НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ПОЛІТЕХНІКА»
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Кафедра комп'ютерних інтелектуальних систем та мереж

ОЗЕЛ Орхан Велі

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

БЕЗПЕКА В ХМАРНИХ СХОВИЩАХ ДАНИХ

Спеціальність 123 – Комп`ютерна інженерія
Спеціалізація – Комп'ютерні системи та мережі

Керівник: Тішин П.М., к.ф-м.н, доцент

Одеса – 2022

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

ОЗЕЛ Орхан Велі
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Безпека в хмарних сховищах даних

керівник проекту (роботи) Тішин П.М. к.ф-м.н, доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання),
затверджені наказом ректора ОНПУ від "__" _____2022_ року №_____

2. Строк подання студентом проекту (роботи) 13.06.2022

3. Вихідні дані до проекту (роботи) завдання на розробку

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1 Аналіз предметної області

2 Завдання на розробку

3 Організація безпеки в хмарних сховищах даних

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)

Апаратна модель безпеки даних, Програмна модель безпеки даних, Система контролю внутрішнього трафіку, Система міжмережного контролю трафіку, Контроль поштової системи, Захист веб-системи сховища, Захист сховищ даних, Система фільтрації трафіку, Інтерфейс адміністрування безпеки

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
	Аналіз предметної області		
	Завдання на розробку		
	Організація безпеки в хмарних сховищах даних		

Студент _____ _____
(підпис) (прізвище та ініціали)

Керівник проекту (роботи) _____ _____
(підпис) (прізвище та ініціали)

Відомість кваліфікаційної роботи бакалавра

№ рядка	Найменування	Кільк.	Примітка
1	Пояснювальна записка	41	
2	Апаратна модель безпеки даних	1	
3	Програмна модель безпеки даних	1	
4	Система контролю внутрішнього трафіку	1	
5	Система міжмережного контролю трафіку	1	
6	Контроль поштової системи	1	
7	Захист веб-системи сховища	1	
8	Захист сховищ даних	1	
9	Система фільтрації трафіку	1	
10	Інтерфейс адміністрування безпеки	1	
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			

АМДР.АМ183.1332

Зм.	Лист	№ докум.	Підпис	Дата
Розробив		Озел Орхан		
Перевірив		Тішин ПМ		
Реценз.				
Н. Контр.				
Затвердив				

Безпека в хмарних сховищах даних

Літ.	Лист	Листів
	1	1

НУ «ОП» ІКС

КІСМ АМ183

АНОТАЦІЯ

Озел О.В. Безпека в хмарних сховищах даних – кваліфікаційна робота бакалавра. Одеса, 2022: 41с., 9 рис., 8 джерел.

Дана робота присвячена розробці системи захисту інформації в хмарних сховищах даних. В роботі розглянуто питання забезпечення конфіденційності, цілісності та доступності даних, які зберігаються.

Розглянуто питання двофакторної аутентифікації з використанням власного поштового сервісу, питання фільтрації трафіку в мережі та із зовнішніми ресурсами. Також здійснено налаштування міжмережних екранів на кінцевих пристроях, журналювання подій на кінцевих пристроях. Для забезпечення посиленого захисту також забезпечено використання таких систем, як запобігання витоку інформації та виявлення вторгнень.

В результаті проектування отримано комплекс програмних та апаратних засобів, які направлені на захист клієнтських та системних даних.

ХМАРНІ СХОВИЩА ДАНИХ, ІНФОРМАЦІЙНА БЕЗПЕКА, ФІЛЬТРАЦІЯ ТРАФІКУ, СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ, АНТИВІРУСНИЙ ЗАХИСТ

ABSTRACT

Ozel O. Security in cloud storage - bachelor's thesis. Odesa, 2022: 41p., 9 pic., 8 sources.

This work is devoted to the development of information protection system in the cloud storage. The paper considers the issues of ensuring the confidentiality, integrity and availability of stored data.

The issues of two-factor authentication using our own mail service, the issue of filtering traffic in the network and with external resources are considered. Also, set up firewalls on end devices, logging events on end devices. Systems such as information leakage prevention and intrusion detection, are also provided to provide enhanced protection.

As a result of the design, a set of software and hardware was obtained, which are aimed at protecting client and system data.

CLOUD STORAGE, INFORMATION SECURITY, TRAFFIC FILTRATION, INVASION DETECTION SYSTEMS, ANTI-VIRUS PROTECTION

ЗМІСТ

ВСТУП

В сучасних умовах функціонування бізнесу, важливу роль відіграє використання інформаційних технології та систем, які вже виступають як невід'ємна частина бізнес-процесів організації. Однією з функцій, яка є дуже важливою, це зберігання операційних даних, які використовуються в процесі діяльності організації. Все частіше підприємства звертаються до сторонніх сервісів для зберігання даних, що обумовлено наступними факторами:

- невисока вартість зберігання в розрахунку на 1 гігабайт;
- висока доступність даних та обладнання;
- делегування частини відповідальності за ризики третім сторонам.

Такий підхід достатньо часто виправданий для невеликих компаній, які не можуть дозволити собі власний дата-центр та наймання відповідних кваліфікованих спеціалістів для обслуговування систем зберігання даних.

Великі компанії напроти, мають можливості для організації власних мереж зберігання даних. Основними перевагами організації власного дата-центру для зберігання даних є повний контроль над інфраструктурою мережі, більша ізольованість системи. До недоліків такого підходу можна віднести вартість володіння такою системою, необхідність найму кваліфікованих кадрів для обслуговування системи.

З боку власників мереж зберігання даних, будь то приватні чи публічні мережі, важливою складовою функціонування системи є забезпечення безпеки даних, тому що порушення однієї зі складових тріади безпеки інформації призводить до наступних наслідків:

- фінансові втрати для власників інформації;
- моральні збитки для власників даних;
- розголошення приватних даних;

– викривлення інформації, що зберігається;

– репутаційні та фінансові втрати для власників мережі зберігання даних.

Виходячи з цього, вкрай важливим є організація захисту даних в мережах зберігання, яка полягає в забезпеченні наступних факторів:

– організація розмежування доступу;

– фільтрація мережевого трафіку;

– шифрування та контроль цілісності даних;

– контроль витоку даних;

– виявлення зловживань та втручань в системи зберігання;

– активний та пасивний моніторинг даних.

Забезпечення виконання цих факторів полягає у використанні програмних та апаратних засобів моніторингу, контролю та аудиту користувачів, програм та процесів які задіяні в системі.

Також впровадженню технічних засобів захисту інформації передує проектування організаційних заходів щодо забезпечення захисту інформації, які регламентують основні правила використання системою, зони відповідальності співробітників, спеціальні уточнення для певних груп користувачів та інше.

1 АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1 Загальні поняття та визначення предметної області

Хмарне сховище, хостинг сервіс провайдер або дата-центр – компанія, що надає послуги з розміщення серверного обладнання, даних та сайтів на своїй території.

Інформаційна безпека – організована система, що налаштована знаходити вразливі місця. Але, щоб це працювало на відповідному рівні – потрібно знати які засоби, методи використовуються для виявлення вразливостей та організації безпеки. Інформація має кілька основних визначень, а саме повідомлення, факти, дані, команди, знання. Безпека – поняття вільності від небезпек та збереженість.

Інформаційна безпека – набір заходів для передбачення несанкціонованого доступу до даних, їх використання або змінення. Надійність забезпечується комплексом заходів безпеки: фізичний захист, захист комунікацій – безпека передачі даних, захист випромінювань, захист комп’ютерів та захист мереж.

Засоби організації безпеки[1]:

– Антивірусне програмне забезпечення - зменшує риски роботи шкідливих програм; але, якщо зловмисник використовує законі програми не допоможе від атаки, та якщо користувач намагається отримати несанкціонований доступ до даних.

– Керування доступом – потрібно для ідентифікації користувачів що мають дозвіл на вхід до системи. Також встановлюються дозволи для користувачів на використання файлів.

– Міжмережеві екрани – це устаткування для керування доступом, що захищає усі внутрішні мережі від зовнішніх атак. Встановлюється між внутрішньою та зовнішньою мережами

– Смарт-карти – аутентифікація користувачів не завжди може бути виконана правильно. Наприклад, використання паролів не саме надійне рішення. Тому замість введення паролів використовуються смарт-карти та зменшуються риски вгадання паролів.

– Біометричні системи – також метод аутентифікації, що зменшує риски вгадування паролів. Біометричні засоби аутентифікації можуть бути: сканери пальців, конфігурації тіла та голосу. Тобто визначення людських характеристик.

1.2 Існуючі види атак

Існують чотири основні типи атак:

- Атаки доступу;
- Атаки модифікацій;
- Атаки на відмову в обслуговуванні;
- Атаки на відмову від обов’язків.

Атаки здійснюються за допомогою розроблених програмних засобів, методів соціального інжинірингу або через дірки в комп’ютерних системах. Коли атака проводиться на інформацію, то вона копіюється до зловмисника.

Атаки доступу – це спроба заволодіти інформацією до якої у зловмисника немає дозволу. Дана атака порушує конфіденційність інформації. Вона є там де є засоби передачі інформації.[2]

Атака типу підглядання – перегляд файлів та документів.

Атака типу підслуховування – використовується за допомогою електронних пристроїв та найчастіше використовується в бездротових мережах. В локальних дротових зловмиснику необхідно фізично знаходитись поруч та підключати пристрої до локальної мережі.

Атака по типу перехват проходить в момент коли інформація передається до пункту призначення. Після чого інформація чи розрушується чи блокується.

Інформація до котрої організовуються атаки може знаходитись на робочих станціях, на серверах, на портативних комп'ютерах, на електронних носіях.

Атаки модифікації – це тип на виправлення інформації та порушення цілісності її. Можливі різновиди атак модифікацій: атака типу заміни існуючої інформації, по типу додавання нових даних, по типу видалення даних[2].

Атаки на відмову в обслуговуванні – в результаті користувач не може отримати дозвіл на користування своєю системою, використовувати інформацію та можливості комп'ютера.

Атака на відмову в доступі до інформації направлена проти інформації та робить її неможливою до використання. Інформація може видалитись, змінитись або перенестись до іншого місця.

Атака на відмову доступу до додатків що обробляють або відображають інформацію, або на комп'ютерну систему де ці додатки виконуються. В результаті не має можливості вирішувати задачі за допомогою того додатку.

Атака на відмову доступу до системи виводить з ладу комп'ютерну систему, в результаті система, додатки та інформація недоступні до використання.

Атака на відмову доступу до засобів зв'язку виводить з ладу комунікаційне середовище. В результаті цілісність системи та інформації не мають доступу[2].

1.3 Напрями захисту даних

Конфіденційність – це служби, що забезпечують секретність інформації. При налаштуванні цієї служби, доступ до інформації отримують

тільки аутентифіковані користувачі. Таким чином вигороджує системи від атак доступу.

Механізми забезпечення конфіденційності файлів:

- Контроль фізичної безпеки;
- Контроль доступу до файлів на комп'ютері;
- Шифрування файлів.

Вимоги до конфіденційності файлів:

- Ідентифікація та аутентифікація;
- Налаштування комп'ютерної системи;
- Керування ключами при використанні шифрування.

Конфіденційність при передачі даних по мережі забезпечується за допомогою шифрування. Також шифрування попереджує атаки підслуховування, але від перехвату інформації не захистить. Це дозволить зробити при надійної системи ідентифікації та аутентифікації.

Конфіденційність потоків даних не відповідає за збереженість даних, що передаються. Ця служба дозволяє аналізаторам трафіку визначати точки між котрими встановлений зв'язок. Забезпечується конфіденційність потоку даних за рахунок скованості інформації, що передається між двома учасниками зв'язку в більшої кількості трафіку даних[3].

Цілісність – це служба що визначає правильність інформації. Якщо система правильно налаштована то має бути впевненість в вірності даних, що передаються та зберігаються. Також для забезпечення найкращого результату безпеки, ця служба повинна працювати в парі з ідентифікацією, щоб перевіряти подліність даних. Вона забезпечує захист від атак модифікації. Попередження атак типу перехват даних забезпечують механізми ідентифікації та аутентифікації, а також шифрування даних. Комплекс цих заходів безпеки забезпечують цілісність даних та попереджують атаки модифікації та відмови від обов'язків [3].

Доступність – служба, що вказує на готовність до роботи, та дозволяє звертатись до комп'ютерних систем, даних та додатків, що знаходяться в цих

системах. Для збереження інформації використовують резервне копіювання та збереження в безпечному місці. Але це не гарантія її збереженості, тому є механізми що направлені на організацію доступності:

– перемикання по відмові – якщо виникла несправність, то проходить відновлення робочого ладу за допомогою резервних апаратних засобів.

– відновлення в аварійних ситуаціях – дозволяє у випадку техногенних катастроф та неможливості отримати доступ до основного обладнання захищає систему, інформацію та дозволяє відновити доступ до даних.

– передбачення атак – це механізми забезпечення доступності використовуються для відновлення систем після атак на відмову в обслуговування. Повністю відновити систему після подібної атаки неможливо, але зменшити наслідки та повернути систему і устаткування до ладу можливо.

Ідентифікаційність – це служба, що використовується паралельно в роботі з іншими службами, щоб збільшити ймовірність попередження атак та збільшити ефективність заходів безпеки. Ідентифікація та аутентифікація показують адміністратору користувачів з боку хто є ким відповідно до дозволів та за кого себе видає.

Аудит – служба що фіксує події в мережі та системі. Аудит працює разом із службами авторизації та аутентифікації. Служба аудиту представляє собою журнали подій, де фіксуються звіти о всіх виконаних діях в системі користувачами [3].

1.4 Організація заходів безпеки для сервісу DNS

Основна задача сервісу DNS – це перетворення доменних імен в мережеві адреси та навпаки. Компоненти сервісу що підлягають захисту: апаратна частина та програмне забезпечення, ПЗ серверів,транзакції, репозиторії та конфігураційні файли. Основні служби безпеки в сервісі – це аутентифікація та цілісність інформації. Механізми безпеки для сервісу:

середовище, де виконуються сервіси DNS (платформа, ПЗ, дані), транзакції DNS (запит та відповідь, динамічне оновлення), адміністрування DNS (алгоритми та ключі, керування ключами і тд.)

Загрози для сервісу DNS[4]:

– ОС або ПЗ будь якого іншого додатку, що виконується на робочій станції DNS може бути підвернено такій атаці, як переповнення буферу, та в результаті не зможе функціонувати сервіс дозволу імен.

– Інша загроза з боку атаки наводнення пакетів, що приводить до порушення зв'язку або переповнення серверу невірними запитами.

– Загроза з внутрішнього боку системи від зловмисника, що має доступ до локальної мережі. В результаті може бути порушений потік повідомлень DNS, якщо проводити атаку типу ARP запитів.

– Загроза на конфігураційний файл призводить до порушень взаємодії між учасниками DNS.

Загрозою для ПЗ DNS може бути переповнення буферу, що дасть шанс до атак DoS та отримання не авторизованого доступу. Щоб попередити подібні випадки організовуються заходи безпеки ПЗ:

– ізолювання ПЗ серверу імен;

– виконання оновлення та останніх версій ПЗ серверу імен;

– виконання ПЗ серверу імен з обмеженнями;

– загрози для даних DNS – зоні та конфігураційні дані.

1.5 Безпека web-серверів

Одна з найчастіших цілей для атак зловмисників є web-сервера. Вони є важливим компонентом служб web, та є додатком, що формує інформацію за протоколом http. Іншим компонентом, менш вразливим, є web-клієнт, та надає доступ до інформації, що знаходиться на web-сервері. Важливо визначити заходи безпеки для web-серверів та мережевої інфраструктури, що їх підтримує. Загрози діляться на [5]:

- використання помилок ПЗ на web-серверів, що створюють динамічні web-сторінки для отримання неавторизованого доступу до web-серверу;
- DoS-атаки можуть буди направлені на web-сервер.

Заходи безпеки:

- конфігурування ОС;
- конфігурування ПЗ web-серверу;
- встановлення механізмів захисту, таких як між мережеві екрани.

1.6 Інструментальні засоби організації безпеки даних

Для визначення вразливостей потрібно тестувати постійно мережу та пристрої на визначення атак. Інструментальні засоби аналізу вразливостей можуть класифікуватись по розміщенню та по інформації. По розміщенню системи аналізу визначають вразливість, аналізуючи існуюче джерело системних даних: склад файлів, параметри конфігурації та іншу о стані системи.

Переваги використання систем аналізу вразливостей [6]:

- дозволяє визначити проблеми в системі;
- дозволяє виконувати тестування безпеки;
- дозволяють вчасно та надійно виявляти зміни в стані систем безпеки, та сповіщати адміністраторів о проблемах;
- комплексна перевірка будь яких змін, що проводяться в системі, гарантуючи рішення питань безпеки.

Недоліки систем аналізу:

- такі системи пов’язані з ОС та з додатками, й потребують додаткового керування;
- деякі системи можуть створювати брехливі тривоги.
- існують деякі види тестів, що можуть руйнувати систему, яку тестують.

2 ЗАВДАННЯ НА РОЗРОБКУ

Забезпечення захисту даних в хмарному сховищі даних так як і в локальній мережі зберігання даних вимагає комплексного підходу, який передбачає впровадження широкого переліку апаратних, програмних та організаційних технології інформаційної безпеки. Потрібно визначити кожні вузли та вимоги до захисту цих вузлів.

2.1 Захист мережевих систем

Захист мережевих систем вимагає забезпечення безпеки передачі даних та мережевого обладнання, яке реалізує функції по передачі трафіку в мережі.

Захист мережевого обладнання передбачає забезпечення її адекватного функціонування сервісів та протоколів.

1. Організація контролю доступу повинна забезпечуватись[6]:

– фільтрацією доступу до обладнання з використанням списків доступу;

– доступ до мережевого обладнання здійснюється з використанням асиметричних ключів, довжиною не менше ніж 2048 бітів;

– використання двофакторної аутентифікації для доступу до систем мережі.

2 Захист конфігурації мережевого обладнання забезпечується наступними функціями:

– резервування конфігурації на резервних серверах;

– використання контролю цілісності конфігураційних файлів;

– дзеркалювання дискового простору з використанням RAID.

Захист від перевантаження трафіку. Контроль трафіку забезпечується засобами моніторингу функціонування інтерфейсів та контролю сервісів на обладнанні[6].

1 Використовується система моніторингу Zabbix, яка забезпечує:

– побудову графіків трафіку на інтерфейсах мережевого обладнання;

– оновлення інформаційної панелі подій на основі встановлених тригерів спрацьовування;

– інформування адміністраторів систем шляхом надсилання поштових повідомлень та з використанням месенджерів.

2 Використання протоколу Syslog дозволяє здійснювати комплексний збір інформації про стан мережевого обладнання:

– статуси мережевих інтерфейсів

– статуси завантаження процесорів;

– статуси використання пам’яті;

– статуси використання дискового простору;

– контроль системи введення та виведення.

2.2 Захист кінцевих пристроїв

Захист кінцевих пристроїв направлений на забезпечення цілісності даних, доступності обладнання та контролю сервісів.

Захист операційної системи здійснюється за рахунок використання, переважно, стороннього програмного забезпечення.

1. Використання антивірусної програми дозволяє здійснювати наступні функції[7]:

– захист від проникнення стороннього програмного забезпечення (вірусів);

– контроль процесів операційної системи;

– контроль трафіку на мережевих інтерфейсах обладнання;

– моніторинг стану обладнання.

2. Використання журналів операційної системи дозволяє виконувати наступні функції:

– контроль стану апаратного та програмного забезпечення обладнання;

– аудит доступу до мережевого обладнання;

– виявлення помилок на обладнанні.

Захист застосувань здійснюється для забезпечення цільових функцій конкретного пристрою[7]:

– антивірусні програми блокують зміну файлів застосувань;

– ведення журналів фіксує зміни які здійсненні застосуваннями або до застосувань;

– система моніторингу контролює доступність сервісів та параметри їх функціонування;

– здійснюється постійний контроль оновлень програмного забезпечення.

2.3 Захист даних

Захист даних передбачає забезпечення їх конфіденційності, цілісності та доступності.

Захист доступності даних вимагає[8]:

– контролю щільності трафіку в мережі;

– контролю мережевих інтерфейсів на всьому обладнанні;

– резервування даних;

– фільтрації трафіку.

Захист конфіденційності даних вимагає:

– використання симетричного шифрування AES192 для даних, що зберігаються та передаються;

– використання аутентифікації та розмежування доступу до даних;

– використання хеш-функції для сховування паролів та контрольних кодів доступу;

– моніторинг діяльності користувачів, процесів та програмного забезпечення.

Контроль цілісності використовується для:

– контролю цілісності ідентифікаційних даних;

– аутентифікації повідомлень всередині мережі;

– зберігання паролів та кодів;

– контролю цілісності даних на серверах.

Резервування даних здійснюється локально на серверах та на резервному обладнанні:

– використання RAID масивів дозволяє здійснювати резервування локальних систем серверів;

– використання серверів резервування для зберігання копій даних та конфігурацій;

– виконується зберігання користувальницьких даних за останні 7 днів та місячна копія;

– резервування конфігурацій здійснюється при внесенні змін;

– зберігається 20 останніх станів конфігурацій обладнання.

3 ОРГАНІЗАЦІЯ БЕЗПЕКИ В ХМАРНИХ СХОВИЩАХ ДАНИХ

Захист даних в сховищах даних вимагає створення комплексної системи інформаційної безпеки, для забезпечення виключення або зниження наступних загроз:

а) захист конфіденційності вимагає забезпечення неможливості засвоєння інформації, яка зберігається в мережі:

– захист ідентифікаційних даних користувачів шляхом їх шифрування;

– захист інформації користувачів шляхом розмежування доступу до неї;

– введення двофакторної аутентифікації (логін/пароль, власний поштовий сервіс, коди підтвердження).

б) захист цілісності даних вимагає унеможливлення втручання в структуру інформації, яка зберігається:

– резервування даних;

– створення цифрових зліпків файлової структури;

– розмежування доступу до інформації.

в) захист доступності даних та сервісів вимагає забезпечення наступних заходів:

– резервування каналів доступу до мережі зберігання даних;

– контроль трафіку для виявлення спроб порушення доступності даних або сервісів;

– резервування внутрішніх ліній зв’язку та мережевого обладнання.

Усі ці вимоги призводять до розробки певного набору заходів які направлені на зниження ризиків порушення безпеки даних:

– організаційні міри забезпечують створення документальних правил, які регламентують поведінку в мережі, правила використання сервісів мережі, рекомендації, щодо захисту інформації та ідентифікаційних даних;

– технічні заходи супроводжуються проектуванням відповідної структури мережі, вибором відповідного мережевого обладнання, використання якого забезпечує підвищення рівня безпеки в мережі;

– програмні заходи регламентують використання програмного забезпечення, яке здійснює контроль, фільтрацію, аналіз та інші дії, які призначені для виявлення загроз інформаційної безпеки.

3.1 Організаційні та програмно-апаратні заходи забезпечення безпеки даних

Організаційні заходи призначені для забезпечення захисту інформації на рівні використання систем зберігання даних, як для користувачів системи, так і для обслуговуючого персоналу:

– правила доступу до системи (використання паролів, правила завантаження даних, зберігання ідентифікаційних даних);

– опис важливості функціонування системи та її цілей;

– визначення відповідальності користувачів за порушення правил використання системи;

– визначення ролей для користувачів та обслуговуючого персоналу системи.

Усі ці та інші заходи направлені на роботу (навчання) безпосередньо людей, які використовують або обслуговують мережу зберігання даних та її сервіси. Проте, на практиці, відповідальність можна покласти тільки на співробітників, а на користувачів реальних механізмів впливу майже немає. Тому, відносини між власниками мережі зберігання даних, та клієнтами, які зберігають дані будуються на основі домовленостей, в яких викладено відповідальність останніх за дотриманням правил користування сервісами.

Апаратна модель захисту даних в мережі заснована на побудові логічної структури мережі, яка описує апаратні засоби забезпечення контролю, фільтрації, блокування трафіку в мережі та сигналізації адміністраторів систем.

Апаратна модель захисту інформації передбачає використання наступних компонентів:

– системи фільтрації трафіку на межі мережі;
– сервер збору інформації про події (syslog-сервер);
– колектор інформації про стан трафіку;
– комутатори мережі (додаткова фільтрація, сенсори мережі);
– сервер для системи виявлення вторгнень;
– сервер моніторингу.

Усі ці, та інші апаратні засоби комутації, фільтрації та контролю потоків даних формують структуру мережі, яка представлена на рисунку 3.1

Програмна модель заснована на використанні модулів, які доповнюють та розширюють можливості апаратної моделі, шляхом додавання функції обробки та аналізу поведінки користувачів, процесів та мережевого трафіку.

Серед програмних модулів, які реалізують захист інформації використовуються наступні:

– вбудовані засоби операційних систем серверів (мережеві екрани IPS, перехоплення трафіку, захист внутрішніх сервісів, журнали подій);
– вбудовані засоби операційних систем мережевого обладнання (фільтрація MAC-адрес, списки контролю доступу);
– система виявлення вторгнень;
– система моніторингу та інформування про події;
– система візуалізації інформації (дошки об’яв, графіки навантаження);
– система запобігання витоку даних;
– антивірусне програмне забезпечення.

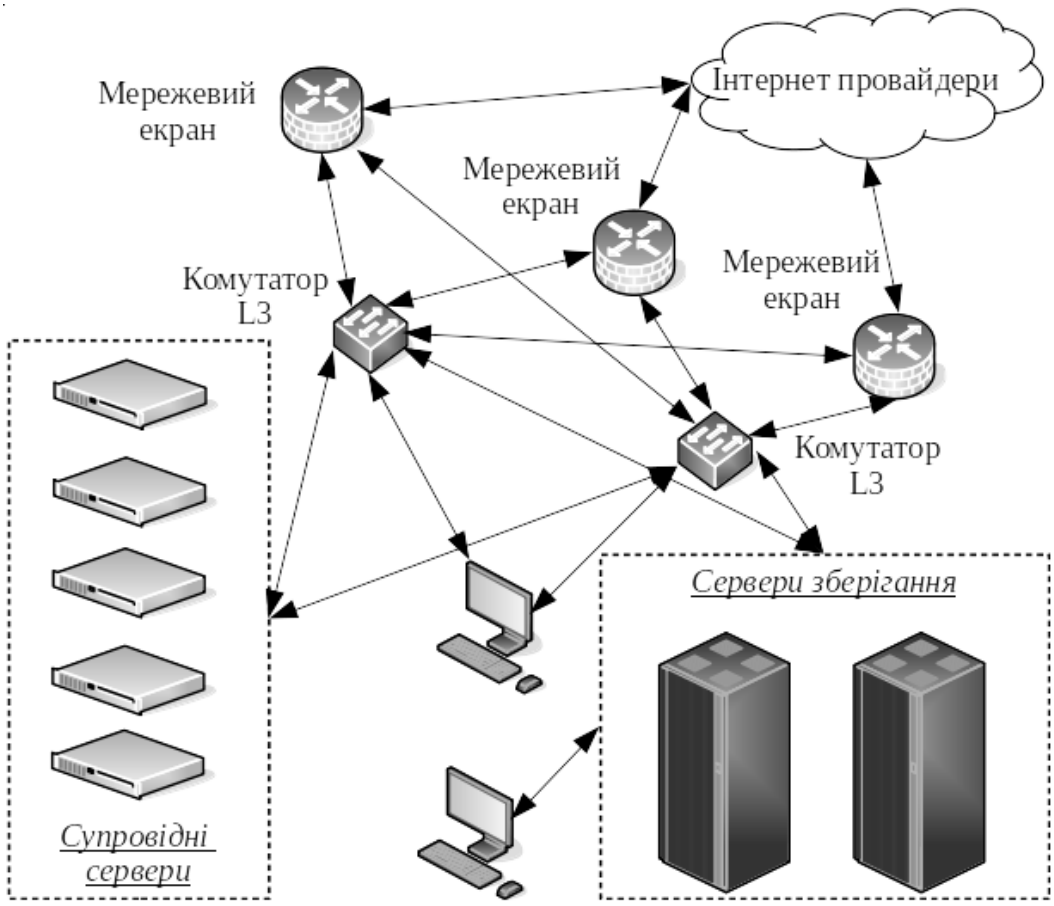

Рисунок 3.1 - Апаратна модель безпеки даних

Модульність даної структури дозволяє, за необхідністю, вилучати певні системи захисту і замінювати їх іншими без втручання в загальну роботу мережі зберігання даних.

Основними складовими інформаційної системи є наступні:

– мережа Інтернет. Здійснення захисту від зовнішніх загроз з мережі Інтернет та витоку даних всередині мережі;

– кінцеві пристрої вимагають контролю як на рівні функціонування операційної системи так і на їх мережевих інтерфейсах;

– мережеві пристрої вимагають захисту конфігурації, а також можуть виступати як сенсори системи захисту та використовувати базові додаткові механізми захисту;

– системи контролю мережі, такі як моніторинг і термінали керування, вимагають захисту від зловживання на рівні операційних систем та застосувань.

Рисунок 3.2 - Програмна модель безпеки даних

До кожного з цих елементів застосовуються певні механізми захисту інформації, які здійснюють безпосередні захисні дії, або використовуються для аналізу безпеки сховищ даних:

– антивірусний захист здійснює контроль кінцевих станцій та серверів мережі зберігання. Контроль здійснюється шляхом аналізу поведінки процесів операційної системи, запитів та відповідей, які обробляються системними сервісами та аналізу файлів які надходять в систему;

– запобігання витоку інформації здійснює контроль серверів зберігання шляхом співвідношення запитів від користувачів та аналізу відповідності до правил надання файлових сервісів в мережі;

– виявлення вторгнень здійснює контроль трафіку між мережевими пристроями шляхом пошуку та виявлення відхилень від нормального трафіку та визначення інших невідповідностей в області комутації трафіку між застосуваннями та обладнанням;

– внутрішня фільтрація трафіку призначена для обмеження доступу до мережевого обладнання та серверів сховища даних;

– фільтрація трафіку на межі здійснює контроль доступу до внутрішніх ресурсів мережі шляхом визначення невідповідностей правилам доступу та співвідношенням об’єктів доступу до списків небезпечних джерел;

– захист від атак відмови в обслуговуванні здійснює контроль надходження трафіку (запитів, сеансів, з’єднань) до мережевого обладнання в мережі. Основна задача - зупинити небажану розсилку до її надходження до серверів та інших кінцевих пристроїв.

Таким чином, розроблений комплекс заходів здійснює автоматизацію більшості типових задач щодо контролю та аналізу трафіку в мережі та визначення і сигналізації про відхилення в роботі мережевого обладнання або мережевих сервісів.

Додатково, необхідно забезпечити адміністраторів системи адекватними засобами сигналізації подій та візуалізації інформації про стан мережі та сервісів. Для цього використовуються системи моніторингу, які дозволяють контролювати та візуалізувати інформацію про задані параметри функціонування мережі та канали зв’язку для оперативного надходження інформації до адміністраторів (чат боти, канали та інше).

3.2 Захист від відмов в обслуговуванні

В ході функціонування хмарних сховищ даних виникають ситуації, коли система, або її окремі компоненти піддаються зовнішнім атакам типу “Відмова в обслуговуванні”. Для забезпечення захисту доступності інформації, що зберігається в системі, та компонент, на котрих вона зберігається необхідно забезпечити контроль інтерфейсів мережевого обладнання, зокрема:

– обсяг трафіку, який проходить через мережевий інтерфейс;

– довжина черги в буферах пам’яті інтерфейсу, або загальної пам’яті пристрою;

– підрахунок кількості пакетів від одного користувача або адреси;

– аналіз протоколів, які використовуються при здійсненні комунікації із зовнішніми мережами та системами.

1 Контроль внутрішніх інтерфейсів.

Для здійснення захисту від DDoS-атак внутрішніх ресурсів мережі зберігання даних, в системі використовується комплексна система аналізу інтерфейсів та трафіку, який через них проходить. Дана система контролює наступні мережеві рівні:

– мережевий рівень. Здійснюється аналіз мережевих пакетів, зокрема мережеві адреси джерела та призначення, для створення сутності “потік” та подальшого аналізу такого потоку;

– транспортний рівень. Аналіз флагів, які встановлені при створенні та підтримці сеансу зв’язку між застосуваннями та виявлення використовуваних застосувань з їх наступним аналізом.

Комплексність аналізу полягає в тому, що необхідно контролювати як інтерфейси комунікаційного обладнання (зокрема, комутаторів) так і на кінцевому обладнанні:

– контроль трафіку на інтерфейсах серверів зберігання даних;

– контроль (вибірковий) застосувань, які реалізовані на серверах зберігання;

– контроль інтерфейсів на комутаторах мережі зберігання даних.

Для цього використовуються такі базові інструменти, які вбудовані в функціонал операційних систем, як:

– утиліта TCPDump, яка дозволяє збирати інформацію з інтерфейсів серверів;

– журнали подій на серверах;

– утиліти, які контролюють запроси до сервісів серверу (mysqladmin).

Для додаткового контролю трафіку використовується протоколи та утиліти, які збирають інформацію про діяльність на комутаторах мережі:

– протокол Netflow, який дозволяє збирати інформацію про трафік на комутаторах, об’єднуючи їх в потоки;

– утиліта munin, яка дозволяє перетворювати інформацію на серверах та мережевому обладнанні у графіки.

Усі модулі, які використовуються для збору інформації, формують певну структуру даних, яка співвідносить інформацію, яка отримана з комутаторів з інформацією, яка отримана з інтерфейсів кінцевого обладнання. Це дозволяє співвідносити параметри трафіку, та виявляти аномалії у потоках даних між серверами та зовнішніми або внутрішніми мережевими компонентами.

Уся отримана інформація збирається та обробляється на колекторі, сервері, який автоматизує аналіз отриманих текстових даних, а також візуалізує передачу трафіка та інші параметри у графіки, які призначені для адміністраторів системи та кінцевих користувачів.

2 Контроль зовнішніх інтерфейсів

Якщо контроль внутрішніх інтерфейсів, в першу чергу, зосереджений на запобіганні виникнення атак відмов в обслуговуванні всередині мережі, контроль зовнішніх інтерфейсів мережевого обладнання забезпечує захист від зовнішніх атак. Хоча, слід зазначити, що частина механізмів, які було розглянуто раніше, також впливають на захист від зовнішніх загроз.

Основний захист від зовнішніх атак відмов в обслуговуванні зосереджений на межі сховища даних (рисунок 3.3):

– контроль трафіку, який надходить з мережі Інтернет здійснюється на двох комутаторах, які виконують функції ядра/розподілу;

шлюзи безпеки, які розташовані між ядром мережі та мережею Інтернет, виконують первинну фільтрацію трафіку, а також блокують загрози, які виявляються на етапі аналізу трафіку на рівні ядра/розподілу.

Для забезпечення контролю межі мережі виконуються основі функції адміністрування безпеки (рисунок 3.4):

– збір даних дозволяє акумулювати інформацію про стан мережевого обладнання, характеристики мережевого трафіку, мережевих сервісів;

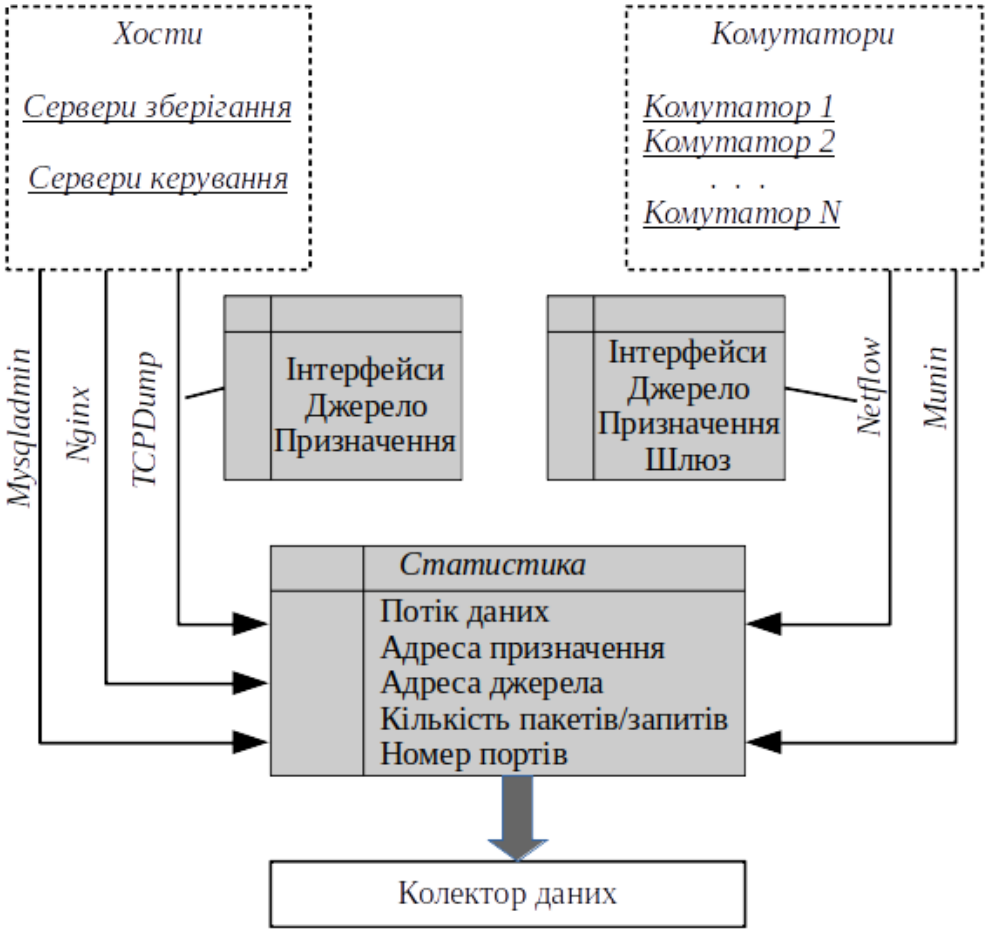

Рисунок 3.3 - Система внутрішнього контролю трафіку

– візуалізація дозволяє представляти отриману інформацію у зручному форматі для сприйняття або подальшого аналізу;

– інформування виконує функції передачі отриманих тригерів для своєчасної реакції на події в мережі;

– втручання передбачає певну реакцію на події в мережі автоматизовано або за участю адміністраторів.

Відповідно до цього, контроль кордону мережі, поділяється на активний та пасивний контроль. Пасивний контроль визначає заходи, які направлені на дії, що не вимагають активного втручання систем чи адміністраторів:

– колектори (syslog сервер) отримують та систематизують інформацію про стан мережевого обладнання;

– система моніторингу, на основі тригерів, які встановлено адміністратором, інформує про події на спеціальному дашборді, де надається основна інформацію про подію (хост, час, тривалість та інше);

– система моніторингу будує графіки використання ресурсів об’єктів, які на неї налаштовані (щільність мережевого трафіку на інтерфейсах обладнання, використання ресурсів процесору та пам’яті, наявність черг запитів до певних сервісів, які розгорнуті на обладнанні).

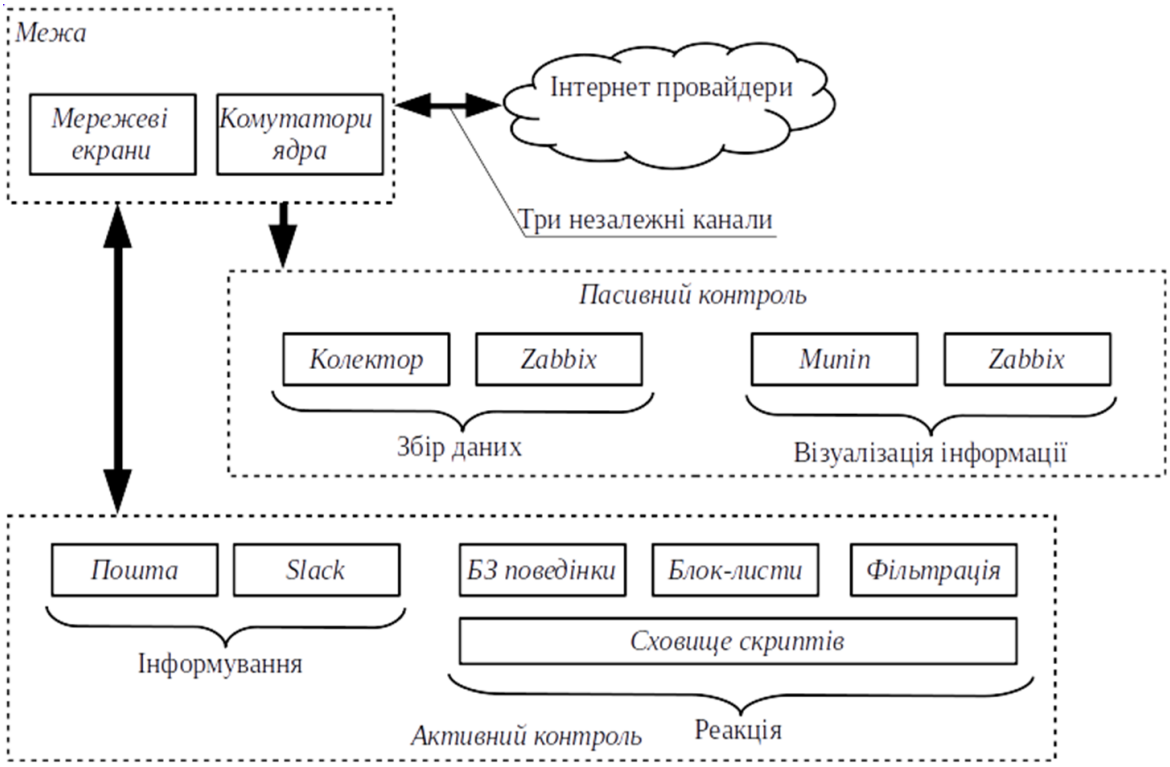

Рисунок 3.4 - Система між мережного контролю трафіку

Активний контроль визначає дії, які необхідно впровадити в разі виявлення відхилень в поведінці мережевих об’єктів або спрацьовування тригерів системи моніторингу. Інформування визначає засіб комунікації з адміністраторами системи та іншими відповідальними особами в разі виявлення загроз безпеці.

В рамках даного проекту визначено два типи інформування, які спрацьовують в залежності від тяжкості події:

– інформування електронною поштою виконується при визначенні подій будь-якої важкості, від інформування до критичного рівня. На пошту

визначених співробітників надсилаються повідомлення з текстом помилки, часовими мітками та іншою супутньою інформацією;

– інформування з використанням месенджерів дозволяє більш оперативно донести інформацію про виникнення події в системі. Тому, цей спосіб використовується в подіях які підпадають під рівень 5 та вище системи syslog з надсиланням короткої інформації про подію та посиланням на систему моніторингу для докладного вивчення.

3.3 Захист від небажаної розсилки

Небажана розсилка спричиняє затори на інтерфейсах серверів сховищ даних, переповнює пам’ять кінцевих станцій та мережевих пристроїв, створює додатковий мережевий трафік, що в сукупності може призвести до затримок в наданні сервісів. Серед основних загроз, які можуть спричиняти небажану розсилку, виявлено наступні:

– розсилка поштового спаму. Розсилка поштових повідомлень як до серверів мережі, так і від серверів до сторонніх поштових сервісів;

– спам-атаки на веб-сервіси мережі;

– розсилка службових повідомлень від кінцевих станцій (серверів);

– розсилка службових повідомлень від мережевих пристроїв.

Вирішуються задачі контролю подібного трафіку шляхом впровадження спеціалізованих систем або власних програм фільтрації та аналізу перехоплення мережевого трафіку.

1 Захист поштового сервісу. В рамках хмарних сховищ даних, поштова система надається як додатковий сервіс, а також приймає участь в аутентифікації користувачів:

– кожний користувач отримує унікальну адресу, яка асоціюється з його обліковим записом;

– поштова адреса використовується в двофакторній аутентифікації;

Виходячи з особливостей роботи поштової системи, існує ризик використання її як базу для спам розсилки, що може призвести до певних загроз та ризиків:

– попадання доменних імен, які використовуються в системі, до чорних списків;

– попадання мережевих адрес системи до чорних списків;

– блокування роботи мережі зберігання даних;

– блокування сервісів системи.

Для запобігання цих загроз використовується ряд заходів, які дозволяють контролювати черги поштових повідомлень, аналіз змісту поштових повідомлень та інше (рисунок 3.5).

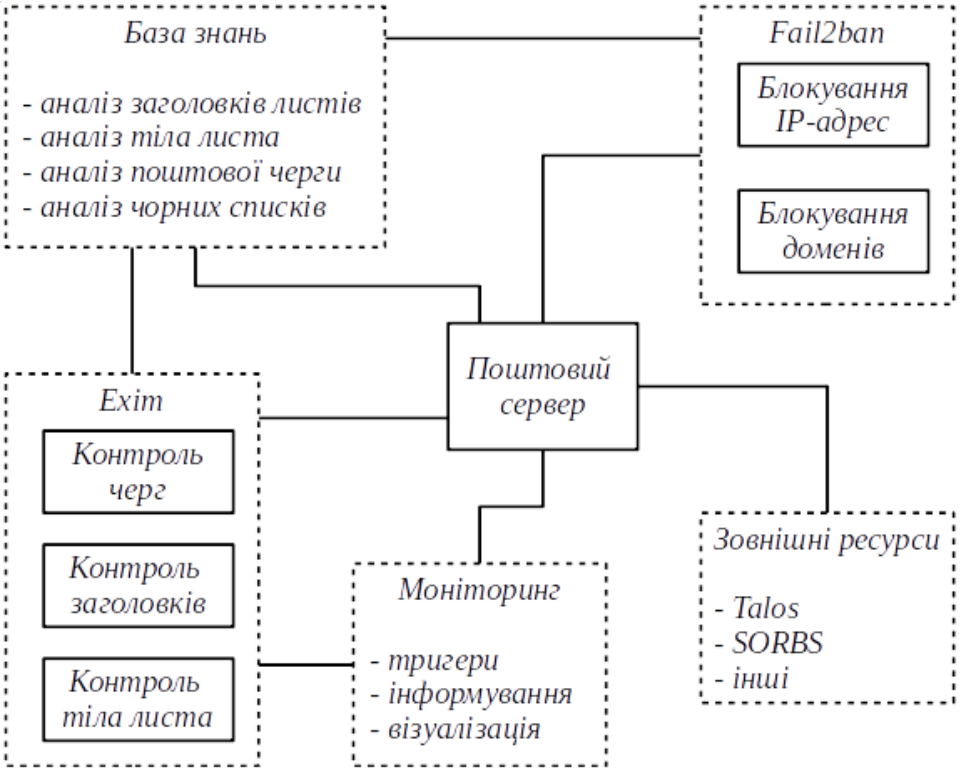

Рисунок 3.5 - Контроль поштової системи

Першим ешелоном захисту є сам поштовий сервіс, програмний інтерфейс якого дозволяє збирати інформацію про передачу повідомлень, зокрема:

– підрахунок поштової черги;

– отримання переліку поштової черги;

– зчитування заголовку повідомлення;

– зчитування тіла повідомлення.

Усі ці елементи дозволяють створювати тригери для системи моніторингу, яка інформує адміністраторів про виявлення відхилень в поведінці поштового сервісу. Агент системи моніторингу передає інформацію про функціонування сервісу до серверу моніторингу, де здійснюється контроль тригерів, візуалізація отриманої інформації, та інформування про перевищення заданих лімітів.

Іншим модулем який контролює безпеку поштового сервісу є fail2ban, який виконує функції програмного інтерфейсу до мережевого екрану та блокує внутрішні і зовнішні джерела небажаної розсилки, керуючись встановленими правилами або іншими командами адміністраторів.

На основі отриманого досвіду, адміністратори формують базу знань, яка містить стандартні, для цільової системи, скріпти, які автоматизують певні аспекти діяльності системи безпеки:

– аналіз вмісту поштових повідомлень (ключові слова, послідовності, семантичних аналіз);

– зчитування чорних листів із зовнішніх ресурсів;

– формування команд поштовому серверу, системі моніторингу.

Таким чином, захист поштового сервісу здійснюється послідовністю отримання інформації про стан системи, порівняння інформації з тригерами та, в разі необхідності, формування реакцій на події з використанням спроектованих скриптів.

2. Захист веб-системи. Веб-системи мережі зберігання використовуються для підтримки веб-сайтів організації та надання графічних сервісів для користувачів системи. Використання веб систем суттєво спрощує використання сервісів за рахунок інтерфейсо-орієнтованого підходу роботи з даними, проте створює додаткові ризики для загальної безпеки мережевої та інформаційної структури.

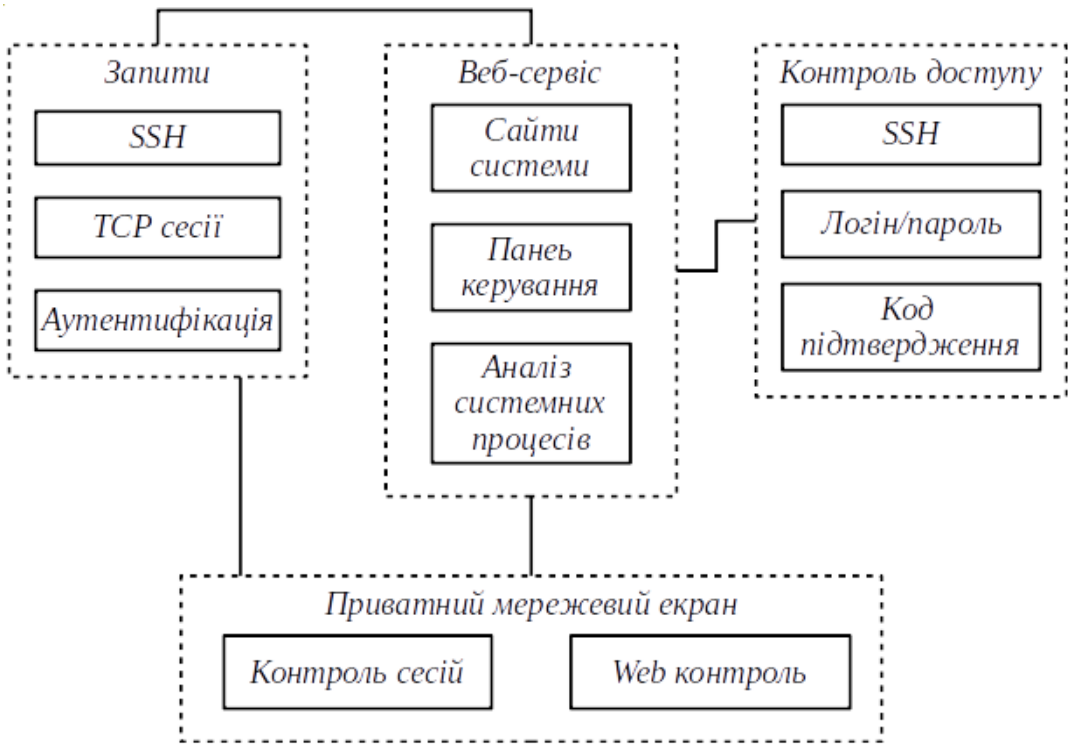

Рисунок 3.6 - Захист веб-системи сховища

Враховуючи, що веб система є однією з тих, що відкрита для доступу ззовні, вона знаходиться під постійним ризиком зламу та інших неправомірних дій. Відкритість веб сервісів вимагає приділення особливої уваги до забезпечення інформаційної безпеки. Основні ризики, які присутні для веб-системи мережі зберігання даних наступні:

– DDoS атака на веб-сервер системи;
– злам системи доступу до серверу;
– зміна інформації на сервері;
– зміна прав доступу користувачів.

Для забезпечення захисту від цих загроз, було прийнято використання кількох модулів операційної системи та кількох зовнішніх сервісів: приватний мережевий екран

3. Захист сховищ даних. Враховуючи, що основна функція системи, це обмін файлів, її робота пов’язана з інтенсивними потоками даних з серверами зберігання. Це сприяє створенню загроз по розсилці файлів, які призводять до наступних ризиків:

– завантаження файлів, які містять зловмисний код (розбиття на частини з подальшим збиранням);

– вичерпання виділеної дискової квоти користувача;

– циклічний перезапис файлів між серверами системи.

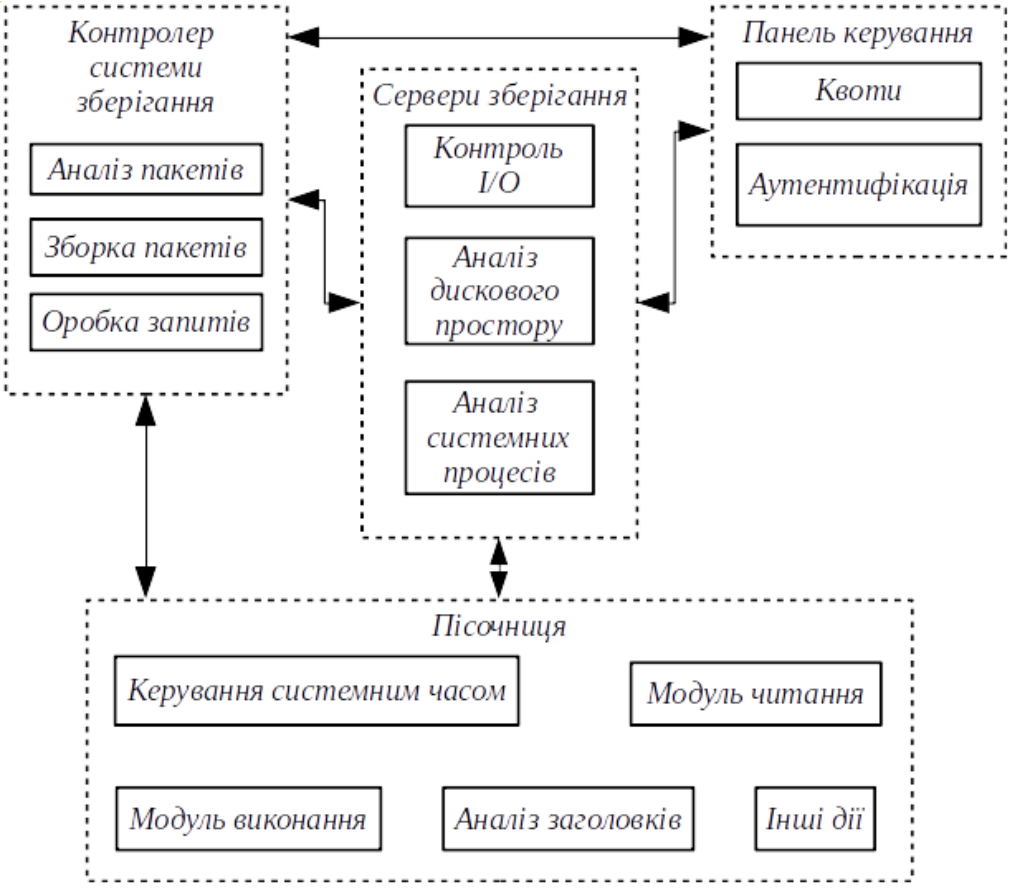

Рисунок 3.7 - Захист сховищ

Для того, щоб знизити ці ризики необхідне впровадження контролю за завантаженням та розсилкою файлів в системі зберігання даних, яка реалізує наступні функції:

– контроль квоти користувача дозволяє відслідковувати використання дискової підсистеми;

– контроль фрагментації файлів з метою виявлення завантаження частин зловмисного коду;

– контроль доступу до файлової системи користувачами системи з метою запобігання використання неавторизованого доступу до дискової підсистеми;

– використання “пісочниці” з метою аналізу вмісту файлів, які завантажуються.

3.4 Фільтрація трафіку

Фільтрація трафіку здійснюється задля обмеження доступу до ресурсів системи для користувачів та процесів, що в свою чергу забезпечує захист таких властивостей інформації як конфіденційність та цілісність.

Також, фільтрація трафіку дозволяє уникнути випадкового доступу до ресурсів особами, які не мають права з ними працювати.

Для забезпечення цих функцій, в мережі використовується два механізми фільтрації трафіку:

– списки контролю доступу забезпечують базові функції фільтрації всередині мережі. Зокрема, обмежується доступ до серверів зберігання та контролеру мережі;

– міжмережеві екрани здійснюють фільтрацію трафіка на мережевому та транспортному рівні. Зокрема, контролюється трафік на межі мережі зберігання.

Дані заходи забезпечують контроль доступу до пристроїв мережі і, в меншій мірі, для контролю трафіку до мережі Інтернет або з неї.

Списки контролю доступу застосовуються на комутаторах третього рівня, які забезпечують рівень розподілу в мережі зберігання. Враховуючи, що списки контролю доступу враховують лише мережеві адреси та порти, фільтрація буде здійснюватись на основі підмереж, створених для системи зберігання.

Для пакетної фільтрації використовуються іменовані списки, які дозволяють легко ідентифікувати призначення списку та об’єкти його застосування. Будь-які правила фільтрації, за замовчуванням, завершуються правилом фільтрації будь-якого трафіку. Таким чином, першими аналізуються правила дозволу, після чого блокується інший трафік.

Для керування доступом використовуються адреси, які призначені внутрішнім хостам мережі.

Додатково, списки контролю доступу використовуються в наступних задачах підтримки мережевих сервісів:

– фільтрація внутрішніх та зовнішніх маршрутів мережі;

– організація VPN каналів мережі.

В даних випадках списки специфікують мережі або хости, які використовуються для передачі даних.

Мережеве екранування здійснюється виділеними пристроями на межі мережі. Так як мережа має три мережевих з'єднання з Інтернет, використовується три окремих шлюза екранування трафіку. Фільтрація трафіку здійснюється за рахунок використання політик безпеки, визначених адміністратором інформаційної безпеки. Даний підхід дозволяє описувати бажану поведінку в мережі зберігання без виявлення шаблонів, сигнатур, аномалій та інших засобів, які вимагають постійного контролю, проектування та оновлення. Загальна система фільтрації представлена на рисунку 3.8.

Уся мережа поділена на зони довіри:

– зона низької довіри призначена інтерфейсам, які реалізують підключення безпосередньо до мережі Інтернет;

– демілітаризована зона визначає середній рівень довіри і призначена для використання систем, до котрих необхідно мати доступ як з середини мережі, так і з мережі Інтернет;

– до довіреної зони віднесені всі сервери системи зберігання даних;

– до транзитної зони відносяться всі комунікаційні пристрої мережі.

Формально, ця зона також визначається як внутрішня довірена зона.

Політика фільтрації визначає базові дії, щодо трафіку в мережі, зокрема:

– весь трафік з недовіреної зони до довіреної заблоковано за замовчуванням;

– весь трафік з довіреної зони до інших дозволено за замовчанням;

– весь трафік з демілітаризованої зони до недовіреної дозволено;
– весь трафік з демілітаризованої зони до довіреної підлягає інспекції.

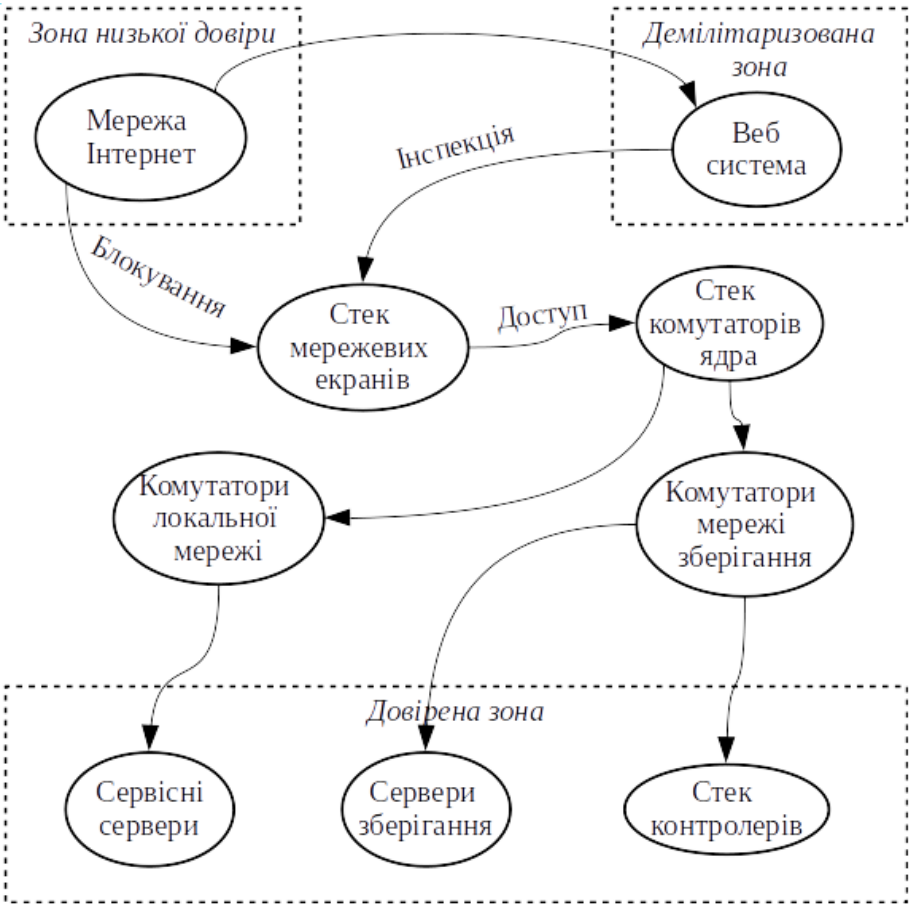

Рисунок 3.8 - Система фільтрації трафіку

Кожному інтерфейсу мережевих екранів, котрі призначені до певної зони надається значення пріоритету, який визначає ступінь довіри. На основі цих пріоритетів визначено, що зона з низьким рівнем довіри не може мати доступ до мережі, ступінь довіри якої вище.

3.5 Інтерфейс аналізу захищеності мережі

Для керування всіма зазначеними вище аспектами безпеки, було спроектовано програмний інтерфейс керування та аналізу безпеки хмарних сховищ даних. З використанням даного інтерфейсу здійснюються наступні функції адміністраторів (рисунок 3.9) системи:

– збір комплексних даних про трафік в мережі;

– збір комплексних даних про стан мережевого та кінцевого обладнання;

– візуалізація отриманих даних;

– візуалізація виявлених помилок (dashboard);

– сигналізація про події;

– інтерфейс доступу для налаштування обладнання.

Візуальна частина інтерфейсу дозволяє отримувати графіки, які визначають стан мережевого обладнання, серверів, мережевого трафіку та сервісів. Також ця частина формує список повідомлень про відхилення параметрів функціонування системи від заданих тригерами, правилами, системними змінними:

– система моніторингу zabbix дозволяє здійснювати візуалізацію широкий діапазону параметрів, включаючи характеристики трафіку, доступність пристроїв та сервісів мережі зберігання;

– система моніторингу zabbix, на основі тригерів, інформує адміністраторів систем про наявність відхилень з використанням поштової системи та системи slack;

– система grafana візуалізує характеристики серверів;

На термінальних серверах мережі здійснюється підключення до пристроїв в мережі з ціллю отримання додаткової інформації про помилки або для здійснення його конфігурації. Для цього використовуються два способи:

– система Ansible дозволяє здійснювати одночасні глобальні операції на серверах та інших пристроях.

– індивідуальне підключення до конкретного пристрою здійснюється з використанням протоколу SSH;

Під глобальними операціями розуміється, наприклад, масове оновлення програмного забезпечення, завантаження типових пакетів та інші операції, які однакові і мають бути здійснені на великої кількості пристроїв.

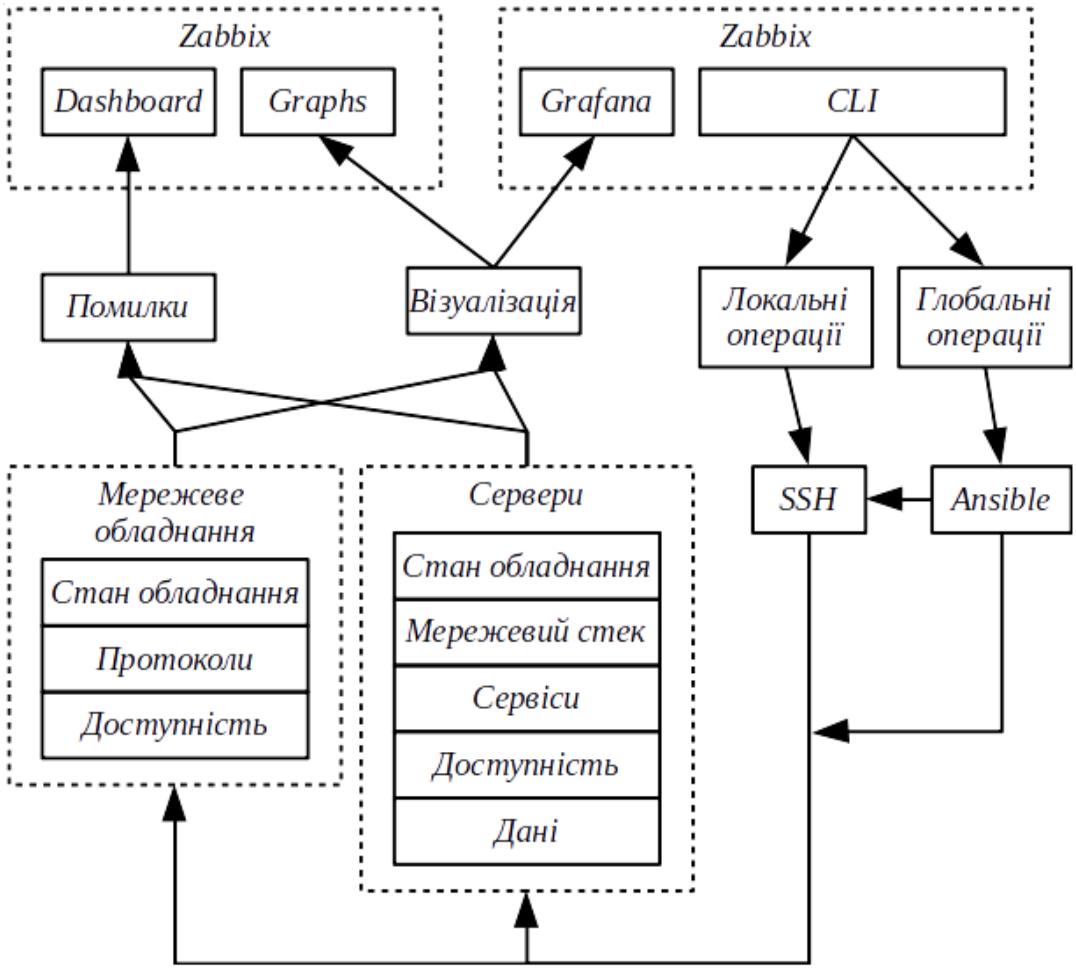

Рисунок 3.9 - Інтерфейс адміністратора

Індивідуальне підключення здійснюється з використанням асиметричного шифрування, що не вимагає введення логінів та паролі кожного підключення. Це дозволяє автоматично з інтерфейсу адміністратора здійснювати консольне підключення до пристрою, з яким потрібно працювати.

3.6 Виявлення зловживань

Враховуючи, що в мережі зберігаються і обробляються дані клієнтів, які мають доступ до підсистем мережі, необхідно забезпечити захист від зловживань в мережі її клієнтами. До зловживань в сховищах даних, в даному проекті віднесено наступні дії:

– завантаження виконавчих файлів (віруси, скрипти та ін.);

– завантаження файлів до інших користувачів;

– завантаження конфігурацій до мережевого обладнання;

– сканування мережі та її пристроїв;

– несанкціонований доступ;

– несанкціонована вивантаження даних;

– інші дії, які не асоційовані з обліковим записом користувача.

Для забезпечення контролю над подібними ризиками втручання в роботу системи необхідно здійснювати аудит дій користувачів, обладнання та процесів на кінцевих хостах. Для цього в проекті передбачено три основних механізми захисту:

– система виявлення вторгнень забезпечує моніторинг поведінки трафіку від кожного користувача з ціллю визначення аномалій в мережевому трафіку;

– антивірусний захист забезпечує контроль кінцевих станцій мережі, зокрема, контроль процесів на хості, виконання задач на хості та інше;

– система запобігання витоків інформації, контролює ризики копіювання та передачі інформації за межі сховищ даних.

Кожна з цих систем є окремим модулем, що дозволяє в майбутньому модифікувати кожний з них, або замінювати більш сучасним.

В якості антивірусного захисту використовується програмне забезпечення ClaimAV, яке є вільним для використання та найчастіше використовується в Linux-системах на серверах.

Захист здійснюється за використанням наступних модулів:

– БД містить усі завантаженні шаблони шкідливого програмного забезпечення, з якими порівнюється поведінка об’єктів системи. Тут також містяться профілі, які використовуються вбудованою системою виявлення вторгнень;

– клієнт завантаження здійснює контроль актуальності баз даних, формує запити на їх оновлення, контролює цілісність шаблонів;

– контроль процесів здійснює перевірку діяльності системних процесів хоста на виявлення шаблону поведінки вірусів та інших видів ПО;

– контроль програм здійснює перевірку програм за переліком, який створено адміністраторами. Визначаються шаблонні поведінки, ресурси з якими взаємодіє програм;

– контроль трафіку здійснює перевірку мережевого трафіку хоста;

– модуль DLP виконує функції по запобіганні витоків інформації з серверів системи;

– пісочниця виконує підозрілі файли та процеси в ізольованому середовищі з ціллю визначення приналежності об’єкту до шкідливого типу ПО.

ВИСНОВКИ

В ході дипломного проектування було розроблено структуру комплексного захисту інформації в хмарних сховищах даних. Система використовується в приватному секторі бізнесу, для зберігання даних організації-власника мережі, та її партнерів.

В ході проектування було визначено основні напрями забезпечення захисту конфіденційності, цілісності та доступності інформації:

– контроль доступу до ресурсів мережі зберігання, який передбачає багатоетапну аутентифікацію користувачів в системі;

– подальший контроль дій користувачів в системі та процесів, які з ними пов’язані;

– багаторівнева фільтрація трафіку, яка полягає у модулях пакетної фільтрації, фільтрації за контентом та фільтрації на основі репутації;

– активний моніторинг мережі зберігання з використанням систем виявлення вторгнень та систем запобігання витоків інформації;

– контроль кінцевих пристроїв мережі з використанням персональних мережевих екранів та антивірусного програмного забезпечення;

– резервування каналів трафіку;

– резервування даних на кінцевих пристроях та на окремих серверах.

Усі ці заходи повинні забезпечити активний контроль подій в мережі зберігання даних, забезпечення конфіденційності та цілісності інформації, а також гарантувати доступність вузлів мережі та, відповідно, даних, які на них зберігаються.

Основними перевагами запропонованого проекту є використання, в більшості випадків, вільного програмного забезпечення, від операційних систем до спеціалізованого програмного забезпечення, висока доступність

вузлів мережі, незалежність від конкретного зовнішнього провайдеру та низький час відклику на запити від користувачів.

До недоліків розробленої системи можна віднести велику кількість модулів та складну структуру їх взаємодії, що може призвести до складнощів в уніфікації організації сховищ даних. Однак, використання єдиного інтерфейсу адміністратора призначене для зменшення впливу подібних недоліків.

Подальший розвиток даної системи полягає в модернізації систем контролю та виявлення вторгнень за рахунок використання систем штучного інтелекту, зокрема машинного навчання та систем прийняття рішень.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Рибальский О.В., Хахановський В.Г., Кудінов В.А. Основи інформаційної безпеки та технічного захисту. // Інформації посібник для курсантів внз мвс україни – 2012 - [Електронний ресурс] URL: https://nni1.naiau.kiev.ua/files/KIT/posibnuk%20tzi.pdf

2. Боршевников, А. Е. Сетевые атаки. Виды. Способы борьбы / А. Е. Боршевников. // Современные тенденции технических наук: материалы I Междунар. науч. конф. — 2011. — [Електронний ресурс] URL: https://moluch.ru/conf/tech/archive/5/1115/

3. Гаврильців М.Т. Інформаційна безпека держави в системі національної безпеки україни – 2020 - [Електронний ресурс] URL: http://lsej.org.ua/2_2020/54.pdf

4. Антон Калинин. Техники использования DNS в атаках вредоносных программ – 2020 - [Електронний ресурс] URL: https://www.anti-malware.ru/analytics/Threats_Analysis/Using-DNS-in-malware-attacks

5. О. Бондаренко, І. Ушкаленко. Безпека web-додатків: актуальні проблеми та їх аналіз – 2017 - [Електронний ресурс] URL: http://repository.vsau.org/getfile.php/17100.PDF

6. Карачка А.Ф. Технології захисту інформації – 2017 - [Електронний ресурс] URL: http://dspace.wunu.edu.ua/bitstream/316497/26564/1/lekzii.pdf

7. К. В. Мілян, Ю. І. Грицю. Особливості організації інформаційної безпеки корпоративної мережі промислової компані – 2013 - ресурс] URL: http://surl.li/cerfb

8. Олександр Архипов, Євгенія Архипова. Особливості розуміння понять «інформаційна безпека» та «безпека інформації» - 2014 - [Електронний ресурс] URL: http://ktpu.kpi.ua/wp-content/uploads/2016/02/st-14_AA_Osoblivosti-rozuminnya-IB_BI.pdf