно до світових стандартів (ISO/IEC 10118-3:2004, FIPS 197, FIPS 198, FIPS 180-2, FIPS 140-2, NIST SP 800-38E, PKCS #5 v.2.0, PKCS #11 v.2.20), економічно та практично задовольнятиме потреби користувачів.

Апробація. Окремі результати роботи доповідались на VII науково-технічній конференції, Тернопіль, ТНТУ, 11 – 12 грудня 2019 р.

Структура роботи. Робота складається з розрахунково-пояснювальної записки та

презентації. Розрахунково-пояснювальна записка складається з вступу, 8 частин, висновків, переліку посилань та додатків. Обсяг роботи: розрахунково-пояснювальна записка – 102 арк. формату А4, презентація – ___ слайдів.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У вступі проведено аналіз актуальності захисту інформації в автоматизованих системах, оскільки, розвиток держави та суспільства напряму залежить від належного рівня комп'ютеризації та процесу розвитку цифрових технологій. Велику роль відіграє електронний документообіг і одним із важливих аспектів сучасного інформаційного простору є спеціальні цифрові носії інформації, що широко використовуються в наш час.

В першій частині проведено аналіз стану питання за літературними та іншими джерелами, обґрунтовано актуальність роботи, виконано постановку задачі на дипломну роботу, виконано огляд основних понять та визначень відповідно до нормативно-правової бази, розглянуто ознаки та типи ідентифікації особи, принцип роботи флеш-носіїв.

В другій частині проведено аналіз, загроз безпеки інформації на цифрових носіях інформації, розглянуто види смарт-карт та USB-токенів.

В третій частині виконано аналіз методів захисту інформації на цифрових носіях інформації, розглянуто загрози безпеки флеш-накопичувачів, охоплено алгоритми шифрування та їх значення у криптографічному захисті інформації. Наведено приклад використання ЦНІ «Лоза - 1».

В четвертій частині розроблено методику безпечного зберігання інформації, сформовано структурну та функціональну схеми методики, розроблено організаційно-правові заходи щодо зменшення кількості вразливостей і зниження ступеня шкоди від загроз, запропоновано правила, які повинні дотримуватись позаштатні адміністратори. Охоплено заходи захисту інформації при роботі з даною методикою. Запропоновані рекомендації щодо тестування продукту шифрування даних, позаштатними адміністраторами служби захисту інформації, також вимоги щодо проведення державної експертизи у галузі криптографічного захисту інформації, для отримання експертного висновку щодо використання (застосування) об’єкта за призначенням. Розроблено заходи у разі втрати чи пошкодження носія інформації. Також опрацьовано та оглянуто принцип шифрування програми VeraCrypt.

В п’ятій частині розглянуто переваги та недоліки програм шифрування: BitLocker та

VeraCrypt. Показано принцип роботи програмиVeraCrypt.

В шостій частині «Обґрунтування економічної ефективності» наводиться розрахунок сумарних витрат щодо впровадження методики безпечного зберігання інформації на цифрових носіях.

В сьомій частині «Охорона праці та безпека в надзвичайних ситуаціях» розглянуто фактори робочого середовища при використанні ЕОМ, що роблять вплив на здоров'я і працездатність людини в процесі праці, також дії в надзвичайних ситуаціях.

В восьмій частині «Екологія» проаналізовано питання статистичного групування в екології та методологію моделювання екологічних проблем.

У загальних висновках щодо дипломної роботи сформульовані загальні висновки щодо розробленої методики захисту інформації на флеш-носіях.

ВИСНОВКИ

Метою захисту інформації має бути збереження цінності критичної інформації, яка є власністю держави або інформації з обмеженим доступом. Виходячи з цього, безпосередні заходи захисту спрямовують не так на самі інформаційні

ресурси, як на збереження даних користувача та надання можливості створення, обробки та надійності зберігання. Ця методика має враховувати особливості інформації, що робить її цінною, а також давати змогу користувачам різних категорій ефективно та безпечно працювати з інформацією.

За результатами роботи можна зробити висновки про ефективність розробленої системи за такими критеріями:

- сумарний річний збиток, розрахований методом еквівалентної шкоди, на порядок перевищує номінальну вартість запропонованої методики і її обслуговування в однорічному періоді;
- величина сумарного річного збитку неприйнятна, тим самим введення в експлуатацію методики є невідкладним заходом щодо забезпечення стабільності діяльності підприємства чи організації.

За результатом роботи, з урахуванням висновків про ефективність методики, можна рекомендувати VeraCrypt на впровадження та проходження державної експертизи.

СПИСОК ОПУБЛІКОВАНИХ АВТОРОМ ПРАЦЬ ЗА ТЕМОЮ РОБОТИ

1. Купчак Ю.А. Методика безпечного зберігання інформації на цифрових носіях [Текст] / Купчак Ю.А. Тези доповіді на VII науково-технічній конференції. – Тернопіль, ТНТУ, 2019. – с. 85.

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.