МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ

НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ
КАФЕДРА СИСТЕМ ІНФОРМАЦІЙНОГО ТА КІБЕРНЕТИЧНОГО ЗАХИСТУ

«На правах рукопису»
УДК 681.3.06

«До захисту допущено»
Завідуючий кафедрою СІКЗ
_____к.т.н. Г.В. Шуклін
«____» _____2023 р.

БАКАЛАВРСЬКА АТЕСТАЦІЙНА РОБОТА

зі спеціальності 125 “Кібербезпека”

на тему: **КОМПЛЕКСНЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ РЕАЛІЗАЦІЇ ВІДДАЛЕНОГО ДОСТУПУ ДО ФАЙЛОВОГО СХОВИЩА**

Студент групи СЗД-41 Пилипенко Павло Павлович _____
(підпис)

Науковий керівник: к.т.н., доц Котенко Андрій Миколайович __ _____
(підпис)

Нормоконтроль ст. викл. Зозуля Сергій Анатолійович _____
(підпис)

КИЇВ – 2023

«ЗАТВЕРДЖУЮ»
Завідувач кафедри СІКЗ
_____ к.т.н. Г.В. Шуклін
(підпис)
«_____»_____ 2023р.

ЗАВДАННЯ

на атестаційну роботу бакалавра

студенту: Пилипенко Павлу Павловичу

1.Тема роботи: Комплексне забезпечення інформаційної безпеки при реалізації віддаленого доступу до файлового сховища, затверджено наказом від «24» лютого 2023р. № 26

2.Термін здачі студентом оформленої роботи «____» _____ 2023р.

3. Об'єкт дослідження: процеси захисту файлового сховища.

4. Предметом дослідження: технології захисту, які забезпечують безпеку інформації в файловому сховищі.

5. Мета роботи: удосконалення та рекомендації щодо застосування методів захисту інформації в файловому сховищі.

6.Перелік питань, які мають бути розроблені:

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз реалізованих технологій захисту файлового сховища;
- аналіз та дослідження існуючих методів захисту файлового сховища;
- створення рекомендацій щодо застосування методів захисту інформації в файловому сховищі.

7. Перелік публікацій

8. Перелік ілюстрованого матеріалу

Презентація матеріалу на слайдах.

9. Дата видачі завдання «____» _____20____р.

Науковий керівник _____ Котенко А.М.
(підпис)

Завдання прийняв до виконання _____ Пилипенко П.П.
(підпис)

КАЛЕНДАРНИЙ ПЛАН

Дата видачі завдання «24» лютого 2023р.

№ з/п	Назва етапів дипломної роботи	Строк виконання етапів роботи	Примітка
1	Підбір науково-технічної літератури	до 26.02.23р.	
2	Обґрунтування актуальності теми роботи	до 27.02.23р.	
3	Написання першого розділу роботи	до 16.03.23р.	
4	Написання другого розділу роботи	до 12.04.23р.	
5	Написання третього розділу роботи	до 08.05.23р.	
6	Написання висновків по роботі	до 11.05.23р.	
8	Підготовка демонстраційних матеріалів	до 18.05.23р.	
9	Підготовка доповіді	до 24.05.23р.	
10	Захист в ДЕК		

Студент: СЗД -41 Пилипенко П.П. _____
(підпис)

Науковий керівник: к.т.н., доц. Котенко А.М. _____
(підпис)

Нормоконтроль: ст. викл. Зозуля С.А. _____
(підпис)

ЗМІСТ

РЕФЕРАТ 5
ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ 7
ВСТУП 8
РОЗДІЛ 1 АРХІТЕКТУРА ФАЙЛОВОГО СХОВИЩА 9
1.1. Ізольоване файлове сховище ..... **Ошибка! Закладка не определена.**
1.2. Секції даних та сховище 15
1.3. Квоти для ізольованого файлового сховища. 15
1.4. Допустиме використання та загрози несанкціонованого доступу .. **Ошибка! Закладка не определена.**
Висновки до розділу 1……
Розділ 2 Засоби захисту інформації в файловому сховищі від несанкціонованого вторгнення ..... **Ошибка! Закладка не определена.**
2.1. SIEM-системи 22
2.2. Засоби антивірусного захисту та міжмережевого екранування 26
2.3. Засоби криптографічного захисту……
Висновки до розділу 2……
РОЗДІЛ 3 Рекомендації щодо практичного застосування систем захисту файлового сховища 57
3.1. Застосування засобів контролю безпеки відповідно до п'ятифазного життєвого циклу ..... **Ошибка! Закладка не определена.**
ВИСНОВОК 57
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ТА ДЖЕРЕЛ 60

РЕФЕРАТ

Дипломна робота містить 61 сторінок, 15 рисунки, 6 таблиць.

Неструктурована інформація уявляє собою одним з головних інформативних активів підприємств різних форм власності. Такою інформативною складовою є електронні документи та файли, які розміщенні в спеціальних файлових сховищах. Такими є паперові документи,. Які належать офісам, файли формату *PDF*, копії різних конфіденційних документів, аудіо та відео інформація. Інакше кажучи довільна інформація, яка не розміщена всередині систем керування базами даних (СКБД), вважається класом неструктурованих даних. Отже для забезпечення захисту такої інформації необхідно створювати спеціальні файлові сховище доступ до якого є обмеженим.

Об'єктом дослідження: процеси захисту файлового сховища.

Предметом дослідження є технології захисту, які забезпечують безпеку інформації в файловому сховищі.

Мета роботи удосконалення та рекомендації щодо застосування методів захисту інформації в файловому сховищі.

Для досягнення вказаної мети виконуються такі основні задачі:

- аналіз реалізованих технологій захисту файлового сховища;
- аналіз та дослідження існуючих методів захисту файлового сховища;
- створення рекомендацій щодо застосування методів захисту інформації в файловому сховищі.

ABSTRACT

Thesis contains 61 pages, 15 figures, 6 tables

Unstructured information is one of the main informative assets of enterprises of various forms of ownership. Such informative components include electronic documents and files stored in special file storages. These are paper documents. Office files, copies of various confidential documents, audio and video information. In other words, arbitrary information that is not stored inside database management systems (DBMS) is considered a class of unstructured data. Therefore, to ensure the protection of such information, it is necessary to create special file storages with limited access.

Object of research: file storage security processes.

The subject of the research is security technologies that ensure the safety of information in the file storage.

The purpose of the work is improvements and recommendations for the use of information security methods in file storage.

To achieve this goal, the following main tasks are performed:

- analysis of implemented file storage security technologies;
- analysis and research of existing file storage security methods;
- creating recommendations for the use of information security methods in file storage.

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ВРС	Віддалене різницеве стиснення	Remote differential compression
РРФС	Реплікація розподіленої файлової системи	Replication of a distributed file system
ВФ	Відновлення файлу	File recovery
САД	Служба активного директорію	Active Directory Service
ССФС	Служба синхронізації файлів системи	System file synchronization service
СКБД	Система керування базами даних	Database management system
РПЗ	Розширена постійна загроза	Advanced Persistent threat
ЛПЗ	Легітимне програмне забезпечення	Legitimate software
ШЛПЗ	Шкідливе легітимне програмне забезпечення	Malicious Legitimate software
SRAM	Статична оперативна пам’ять з довільним доступом	Static random access memory
TDMA	Метод часового поділу	Time division multiple access
WLAN	Метод часового поділу	Wireless Local Area Network
ВЧ	Високі частоти	
ЗЗІ	Засоби захисту інформації	
ІС	Інформаційна система	
ІТС	Інформаційно-телекомунікаційна система	
ОЗП	Оперативний запам’ятовувальний пристрій	
УВЧ	Ультра високі частоти	

ВСТУП

Захист інформації, яка зберігається у відповідних файлових сховищах об`єкту інформаційної діяльності є головною проблемою для довільної компанії. Тому завдання захисту інформації від несанкціонованого доступу до конфіденційної та таємної інформації завжди є головним пріоритетом в діяльності компанії.

Актуальність теми полягає в тому, що проблема захисту сховищ неструктурованих є одним з гострих питань підприємств довільної форми власності. Для визначення способів захисту такої інформації та постановки технічних завдань для вирішення цих проблем, необхідно в першу чергу розуміти те, що несанкціонований доступ до такої інформації може призвести до величезних збитків. За різними оцінками, середній обсяг неструктурованих даних може досягати 80% загального обсягу всієї електронної інформації, яка зберігається в файловому сховищі. При цьому велика частина неструктурованих даних в багатьох випадках є не корисною. У багатьох файлових сховищах можна знайти дублікати документів, які створюються співробітниками через відсутність контролю копіювання, застарілі файли, до яких не зверталися кілька років, і контент, не пов'язаний з діяльністю компанії, а саме фото, відео, файли.

Об’єктом дослідження: процеси захисту файлового сховища.

Предметом дослідження є технології захисту, які забезпечують безпеку інформації в файловому сховищі.

Мета роботи удосконалення та рекомендації щодо застосування методів захисту інформації в файловому сховищі.

Для досягнення вказаної мети виконуються такі основні задачі: аналіз реалізованих технологій захисту файлового сховища; аналіз та дослідження існуючих методів захисту файлового сховища; створення рекомендацій щодо застосування методів захисту інформації в файловому сховищі.

РОЗДІЛ 1 АРХІТЕКТУРА ФАЙЛОВОГО СХОВИЩА

1.1. Ізольоване файлове сховище

Відкрита розподілена система для спільної роботи з файлами надає середовище, в якому група географічно розподілених користувачів може взаємодіяти для ефективної роботи з файлами, а також забезпечує цілісність цих даних. Стандартна локальна екосистема файлового сервера, яка підтримує велику кількість одночасних користувачів і елементів вмісту, використовує реплікацію розподіленої файлової системи (РРФС) для планування реплікації та регулювання пропускної здатності.

РРФС застосовує алгоритм стиснення, який відомий як віддалене різницеве стиснення (ВРС), за допомогою якого можна ефективно оновлювати файли в мережі з обмеженою пропускною здатністю. Він виявляє операції вставки, видалення і перерозподілу даних у файлах. РРФС може реплікувати тільки змінені блоки файлів під час оновлення файлів. Існують також середовища файлових серверів, де щоденні резервні копії створюються в періоди низького навантаження і використовуються для аварійних потреб. Реалізація РРФС відсутня. На рисунку 1.1 представлено середовище файлового сховища з реалізованим РРФС.

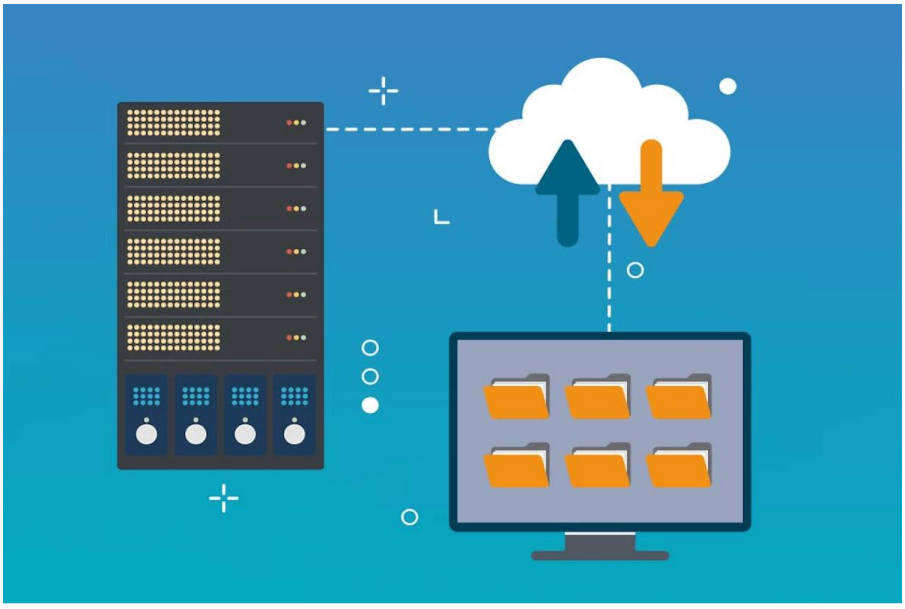


Рисунок 1.1. Середовище файлового сховища

З рисунку 1.1 можна відмітити, що кілька файлових сховищ, які мають назву учасників, здійснюють якісну реалізацію у реплікації файлів в групі реплікації.

Та інформація, яка зберігається в реплікаційній папці доступна усім користувачам, які надсилають запити будь-якому клієнту, навіть при умові, що він перебуває поза мережею.

Файлове сховище можна реплікувати в системі за допомогою відновлення файлу (ВФ). Якщо один або кілька локальних файлових сховищ не є доступною, то в системі можна запустити віртуальні машини відновлення. Вони можуть локально обробляти запити від клієнтів за умови, що є *VPN* -з'єднання " *set – set* " і в системі налаштована служба активного директорію (САД). Цей метод можна використовувати за наявності налаштованого середовища РРФС або простого середовища файлового сховища без РРФС.

У кластеризованому середовищі файлового сховища з реалізованою реплікацією РРФС існує можливість поширити локальну РРФС в системі. Далі віртуальна система спроможна виконувати функції файлового сервера.

При умові, що задана функціональна залежність *VPN* -з'єднання " *set – set* " та САД налаштовані, а реплікацію РРФС реалізовано, то при умові недоступності локальних файлових серверів, користувачі спроможні приєднуватись до віртуальної машинної системи, функції якої обробляти запити.

Даний підхід дає можливість створювати файлове сховище при умові, коли на віртуальних машинах налаштовані конфігурації, які системи ВФ не підтримує.

Як приклад можна розглянути загальний диск кластера, який в багатьох випадках використовується в середовищах файлових сховищ. РРФС має достатню надійність функціонування в середовищах з низькою пропускною спроможністю і середньою швидкістю зміни інформації. З врахуванням додаткової витрати на віртуальну машину системи, яка спроможна працювати протягом неперервного часу.

За допомогою служби синхронізації файлів системи (ССФС) для реплікації файлів. Це пов`язано з тим, що при плануванні використовувати хмару в якості віртуальної машини системи, то вибір ССФС синхронізує повністю керовані загальні папки в хмарі. Доступ до цих папок можна отримати за стандартним галузевим протоколом *SMB*. Файлові ресурси системи в таких умовах дає можливість одночасного підключення до хмарних або локальних розгортань

існуючих операційних систем. На рисунку 1.2 представлено схему, яка допомагає визначити стратегію для використання в середовищі файлового сховища.

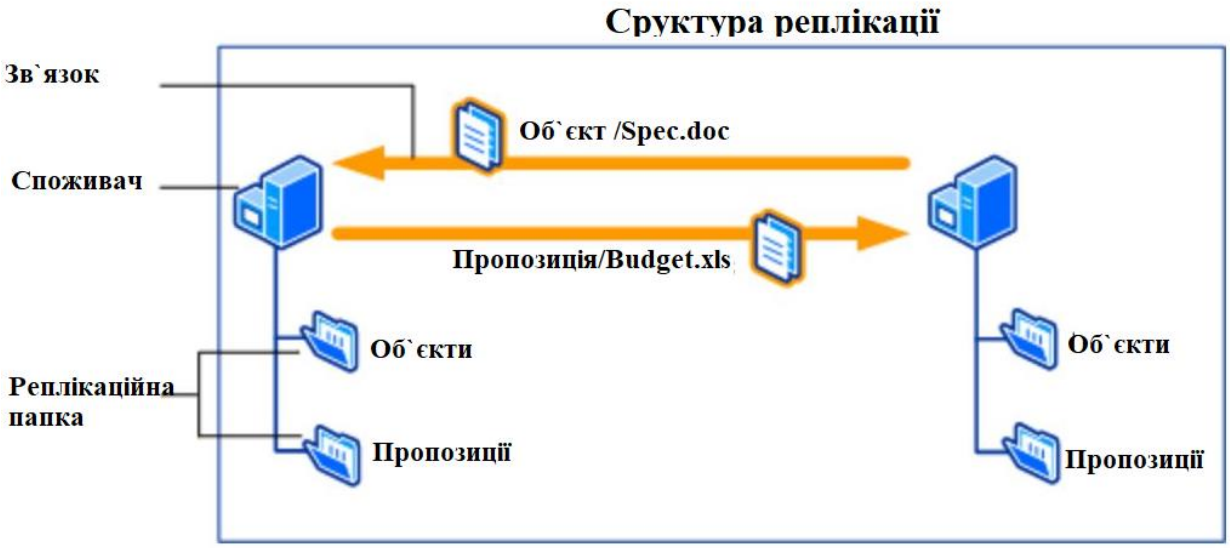


Рисунок 1.2. Структурна схема динаміки забезпечення файлового сховища

В таблиці 1.1 представлено фактори, які впливають на відновлення інформація, яка може бути вилучена в файловому сховищі.

Таблиця 1.1

Середовище	**Заходи забезпечення**	**Необхідні умови забезпечення**
Середовище файлового середовища при застосуванні або за відсутністю РРФС	Застосування ВФ для використання реплікації	ВРС не підтримує кластери загальних дисків та інших пристроїв зберігання інформації, які спроможні приєднуватись до мережі *NAS*. ВФ не підтримує *SMB* 3.0. Віртуальна машина впроваджує зміни виключно при умові

		внесення в файли зміни обновлення в початковому розташуванні файлів. ВФ пропонує здійснювати практичну синхронну реплікацію даних, що в свою чергу призводить при умові незапланованої здійснення відмови призводить до втрати певних даних та зможуть виникнути проблеми невідповідності USN.
Середа файлового сервера з застосуванням РРФС	Розповсюдження РРФС на віртуальну машину *IaaS Azur*	РРФС якісно працює в середовищах, які мають велику стиснуту пропускну спроможність. Для такого підходу необхідно мати віртуальну машину *Azur* , протягом всього часу знаходиться в стані запуску.
Віртуальна машина *IaaS Azur*	Синхронізація файлів *Azur*	У сценарії аварійного відновлення під час використання служби синхронізації файлів протягом часу відпрацювання відмови необхідно виконати дії вручну, щоб

		переконатися, що загальні файлові ресурси доступні на клієнтському комп'ютері у прозорий спосіб. Для служби синхронізації файлів необхідно відкрити порт 445 з клієнтського комп'ютера.

Для підключення "*мережа – мережа*" важливим є встановити пряме з'єднання між локальним сайтом та мережею *Azur*. Це дозволить здійснювати обмін даними між серверами. Використання захищеного під'єднання VPN "*мережа – мережа*" до віртуальної мережі *Azur*, дає можливість здійснювати аварійне відновлення.

РРФС залежить від активного директорію. Це означає, що ліс активного директорію з локальними контролерами домену поширюється на сайт аварійного відновлення в *Azur*. Варто відмітити, що при відсутності спроможності використовувати РРФС, а при цьому передбачуваним користувачам потрібно надати доступ, то виконання цих дій є обов`язковим.

Сервіс файлів *Azur* в багатьох випадках використовують для повної заміни або доповнення традиційних локальних файлових сховищ або пристроїв *NAS*. Загальні ресурси сервісу файлів *Azur* також можна адаптувати за допомогою сервісу синхронізації файлів на локальні або хмарні сервери *Windows Server* для якісного та розподіленого кешування даних у місці їх зберігання. Здійснимо ретельний опис щодо рекомендацій для аварійного відновлення віртуальних машин *Azur*, які в свою чергу спроможні реалізувати можливості, еквівалентні можливостям файлових сховищ.

- Необхідно здійснювати увімкнення захисту комп'ютерів за допомогою *Site* Re cov*ery*.

- Необхідно використовувати службу синхронізації файлів для виявлення файлів із віртуальної машини, що виконує функції файлового сховища, у хмару.

- Необхідно використовувати функцію плану відновлення *Site* Re cov*ery*. Це дає можливість додати *скрипти* для під'єднання спільної папки *Azur* та отримати доступ до цієї папки на віртуальній машині.

Є в першу чергу створення облікового запису зберігання інформації в *Azur*. При відсутності зайвого сховища яке має доступ на читання для облікових записів зберігання, то в разі збою стає доступним виключно на читання власних даних із додаткової області. Наступним кроком є створення файлового ресурсу. Для цього запускають службу синхронізації файлів на файловому сервері *Azur*. Після чого створюють групу синхронізації, тобто фінішні точки в групі синхронізації входять в стан синхронного керування. Група синхронізації повинна містити принаймні одну хмарну фінішну точку, яка уявляє собою загальний файловий ресурс *Azur*. Однак вона ще повинна містити одну серверну фінішну точку, яка уявляє собою маршрут в *Windows Serwer*. В результаті власні файли синхронізуються між спільними файловими ресурсами *Azur* та локальним сховищем. При виникненні аварії в локальному середовищі необхідно виконати відпрацювання відмови, використовуючи план відновлення. Це здійснюється за рахунок додавання *скрипта*, щоб під'єднати спільний файловий ресурс *Azur* та отримати доступ до нього на віртуальній машині. За наявності локальних споживачів, які звертаються до віртуальних машин файлового сервера *IaaS*, необхідно в першу чергу встановіть *VPN*-підключення "*мережа – мережа*" між локальним сайтом та мережею *Azur*. Після цього реалізується розповсюдження локальної служби активного директорію та здійснюється налаштування аварійного відновлення комп'ютера файлового сервера *IaaS* у додаткову область.

Нижче описано інструкцію щодо виконання реплікації віртуальної машини *VMware*. В першу чергу необхідно підготувати ресурси *Azur* для реплікації

локальних комп'ютерів. Після цього встановлюється *VPN*-підключення " *мережа – мережа* між локальним сайтом та мережею *Azur*. Після цього здійснюється розповсюдження локальної служби активних директорій.

За допомогою служби синхронізації файлів *Azur* можна реплікувати файли в хмару. У разі збою і недоступності локального файлового сервера ви можете під'єднати потрібне розташування файлів із хмари і продовжити обробляти запити з клієнтських комп'ютерів.

-

1.2. Секції даних та сховище

Коли додаток зберігає дані у файлі, обирати ім'я файлу та місце його зберігання слід так, щоб мінімізувати вірогідність того, що місце зберігання даних буде доступним для інших додатків, а отже, стане вразливим до пошкодження. За відсутності стандартної системи для розв'язання подібних проблем імпровізоване розроблення засобів мінімізації конфліктів зберігання може стати надмірно складним, а його результати - ненадійними.
В ізольованому сховищі дані завжди ізольовані за користувачем або збіркою. Збірка ідентифікується обліковими даними, такими як джерело або суворе ім'я. Дані також можуть бути ізольовані за доменом програми за допомогою подібних облікових даних.

В ізольованому сховищі застосунок зберігає дані в унікальному осередку даних, прив'язаному до одного з аспектів, що ідентифікують код, наприклад, до видавця або підпису. Клітинка даних - це абстракція, а не певне місце зберігання. Вона складається з одного або декількох файлів для ізольованого зберігання, званих сховищами, які містять дійсні адреси каталогів, у яких зберігаються дані. Наприклад, додаток може мати пов'язану з ним комірку даних, а дійсне зберігання даних для цього додатка може здійснюватися в каталозі файлової системи. Дані, що зберігаються у сховищі, можуть бути будь-якого типу, від інформації про користувацькі налаштування до стану програми. Для розробника розташування комірки даних є прозорим. Сховища зазвичай знаходяться на клієнті, але серверний додаток може використовувати ізольовані

сховища для інформації шляхом уособлення користувача, від імені якого він діє. В ізольованому сховищі інформація також може зберігатися на сервері з профілем користувача, який можна переміщати, що забезпечує її переміщення разом із користувачем.

1.3. Квоти для ізольованого файлового сховища.

Квота уявляє собою обмеження доступного для використання обсягу сховища, для якого необхідно здійснити ізоляцію. Квота враховує байти файлового простору, а також службові дані, пов'язані з каталогом та іншою інформацією у сховищі. Ізольоване сховище використовує квоти дозволу, які являють собою допустимі межі зберігання, що встановлюються за допомогою об'єктів *Isolated Storage Permission*. При спробі записати дані в перевищення квоти виникає виняток *Isolated Storage Permission*. Політика безпеки, яку можна змінити за допомогою *NET* засобу налаштування платформи *Mscorcfg.msc*, виявляє які дозволи надаються коду. Для коду, якому надано дозвіл *Isolated Storage Permission*, визначається сховище, найбільший розмір якого задається властивістю *UserQuota*. Проте, оскільки код може обходити квоти дозволу, використовуючи різні посвідчення користувача, ці квоти більшою мірою мають характер рекомендацій щодо роботи коду, аніж виступають у ролі суворих обмежень.

До сховищ, які спроможні переміщуватись квоти не застосовуються. Враховуючи це, для їхнього використання код повинен мати у своєму розпорядженні дозволи дещо вищого рівня. Значення перетворень *Assembly Isolation By Roa*min*g User* та *Domain Isolation By Roa*min*g User* визначають дозвіл на використання сховища, яке підлягає ізоляції для профілю користувача, що переміщується.

Використання ізольованого зберігання дає змогу частково довіреним додаткам зберігати дані під контролем політики безпеки комп'ютера. Це

особливо зручно під час роботи з компонентами, які завантажуються і які не викликають у співробітника повної довіри. Політика безпеки не завжди надає такому коду право доступу до файлової системи з використанням стандартних механізмів *введення – виведення*. Однак за замовчуванням код, що запускається з локального комп'ютера, з локальної або глобальної мережі отримує право на використання ізольованого сховища.

Адміністратори можуть обмежувати розміри ізольованого сховища, доступного застосунку або користувачеві, залежно від відповідного рівня довіри. Крім того, адміністратори можуть видалити всі дані, що зберігаються. Щоб створити ізольоване сховище або отримати доступ до нього, коду необхідно надати відповідний дозвіл *Isolated Storage File Permission*.

Для доступу до ізольованого сховища коду мають бути призначені всі необхідні права операційної системи власної платформи. Повинні бути виконані вимоги списків управління доступом, які визначають, які користувачі мають права на користування файловою системою *NET* Додатки вже мають права операційної системи на доступ до ізольованого сховища, якщо вони не виконують уособлення. У такому разі відповідальність за забезпечення наявності в уособлюваному для користувача прав, необхідних для доступу до ізольованого сховища, несе додаток. Такий доступ дає змогу коду, що запускається або завантажується через *Internet*, виконувати читання і запис в області зберігання, що належить конкретному користувачеві.

Для управління доступом до ізольованого сховища середовище *CLR* використовує об'єкти *Isolated Storage File Permission*.

Кожен об'єкт має властивості, які визначають такі значення:
- дозволене використання, яке вказує тип дозволеного доступу. Значення є членами перерахування *Isolated Storage Containment*.

Середовище виконання вимагає дозволу *Isolated Storage File Permission* під час першої спроби відкрити сховище. Рішення про надання цього дозволу

визначається з урахуванням надійності коду. Якщо дозвіл видається, значення квоти використання і сховища визначаються політикою безпеки і запитом коду на отримання дозволу *Isolated Storage File Permission*. Політика безпеки задається за допомогою *NET* засобу налаштування платформи *Mscorcfg.msc*. Перед тим, те програмне забезпечення, яке має бути викликано, у стеку викликів перевіряються на наявність щонайменше одного відповідного дозволу на використання. Середовище виконання також перевіряє наявність квоти у коду, який відкрив або створив сховище, у яке записується файл. Якщо всі ці умови виконані, то видається дозвіл. Квота перевіряється щоразу під час запису файлу в сховище.

Коду програми не потрібно запитувати дозвіл, оскільки середовище *CRL* надасть відповідний дозвіл *Isolated Storage File Permission*, виходячи з політики безпеки. Однак важливим є здійснювати запит на певні дозволи для свого додатка, включно з *Isolated Storage File Permission*.

1.4. Допустиме використання та загрози несанкціонованого доступу

Дозволене використання, задане за допомогою *Isolated Storage File Permission*, визначає ступінь, у якій коду дозволено створювати та використовувати ізольоване сховище. У такій таблиці наведено відповідність між дозволеним використанням і типами ізоляції, а також коротко описано ризики безпеки, пов'язані з кожним із видів дозволеного використання. В таблиці 1.2 представлено загальна характеристика параметрів, які забезпечують загрози від несанкціонованого доступу.

Таблиця 1.2

Допустиме використання	**Типи ізоляції**	**Ризики несанкціонованого доступу**
None	Відсутній дозвіл на ізольоване сховище	Несанкціонований доступ відсутній
DomainIsolationByUser	Ізоляція за користувачами, доменами та збірками. Кожна збірка має окреме вкладене сховище всередині домену. Сховища, що використовують цей дозвіл, також здійснюється неявне ізолювання комп'ютером.	Цей рівень дозволу залишає можливість несанкціонованого надмірного використання ресурсів, хоча застосування квот робить це складним. Цей процес називається атакою типу " *відмова від обслуговування* ".
*DomainIsolationByRoa*min *gUser*	Аналогічно *DomainIsolationByUser* , крім того, що сховище зберігається в переміщуване розташування, якщо застосовуються переміщувані профілі користувачів і не задіються квоти.	Оскільки квоти доводиться відключати, то ресурси зберігання більш уразливі до атаки типу " *відмова від обслуговування* ".

AssemblyIsolationByUser	Ізоляція за користувачами та збірками. Сховища, що використовують цей дозвіл, також здійснюється неявна ізоляція комп'ютером.	На цьому рівні застосовуються квоти для запобігання атак типу " *відмова від обслуговування* ". Та сама збірка в іншому домені може мати доступ до сховища, що може призвести до витоку інформації між додатками
AssemblyIsolationByRoa min *gUser*	Аналогічно *AssemblyIsolationByUser* , відмінність в тому, що сховище зберігається в переміщуване розташування, якщо застосовуються переміщувані профілі користувачів і не застосовуються квоти.	Аналогічно *AssemblyIsolationByUser* , за відсутністю квот; ризик несанкціонованого доступу типу " *відмова від обслуговування* " зростає.
Ad min *isterIsolatedStorageByUser*	Ізоляція за користувачами. Зазвичай цей рівень дозволу використовують тільки засоби	Доступ із цим рівнем дозволу дає змогу коду переглядати або видаляти будь-які файли та каталоги ізольованого сховища

	адміністрування або налагодження.	користувача (незалежно від ізоляції збірки). Ризики, крім іншого, включають витік інформації та втрату даних.
UnrestrictedIsolatedStorage	Ізоляція за всіма користувачами, доменами та збірками. Зазвичай цей рівень дозволу використовують тільки засоби адміністрування або налагодження	Цей дозвіл може призвести до втрати захищеної інформації всіх ізольованих сховищ для всіх користувачів.

NET Платформа та *NET* ядро пропонують ізольоване сховище як механізм збереження даних для користувача, додатка або компонента. Це застарілий компонент, який спочатку розроблявся для сценаріїв управління доступом для коду, які зараз оголошені нерекомендованими. Для зчитування даних через межі довіри можна використовувати різні засоби та інтерфейси *API* ізольованого сховища. Як приклад можна привести зчитування даних з області на рівні комп'ютера може здійснювати агрегацію інформації з інших, можливо, менш довірених облікових записів користувачів на робочих місцях. Компоненти або додатки, які зчитують дані з областей ізольованого сховища на рівні робочого місця, повинні бути обізнані про наслідки такого зчитування.

Висновок до розділу 1

API або засіб *storeadm.exe/machine/list* є компонентами, які передбачають роботу з надійними даними. Якщо зловмисник може помістити шкідливі дані в сховище на рівні комп'ютера, їх можна використовувати для атаки з

підвищенням привілеїв у контексті того користувача, який виконує ці команди. Під час роботи в багатокористувацькому середовищі рекомендується розглянути можливість використання функцій ізольованого сховища, призначених для області робочого місця. Якщо додаток має зчитувати дані з розташування на рівні комп'ютера, рекомендується зчитувати дані з такого розташування, яке доступне для запису тільки обліковим записам адміністратора. Каталог *%PROGRGRAMFILES%* і кущ реєстру *HKLM* є прикладами розташувань, які доступні для запису тільки адміністраторам, а для читання дозволено всім співробітникам. Тому дані, зчитані з цих розташувань, вважаються надійними. Якщо додаток має використовувати область робочого місця у багатокористувацькому середовищі, перевіряйте вміст будь-якого файлу, що зчитується зі сховища на рівні робочого місця. Якщо додаток не спроможний реалізувати графи об'єктів із таких файлів, рекомендується використовувати безпечніші засоби, такі як *XmlSerializer*, замість небезпечних, таких як *BinaryFormatter* або *NetDataContractSeridizer*.

РОЗДІЛ 2 ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В ФАЙЛОВОМУ СХОВИЩІ ВІД НЕСАНКЦІОНОВАНОГО ВТОРГНЕНЯ

2.1. Siem- системи

SIEM управління інформацією та подіями безпеки *SIEM* пропонує моніторинг та аналіз подій у режимі реального часу, а також відстеження та реєстрацію даних про безпеку для цілей дотримання нормативних вимог або аудиту.

Простіше кажучи, *SIEM* уявляє собою рішення для забезпечення безпеки, яке допомагає організаціям розпізнавати потенційні загрози безпеці та вразливості до того, як вони встигнуть порушити бізнес-операції. Воно виявляє аномалії в поведінці користувачів і використовує штучний інтелект для автоматизації багатьох ручних процесів, пов'язаних з виявленням загроз і реагуванням на інциденти, і стало основним інструментом в сучасних

операційних центрах безпеки (СОЦБ) для управління безпекою і дотриманням нормативних вимог.

Протягом достатнього часу *SIEM* стала чимось більшим, ніж інструменти управління журналами, які їй передували. На теперішній час *SIEM* пропонує розширену аналітику поведінки користувачів і організацій завдяки можливостям штучного інтелекту і машинного навчання. Це високоефективна система оркестрування даних для управління загрозами, що постійно змінюються, а також дотримання нормативних вимог і звітності.

На найпростішому рівні всі рішення *SIEM* виконують певні функції агрегації, консолідації та сортування даних з метою виявлення загроз і дотримання вимог щодо відповідності даних. Хоча деякі рішення відрізняються за можливостями, більшість з них пропонують однаковий базовий набір функцій:

1. Функція керування журналами

SIEM система збирає дані про події з широкого кола джерел по всій мережі організації. Журнали і потокові дані від користувачів, додатків, активів, хмарних середовищ і мереж збираються, зберігаються і аналізуються в режимі реального часу, надаючи спеціалістам інформаційних технологій і службам безпеки можливість автоматично керувати журналом подій і даними мережевого потоку в одному централізованому місці.

Деякі рішення *SIEM* систем також інтегруються зі сторонніми каналами розвідки загроз, щоб співвідносити свої внутрішні дані про безпеку з раніше розпізнаними сигнатурами і профілями загроз. Інтеграція з каналами загроз в режимі реального часу дозволяє командам блокувати або виявляти нові типи сигнатур несанкціонованого доступу до файлових сховищ.

2. Функція кореляції та аналітики подій

Кореляція подій є невід'ємною частиною будь-якого рішення *SIEM* системи. Використовуючи розширену аналітику для виявлення і розуміння складних шаблонів даних, кореляція подій дає можливість швидко знаходити і зменшувати потенційні загрози для безпеки бізнесу. Рішення *SIEM* систем

значно покращують середній час виявлення та математичне сподівання часу реагування для команд *IT*-безпеки, розвантажуючи ручні робочі процеси, пов'язані з поглибленим аналізом подій, пов`язаних з несанкціонованим доступом до файлового сховища.

3. Функція моніторингу інцидентів та оповіщення про загрози

Завдяки централізованому управлінню локальною та хмарною інфраструктурою, рішення *SIEM* систем здатні ідентифікувати всі об'єкти середовища інформаційних технологій. Це дозволяє технології *SIEM* відстежувати інциденти безпеки для всіх підключених користувачів, пристроїв і додатків, класифікуючи аномальну поведінку в міру її виявлення в мережі. Використовуючи адаптовані, заздалегідь визначені правила кореляції, адміністратори можуть негайно отримати сповіщення і вжити відповідних заходів для його усунення до того, як воно матеріалізується в більш серйозні проблеми безпеки.

4. Функція управління вимогам стандартам та звітності

Рішення *SIEM* систем є популярним вибором для організацій, що підлягають різним формам нормативно-правового регулювання. Завдяки автоматизованому збору та аналізу даних, *SIEM* системи є цінним інструментом для збору та перевірки даних про дотримання нормативних вимог у всій бізнес-інфраструктурі. Рішення *SIEM* систем можуть генерувати звіти про відповідність вимогам *PCI – DSS* , *GDPR* , *HIPPA* , *SOX* та інших стандартів у режимі реального часу, зменшуючи навантаження на управління безпекою та виявляючи потенційні порушення на ранніх стадіях, щоб їх можна було усунути. Багато рішень *SIEM* систем постачаються з попередньо вбудованими, готовими до використання надбудовами, які можуть генерувати автоматизовані звіти, розроблені відповідно до вимог нормативно-правових актів.

Незалежно на те, наскільки великою чи малою є організація, активні кроки для моніторингу та зменшення ризиків в несанкціонованому доступі до файлового сховища є вкрай важливими. Рішення *SIEM* системи приносять

користь підприємствам різними способами і стали важливим компонентом в оптимізації робочих процесів безпеки. Ось деякі з цих переваг:

- ***розширене розпізнавання загроз у режимі реального часу***. Рішення *SIEM* систем для активного моніторингу всієї інфраструктури значно скорочують час, необхідний для виявлення потенційних мережевих загроз та завад, а також реагування на них, допомагаючи зміцнити систему безпеки в міру масштабування організації.
- ***аудит відповідності нормативним вимогам***. Рішення *SIEM* систем забезпечують централізований аудит відповідності та звітність по всій бізнес-інфраструктурі. Розширена автоматизація спрощує збір та аналіз системних журналів і подій безпеки, щоб зменшити використання внутрішніх ресурсів, одночасно відповідаючи суворим стандартам звітності про відповідність.

- ***автоматизація на основі штучного інтелекту*** Сучасні рішення *SIEM* нового покоління інтегруються з потужними можливостями оркестрування, автоматизації та реагування на загрози, що заощаджує час і ресурси команд розробки інформаційних технологій, які керують інформаційним захистом бізнесу. Використовуючи глибоке машинне навчання, яке автоматично адаптується до поведінки мережі, ці рішення можуть обробляти складні протоколи ідентифікації загроз та реагування на інциденти за значно менший час, ніж фізичні команди.
- ***Підвищення організаційної ефективності***. За рахунок покращеній видимості середовищ інформаційних технологій, яку вона забезпечує, *SIEM* може стати важливим фактором підвищення ефективності роботи між відділами. Завдяки єдиному уніфікованому представленню системних даних та інтегрованому різних заходів, команди можуть ефективно спілкуватися та співпрацювати під час реагування на події та інциденти безпеки. Щоб дізнатися більше про переваги управління інформацією та подіями безпеки, а також про те, чи підходить це рішення для власного бізнесу, ознайомтеся з додатковими ресурсами *SIEM* від експертів компанії IBM з питань захисту інформації в файловому сховищі.

Також, дані системи спроможні виявляти сучасні та невідомих загрози з огляду на те, як швидко змінюється ландшафт інформаційного захисту, організаціям необхідно мати можливість покладатися на рішення, здатні виявляти і реагувати як на відомі, так і на невідомі загрози з захисту інформації в файловому сховищі. Використовуючи інтегровані канали розвідки загроз і технологію штучного інтелекту, рішення *SIEM* систем можуть успішно протистояти сучасним загрозам безпеки, таким як:

- **Інсайдерські загрози** уявляють собою вразливості системи захисту або несанкціонованого втручання, що походять від осіб, які мають санкціонований доступ до мереж і цифрових активів компанії. Ці атаки можуть бути наслідком компрометації облікових даних.
- **Фішингові атаки** уявляють собою атаки соціальної інженерії під виглядом довірених осіб, які часто використовуються для крадіжки даних користувачів, облікових даних для входу в систему, фінансової інформації або іншої конфіденційної бізнес-інформації.
- *SQL*-**ін'єкції** уявляють собою шкідливий код, що виконується через скомпрометовану веб-сторінку або додаток, призначений для обходу заходів безпеки та додавання, модифікації або видалення записів у базі даних *SQL*.
- *DDoS*-**атаки** уявляють собою розподілені атака на відмову в обслуговуванні (*DDoS*-атака), призначена для бомбардування мереж і систем некерованим трафіком, що знижує продуктивність веб-сайтів і серверів до неможливості їх використання.
- **Витіснення даних** - крадіжка або витіснення даних зазвичай досягається шляхом використання поширених або легко зламаних паролів на мережевих ресурсах або за допомогою розширеної постійної загрози (РПЗ).

2.2. Засоби антивірусного захисту та міжмережевого екранування

Легітимне програмне забезпечення (ЛПЗ) уявляє собою програмне забезпечення, що розробляється та розповсюджується легально і може використовуватися в повсякденній роботі для виконання певних завдань. Прикладами таких програм є програми з функціоналом фінансового контролю, віддаленого адміністрування, спеціальні програми, функціями яких є захист інформації від несанкціонованого витоку конфіденційної та таємної інформації.

ЛПЗ, яке використовується для несанкціонованого доступу до конфіденційної інформації, яка зберігається в файловому сховищі, носить назву шкідливим легітимним програмним забезпеченням (ШЛПЗ).

Розробники шкідливого програмного забезпечення, яке має легітимні засоби мають в першу чергу визначити мету, яку переслідує зловмисник, та завдання, як шлях досягнення поставлених цілей.

Метою розробки ШЛПЗ є стеження за користувачем інформаційної системи та отримання згодом права доступу до інформаційних ресурсів, за допомогою яких буде існувати можливість отримати доступ до необхідних даних. Протягом довгострокового стеження за користувачем можна отримати наступну конфіденційну інформацію, а саме його персональні дані, коди доступу на різних сайтах, періоди часу перебування користувача в різних місцях та коди доступу до файлового сховища. Також файлове сховище може містити акаунти в соціальних мережах, які в майбутньому можуть бути досліджені для отримання більш точної інформації щодо користувача або отримати матеріальну винагороду від третіх осіб, які зацікавлені в інформації щодо користувача.

Під персональними даними користувача будемо розуміти довільну інформацію, що стосується прямо чи опосередковано визначеної або визначуваної користувача. Персональними даними користувача є:

- прізвище ім`я по батькові та адреса мешкання користувача;

- відомості про дохід фізичної особи, паспортні дані, індивідуальний податковий номер;

- інформація про расову та національну належність, приватне життя, стан здоров'я тощо.

Персональні дані можуть бути представлені й іншим видом. Цієї інформації абсолютно достатньо для того, щоб скласти повну картину про життя людини для подальшого інформаційного впливу на неї.

Завдання ШЛПЗ створюється за рахунок мети, тобто потреб, яким має задовольняти програма, а саме:

- доступ до файлового сховища користувача має здійснюватися в будь-який час за бажанням зловмисника;

- можливість отримувати інформацію у віддаленому доступі, так і управління ним;
- збереження всіх текстів, що набираються на клавіатурі з метою подальшого вилучення паролів із них;

- можливість запису екрана або постійного знімка екрана з інтервалами (для випадків, коли у зловмисника немає можливості контролювати користувача при наявності потреби на це;

- усі дії ШЛПЗ мають бути невидимі для звичайного користувача.

План розробки ШЛПЗ на прикладі того, що необхідно здійснити заходи щодо захисту від шкідливого легітимного програмного забезпечення, необхідно проаналізувати процес розробки відповідного шкідливого програмного забезпечення, а також заходи зловмисника на конкретному прикладі. Виходячи з мети та завдань, які були задіяні до шкідливого програмного забезпечення, реалізується відповідний план дій. План реалізації містить усі етапи створення підсумкового шкідливого комплексу, який згодом готовий до впровадження. Структурну схему такого плану представлено на рисунку 2.1.

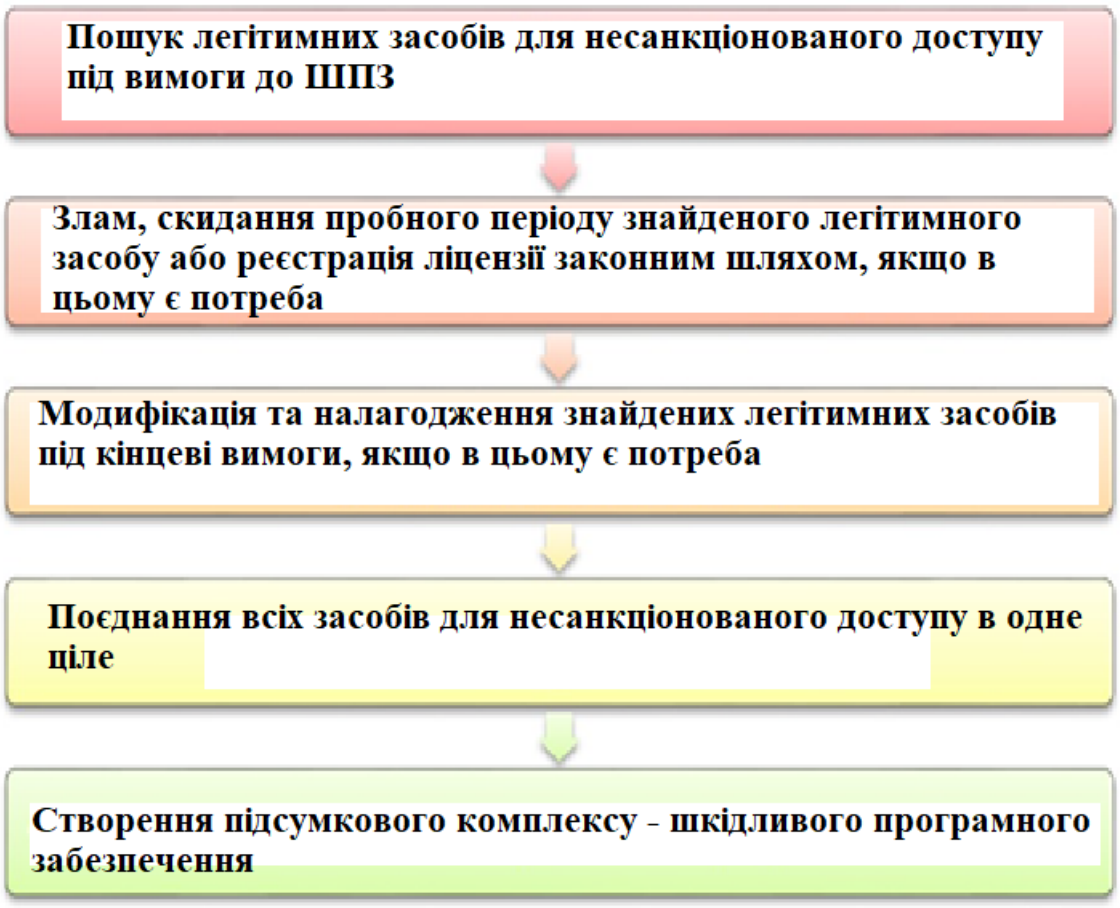


Рисунок 2.1. Структурна схема підсумкового комплексу ШПЗ

Перший етап - пошук легітимних засобів для несанкціонованого доступу до конфіденційної інформації під вимоги до шкідливого програмного забезпечення включає вивчення наявних програм на ринку програмного забезпечення, які повністю або частково задовольняють завданням майбутнього шкідливого програмного забезпечення. При виборі відповідних програм необхідно визначити тестовий період або вимагають здійснити покупку, то зловмиснику вдається здійснити злом, або скидання пробного періоду. Наразі, коли це зробити не вдається, то відбувається реєстрація ліцензії законним шляхом.

Найчастіше відбувається те, що знайдені засоби не повністю задовольняють завданням шкідливого програмного забезпечення та меті зловмисника. У таких випадках наявне програмне забезпечення модифікують і налаштовують, якщо є така можливість.

Після того, як усі складові майбутнього шкідливого програмного забезпечення підготовлені, то з`являється потреба об'єднати їх в один файл.

Спроба запуску одного файлу більша, за спробу запуску декількох файлів. Реалізація підсумкового комплексу ШЛПЗ здійснюється найчастіше разом із етапами, що їм передують. На поточному етапі здійснюється пропис правил запуску створеного файлу, мітка підсумкового файлу, а також заходи після запуску.

Протягом пошуку легітимних засобів для несанкціонованого доступу до файлового сховища, зловмисник завжди враховує те, що антивірусне програмне забезпечення миттєво відреагує на нього. Навіть на стандартне програмне забезпечення в антивірусному ПЗ може бути хибне реагування. В таких випадках відбувається уточнення щодо реакції антивірусних засобів на файл, який зловмисник використовує для досягнення своєї мети.

VirusTotal (*virustotal.com*) уявляє собою безкоштовну службу, яка здійснює аналіз невідомих файлів та посилань (*URL*) щодо виявлення *вірусів*, *хробаків*, *троянів* та іншого шкідливого програмного забезпечення.

Результати перевірок файлів сервісом не залежать від певного творця програмного забезпечення, яке унеможлює успішну реалізацію мети зловмисника. *VirusTotal* (*virustotal.com*) має банк кількох десятків антивірусного забезпечення, що дає змогу здійснювати якісні висновки щодо небезпеки файлу порівняно з певним продуктом, виявляти хибні спрацьовування певного антивірусного програмного забезпечення, або, навпаки, неспрацьовування на поточну загрозу, можливо, вже внесену іншими виробниками у свій банк.

Виходячи із завдань, зловмиснику необхідно знайти легітимний продукт для віддаленого керування доступом до файлового сховища. Крім того, він повинен складатися в довірчих списків, для подальшої реалізації антивірусних програм, які працювали би без збоїв. Варто зазначити, що програма для віддаленого доступу за своєю природою не є шкідливою, тому зловмисники беруть практично будь-яку подібну програму, яка задовольняє їх умовам.

Таким програмним забезпеченням, яке здійснює віддалене керування автоматизованою системою, є *RMS* (Re*mote Manipulator Sestem*).

(Re*mote Manipulator Sestem*) уявляє собою продукт для керування віддаленим робочим столом, що надає простий і безпечний доступ до автоматизованої системи в будь-якій точці земної кулі. *RMS* складається з двох основних модулів:

- модуль керування "*Клієнт*";

- віддалений модуль "*Хост*".

Модуль "*Клієнт*" призначений для під'єднання до віддалених робочих станцій, на яких встановлено "*Хост*". *Клієнт* надає зручний інтерфейс для керування списком з'єднань, побудови карти мережі, пошуку віддалених робочих станцій та керування ними в різних режимах.

Модуль "*Хост*" необхідно встановлювати на кожній віддаленій робочій станції, до якої необхідно постійно мати доступ. Цей модуль дає змогу віддалено керувати автоматизованою системою, на якій його встановлено. Можливе віддалене встановлення модулів *Клієнт* , також уявляє собою систему конфігурації дистрибутиву *Хост*.

Кожний легітимний засіб необхідно постійно перевіряти за допомогою *Virus Total* (*virustotal.com*), щоб упевнитися, що антивірусні програми не мають помилкового спрацьовування на підібране програмне забезпечення. Звіт сервісу *Virus Total* (*virustotal.com*) останньої версії *RMS* модуля "*Клієнт*" представлено на рисунку 2.2.

SHA256	92528e91923c5e3bf066d96916545fdec44c536919da282eb41b4c5ebb23c1fe
Ім`я файлу	rms.viewer6.5.ru.msi
Користувач виявлення	4 / 54
Дата аналізу	2017-01-02 02:14:26 UTC (0 минут назад)

Аналіз | Відомості про файл | Походження | Додаткові відомості | Коментар

Антивірус	Результат
AVware	Trojan.Win32.Generic!BT
AegisLab	Remoteadmin.W32.Agent!c
Antiy-AVL	RiskWare[RemoteAdmin]/Win32.Agent
Kaspersky	not-a-virus:HEUR:RemoteAdmin.Win32.Agent.gen
ALYac	

Рисунок 2.2. Звіт аналізу роботи *RMS* модуль "*Клієнт*"

Звіт сервісу *Virus Total* (*virustotal.com*) останньої версії *RMS* модуля "*Хост*" представлено на рисунку 2.3.

SHA 256	41a1196466c093d756808152f019218138d45b3f7dc4c3c197f80f3ef86f8362
Ім`я файлу	rms.host6.5.ru.msi
Показник виявлення	2 / 53
Дата аналізу	2017-01-02 02:14:35 UTC (1 минута назад)

Аналіз | Відомості про файл | Походження | Додаткові відомості | Коментар

Антивирус	Результат
AVware	Trojan.Win32.Generic!BT
Antiy-AVL	RiskWare[RemoteAdmin]/Win32.RMS.nd
ALYac	

Рисунок 2.3. Звіт аналізу роботи *RMS* модуль "*Хост*"

З наведених малюнків можна зробити висновок, що програмне забезпечення задовольняє поставленим завданням, оскільки з 86 антивірусного програмного забезпечення лише 3 показали, що програмне забезпечення є підозрілим. У модуля "*Клієнт*" є спрацьовування від антивірусного програмного забезпечення "*Kaspersky*". Оскільки впроваджуватися користувачу буде винятково модуль "*Хост*", то результати сканування модуля "*Клієнт*" не відіграють особливої ролі, оскільки він буде встановлений на автоматизованій системі зловмисника.

Отримуючи позитивні результати попередніми завданнями підсумкового шкідливого програмного забезпечення, важливим є знайти програму для запису тексту з клавіатури. Таким програмним забезпеченням, що виконує зазначену функцію, є *Punto Switcher*.

Punto Switcher уявляє собою програмне забезпечення для автоматичного перемикання між різними розкладками клавіатури та є безкоштовною для некомерційного використання. Основне призначення даного програмного забезпечення є збільшення продуктивності та зручності під час роботи з автоматизованою системою, яка працює у фоновому режимі.

Серед стандартних можливостей даного програмного забезпечення таких як зміна розкладки, заміна поєднання клавіш для перемикання мови, виправлення друкарських помилок, перетворення чисел на текст та інше, є функція ведення щоденника, тобто збереження всіх текстів, які набираються на клавіатурі. У зв'язку з цим зловмисники використовують старі версії цього програмного забезпечення, де такі обмеження відсутні.

Звіт перевірки на сервісі *Virus Total* (*virustotal.com*) представлено на рисунку 2.4.

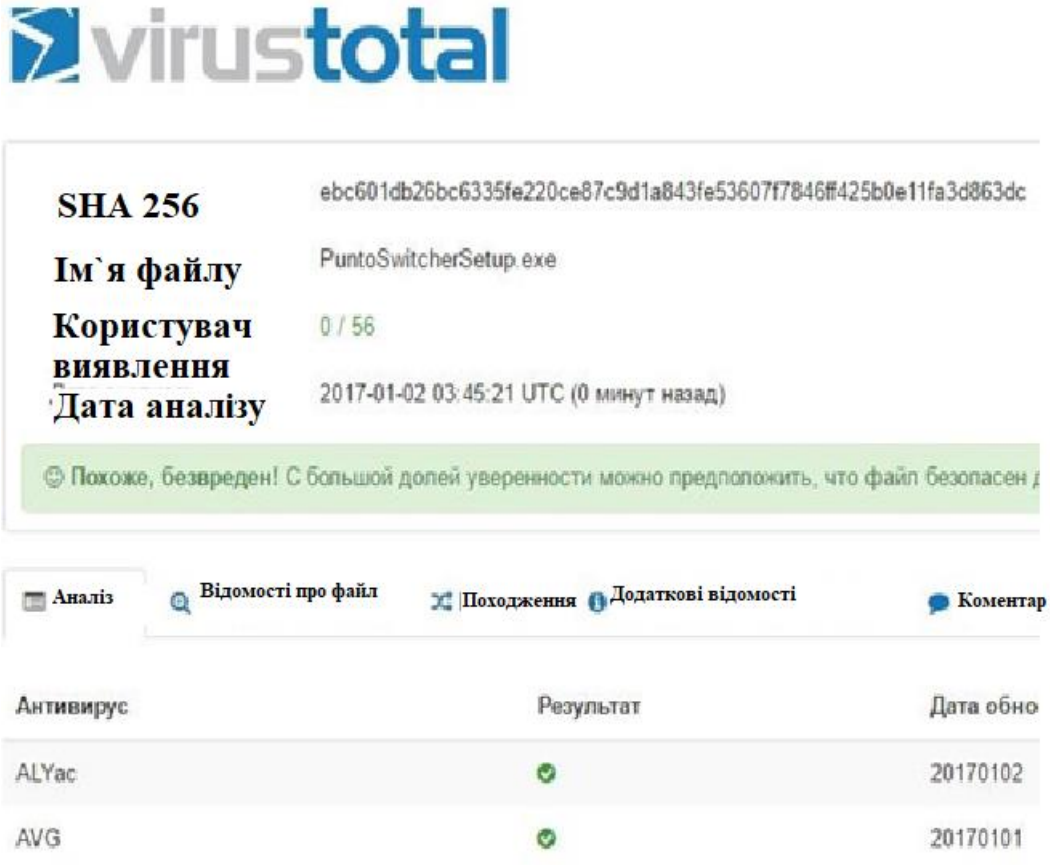


Рисунок 2.4. Звіт аналізу дистрибутиву *Punto Switcher*

З рисунку 2.4 можна зробити висновок, що програмне забезпечення задовольняє поставленим завданням, оскільки з 78 антивірусних програм жодна не показала, що програмне забезпечення є підозрілим.

Для впровадження шкідливого програмного забезпечення в файлове сховище користувача необхідно здійснити зосередження в одному виконуваному файлі. Отже, в цьому випадку здійснюється підвищення спроможності запуску програмного забезпечення з невідомого джерела.

Для того, щоб ця вимога була реалізованою, зловмисники використовують *джойнери*. *Джойнери* (*joiner*) уявляє собою програмне забезпечення, яке дає змогу "*склеювати*" шкідливе програмне забезпечення з будь-яким файлом у кінцевий формат "*.exe*" . Отже, певна кількість легітимних засобів можна з'єднати в одне ціле.

Найпростішим *джойнером* є довільне програмне забезпечення, яке створює

архів даних. Таке програмне забезпечення спроможне створювати архіви, які самі розпаковуються та мають розширення "*.exe*".

Підсумковий такий архів представлено на рисунку 2.5.

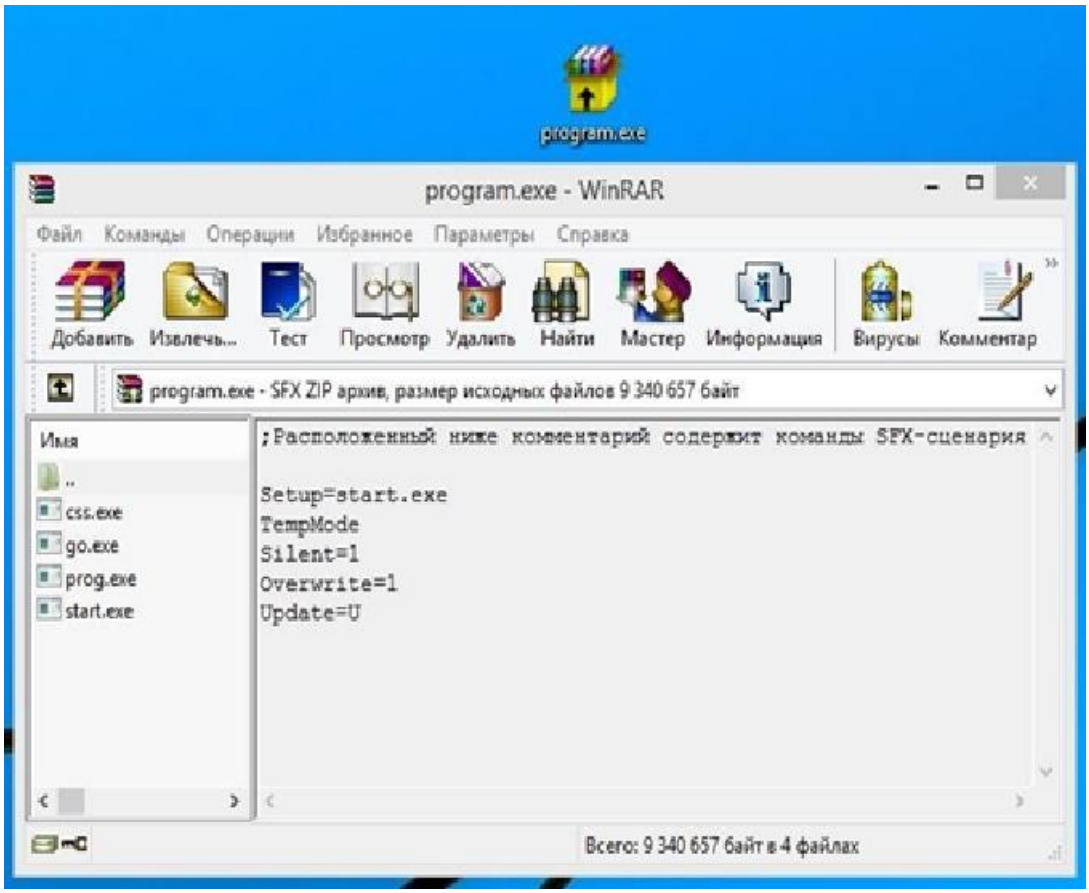


Рисунок 2.5. Демонстрація підсумкового архіву

де:

- "*css.exe*" - програма *Punto Switcher*;

- "*go.exe*" - програма (Re*mote Manipulator Sestem*);

- "*prog.exe*" - програма, під яку маскується шкідливе програмне забезпечення;

- "*star.exe*" - файл запуску ланцюжка зазначених програм.

На базі проведених досліджень запропоновано методику захисту інформації, яка зберігається в файловому сховищі, від ШЛПЗ, яке має намір несанкціонованого доступу до конфіденційної інформації. Дана методика має дві складові заходів: організаційні заходи та технічні заходи.

За своїм змістом організаційні заходи уявляють собою основну діяльність щодо забезпечення фізичного захисту яким є доступ до об`єкту інформаційної діяльності, розробці організаційно-розпорядницькій документації та проведенню заходів по навчанню співробітників.

Технічні заходи включають в себе недопущення витоку та визначення можливості отримати несанкціонований доступ за допомогою програмних та апаратних засобів.

Загальний перелік заходів, які пропонуються в даній методиці представлено на рисунку 2.6.

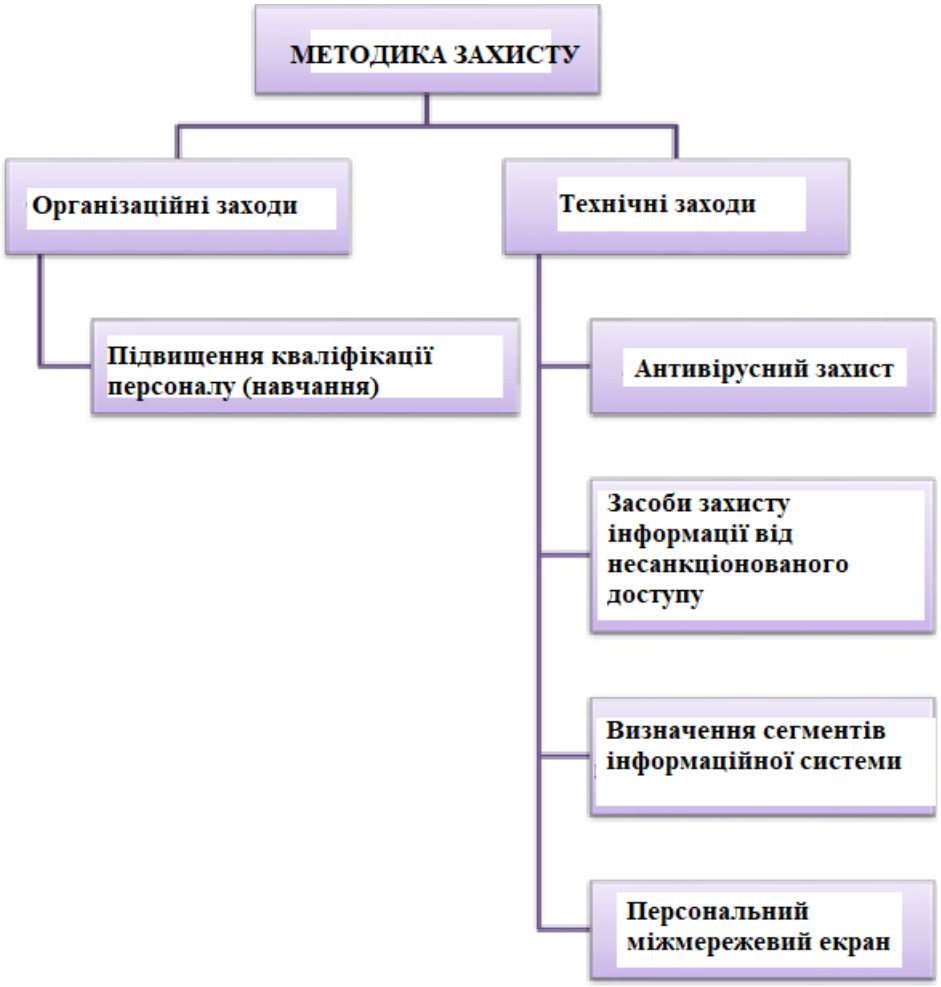


Рисунок 2.6. Класифікація засобів захисту файлового сховища від ШЛПЗ

Під організаційними заходами розуміється підвищення обізнаності персоналу організації в галузі захисту інформації. Отже, такі заходи дають можливість знизити ризик виникнення навмисних або ненавмисних дій користувачів, результатом яких може бути відмова в обслуговуванні частини

інформаційної системи, витік важливої конфіденційної та таємної інформації або порушення доступу до ресурсів.

Підвищення обізнаності персоналу в галузі захисту інформації потребує розроблення такої документації:

- програма підвищення обізнаності та плану її реалізації;
- політика навчання та підвищення обізнаності персоналу в галузі захисту інформації;
- методика оцінювання рівня обізнаності персоналу в галузі захисту інформації.

Навчання та підвищення обізнаності персоналу в галузі захисту інформації можна проводити в різних формах:

- очне навчання;
- дистанційне навчання у вигляді електронних курсів та вебінарів;
-самостійне вивчення виданих курсів.

Варто зазначити, що самостійне навчання за допомогою виданих на руки співробітникам матеріалів є самим ефективним, оскільки саме такий підхід дає належний результат. Для регулярного навчання і підвищення обізнаності працівників очне навчання також невигідне, оскільки відрив співробітників від основної діяльності негативно впливає на робочий процес підприємства. Тому важливо поставитися до складання плану з навчання з належною увагою. Ефективною є дистанційна форма навчання за електронними курсами або онлайн-конференціями з можливістю його проміжного і підсумкового контролю та оцінки.

Самим вигідним та ефективним є комплексний підхід до навчання та підвищення обізнаності персоналу в галузі захисту інформації. У такому разі можливо паралельно проводити заняття відразу на декількох рівнях, комбінуючи різні форми:

- очне навчання за допомогою інструктажу із забезпечення інформаційної безпеки;
- інформаційні розсилки персоналу з висвітленням актуальних питань інформаційної безпеки, важливих для співробітників змін у законодавстві;
- консультації з питань інформаційної безпеки у формі вільної бесіди на нарадах.

Оцінка рівня обізнаності персоналу необхідна не тільки для аналізу отриманих співробітниками знань і умінь, а й для оформлення звітності про засвоєння співробітниками матеріалу. Також складається лист ознайомлення з матеріалами, виданими під час інструктажу.

У пропонованій методиці технічні заходи захисту від шкідливого легітимного програмного забезпечення являють собою такі програмні та технічні рішення:

- антивірусний захист;
- засоби захисту інформації від несанкціонованого доступу до інформації;
- розбиття інформаційної системи на сегменти;
- персональний між мережевий екран.

Не всі представлені заходи здатні повністю вирішити проблеми захисту файлового сховища від ШЛПЗ. Це можливо тільки в разі сукупного їх використання.

Програма антивірусного захисту уявляє собою програмне забезпечення, націлене на забезпечення інформаційної безпеки корпоративної мережі від шкідливого програмного забезпечення.

На теперішній час присутні два головних підходи виявлення шкідливого програмного забезпечення:

- сигнатурні підходи уявляють собою способи виявлення, які базуються на порівнянні файлу з відомими зразками, що містяться в базі сигнатур, тобто в базі даних відомого шкідливого програмного забезпечення;

- евристичні підходи уявляють собою способи виявлення, які базуються на припущенні, що сканований файл може бути вже пошкоджений шкідливим програмним забезпеченням.

Аналізуючи проблему ШЛПЗ, можна зробити висновок, що захист за допомогою антивірусного програмного забезпечення не спроможний виявляти програмне забезпечення такого типу. Однак на практиці виявлено, що антивірусне програмне забезпечення спроможно скласти конкуренцію.

Дія ШЛПЗ є цілком законною, тому евристичні методи з великою часткою ймовірності не дадуть тих результатів, які очікують. Підходи евристичного сканування не забезпечують низький ризик захисту від нових, відсутніх у базі сигнатур шкідливого програмного забезпечення. При цьому надмірна чутливість і підозрілість евристичного аналізатору може викликати велику кількість помилкових спрацьовувань.

Варто відмітити, що на теперішній час існує велика кількість простих способів ввести в оману евристичний аналізатор. Як правило, перш ніж поширювати ШЛПЗ, його розробники досліджують наявне розповсюджене антивірусне програмне забезпечення, обходячи її детектування на шкідливому файлі протягом процесу евристичного сканування.

У разі, коли ШЛПЗ поширюється протягом тривалого часу, не змінюючи вмісту файлу, то сигнатурні методи виявлення шкідливого програмного забезпечення при цьому дадуть позитивний результат, оскільки багато розробників антивірусного програмного забезпечення за приватними запитами вносять інформацію про програму у свої бази сигнатур, які працюють за принципом "*чорного*" списку. Однією з головних властивостей сигнатурного аналізу є точна ідентифікація типу вірусного програмного забезпечення.

Отже, програмне забезпечення, функція якого є антивірусний захист, частково спроможне вирішити проблему, яка виникає завдяки ШЛПЗ.

Встановлення антивірусного програмного забезпечення уявляє собою один із перших і найважливіших заходів у боротьбі зі шкідливим програмним забезпеченням. У цьому випадку теж не можна виключати його корисність, але у випадку з ЛШПЗ антивірусне програмне забезпечення починає старт його детектування не в момент виявлення, що є достатньо величезною загрозою для інформаційної системи.

Засоби захисту інформації від несанкціонованого доступу, які можуть бути представлені у вигляді програмного забезпечення, технічного або програмно-технічного забезпечення, призначені для запобігання або суттєвого ускладнення несанкціонованого доступу до конфіденційної та таємної інформації.

Найпоширенішим програмним забезпеченням є:

- системи *Secret Net*;

- системи *Dallas Lock*.

Основними захисними функціями, які реалізуються різними програмними засобами при інформаційному захисті від несанкціонованого доступу є:

- контроль доступу користувачів в систему;

- розмежування доступу користувачів до пристроїв в файловому сховищі;

- розмежування доступу користувачів до конфіденційної та таємної інформації;

- створення для користувачів замкнутого програмного середовища;

- контроль потоків конфіденційної інформації;

- контроль виведення конфіденційної та таємної інформації на друк;

- контроль цілісності ресурсів, що захищаються;

- контроль апаратної конфігурації системи;

- без інверсне знищення вмісту файлів при їх видаленні;

- реєстрація подій безпеки;

- збір і зберігання журналів.

Системи захисту інформації від несанкціонованого доступу дають змогу заборонити запуск програмного забезпечення, яке адміністратор визнав як *чорний* список. Такий функціонал спроможний захистити інформаційну систему від несанкціонованих прав за допомогою прикладного або системного програмного забезпечення або запуск небажаного програмного забезпечення, які можна знайти в публічному доступі.

Засоби захисту інформації від несанкціонованого доступу дають змогу створити замкнене програмне середовище, яке уявляє собою режим, у якому користувач може запускати тільки ті програми, які внесені адміністратором до *білого* списку систем захисту інформації . Цей функціонал дає змогу захиститися від практично будь-якого шкідливого програмного забезпечення, яке входить до складу легітимного.

Досвід показав, що такий підхід можливий виключно на державних підприємствах, в яких процес робочого часу суворо регламентований. У комерційних організаціях це виглядає інакше. Отже такий захід захисту від ШЛПЗ може порушити робочий процес або визначити очевидні незручності в процесі функціонування. Таким чином, створення *білого* списку програмного забезпечення для того, щоб надалі співробітники не відчували дискомфорт у роботі є однією з важливих завдань систем захисту інформації.

Для коректного налаштування замкнутого програмного середовища необхідно виконати певну кількість кроків.

Крок 1. Здійснюється вхід в систему від імені користувача, права якого в майбутньому будуть обмежені;

Крок 2. Здійснюється встановлення на робоче місце співробітника пакет прикладного програмного забезпечення яке необхідне виключно для робочого процесу і виконання посадових обов'язків персонального робочого місця;

Крок 3. Здійснюється заміна користувача, а також проводиться вхід в систему під обліковим записом адміністратора безпеки. При цьому відбувається запуск оболонки адміністратора.

Крок 4. для групи "*ZPS – gr*" у глобальних налаштуваннях заборонити запуск усіх програм ;

Крок 4. У дескрипторі "*Параметри за замовченням*" увімкнути повний аудит відмов;

Крок 5. Здійснити налаштування неактивного режиму роботи програмного забезпечення. Крім того здійснити процес очистки журналу ресурсів;

Крок 6. Здійснити перезавантаження обчислювальної системи та здійснити вхід в операційну систему під обліковим записом користувача. Після цього запустити все те програмне забезпечення, до якого у користувача є санкціонований доступ;

Крок 7. Здійснити заміну користувача та увійти під обліковим записом адміністратора безпеки. Запустити оболонку адміністратора та відкрити журнал ресурсів;

Крок 8. За допомогою фільтру, знайти всі ресурси з результатом "*помилка*". Кожному з них у властивості "*права для файлів*" призначити дискреційні права "*тільки читання*";

Крок 9. Здійснити процес вимикання "*м`який режим*" та за необхідності вимкнути раніше виставлений "*аудит доступу*".

Варто відмітити, що не для всіх додатків є притаманне простий їх запуск. Деякі складні додатки під час свого запуску завантажують не всі модулі, які спроможні бути виконані, а тільки ті, які необхідні в поточний момент часу, а решту модулів вони довантажують в процесі динамічних змін, протягом виробничого циклу. Отже після запуску програми необхідно виконати всі основні дії програмного забезпечення для подальшої роботи.

Досвід показує, що існує ймовірність того, що коли не всі необхідні для роботи користувача виконувані файли заносяться в список. Оскільки деякі програми викликають будь-які інші виконувані файли тільки під час активізації певних функцій. Якщо після увімкнення замкненого програмного середовища у користувача якийсь застосунок став працювати неправильно, то цей результат можна миттєво виявити в журналі доступу до ресурсів. У такому разі, для додаткових виконуваних файлів необхідно додати аналогічне право на виконання "*тільки читання*".

Після створення замкнутого програмного середовища повністю виключається випадкове впровадження шкідливого програмного забезпечення від імені користувачів, які мають обмежений доступ. Отже, користувач може запускати тільки те програмне забезпечення, яке дозволено адміністратором безпеки.

Розбиття інформаційної системи на кластери уявляє собою процес нейтралізації загрози ШЛПЗ, що передбачає поділ загальної мережі підприємства на два кластери:

- кластер, що має доступ до внутрішньої мережі підприємства та не має доступу до мережі *Inthernet*;

- кластер, що має доступ до мережі *Inthernet* та не має доступу до внутрішньої мережі підприємства.

За рахунок проведеної кластеризації інформаційної системи можна отримати повністю захищену внутрішню мережу організації та за потреби доступ до мережі "*Inthernet*" для розв'язання завдань протягом виробничого циклу.

Кластеризацію можливо здійснювати не одним способом:

Спосіб 1. Проводиться встановлення двох комп'ютерів співробітникам, яким необхідно працювати як у внутрішній мережі організації, так і в *Inthernet*;

Спосіб 2. Проводиться створення "*абонентського пункту*" який уявляє собою окреме приміщення з комп'ютерами для взаємодії з мережею *Inthernet*;

Спосіб 3. Здійснюється встановлення сервера на базі *Windows* з доступом в *Inthernet* та надання доступу за Re*mote Desktop* Pr*otocol* з комп'ютерів користувачів.

Незалежно від способів кластеризації варто застосовувати технології апаратного між мережевого екранування, що дасть можливість ефективно розмежувати частини мережі. Кожен спосіб цієї методики має свої переваги та недоліки.

Протягом встановлення двох комп'ютерів користувачам, яким необхідно працювати як у внутрішній мережі організації, так і в *Inthernet*, є низка особливостей:

- два комп'ютери на одному робочому місці істотно займають місце;
- немає необхідності відлучатися з робочого місця для доступу в мережу *Inthernet*
- для багатьох підприємств таке рішення має високу вартість для реалізації.

Для такого способу схему мережі під час кластеризації представлено на рисунку 2.7. На даному рисунку *автоматизоване робоче місце* уявляє собою програмно-технічний комплекс для автоматизації виробничого процесу.

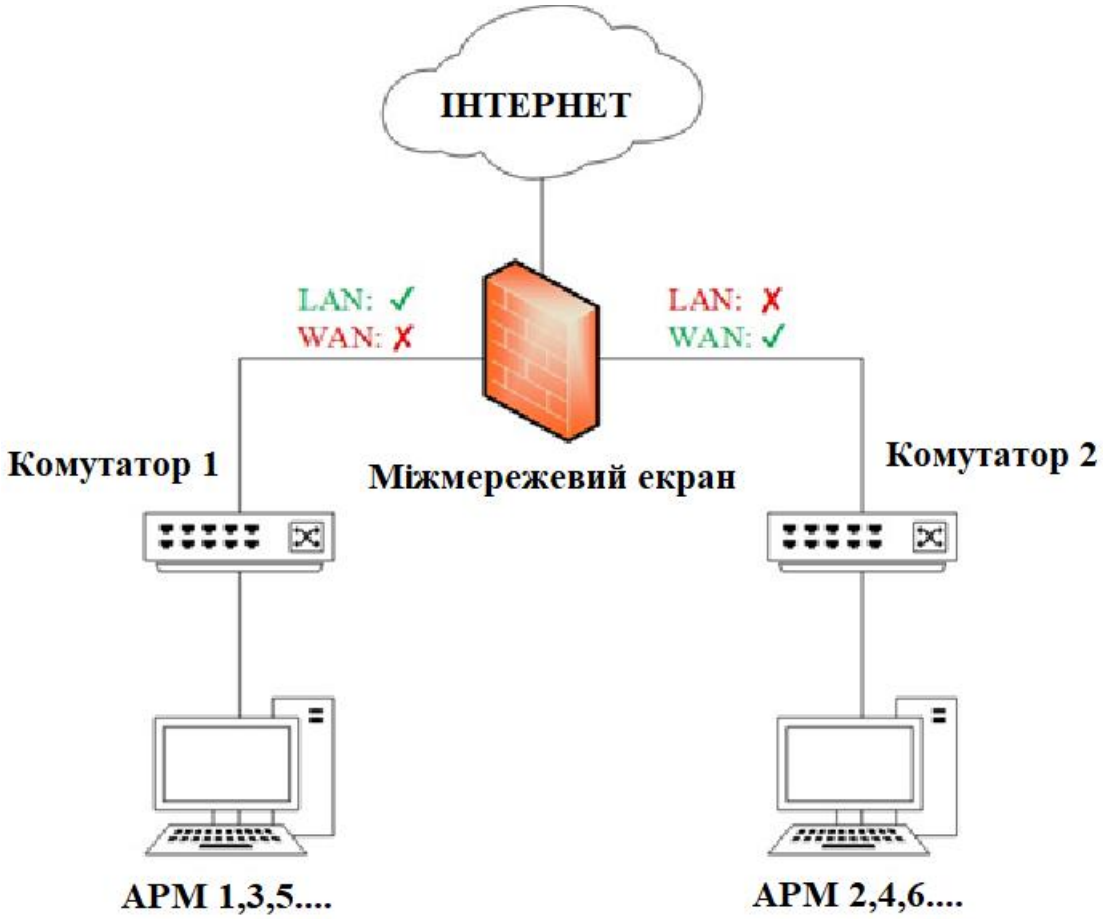


Рисунок 2.7. Схема мережі при розбитті інформаційної системи на сегменти

WAN - це доступ у глобальну мережу "*Inthernet*", а *LAN* - доступ до локальної мережі організації, тобто іншим робочим станціям, які знаходяться на підприємстві. Комутатори призначені виключно для з'єднання декількох кінцевих точок комп'ютерної мережі в межах одного кластеру мережі. Між мережеве екранування дає спроможність розділити загальну мережу на два кластери за допомогою програмних налаштувань у ньому.

Крім того, між мережевий екран, представлений на рисунку 2.7 виконує основні функції маршрутизатора, що не потребує його наявності.

У рамках цього способу на обидва комп'ютери, якщо необхідно, встановлюють системи захисту інформації від несанкціонованого доступу з метою заборонити підключення мобільних носіїв, оскільки вони є носіями

інформації, яку можна перенести з одного комп'ютера на інший та встановити шкідливе програмне забезпечення на цьому комп'ютері, що обробляє конфіденційну та таємну інформацію. Заборону мобільних носіїв можливо здійснити і штатними засобами *Windows*, але таке рішення не дає достовірності в захисті, а також немає можливості проконтролювати цю заборону, переглянувши *журнал безпеки*.

При створенні "*абонентського пункту*", яке уявляє собою окреме приміщення з робочими місцями для взаємодії з мережею *Internet* для яких притаманні властиві особливості:

- необхідне наявність окремого приміщення;

- користувачі повинні відлучитися зі власного робочого місця для доступу в мережу "*Internet*";

- з фінансової точки зору це рішення має меншу вартість, ніж кластеризація мережі за допомогою встановлення двох робочих місць для користувачів. Схему мережі за такого способу кластеризації представлено на рисунку 2.8.

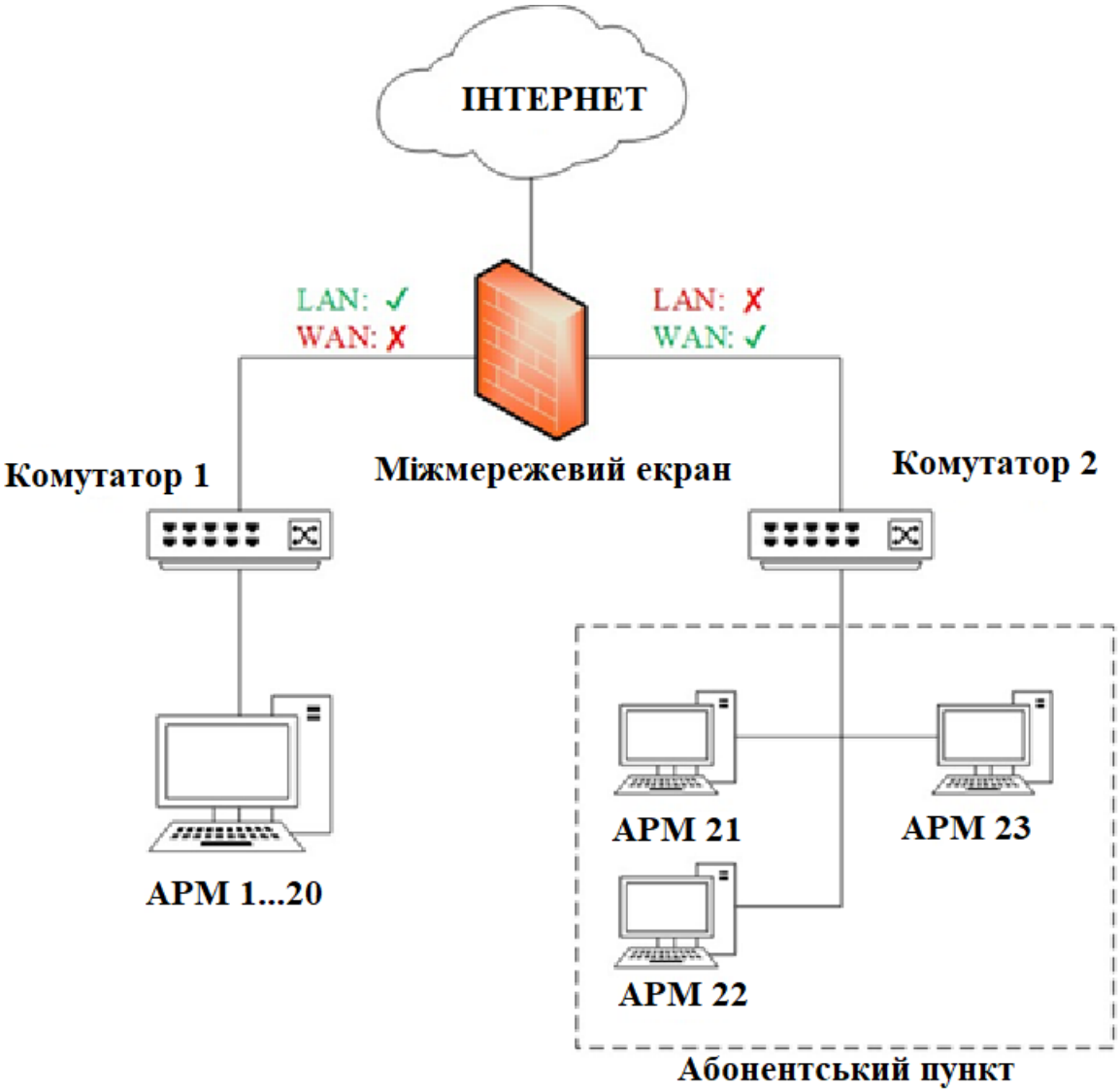


Рисунок 2.8. Схема мережі при кластеризації

У рамках цього способу на всі робочі місця ставиться системи захисту інформації від несанкціонованого доступу з метою заборонити підключення мобільних носіїв, як і в попередньому методі. Аналогічним способом може бути встановлення робочих місць на базі операційної системи *Linux*, щоб надалі використовувати місце як термінал, де будуть доступні користувачам виключно необхідне програмне забезпечення, що в свою чергу призводить до менших витрат.

При встановленні сервера на базі *Windows* з доступом в інтернет і надання доступу по *RDP* з робочих місць користувачів присутні власні особливості, які визначають доцільність даного методу:

- відсутня необхідності в наявності окремого приміщення або займати комп`ютер користувача;

- у користувачів відсутні необхідності залишати свій комп`ютер;
- з фінансової точки зору це рішення може виявитися як найменшими витратами з усіх представлених, так і великими витратами, ніж створення "*абонентського пункту*".

RDP уявляє собою протокол, який використовується для віддаленого підключення співробітника до сервера.

Схему мережі даного способу кластеризації представлено на рисунку 2.9.

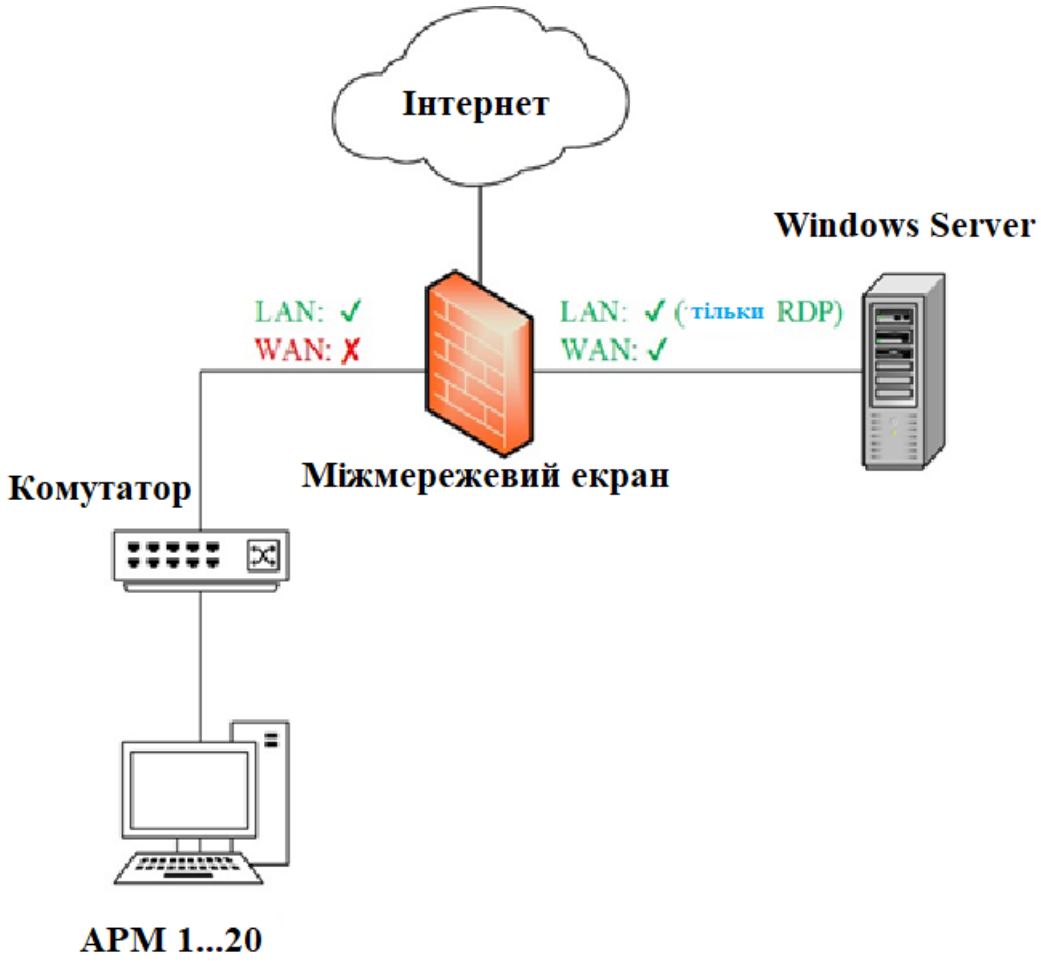


Рисунок 2.9. Схема мережі кластеризації

У межах такого способу відсутні необхідності ставити на сервер системи захисту інформації від несанкціонованого доступу. При необхідності встановлюється на сервери для контролю входів та моніторингу доступу до ресурсів.

Варіація цього методу дає змогу зробити його одним із найдешевших у реалізації.

Також необхідно в налаштуваннях *RDP* з'єднання заборонити використання спільного буферу обміну, щоб унеможливити копіювання файлу з сервера на робоче місце користувача, який обробляє конфіденційну та таємну інформацію.

Отже, самим раціональним способом кластеризації інформаційної системи є встановлення сервера на базі *Windows* із доступом до інтернету та надання доступу до сервера через *RDP* з робочих місць користувачів.

Цей метод є водночас вимагає найменших витрат та вимагає найменшого навантаження як для системного адміністратора, який здійснює проектування системи інформаційного захисту, так і для співробітників організації за рахунок економії часу на переміщення до "*абонентського пункту*".

Особистий між мережевий екран уявляє собою програмне забезпечення інформаційного захисту, який встановлено на робочому місці співробітника і який призначено для фільтрації мережевого трафіку, що проходить, винятково для цього робочого місця.

На теперішній час розробники відомих засобів інформаційного захисту від несанкціонованого доступу включають функціонал між мережевого екранування. Так, між мережевий екран уявляє собою додатковий модуль системи інформаційного захисту *Dallas Lock*, а також входить до складу *Secret Net Studio*.

З огляду на те, що для нейтралізації інших загроз в організації в багатьох випадках необхідно встановлювати системи захисту інформації від несанкціонованого доступу, то цей спосіб захисту від ШЛПЗ вимагає достатніх витрат.

Метод захисту за допомогою власного між мережевого екрану дає змогу здійснювати роботи між мережевого екранування за принципом "*білого*" листа , інакше кажучи існує можливість пропускати винятково ті з'єднання, які дозволені. У рамках "*білого*" листа дозволяються основні ресурси, пов'язані з робочим процесом, і пошукові сервіси.

2.3. Засоби криптографічного захисту

З урахуванням стрімкого розвитку комп'ютерних технологій та інформаційного поля дедалі актуальнішими стають питання, пов'язані з захистом інформації. В цьому випадку розуміються дії, спрямовані на запобігання несанкціонованому та ненавмисному видаленню, викривленню, псуванню, перегляданню та редагуванню, використанню та будь-яким іншим можливим операціям, які здійснюють особи підприємств, компанії, зловмисники, шкідливе програмне забезпечення, які не мають на це прав.

Основні методи та засоби захисту даних наведено на рис. 2.10.

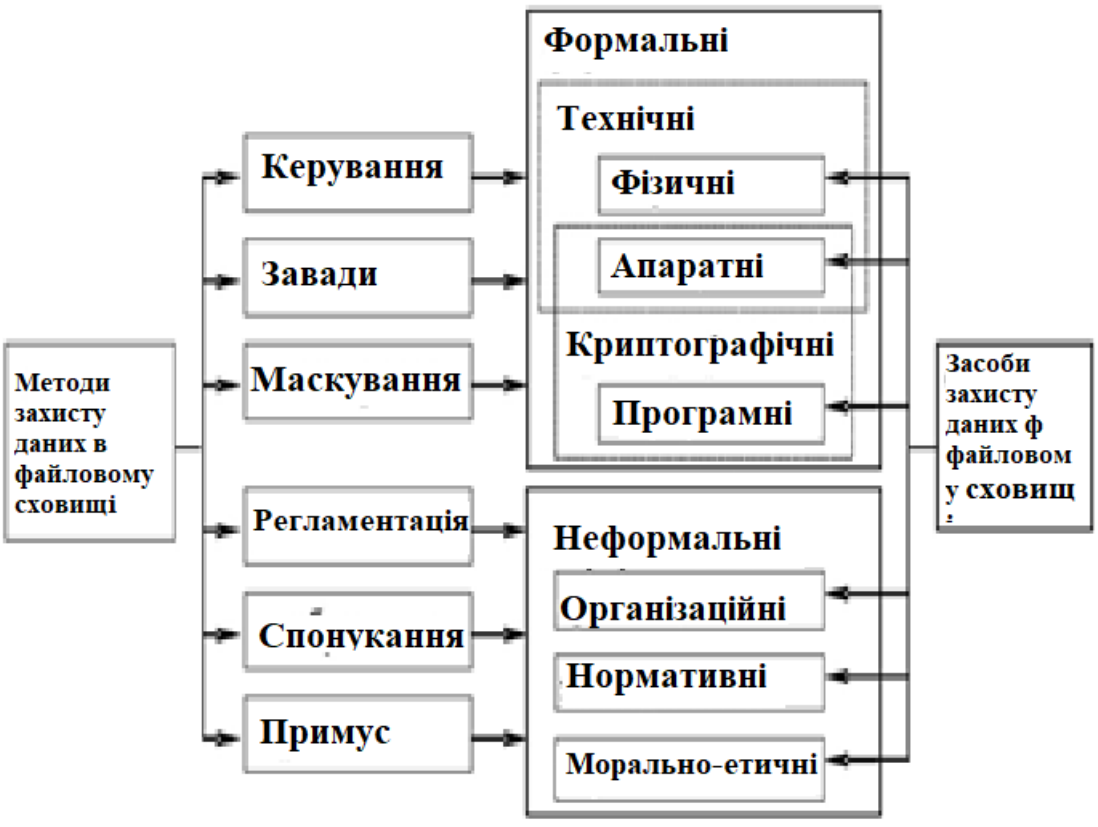


Рисунок 2.10. Методи та засоби захисту даних в файловому сховищі

Засоби захисту інформації поділяються на кілька груп: фізичні, апаратні, програмні або криптографічні, організаційні, етичні та законодавчо-правові. Криптографія, яка перекладається з грецької, як "*потайки пишу*" є наукою, що займається забезпеченням цілісності, автентифікації та конфіденційності інформаційних даних.

Відображення конфіденційності та забезпечення цілісності інформації пов'язані, та в багатьох випадках методи та засоби вирішення одного завдання допомагають з вирішенням іншого.

Крім шифрування та дешифрування, криптографія займається ще й управлінням ключами, електронними цифровими підписами, захистом інформації на рівні квантової фізики, отриманням прихованої інформації.

До методів криптографічного захисту інформації застосовують різні системи класифікації, зокрема за формою впливу на початкову інформацію їх поділяють на чотири підгрупи як це показано на рисунку 2.11.

Рисунок 2.11. Методи криптографічного перетворення інформації

Стенографія уявляє собою розміщення прихованої інформації всередині відкритої. Метою такого методу є:

- Підтвердження деякого виду права завдяки впровадженню назви у вигляді стенографічного водяного знаку;

- створення цифрових відбитків для протекції виключного права;
- для захисту справжності документів та подальшого виявлення фальшивої та підробленої інформації;

- безпосередня передача прихованих даних, різними способами так, щоб зловмисник не міг розпізнати про сам факт передачі даних.

Кодування уявляє собою процес заміни деяких речень, смислових конструкцій або слів кодами. При здійсненні оберненого процесу шифрування інформації застосовують словники або таблиці, якими володіють обидві сторони. Цей процес застосовується в обмеженій тематиці тексту через необхідність застосування словників. До недоліків кодування можна віднести ще й необхідність періодичної зміни словників, та їх подальше поширення, щоб уникнути розкриття коду.

Стиснення інформативних даних до методів криптографічного перетворення інформації належить умовно та даний процес полягає в зменшенні обсягу різними способами. Даний метод не є ефективним без інверсного перетворення інформації, яка отримується у вигляді вихідної. Крім того стиснення не є безпечним та надійним методом. Це пов`язано з тим, що за допомогою статистичних методів дослідження, процес дешифровки інформації здійснюється легко.

Процес шифрування уявляє собою процес в якому деякий набір дій та перетворень інформативних даних з подальшим отриманням закритої інформації та можливістю її зворотного дешифрування. З розвитком обчислювальної техніки, почали створюватися нові способи шифрування, дешифрування, а також види кібератак на захищену інформацію з урахуванням можливостей сучасних технологій.

Під кібератакою розуміють процес розшифрування інформації особами, які не мають право доступу до ключів або алгоритму шифрування.

Шифрування може бути симетричним або асиметричним, залежно від кількості ключів. Якщо достатньо мати тільки один ключ, то шифрування є симетричним. Якщо необхідно мати два ключі, то шифрування є асиметричним.

Для забезпечення інформаційної безпеки та захисту інформації до методів шифрування виносяться певні вимоги, а саме:

- шифр повинен мати високій ступінь стійкості;

- відсутність спроможності в аналітичному способу дешифрування;

- підбір ключа повинен мати високий рівень складності;

- об`єм захищеної інформації не повинен перевищувати об`єм вихідної інформації;

- не допускається втрату або спотворення інформації в процесі шифрування;

- помилки, що виникають під час процесу шифрування, не повинні порушувати цілісність інформації;

- час дешифрування не повинен бути довгим;

- фінансові витрати, що виникають в процесу дешифрування і шифрування не повинні бути великими.

Схему системи криптографічного захисту представлено на рисунку 2.12.

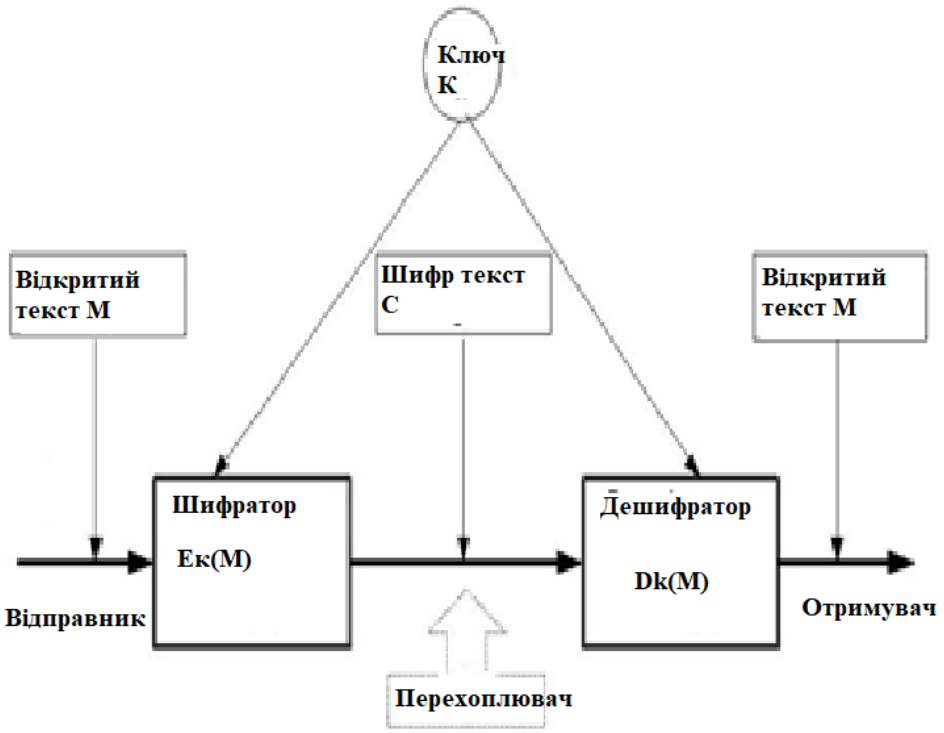


Рисунок 2.12. Схема системи криптографічного захисту

Процес реалізації симетричного шифрування збереження даних в файловому сховищі здійснюється наступним чином. На рисунку 2.12: M є інформація, яку необхідно передати відправником одержувачу. Перехоплювач уявляє собою суб`єкт, який бажає заволодіти M.

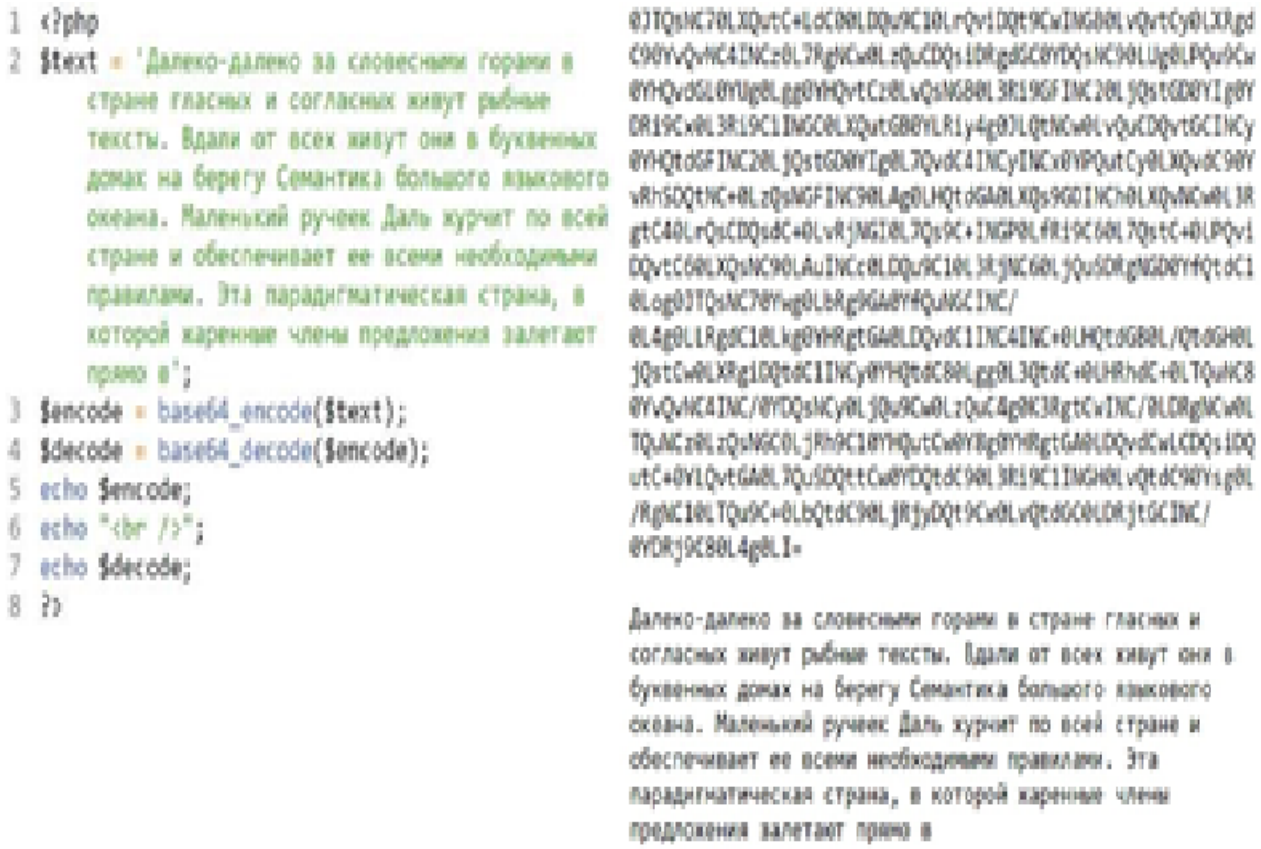
Для передачі M незахищеним каналом передачі інформативного сигналу, здійснюється шифрування M з використанням інверсного перетворення $E_к$. За рахунок цьому отримуються захищені від читання дані $C = E_к(M)$.

При отриманні зашифрованої інформації $C = E_к(M)$ одержувач здійснює його перетворення до вихідного, використовуючи дешифратор $D_к(C)$ та ключ K

Система криптографічного захисту має велику кількість різноманітних варіантів реалізації, а саме апаратне забезпечення, набір інструкцій, програмне забезпечення, все це дає змогу зашифрувати інформацію і дешифрувати різними способами.

Мовою програмування за допомогою якої здійснюється реалізація шифрування є PHP.

За допомогою алгоритму *base*64 дає змогу здійснити шифрування та розшифрування інформації, без використання ключів. Приклад реалізації *base*64 представлено на рисунку 2.13.



А) відкритий текст M ; Б) зашифрований текст $C = E_к(M)$ та $D_к(C)$

Рисунок 2.13. Фрагмент шифрування тексту в файл для збереження в файловому сховищі

В якості тексту для здійснення шифрування, було взято "*текст риба*", який використовується в програмуванні для створення тимчасового контенту. На рисунку 2.13 А) наведено відкритий текст програми M, а на рисунку 2.13, Б) представлено результат її виконання, у якому спочатку є зашифрований текст $C = E_к(M)$, а після нього вихідний текст $D_к(C)$.

Для реалізації симетричного шифрування мовою програмування *PHP* використовується бібліотека *OpenSSL*, а саме функції *openssl encrypt* та *openssl decrypt*. В бібліотеці *OpenSSL* міститься велика кількість різноманітних функцій та методів симетричного й асиметричного шифрування. Приклад реалізації програми симетричного шифрування представлено на рисунку 2.14.

```php
<?php
    define('ENCRYPTION_KEY', 'e3f088b6edfcf6fff70654021c7c2e43');

    $text = 'Далеко-далеко за словесными горами в стране гласных и согласных живут рыбные тексты.';
    $encrypt = func_encript($text, ENCRYPTION_KEY);
    echo $encrypt.'<br>';
    $decrypt = func_decrypt($encrypt, ENCRYPTION_KEY);
    echo $decrypt;

function func_encript($encrypt, $key) {
    $encrypt = serialize($encrypt);
    $iv = mcrypt_create_iv(mcrypt_get_iv_size(MCRYPT_RIJNDAEL_256, MCRYPT_MODE_CBC), MCRYPT_DEV_URANDOM);
    $key = pack('H*', $key);
    $mac = hash_hmac('sha256', $encrypt, substr(bin2hex($key), -32));
    $passcrypt = mcrypt_encrypt(MCRYPT_RIJNDAEL_256, $key, $encrypt.$mac, MCRYPT_MODE_CBC, $iv);
    $encoded = base64_encode($passcrypt).'|'.base64_encode($iv);
    return $encoded;
}

function func_decrypt($decrypt, $key) {
    $decrypt = explode('|', $decrypt.'|');
    $decoded = base64_decode($decrypt[0]);
    $iv = base64_decode($decrypt[1]);
    if(strlen($iv)!=mcrypt_get_iv_size(MCRYPT_RIJNDAEL_256, MCRYPT_MODE_CBC)){ return false; }
    $key = pack('H*', $key);
    $decrypt = trim(mcrypt_decrypt(MCRYPT_RIJNDAEL_256, $key, $decoded, MCRYPT_MODE_CBC, $iv));
    $mac = substr($decrypt, -64);
    $decrypt = substr($decrypt, 0, -64);
    $calcmac = hash_hmac('sha256', $decrypt, substr(bin2hex($key), -32));
    if($calcmac!==$mac){ return false; }
    $decrypt = unserialize($decrypt);
    return $decrypt;
}
?>
```

Рисунок 2.14. Програма симетричного шифрування

Висновок до розділу 2

1.В кожній компанії є критично важлива інформація, яка потребує захисту від зловмисників, які намагаються отримати до доступ до цієї інформації, так як це є важливим елементом стійкості установи.

2.Існує можливість витратити багато часу та ресурсів і вибудувати систему захисту самостійно. Але створення засобів захисту інформації, які допомагають автоматизувати захист інформації та пов'язані з цим процеси забезпечують більш надійний та швидкий захист.

3.Методи захисту інформації, зокрема системи криптографічного захисту інформації в файловому сховищі відіграють важливу роль у сучасному, наповненому інформацією кіберпросторі. Уявлення про засоби протекції необхідні для нормального функціонування передавання та зберігання конфіденційної та таємної інформації.

РОЗДІЛ 3 РЕКОМЕНДАЦІЇ ЩОДО ПРАКТИЧНОГО ЗАСТОСУВАННЯ СИСТЕМ ЗАХИСТУ ФАЙЛОВОГО СХОВИЩА

Щоб заощадити місце на накопичувачах, для зберігання безлічі файлів будь-якого призначення можна використовувати файлові сервери. Який комп'ютер називається файловим сервером? Це спеціалізований пристрій, який адаптовано для зберігання великих обсягів інформації будь-якого типу. Доступ до нього є у великої кількості користувачів, для цього використовуються власні девайси.

Файловий сервер для малого офісу здатний істотно полегшити роботу будь-якої компанії. Крім того, його використання відкриває перед користувачами ще низку можливостей:

- сервер для файлів дає змогу розділити області зберігання за будь-яким типом, є можливість налаштувати допуск до інформації для певних осіб;\

- чудові умови для безпеки інформації;

- можна розділити обсяг простору на сервері. Файловий сервер (файл сервер) - це чудова можливість віддаленого зберігання інформації, для безперебійної роботи якого потрібен потужний процесор.

Найчастіше основним критерієм поділу на типи є спеціалізація файл сервера. Розрізняють два основних типи:
- виділені, які найчастіше використовують для простого зберігання файлів, для такого сервера можна підібрати будь-яку операційну систему, оператор внесе всі необхідні налаштування, і машину можна буде використовувати за її прямим призначенням;
- невиділені сервери - крім зберігання інформації, може встановлюватися велика кількість додаткових налаштувань, наприклад, спільний доступ, централізоване управління і багато іншого.
Організація файлового зберігання передбачає різні типи доступу до інформації. Найчастіше доступ надається за протоколом FTP, але можна вибрати й інший тип доступу, який надасть більше можливостей користувачеві.

Ще одна класифікація файлових серверів передбачає поділ за технічними характеристиками:

- Для невеликих офісів або домашнього використання чудово підійде звичайний персональний комп'ютер.

- Спеціалізовані сервери мають відразу кілька накопичувачів, що істотно збільшує доступний обсяг пам'яті, вони забезпечені мережевими картами, стабілізаторами напруги, тому цілком зможуть забезпечити безперебійний доступ до інформації. Такі файлові сховища - це чудовий вибір для великих компаній.

- Кластери файлових серверів, вони мають кілька машин у складі, тому забезпечують не тільки великий обсяг інформації, а й високу швидкість обміну нею. Вони чудово підійдуть для великих компаній, зокрема й тих, які мають представництва в різних містах.

Вибір файлового сервера насамперед залежить від потреб фізичної особи або компанії.

Зберігання файлів на сервері повністю безпечне і виключає будь-який витік інформації. Крім того, під час вибору сервера варто приділити увагу таким моментам:

- насамперед варто звернути увагу на обсяг пам'яті, її має бути достатньо для резервного копіювання та розміщення інформації;
- оперативна пам'ять теж дуже важлива, вона забезпечує потрібну швидкість передачі;
- мережева карта, найкраще з високою пропускною здатністю;
- надійність обладнання.

Як організувати файлове сховище? Насамперед потрібно розмежувати права на читання і запис, зробити роздільні каталоги, встановити квоти на обсяг. Український або закордонний файловий сервер можна взяти в оренду в компанії XServer. У нас знайдеться сервер як для невеликого офісу, так і для великого підприємства. Ми гарантуємо нашим клієнтам повну безпеку даних завдяки

щоденному резервному копіюванню, повну підтримку, якісне програмне забезпечення.

ВИСНОВОК

1.Якщо йдеться про класичні додатки, ізольоване сховище - це механізм зберігання даних, що забезпечує ізоляцію та безпеку шляхом визначення стандартизованих способів зіставлення коду зі збереженими даними. Стандартизація також має й інші переваги.

2.Адміністратори можуть використовувати інструменти управління ізольованим зберіганням для конфігурування простору зберігання файлів, встановлення політики безпеки та видалення невикористовуваних даних.

3.При ізольованому зберіганні немає необхідності вказувати унікальні шляхи для безпечного розміщення коду у файловій системі, і дані захищені від інших застосунків, що мають доступ тільки до ізольованого зберігання. Н

4.Немає потреби в апаратно закодованій інформації, що вказує місце розміщення області зберігання даних програми.

5. Ізольоване сховище недоступне для додатків Магазину Windows 8.x. Замість цього використовуйте класи даних додатків у просторах імен Windows.Storage, включених в API середовища виконання Windows для зберігання локальних даних і файлів.

6. Коли додаток зберігає дані у файлі, обирати ім'я файлу та місце його зберігання слід так, щоб мінімізувати вірогідність того, що місце зберігання даних буде доступним для інших додатків, а отже, стане вразливим до пошкодження. За відсутності стандартної системи для розв'язання подібних проблем імпровізоване розроблення засобів мінімізації конфліктів зберігання може стати надмірно складним, а його результати - ненадійними.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ ТА ДЖЕРЕЛ

1. A. Suliman, M. K. Shankarapani, S. Mukkamala and A. H. Sung. RFID malware Cards and security devices for personal identification — Contactless proximity objects — Part 2: Radio frequency power and signal interface [Електронний ресурс] // ISO/IEC 14443-2:2020. – 2020. – Режим доступу до ресурсу: https://www.iso.org/standard/73597.html.

2. Guidelines for RFID-based Electronic Article Surveillance [Електронний ресурс]. – 2009. – Режим доступу до ресурсу: https://www.rfidjournal.com/gs1-releases-guidelines-for-rfid-based-electronic-article-surveillance.

3. IDTechEx: RFID System Frequencies. An overview of RFID frequencies for chip based tags. [Електронний ресурс]. – 2004. – Режим доступу до ресурсу: http://www.idtechex.com/.

4. L. Avanco, A. E. Guelfi, E. Pontes, A. A. A. Silva, S. T. Kofuji and F. Zhou. An effective intrusion detection approach for jamming attacks on RFID systems. International EURASIP Workshop on RFID Technology (EURFID); 2015; Rosenheim, Germany. p. 73–80.

5. Methodology for Evaluating Security in Commercial RFID Systems / T.M. Fernández-Caramés, P. Fraga-Lamas, M. Suárez- Albela, L. Castedo., 2017.

6. OpenPCD Reader [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://www.meriac.com.

7. Vogt H. Efficient Object Identification with Passive RFID Tags / Harald Vogt. – Zürich: Department of Computer ScienceSwiss Federal Institute of Technology (ETH), 2002. – 98 с

8. Y. Fu, C. Zhang and J. Wang. A research on Denial of Service attack in passive RFID system. In: International Conference on Anti-Counterfeiting Security and Identification in Communication (ASID); 2010; Chengdu, China. p. 24–28.

9. Fragmentation attacks. In: International Symposium on Collaborative Technologies and Systems; 2008; Irvine, United States.

10. Агафьин С. С. LW-КРИПТОГРАФИЯ: ШИФРЫ ДЛЯ RFID-СИСТЕМ / С. С. Агафьин // Безопасность информационных технологий / С. С. Агафьин., 2011. – С. 30–33.

11. Гнатюк М. А. ДИФРАКЦИЯ ЭЛЕКТРОМАГНИТНОЙ ВОЛНЫ НА КАСКАДНОМ СОЕДИНЕНИИ ПРЯМОУГОЛЬНЫХ ВОЛНОВОДОВ / М. А. Гнатюк, В. М. Морозов, С. В. Марченко. // ХНУРЕ. – 2019. – №196. – С. 130–137.

12. Горбачов В. Е. ОБЗОР ПРОБЛЕМ БЕЗОПАСНОСТИ И ПРОЕКТИРОВАНИЯ ЗАЩИЩЕННЫХ ЭЛЕКТРОННЫХ СИСТЕМ / В. Е. Горбачов, К. Б. Абдулрахман. // ХНУРЕ. – 2017. – №191. – С. 113–119.

13. Горбенко І. Д. ДОСЛІДЖЕННЯ СТРУКТУРИ СПЕКТРІВ СИГНАЛОВ З ЛІНІЙНОЮ ЧАСТОТНОЮ МОДУЛЯЦІЄЮ / І. Д. Горбенко, О. А. Замула. // ХНУРЕ. – 2018. – №193. – С. 192–198.

14. Горбенко І. Д. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ПОМЕХОЗАЩИЩЕННОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ В УСЛОВИЯХ РАЗЛИЧНЫХ ВНУТРЕННИХ И ВНЕШНИХ ВОЗДЕЙСТВИИ / І. Д. Горбенко, А. А. Замула, В. Л. Морозов. // ХНУРЕ. – 2017. – №189. – С. 5–14.

15. Горбенко Ю. І. УДОСКОНАЛЕНИЙ МЕХАНІЗМ ОДНОРАЗОВИХ КЛЮЧІВ ДЛЯ ПОСТКВАНТОВОГО ПЕРІОДУ НА ОСНОВІ ГЕШ-ФУНКЦІЙ [Електронний ресурс] / Ю. І. Горбенко, К. В. Ісірова // ХНУРЕ. – 2017. – Режим доступу до ресурсу: https://nure.ua/wp content/uploads/2017/Scientific_editions/191/5.pdf.

16. Описание процесса радиочастотной идентификации [Електронний ресурс] – Режим доступу до ресурсу: http://asupro.com/gps-gsm/meansidentification/reference/description-process-rfid.html.

17. Сальников Д. С. МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ДЛЯ БЕСПРОВОДНЫХ СИСТЕМ СВЯЗИ МИЛЛИМЕТРОВОГО ДИАПАЗОНА ВОЛН / Д. С. Сальников, А. І. Цопа. // ХНУРЕ. – 2018. – №192. – С. 140–148.