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

ШЕВЧЕНКО Валентина Анатоліївна

КВАЛІФІКАЦІЙНА РОБОТА МАГІСТРА

ДОСЛІДЖЕННЯ МЕТОДІВ ЗАХИСТУ ДАНИХ ЛАБОРАТОРІЇ З ВІДДАЛЕНИМ ДОСТУПОМ. ДОСТУПНІСТЬ

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

Керівник: Мартинюк Олександр Миколайович,
К.т.н, доцент кафедри КІСМ

Одеса – 2021

З А В Д А Н Н Я

НА ДИПЛОМНИЙ ПРОЕКТ (РОБОТУ) СТУДЕНТУ

Шевченко Валентина Анатоліївна
(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) Дослідження методів захисту даних лабораторії з віддаленим доступом. Доступність.

керівник проекту (роботи) Мартинюк О.М к.т.н., доцент,
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом ректора ОНПУ від "__"____11_____2021_ року №_

2. Строк подання студентом проекту (роботи) 01.12.2021

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

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) 1 Технології захисту даних в лабораторіях з віддаленим доступом
2 Дослідження методів забезпечення захисту даних інформаційних систем
3 Методи забезпечення доступності інформаційних систем

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень)
Характеристика роботи, Заходи та механізми, що забезпечують доступність, Архітектура лабораторії з віддаленим доступом, Загальна модель забезпечення доступності ІС, Апаратна модель забезпечення доступності, Вплив апаратної моделі на доступність. Опис параметрів, Програмна модель захисту інформації, Опис параметрів програмної моделі, Модель контролю трафіку, Система міжмережного контролю трафіку, Модель захисту веб-системи мережі, Метод захисту доступності, Оцінка забезпечення доступності. Висновки

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
1	Технології захисту даних в лабораторіях з віддаленим		
	доступом		
2	Дослідження методів забезпечення захисту даних		
	інформаційних систем		
3	Методи забезпечення доступності інформаційних систем		

Студент _____ _____
(підпис) (прізвище та ініціали)

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

Відомість кваліфікаційної роботи бакалавра

№ рядка	Найменування	Кільк.	Примітка
1	Пояснювальна записка	69	
2	Характеристика роботи	1	
3	Заходи та механізми, що забезпечують доступність	1	
4	Архітектура лабораторії з віддаленим доступом	1	
5	Загальна модель забезпечення доступності ІС	1	
6	Апаратна модель забезпечення доступності	1	
7	Вплив апаратної моделі на доступність. Опис параметрів	1	
8	Програмна модель захисту інформації	1	
9	Опис параметрів програмної моделі	1	
10	Модель контролю трафіку	1	
11	Система міжмережного контролю трафіку	1	
12	Модель захисту веб-системи мережі	1	
13	Метод захисту доступності	1	
14	Оцінка забезпечення доступності. Висновки	1	
15			
16			
17			
18			
19			
20			
21			
22			
23			
24			

АМДП.АМ161м.2020

Зм.	Лист	№ докум.	Підпис	Дата
Розробив		Шевченко В.А		
Перевірив		Мартинюк О.М		
Реценз.				
Н. Контр.				
Затвердив				

Дослідження методів захисту даних лабораторії з віддаленим доступом. Доступність

Літ.	Лист	Листів
	1	1

«Одеська політехніка»

ІКС КІСМ АМ161м

АНОТАЦІЯ

Шевченко В.А. Дослідження методів захисту даних лабораторії з віддаленим доступом. Доступність – кваліфікаційна робота магістра. Одеса, 2021: 69стр., 10 рис., 9 джерел.

Об'єкт дослідження – процес оцінки доступності даних інформаційних систем..

Предмет дослідження – лабораторії з віддаленим доступом.

Дана робота присвячена дослідженню існуючих систем захисту інформації в інформаційних системах. В роботі розглянуто питання забезпечення доступності даних в лабораторії з віддаленим доступом.

Основні кроки для досягнення мети – це дослідження існуючих технологій створення віртуальних лабораторій, засобів організації доступу до віддалених лабораторій та протоколів віддаленого доступу, дослідження методів захисту даних та забезпечення доступності, розробка моделей захисту даних від поширених атак на доступність, розробка методу забезпечення захисту доступності.

В результаті дослідження запропонований метод забезпечення захисту доступності даних в інформаційних системах, зокрема в лабораторії з віддаленим доступом. Метод включає в себе кооперацію апаратних та програмних засобів захисту даних.

ІНФОРМАЦІЙНА БЕЗПЕКА, СИСТЕМИ ВИЯВЛЕННЯ ВТОРГНЕНЬ, АНТИВІРУСНИЙ ЗАХИСТ, МОДЕЛІ ЗАХИСТУ ДАНИХ, ДОСТУПНІСТЬ

ABSTRACT

Shevchenko V.A. Research of the laboratory with remote access data protection methods. Accessibility is a master's degree. Odessa, 2021: 69 pages, 10 figures, 9 sources.

Object of research - the process of assessing the availability of data information systems ..

The subject of research - laboratories with remote access.

This work is devoted to the study of existing information security systems in information systems. The paper considers the issue of ensuring the availability of data in the laboratory with remote access.

The main steps to achieve this goal are the study of existing technologies for creating virtual laboratories, means of organizing access to remote laboratories and remote access protocols, research on data protection and accessibility methods, development of data protection models against common access attacks, development of security protection methods.

As a result of research the method of maintenance of protection of availability of data in information systems, in particular in laboratory with remote access is offered. The method includes the cooperation of hardware and software data protection.

INFORMATION SECURITY, INVASION DETECTION SYSTEMS, ANTI-VIRUS PROTECTION, DATA PROTECTION MODELS, AVAILABILITY

ЗМІСТ

ВСТУП

В сучасних умовах функціонування бізнесу, дуже важливу роль відіграє використання інформаційних технології та систем, які вже виступають як невід’ємна частина бізнес-процесів організації.

Лабораторії з віддаленим доступом являє собою програмно-апаратний комплекс, що дозволяють проводити досліди без безпосереднього контакту з реальною установкою або при повній відсутності такої. У першому випадку ми маємо справу з так званої лабораторної установкою з віддаленим доступом, до складу якої входить реальна лабораторія, програмно-апаратне забезпечення для управління установкою і візуалізації отриманих даних, а також засоби комунікації. У другому випадку процеси моделюються за допомогою комп'ютера та встановленого програмного забезпечення.

Необхідність створення віртуальних лабораторій з віддаленим доступом в галузі освіті виникла у зв'язку з труднощами застосування в деяких випадках реальних лабораторій. Віртуальні лабораторії з віддаленим доступом володіють наступними перевагами в порівнянні з реальними:

– відсутність необхідності придбання дорогого обладнання;

– можливість проникнення в тонкощі процесів і спостереження відбувається в іншому масштабі часу, що актуально для процесів, що протікають за частки секунди або, навпаки, що тривають протягом декількох років;

– безпека підключення та захист даних є важливим плюсом використання віртуальних лабораторій з віддаленим доступом;

– у зв'язку з тим, що управлінням віртуальним процесом займається комп'ютер, з'являється можливість швидкого проведення серій

дослідів з різним значенням вхідних параметрів, що часто необхідно для визначення залежностей вихідних параметрів від вхідних;

– деякі роботи вимагають подальшої обробки досить великих масивів отриманих цифрових даних, які виконуються на комп'ютері після проведення серії експериментів. Слабким місцем у цій послідовності дій при використанні реальної лабораторії є введення отриманої інформації в комп'ютер. У віртуальній лабораторії цей крок відсутній, так як дані можуть заноситися в електронну таблицю результатів безпосередньо при виконанні дослідів користувачем або автоматично. Таким чином, заощаджується час і значно зменшується відсоток можливих помилок;

– можливість використання віртуальної лабораторії в дистанційному навчанні, коли в принципі відсутня можливість роботи в лабораторіях університету.

На жаль, кількість існуючих на даний момент віртуальних лабораторій, що застосовуються в навчальному процесі, досить мале. Це пов'язано, в першу чергу, з дорожнечею їх розробки, що призводить до наступних наслідків:

– віртуальні лабораторії, розроблені професійними програмістами, дизайнерами та спеціалістами, моделюється області, коштують дуже дорого, що заважає їх широкому поширенню. З іншого боку, малі можливості поширення створюють малі стимули для їх виробництва;

– створення віртуальних лабораторій непрофесіоналами може призвести до задовільних результатів лише при моделюванні вузького класу явищ. Їх поширення пов'язано з невисокою вартістю і практичною відсутністю альтернатив.

Звичайно, віртуальним лабораторіям притаманні деякі недоліки, головним з них є відсутність безпосереднього контакту з об'єктом дослідження, приладами та апаратурою. Досвід роботи з реальними приладами необхідний, тому розумним рішенням буде поєднання

використання реальних і віртуальних лабораторій в освітньому процесі з урахуванням притаманним їм переваг та недоліків.

Важливою складовою функціонування таких лабораторій є забезпечення безпеки даних, тому що порушення однієї зі складових тріади безпеки інформації призводить до наступних наслідків:

– моральні збитки для власників даних;
– розголошення приватних даних;
– викривлення інформації, що зберігається;

Визначення методів захисту даних дозволяє:

– організовувати розмежування доступу;
– проводити фільтрацію мережевого трафіку;
– проводити шифрування та контроль цілісності даних;
– контролювати виток даних;
– розпізнавати зловживання та втручання в системи зберігання;
– проводити 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 дослідження та розробка організаційних заходів щодо забезпечення захисту інформації, які регламентують основні правила використання системою, зони відповідальності, спеціальні уточнення для певних груп користувачів та інше.

Метою магістерської кваліфікаційної роботи є підвищення доступності даних в задачах забезпечення захисту даних в лабораторіях з віддаленим доступом, шляхом дослідження існуючих методів та розробки моделей процесів порушення безпеки.

Для досягнення поставленої мети ставляться наступні задачі:

– дослідити типи віртуальних лабораторій;

- визначити архітектуру лабораторії з віддаленим доступом;

- провести аналіз існуючих методів, моделей та стандартів оцінки захисту даних, які використовуються в галузі інформаційної безпеки;

- провести дослідження засобів доступу до подібних лабораторій;

– визначити засоби захисту даних та типи дані, що підлягають захисту;

- визначити поняття доступності;

- розробити моделі забезпечення захисту даних в інформаційних системах;

- розробити загальну систему забезпечення доступності

Об'єкт дослідження – процес оцінки доступності даних інформаційних систем..

Предмет дослідження – лабораторії з віддаленим доступом.

Методи дослідження. Основними методами дослідження були теорія графів, теорія множин, математична статистика.

Наукова новизна полягає у розвитку моделей аналізу та оцінки захищеності даних в дистанційних інформаційних системах, які використовуються при передачі даних та підключенні до лабораторій з віддаленим доступом.

Практичне значення отриманих результатів. Розроблені моделі та мотод були реалізовані для оцінки якості інформаційної безпеки, використання їх дозволить підвищити доступність даних при використанні методу в лабораторії з віддаленим доступом

Публікації. Початкові результати, одержані у кваліфікаційній роботі магістра, опубліковані на XI міжнародній науковій конференції студентів і молодих учених «Сучасні інформаційні технології» / «Modern Information Technology» (13-14 травня 2021 р.) Державного університету «Одеська політехніка» як тези конференцій.

В першому розділі розглянуті питання віртуальних лабораторій. Для визначення питань безпеки спочатку розглянуті типи віртуальних лабораторій, їх призначення та особливості. Окрема увага приділяється типу

лабораторій з віддаленим доступом, оскільки поняття віртуальна лабораторія досить об’ємне, тому необхідно поставити завдання в більш конкретному випадку. Так як лабораторія в навчальному закладі має фізичне розташування та фізичне обладнання, до якого необхідно мати доступ для проведення експериментів тому тип віртуальної лабораторії з віддаленим доступом найбільш підходить. Коли визначено який тип лабораторії, то проводиться дослідження з визначення підходящою архітектурою. Також в першому розділі необхідно було дослідити технології віддаленого доступу, для того, щоб зрозуміти яким чином буде проведено підключення до лабораторії, яким чином буде користувач отримувати доступ до неї, яким чином він буде працювати. Виходячи з цих вимог було визначено основну технологію віддаленого доступу – це технологія віддаленого робочого столу. Цей підхід має ряд недоліків, таких як постійне підключення та контроль за підключеннями, але й ряд переваг, однієї з яких є простота з’єднання та готові рішення. Наступним кроком було дослідження протоколів для організації віддаленого доступу. Оскільки визначена технологія віддаленого доступу вже вбудована в ОС, та сучасні браузери тому вона має вже свої вбудовані засобі та протоколи організації віддаленого доступу. Для подібного підключення потрібно використовувати вже існуючи додатки та ПЗ.

Другий розділ кваліфікаційної роботи присвячений дослідженню методів захисту даних в інформаційних системах. В темі кваліфікаційної роботи акцент поставлений на захист даних лабораторії з віддаленим доступом. В першому розділі визначились з поняттям лабораторії з віддаленим доступом, з основними складовими елементами, та визначили, що як і інша будь яка система – робота лабораторії з віддаленим доступом це складова інформаційної системи. Тому щоб зрозуміти захист даних лабораторії необхідно дослідити технології та засоби захисту даних в інформаційних системах, дослідити та визначити методи, використання котрих в роботі з інформаційними системами забезпечують захист даних.

Перед початком дослідження необхідно поставити завдання до дослідження, конкретизувати мету дослідження та визначити кроки для вирішення задач для досягнення поставленої мети Першим кроком була розробка моделі архітектури лабораторії з віддаленим доступом, поділені складові частини на логічні групи та наведена структура підключення. . Другим кроком було дослідження засобів організації доступу до лабораторії з віддаленим доступом та захисту даних в ній у заданій архітектурі. Для визначення та розробки моделей захисту даних також необхідно розібратись в основних поняттях та визначеннях та наведені основні, що будуть використовуватись при створенні моделей.

В останньому розділі роботи наведені моделі захисту даних при різних умовах, а також акцентовані на забезпечені доступності даних в інформаційних системах. Сформована математична модель доступності. Визначені основні складові: програмна та апаратна. Наведені моделі організаційних заходів забезпечення доступності. Сформована найвідоміша атака - це «відмова в обслуговуванні», та розроблена модель захисту від атаки. Розроблені моделі захисту даних від атак небажаної розсилки, таких як захист поштового сервісу, захист веб-систем та захист сховищ. Для загального розуміння принципів захисту досліджено та розроблено модель по виявлено зловживань. Досліджено основний підхід до забезпечення доступності – резервування, визначено принцип цього підходу, розроблені моделі резервування даних як в апаратній частині так і в програмній.

Наприкінці роботи наданий комплексний підхід до забезпечення доступності, де по крокам надані основні моменти, що необхідно виконати для отримання добрий результатів з захисту доступності даних. Наведені результати дослідження у висновках.

1 ТЕХНОЛОГІЇ ЗАХИСТУ ДАНИХ В ЛАБОРАТОРІЯХ З ВІДДАЛЕНИМ ДОСТУПОМ

1.1 Архітектура лабораторій віддаленого доступу

Конфігурація типової лабораторії для дистанційного лабораторного практикуму включає центральний сервер, який координує роботу десятка персональних комп’ютерів, локальних та віддалених споживачів, та використовує інфраструктуру віртуальних робочих столів VDI за допомоги засобів віртуалізації Hyper-V.

Система дистанційного лабораторного практикуму може бути використана для певного кола дослідницьких завдань або промислових технологій.

Найпростіша конфігурація дистанційного лабораторного практикуму включає лабораторну установку з електронним управлінням, веб-камеру за бажанням, інтерфейс для передачі даних з установки на комп'ютер та сервер, через який забезпечує зв'язок з робочим місцем клієнта, приєднаним до мережі інтернету. На комп'ютері клієнта встановлено програмне забезпечення, яке дозволяє працювати з експериментальною установкою, прочитувати експериментальні дані і обробляти ці дані (обробка може відбуватися також off-line).

Подібні системи можуть використовуватися для отримання, обробки та зберігання експериментальних даних одночасно кількома групами дослідників і фізичними особами, які перебувають на значній відстані.

Такий підхід вимагає, звичайно, досягнення певної культури проведення експериментів та навиків роботи з такими лабораторіями, що в

подальшому може дозволити значно збільшити мережу таких лабораторії, а також організовувати ефективний обмін та обробку даних.

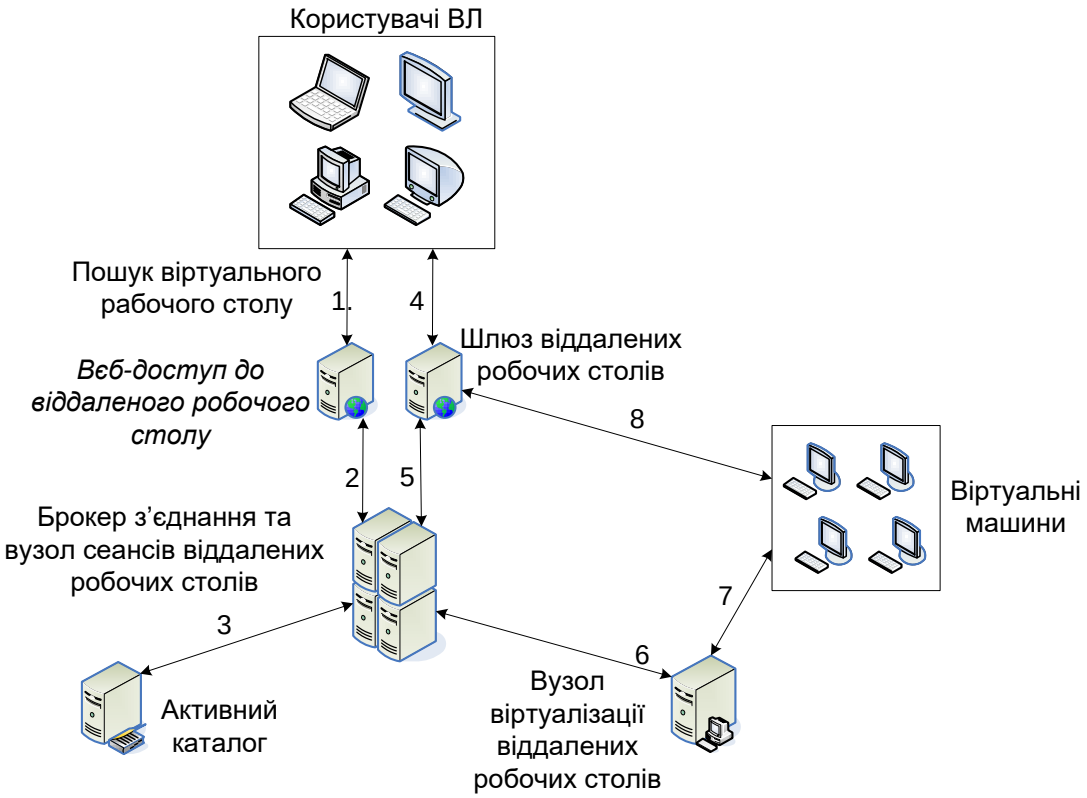

Рисунок 1.1 – Організація багатокористувацького доступу

Наданий шаблон віртуальної лабораторії з віддаленим доступом для пред'явлення відмінного результату з точки зору безпеки та відмово стійкості має мати: доступні інтерфейси та визначені протоколи передачі даних між сервером, користувачами та лабораторною установкою – стендами.

1.2 Дослідження технології віддаленого доступу до систем

Віддалений доступ до мережі лабораторії - це технологія віддаленого доступу зі складу служби маршрутизації та віддаленого доступу, включеної в ОС.

Віддалений доступ до мережі дозволяє користувачам віддаленого доступу підключатися до сервера віддаленого доступу за допомогою інфраструктури глобальної мережі (WAN).

1.2.1 Віддалений доступ до мережі на платформі Windows.

Підключення віддаленого доступу містить наступні компоненти:

- Клієнт віддаленого доступу.

- Сервер віддаленого доступу - приймає підключення віддаленого доступу і переадресує пакети між клієнтами віддаленого доступу і мережею, за якою закріплений сервер віддаленого доступу.

- Інфраструктура глобальної мережі. Фізичне або логічне з'єднання між сервером і клієнтом віддаленого доступу забезпечується обладнанням для віддаленого доступу до мережі, встановленому на клієнті і сервері віддаленого доступу, а також інфраструктурою глобальної мережі. Специфіка обладнання віддаленого доступу та інфраструктури глобальної мережі залежить від типу підключення.

1.2.2 Віддалений доступ з використанням віртуальних робочих столів (VDI)

Роль сервера "Служби віддалених робочих столів" надає технології, які дозволяють користувачам підключатися до віртуальних робочих столів, користуватися віддаленими програмами за допомогою додатків RemoteApp і робочих столів на основі сеансів або віртуальних машин. Служби віддалених робочих столів надають користувачам доступ до віддалених підключень з мережі організації або з Інтернету.

Служби віддалених робочих столів забезпечують поліпшену підтримку наступних сценаріїв:

- Розгортання інфраструктури віртуальних робочих столів.
- Розгортання віртуалізації сеансів.
- Централізована публікація ресурсів.
- Всебічну взаємодію з користувачем через протокол віддаленого робочого столу (RDP).

1.2.3 Розгортання інфраструктури віртуальних робочих столів (VDI)

Служби віддалених робочих столів пропонують нові способи ефективного налаштування віртуальних робочих столів та управління ними:

- єдина централізована взаємодія;

- автоматизоване і просте управління з єдиним образом – автоматизація методів розгортання та управління віртуальними робочими столами у складі пулу за допомогою шаблону віртуального робочого столу.

- персоналізація користувача - використання дисків та профілів користувачів, щоб захистити персональні налаштування користувача при розгортанні віртуальних робочих столів у складі пулу.

- менш дороге сховище - використання для віртуальних робочих столів у складі пулу недорогого локального сховища з функцією динамічної міграції між головними комп'ютерами. Особисті віртуальні робочі столи можуть використовувати менш дороге центральне сховище SMB .

1.2.4 Розгортання віртуалізації сеансів

Розгортання віртуалізації сеансів в службах віддалених робочих столів пропонує нові способи ефективного налаштування робочих столів на основі сеансів та управління ними. У колишніх версіях служб віддалених робочих столів поточне управління серверами вузлів сеансів віддалених робочих столів здійснюється на рівні сервера. Сценарій розгортання віртуалізації сеансів дозволяє використовувати централізоване управління та встановлення. Віртуалізація сеансів має наступні переваги:

- централізована взаємодія - це можливість швидко розгорнути віртуалізацію сеансів і управляти розгортанням.

- спрощене і централізоване розгортання - проста установка на базі сценарію, дозволяє створити відразу цілу колекцію сеансів.

- персоналізація користувача - диски профілів користувачів дозволять зберегти персональні параметри користувачів для колекцій сеансів.

- централізоване керування - керування усіма серверами вузлів сеансів віддалених робочих з одного розташування .

- рівний розподіл мережі - динамічно розподіляє доступну пропускну здатність між активними сеансами залежно від їх кількості, щоб забезпечити рівне використання смуги пропускання.

- рівний розподіл диска - не дозволяє сеансам надмірно використовувати диск, рівномірно розподіляючи між ними вводи та висновки диска.

- рівний розподіл ЦП - динамічно розподіляє час процесора між активними сеансами залежно від їх кількості та навантаження.

Розгортання віртуалізації сеансів включає сервери вузлів сеансів віддалених робочих столів і сервери інфраструктури, наприклад, сервери ліцензування віддалених робочих столів , посередник підключень віддалених робочих столів , шлюз віддалених робочих столів і сервери веб - доступу до віддалених робочих столів .

Колекція сеансів - це група вузлів - серверів сеансів віддалених робочих столів для конкретного сеансу. Колекція сеансів використовується для публікації одного з таких ресурсів як сеансові робочі столи та віддалені додатки RemoteApp.

1.2.5 Централізована публікація ресурсів

Служби віддалених робочих столів дозволяють з централізованої консолі публікувати і управляти такими ресурсами. Завдяки новій можливості публікації є можливість переглянути архів призначених користувачам ресурсів, змінити опубліковані ресурси будь-якої колекції і змінити властивості опублікованих ресурсів .

Крім централізованої консолі, можливо налаштовувати URL - адресу підключення до віддалених робочих столів і додатків RemoteApp за допомогою групової політики , а потім давати користувачам доступ до URL - адреси автоматично за допомогою адреси електронної пошти.

Централізована публікація ресурсів забезпечує кінцевого користувача взаємодією, яка може замінити локально встановлені додатки.

Служби віддалених робочих столів — це роль сервера, складається з декількох служб ролі:

- вузол віртуалізації віддалених робочих столів, який виконує розгортання колекцій віртуальних робочих столів (як персональних, так і в складі пулу) в організації за допомогою підключення до віддалених робочих столів і додатків RemoteApp;

- вузол сеансів віддалених робочих столів дозволяє серверу розміщувати віддалені додатки RemoteApp або робочі столи на основі сеансів. Користувачі можуть підключатися до серверів вузлів сеансів віддалених робочих столів в колекції сеансів, щоб запускати програми, зберігати файли і використовувати ресурси на цих серверах;

- посередник підключень до віддаленого робочого столу дозволяє користувачам відновлювати підключення до існуючих віртуальним робочих столів, віддаленим додаткам RemoteApp і робочих столів на основі сеансів, а також дозволяє рівномірно розподіляти навантаження між серверами вузлів сеансів, віддалених робочих столів в колекції сеансів або між віртуальними робочими столами у складі пулу в колекції таких робочих столів. Також надає доступ до віртуальних робочих столів в колекції віртуальних робочих столів;

- веб-доступ до віддалених робочих столів дозволяє користувачам отримати доступ до підключення к віддаленим робочим столам і програмам RemoteApp;

- шлюз віддалених робочих столів дозволяє авторизованим користувачам підключатися через Інтернет до віртуальних робочих столів, віддалених програм RemoteApp і робочих столів на основі сеансів в мережі організації.

1.3 Дослідження протоколів організації віддаленого доступу

Існує безліч мережевих протоколів для підключення та передачі даних через мережу Інтернет. Деякі з таки х відповідають за безпеку даних, що передаються. Також є протоколи для віддаленого підключення, що відповідають завданню на дослідження. Окремо розглянемо основні з таких протоколів.

1.3.1 Протокол віддаленого робочого стола

Протокол віддаленого робочого стола (Remote Desktop) є прикладним протоколом, що базується на TCP. Після установки з'єднання на транспортному рівні ініціюється RDP-сесія , в рамках якої узгоджуються різні параметри передачі даних. Після успішного завершення фази ініціалізації сервер терміналів починає передавати клієнту графічний висновок і очікує вхідні дані від клавіатури і миші. В якості графічного виведення може виступати як точна копія графічного екрану, передана як зображення, так і команди на відрисовку графічних примітивів. Передача виводу за допомогою примітивів є пріоритетною для протоколу RDP, оскільки значно економить трафік; а зображення передається лише в тому випадку, якщо інше неможливо з якихось причин. RDP-клієнт обробляє отримані команди і виводить зображення за допомогою своєї графічної підсистеми. Користувальницький ввід за замовчуванням передається за допомогою скан - кодів клавіатури. Сигнал натискання і відпускання клавіші передається окремо за допомогою спеціального флагу.

RDP підтримує кілька віртуальних каналів у рамках одного з’єднання, які можуть використовуватися для забезпечення додаткового функціоналу.

Характеристики віртуальних каналів узгоджуються на етапі встановлення з'єднання.

1.3.2 Забезпечення безпеки при використанні протоколу RDP

Специфікація протоколу RDP передбачає використання одного з двох підходів до забезпечення безпеки:

- Standard RDP Security (вбудована підсистема безпеки) -
- Enhanced RDP Security (зовнішня підсистема безпеки)

При використанні вбудованих засобів безпеки аутентифікація, шифрування та забезпечення цілісності реалізується засобами, закладеними в RDP – протокол.

Принцип аутентифікації сервера виконується:

- При старті системи генерується пара RSA – ключів.
- Створюється сертифікат (Proprietary Certificate) відкритого ключа.
- Сертифікат підписується RSA - ключем, зашитим в операційну систему.
- Клієнт підключається до сервера терміналів і отримує Proprietary Certificate.
- Клієнт перевіряє сертифікат і отримує відкритий ключ сервера (даний ключ використовується надалі для узгодження параметрів шифрування)
- Аутентифікація клієнта проводиться при введенні імені користувача та пароля.

Шифрування використовує потоковий шифр RC4. При установці з'єднання після узгодження необхідної довжини ключа, генерується два різних ключа: для шифрування даних від клієнта і від сервера.

Цілісність повідомлення досягається застосуванням алгоритму генерації MAC (Message Authentication Code) на базі алгоритмів MD5 і SHA1.

При використанні зовнішніх підсистем захисту використовуються зовнішні модулі забезпечення безпеки: TLS 1.0, CredSSP.

При використанні TLS сертифікат сервера можна генерувати засобами Terminal Services або вибирати існуючий сертифікат зі сховища Windows.

Протокол CredSSP являє собою поєднання функціоналу TLS, Kerberos і NTLM.

1.3.3 Протокол PPP

Для того, щоб організувати зв'язок через канал з безпосереднім з'єднанням, який ініціює PPP, на початку відправляє пакети LCP для завдання конфігурації з'єднання, а також перевірки каналу передачі даних. Після того, як канал встановлений і пакетом LCP виконано необхідне узгодження факультативних засобів, який ініціює PPP відправляє пакети NCP, щоб вибрати і визначити конфігурацію одного або більше протоколів мережевого рівня. Як тільки конфігурація кожного обраного протоколу визначена, дейтаграми з кожного протоколу мережевого рівня можуть бути відправлені через даний канал. Канал зберігає свою конфігурацію до тих пір, поки пакети LCP або NCP явно не закриють його або поки не відбудеться якесь зовнішнє подія.

Протокол PPP може працювати через будь-який інтерфейс DTE/DCE. Єдиним абсолютним вимогою, яке пред'являє PPP, є вимога забезпечення дубльованих схем (або спеціально призначених, або перемикаються), які можуть працювати як у синхронному, так і в асинхронному послідовному режимі, прозорому для блоків даних канального рівня PPP. Протокол PPP не пред'являє будь-яких обмежень, що стосуються швидкості передачі інформації, крім тих, які визначаються використовуваним інтерфейсом DTE / DCE.

Протокол PPP для достатньої універсальності і застосовності до широкої різноманітності систем включає протокол контролю каналу LCP (Link Control Protocol). LCP використовується, щоб автоматично погоджувати опції формату інкапсуляції, змінювати межі розмірів пакетів, виявляти зациклення ланки і інші помилкові ситуації, пов'язані з відмінностями конфігурацій, і розривати зв'язок. Його інші додаткові засоби обслуговування - це аутентифікація ідентичності однорангового об'єкта на каналі і визначення, коли зв'язок функціонує належним чином, а коли - ні. Процес LCD проходить через чотири чітко розрізннені фази:

- організація каналу та узгодження його конфігурації. Перш, ніж може бути здійснений обмін якими-небудь дейтаграммами мережевого рівня, LCP

спочатку повинен відкрити зв'язок і узгодити параметри конфігурації. Ця фаза завершується після того, як буде відправлений і прийнятий пакет підтвердження конфігурації;

- визначення якості каналу зв'язку. LCP забезпечує необов'язкову фазу визначення якості каналу, яка слідує за попередньою фазою. У цій фазі перевіряється канал з метою з'ясування, чи є якість каналу достатнім для виклику протоколів мережевого рівня. Ця фаза є повністю факультативної. LCP може затримати передачу інформації протоколів мережевого рівня до завершення цієї фази;

- узгодження конфігурації протоколів мережевого рівня. Після того, як LCP завершить фазу визначення якості каналу зв'язку, відповідними NCP може бути вибрана конфігурація мережевих протоколів, і вони можуть бути в будь-який момент викликані і звільнені для подальшого використання. Якщо LCP закриває даний канал, він інформує про це протоколи мережевого рівня, щоб вони могли вжити відповідних заходів;

- припинення дії каналу. LCP може в будь-який момент закрити канал. Це зазвичай робиться за запитом користувача, але може відбутися також через фізичну подію (втрата носія або закінчення періоду таймера).

Канали PPP мають багато проблем з використовуваним сімейством мережевих протоколів. Наприклад, призначення і керування адрес IP, які є проблемою навіть в ЛВС, є особливо важкими для комутованих каналів точка-точка (point-to-point). Ці проблеми вирішуються сімейством протоколів контролю мережі (NCPs - Network Control Protocols), кожен з яких відповідає за певні функції, необхідні відповідними протоколами мережевого рівня.

1.3.4 Протокол віддаленого доступу

Протокол SSH використовується для організації безпечного входу в віддалену систему (login) та організації інших безпечних служб через мережі, що не забезпечують безпеки. Протокол включає три основних компоненти:

- протокол транспортного рівня забезпечує аутентифікацію серверів, конфіденційність і цілісність. Цей протокол може також забезпечувати стиснення інформації. Транспортний рівень працює в основному з використанням з'єднань TCP/IP, але може бути реалізований і на базі інших потоків даних з гарантованою доставкою;

- протокол аутентифікації користувачів використовується на серверах для перевірки повноважень клієнтів. Цей протокол працює на основі протоколу транспортного рівня;

- протокол сполук забезпечує мультиплексування шифрованого тунелю в кілька логічних каналів і працює поверх протоколу аутентифікації користувачів.

Клієнт передає один запит на обслуговування в процесі організації захищеного з'єднання на транспортному рівні. Інший запит на обслуговування передається після успішної перевірки повноважень клієнта. Таке рішення забезпечує можливість створення нових протоколів і їх спільного використання з перерахованими вище протоколами.

Протокол сполук забезпечує канали, які можуть використовуватися для вирішення цілого ряду завдань. Забезпечуються стандартні методи для організації захищених shell-сесій і перенаправлення («тунелювання») довільних портів TCP/IP і з'єднань X11.

Пакети SSH використовують номери повідомлень від 1 до 255. Ці номери розподілені між різними компонентами:

а) Протокол транспортного рівня:

- 1 - 19 – базові повідомлення транспортного рівня (наприклад, disconnect, ignore, debug і т. п.);

- 20 - 29 – узгодження алгоритму;

- 30 - 49 – повідомлення, пов'язані з обміном ключами (допускається збіг номерів для різних методів аутентифікації).

б) Протокол аутентифікації користувачів:

- 50 - 59 – базові повідомлення протоколу аутентифікації;

- 60 - 79 – повідомлення, пов'язані з методом аутентифікації (допускається збіг номерів для різних методів).

в) Протокол сполук:

- 80 - 89 – базові повідомлення протоколу;

- 90 - 127 – повідомлення, пов'язані з каналом.

г) Зарезервовано для клієнтських протоколів:

- 128 - 191 – резерв.

д) Локальні розширення:

- 192 - 255 – локальні розширення.

SSH-тунель - це тунель, створюваний за допомогою SSH-з'єднання і використовується для шифрування даних. Використовується для того, щоб забезпечити передачу даних в Інтернеті (аналогічне призначення має IPsec). При пересиланні через SSH-тунель незашифрований трафік будь-якого протоколу шифрується на одному кінці SSH-з'єднання і розшифровується на іншому.

Практична реалізація може виконуватися кількома способами. Створенням Socks-проксі для додатків, які не вміють працювати через SSH-тунель, але можуть працювати через Socks-проксі. Використанням додатків, які вміють працювати через SSH-тунель. Створенням VPN-тунелю, підходить практично для будь-яких додатків.

Якщо програма працює з одним певним сервером, можна налаштувати SSH-клієнт таким чином, щоб він пропускав через SSH-тунель TCP-з'єднання, що приходять на певний TCP-порт машини, на якій запущений SSH-клієнт.

SSH протокол прикладного рівня. SSH-сервер зазвичай прослуховує з'єднання на TCP-порту 22. Для аутентифікації сервера в SSH використовується протокол аутентифікації сторін на основі алгоритмів електронно-цифрового підпису RSA або DSA. Для аутентифікації клієнта також може використовуватися ЕЦП RSA або DSA, але допускається також аутентифікація за допомогою пароля (режим зворотної сумісності з Telnet) і

навіть ip-адреси хоста (режим зворотної сумісності з rlogin). Аутентифікація по паролю найбільш поширена оскільки пароль передається по зашифрованому віртуальному каналу. Аутентифікація за ip-адресою небезпечна, цю можливість найчастіше відключають. Для створення загального секрету (сеансового ключа) використовується алгоритм Діффі - Хеллмана (DH). Для шифрування переданих даних використовується симетричне шифрування, алгоритми AES, Blowfish або 3DES. Цілісність передачі даних перевіряється за допомогою CRC32 в SSH1 або HMAC-SHA1/HMAC-MD5 в SSH2. Для стиснення шифрованих даних може використовуватися алгоритм LempelZiv (LZ77), який забезпечує такий же рівень стиснення, що і архіватор ZIP. Стиснення SSH включається лише по запиту клієнта, і на практиці використовується рідко.

1.3.5 Протокол безпечної передачі даних

Основне призначення протоколів IPSec - забезпечення безпечної передачі даних по мережах IP. Застосування IPSec гарантує:

- цілісність, тобто що дані при передачі не були спотворені, втрачені або продубльовані;
- автентичність, тобто що дані були передані тим відправником, який довів, що він той, за кого себе видає;
- конфіденційність, тобто дані передаються у формі, що запобігає їх несанкціонований перегляд.

Ядро IPSec складає три протоколи: протокол аутентифікації (Authentication Header, AH), протокол шифрування (Encapsulation Security Payload, ESP) і протокол обміну ключами (Internet Key Exchange, IKE). Функції з підтримання захищеного каналу розподіляються між цими протоколами наступним чином:

- протокол AH гарантує цілісність і автентичність даних;
- протокол ESP шифрує дані, що передаються, гарантуючи конфіденційність. Також підтримує аутентифікацію і цілісність даних;

– протокол IKE вирішує допоміжне завдання автоматичного надання кінцевим точкам каналу секретних ключів, необхідних для роботи протоколів аутентифікації і шифрування даних.

Можливості протоколів AH і ESP частково перекриваються. Протокол AH відповідає тільки за забезпечення цілісності і аутентифікації даних, в той час як протокол ESP більш потужний, так як може шифрувати дані, а крім того, виконувати функції протоколу AH (хоча, як побачимо пізніше, аутентифікація і цілісність забезпечуються ним у дещо скороченому вигляді). Протокол ESP може підтримувати функції шифрування і аутентифікації/ цілісності в будь-яких комбінаціях, тобто або і ту і іншу групу функцій, або тільки аутентифікацію/цілісність, або тільки шифрування.

Для шифрування даних в IPSec може бути застосований будь-який симетричний алгоритм шифрування, який використовує секретні ключі. В основі забезпечення цілісності та аутентифікації даних також лежить один із прийомів шифрування - шифрування за допомогою односторонньої функції (one-way function), званої також хеш-функцією (hash function) або дайджест-функцією (digest function). Ця функція, застосована до даних, дає в результаті значення-дайджесту, що складається з фіксованого невеликого числа байт. Дайджест передається в IP-пакеті разом з вихідним повідомленням. Одержувач, знаючи, яка одностороння функція шифрування була застосована для складання дайджесту, заново обчислює його, використовуючи вихідне повідомлення. Якщо значення отриманого і обчисленого дайджестів збігаються, це означає, що вміст пакету під час передачі не було піддано ніяким змінам. Володіння дайджесту не дає можливості відновити вихідне повідомлення і тому не може бути використано для захисту, але зате воно дозволяє перевірити цілісність даних.

Поділ функцій захисту між двома протоколами AH і ESP викликано застосовуваної в багатьох країнах практикою на обмеження експорту та/або

імпорту засобів, що забезпечують конфіденційність даних шляхом шифрування. Кожен з цих двох протоколів може використовуватися як самостійно, так і одночасно з іншим, так що в тих випадках, коли шифрування через діючих обмежень застосовувати не можна, систему можна постачати тільки з протоколом AH. Природно, захист даних лише за допомогою протоколу AH в багатьох випадках буде недостатньою, так як приймаюча сторона в цьому випадку буде впевнена тільки в тому, що дані були відправлені саме тим вузлом, від якого вони очікуються, і дійшли у тому вигляді, в якому були відправлені. Від несанкціонованого перегляду до шляху проходження даних протокол AH захистити не може, оскільки не шифрує їх. Для шифрування даних необхідно застосовувати протокол ESP, який може також перевірити їх цілісність і автентичність.

Для того щоб протоколи AH і ESP могли виконувати свою роботу із захисту даних, що передаються, протокол IKE встановлює між двома кінцевими точками логічне з'єднання, яке в стандартах IPSec носить назву «безпечна асоціація» (Security Association, SA). Встановлення SA починається з взаємної аутентифікації сторін, тому що всі заходи безпеки втрачають сенс, якщо дані передаються або приймаються не від тієї особи. Обираєте далі параметри SA визначають, який з двох протоколів, AH або ESP, застосовується для захисту даних, які функції виконує протокол захисту: наприклад, тільки аутентифікацію та перевірку цілісності або, крім того, ще й захист від помилкового відтворення. Дуже важливим параметром безпечної асоціації є так званий криптографічний матеріал, тобто секретні ключі, що використовуються в роботі протоколів AH і ESP. Система IPSec дозволяє застосовувати і ручний спосіб встановлення безпечної асоціації, при якому адміністратор конфігурує кожен кінцевий вузол таким чином, щоб вони підтримували узгоджені параметри асоціації, включно і таємні ключі.

1.4 Висновки до розділу

В першому розділі були розглянуті теоретичні відомості про створення віддалених лабораторій. Розглянуті різновиди віддалених лабораторій, віртуальних лабораторій та лабораторій з віддаленим доступом. Визначена різниця між створенням та побудовою таких лабораторії. Визначені основні задачі,що покладаються в кожному випадку окремо. Проаналізована робота користувача в різних за типом віддалених лабораторіях та визначені переваги та недоліки при роботі. В кожній з таких лабораторій вирішуються спеціалізовані завдання.

В темі магістерської роботи де потрібно дослідити методи захисту даних вказаний тип лабораторії з віддаленим доступом, тому в цьому розділі наведена архітектура подібної типової лабораторії. Визначено, що така лабораторія має свої фізичне розташування та оснащення реальним обладнанням. Так як, до такого обладнання є доступ тільки з фізичної лабораторії, то вирішено зробити віддалений доступ до неї.

В подібній структурі видно, що при такому підході є дані, котрим потрібно забезпечити захист, а також забезпечити доступність до них авторизованим користувачам.

В першому розділі були розглянуті протоколи, що забезпечують віддалене підключення та керування. Розглянуті питання організації віддаленого доступу.

2 ДОСЛІДЖЕННЯ МЕТОДІВ ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДАНИХ ІНФОРМАЦІЙНИХ СИСТЕМ

2.1 Завдання на дослідження

Сучасні комп'ютерні технології спричинили можливість перенесення у віртуальне середовище багатьох форм і способів навчання. Одним з логічних етапів розвитку нових форм навчання є створення віртуальних лабораторій, які містять у собі цифрові аналоги лабораторій університету, з усіма необхідними інструментами, а також організація віртуальних лабораторій з віддаленим доступом до реального фізичного обладнання лабораторій.

Особливо важлива роль віртуалізації у питаннях пов'язаних з безпекою програм та даних. В цьому випадку досить часто необхідно працювати з операційною системою (ОС) з правами адміністратора та втручатися в налаштування важливих служб. Але в процесі навчання природнім чином виникають помилки, які можуть привести до подальшої некоректної роботи ОС. Якщо б такі експерименти проводились на реальних комп'ютерах, то після кожної лабораторної роботи потрібно було б пере налаштовувати значну частину комп'ютерів в лабораторії.

Безпека інформації базується на базовій моделі безпеки, яка передбачає три складові: конфіденційність, цілісність і доступність. Для забезпечення цілісності та конфіденційності є такі рішення:

1. Використання методів розгортання мережевої інфраструктури: метод дублювання дисків з використанням утиліти Sysprep; метод віддаленої установки з використанням сервера віддаленого встановлення ОС (RIS).

2. Забезпечення безпеки зберігання даних: технологія створення тіньових копій даних; архівація даних (backup); створення відмовостійких томів для зберігання даних (RAID).

3. Використання програмних засобів: центр забезпечення безпеки Windows Security Center, налаштування виключень для вбудованого брандмауера Windows за допомогою локальних політик.

4. Використання систем аналізу захищеності мережі для виявлення вразливостей.

5. Використання засобів для захисту від шкідливого програмного забезпечення.

Забезпечення захисту інформації в темі, що досліджується, вимагає комплексного підходу, який передбачає впровадження широкого переліку апаратних, програмних та організаційних технології інформаційної безпеки.

Дана магістерська робота направлена на дослідження методів захисту даних в лабораторіях з віддаленим доступом. Як видно зі вступного слова, це означає комплексний підхід до захисту даних, використовуючи різні засоби та технології. Основним напрямком дослідження цієї теми роботи є дослідження захисту даних з боку особливості їх доступності:

1. Дослідження захисту даних в мережі лабораторії з боку мережевого обладнання - функціонування сервісів та протоколів: контроль доступу (фільтрацією доступу до обладнання з використанням списків доступу; доступ до мережевого обладнання з використанням асиметричних ключів; двофакторна аутентифікація для доступу до систем мережі), захист конфігурації (резервування конфігурації на резервних серверах; використання контролю цілісності конфігураційних файлів; дзеркалювання дискового простору з використанням RAID)

2. Дослідження захисту кінцевих пристроїв направлених на забезпечення цілісності даних, доступності обладнання та контролю сервісів. Використання програмних засобів.

3. Дослідження захисту доступності даних: контроль щільності трафіку в мережі; контроль мережевих інтерфейсів на всьому обладнанні; резервування даних; фільтрації трафіку. Резервування даних здійснюється локально на серверах та на резервному обладнанні:

– резервування локальних систем серверів з використанням RAID масивів;

– використання серверів резервування для зберігання копій даних та конфігурацій;

– резервування конфігурацій при внесенні змін.

Метою магістерської кваліфікаційної роботи є підвищення доступності даних в задачах забезпечення захисту даних в лабораторіях з віддаленим доступом, шляхом дослідження існуючих методів та розробки моделей процесів порушення безпеки.

Для досягнення поставленої мети ставляться наступні задачі:

– дослідити типи віртуальних лабораторій;

- визначити архітектуру лабораторії з віддаленим доступом;

- провести аналіз існуючих методів, моделей та стандартів оцінки захисту даних, які використовуються в галузі інформаційної безпеки;

- провести дослідження засобів доступу до подібних лабораторій;

– визначити засоби захисту даних та типи дані, що підлягають захисту;

- визначити поняття доступності;

- розробити моделі забезпечення захисту даних в інформаційних системах;

- розробити загальну систему забезпечення доступності

Об'єкт дослідження – процес оцінки доступності даних інформаційних систем..

Предмет дослідження – лабораторії з віддаленим доступом.

Методи дослідження. Основними методами дослідження були теорія графів, теорія множин, математична статистика.

Наукова новизна полягає у розвитку моделей аналізу та оцінки захищеності даних в дистанційних інформаційних системах, які використовуються при передачі даних та підключенні до лабораторій з віддаленим доступом.

Практичне значення отриманих результатів. Розроблені моделі та мотод були реалізовані для оцінки якості інформаційної безпеки, використання їх дозволить підвищити доступність даних при використанні методу в лабораторії з віддаленим доступом

2.2 Дослідження архітектури лабораторії з віддаленим доступом

Для визначення архітектури лабораторії з віддаленим доступом де буде проведено дослідження засобів та методів захисту інформації потрібно визначити вузли керування системою, які дозволять забезпечити апаратно-програмний комплекс доступу до ресурсів лабораторії. Структура типової лабораторії з віддаленим доступом поділяється на три групи:

- перша група – це фізичне устаткування реальної лабораторії: персональні комп’ютери або ноутбуки, лабораторні устаткування та обладнання, комутаційне обладнання для з’єднання усіх складових лабораторії в єдину кабельну систему. Для керування внутрішньою мережею потрібен сервер, а також для збереження виконаних в лабораторії даних.

- друга група – локальні абоненти: це усі абоненти що мають підключення в локальній мережі закладу.

- третя група – віддалені зв’язки – це усі зв’язки територіально віддалених абонентів, які здійснюють доступ до об’єктів через глобальну мережу Інтернет.

Основними елементами мережі є комутаційні об’єкти (комутатори та маршрутизатори) що виконуються функції з’єднання, при необхідності

агрегацію лабораторного устаткування та централізований доступ до обладнання.

Рисунок 2.1 – Архітектура лабораторії з віддаленим доступом

Принцип роботи в лабораторії з віддаленим доступом такий, що віддалений користувач запитує доступ з лабораторії, підключається до лабораторії та генерує код програми для дозволеного обладнання. Сервер надає доступ до вільного обладнання. Для цього формується таблиця MAC-адрес пристроїв. Інформаційні потоки даних через даний вузол обмежені можливостями програмного забезпечення на формування об’єктних файлів у розмірі до 8 Мб. При одночасної передачі всіх файлів через кожний порт комутатору, не очікується перевантаження даного пристрою.

2.3 Дослідження засобів організації доступу до лабораторії

Для організації доступу до лабораторій з віддаленим доступом використовуються наступні кроки:

– аутентифікація абонентів;

– авторизація абонентів;

– моніторинг мережі;

– визначення правил та прав користування ресурсами.

Необхідно організувати взаємодію головного комутатору лабораторії із сервером. Ці кроки можна вирішити за допомого програмно-апаратних заходів. Процес аутентифікації та авторизації вирішений на комутаторі. А також, щоб організувати різний доступ у абонентів, то їх поділено на групи. Це дозволить чітко визначати користувачів за ідентифікатором та визначати правила та права доступу. На основі ідентифікаторів та груп кожному абоненту присвоюються відповідні права та пріоритети. Дані записи створюють зв’язний список параметрів для кожного абонента, який можна визначити як $E = F(ID_{group}, ID_{user}, S_i)$, де полями списку є ідентифікатори групи та абонента, а також вектор S_i, який визначає права доступу конкретного абонента. Даний список демонструє співвідношення абонента з ресурсами системи на визначених правах. Даний підхід використовується як мандатний метод доступу. Даний метод управління доступом необхідний для реалізації захисту проектів учасників лабораторії та баз даних лабораторій.

2.3.1 Організація сеансу роботи у лабораторії

Якщо абонент проходить усі етапи аутентифікації та авторизації, наступним етапом є організація віддаленої роботи з об’єктами керування.

Організація сеансів роботи з обладнанням покладається на сервер управління, який повинен оптимально визначити порядок роботи у мережі. Для даної функції необхідно провести зв’язку параметрів для кожного абонента, який претендує на сеанс:

– визначення пристрою керування;

– визначення таймеру сеансу.

При ініціюванні сеансу з кожним абонентом асоціюється вільний контролер, перелік яких зберігається на сервері. Для асоціації необхідно вказати мережеві параметри обладнання. Дані заходи також необхідні для ініціалізації контролеру на програмному забезпеченні. Як вказувалося раніше, контролер агрегації зберігає таблицю співвідношень адрес контролерів з портами.

Для забезпечення рівноправного доступу необхідно організувати розмежування роботи з обладнанням за часом. Для даної функції використовується таймер, який ініціює зворотній відлік часу сеансу при ініціюванні даного сеансу. На сервері управління зберігається інформація часу до завершення сеансу роботи.

2.3.2 Моніторинг мережі лабораторії, як засіб захисту даних

В мережі віддаленої лабораторії передбачена система моніторингу ресурсів, функції якої наступні:

– контроль цілісності даних;

– контроль підключень до мережі;

– контроль активності у мережі.

Кожна з функцій даної системи забезпечує додатковий контроль доступу до ресурсів мережі.

Функція контролю цілісності даних виконує моніторинг баз даних у мережі. Здійснюється моніторинг бази користувачів, з ціллю зберігання облікових записів та прав доступу абонентів системи. Також виконується моніторинг змін у сховищі проектів, для детектування змін у ній та ініціаторів даних змін.

Функція підключень контролює суб’єкти мережі. В даному контексті маються на увазі абоненти, які здійснили вхід до мережі (активних) та обладнання лабораторій. Дана функція зв’язана з функцією контролю

активності у мережі. Дана зв’язка дозволяє вести облік активних абонентів, дії, які вони здійснюють у мережі та виявляти зміни у даних.

Функція контролю підключень та активності моніторингу реалізована як клієнт-серверна система, де сервер керування з регламентованою періодичністю проводить запроси до клієнтів та основі їх відповідей проводить порівняння характеристик отриманих значень з тими які присвоєні конкретному абоненту.

2.4 Дослідження засобів захисту даних

Захист інформаційних систем вимагає створення комплексної системи інформаційної безпеки, для забезпечення виключення або зниження наступних загроз та захист від них:

1. захист конфіденційності вимагає забезпечення неможливості засвоєння інформації, яка зберігається в системі:
   a. захист ідентифікаційних даних користувачів шляхом їх шифрування;
   b. захист інформації користувачів шляхом розмежування доступу до неї;
   c. введення двофакторної аутентифікації (логін/пароль, власний поштовий сервіс, коди підтвердження).
2. захист цілісності даних вимагає унеможливлення втручання в структуру інформації, яка зберігається:
   a. резервування даних;
   b. створення цифрових зліпків файлової структури;
   c. розмежування доступу до інформації.
3. захист доступності даних та сервісів вимагає забезпечення наступних заходів:
   a. резервування каналів доступу до мережі зберігання даних;

b. контроль трафіку для виявлення спроб порушення доступності даних або сервісів;

c. резервування внутрішніх ліній зв’язку та мережевого обладнання.

Заходи, що направлені на зниження ризиків порушення безпеки даних:

– організаційні міри забезпечують створення документальних правил, які регламентують поведінку в мережі системи, 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.

2.5 Основні поняття та визначення забезпечення доступності даних

Перед початком дослідження щодо захисту даних у ключі доступності, потрібно визначитись з основними поняттями, щоб правильно обрати методи захисту та забезпечення доступності.

Непрацездатність – стан елементів системи, коли вони не здатні виконати хоча б одну зі своїх функцій.

Відмова – подія яка вказує на порушення працездатності елементів та об’єктів системи.

Напрацюванням – є тривалість роботи об’єктів системи, що визначається в одиницях часу або в кількості циклів. Напрацювання до відмови – час від початку роботи до першої відмови. Напрацювання між відмовами – час від початку роботи після пере налаштування до наступної

відмови. Середнє напрацювання між відмовами називається напрацюванням на відмову.

Безвідмовність – властивість елементів та об’єктів безперервно зберігати працездатність з потоком визначеного часу або напрацювання.

Живість – властивість об’єктів зберігати обмежену працездатність при несправностях або відмові деяких компонентів. Таке поняття частіше називають відмовостійкістю.

Відмовостійка система – система, що має властивість безвідмовної роботи після відмови окремих елементів.

Ймовірність безвідмовної роботи – ймовірність того, що в проміжку заданого напрацювання відмова не виникне.

Коефіцієнт готовності – ймовірність того, що об’єкт буде працездатним в будь який момент часу, крім запланованих періодів, коли його робота не передбачається.

Резервування системи цілком – загальне, та роздільне – резервування окремих елементів системи.

Кратність резерву – відношення числа резервних елементів до резервуємих.

Дублювання – резервування з кратністю резерва один до одного.

Надійність – властивість об’єкта зберігати в часі значення усіх параметрів та виконувати потрібні функції в заданих умовах використання.

2.6 Висновки до розділу

У другому розділі кваліфікаційної роботи магістра основними кроками дослідження були:

– визначити завдання на дослідження: актуальність даного напряму дослідження, визначити мету та задачі дослідження, проблематику даної теми та кроки реалізації дослідження. Визначити практичну

значимість даного дослідження та подальший розвиток розроблених кроків. Визначити напрям діяльності.

- Для реалізації поставлених задач потрібно дослідити архітектури побідного напряму. Визначити типову архітектуру інформаційної системи, дані якої необхідно захистити.
- Дослідити існуючи рішення. Визначити переваги та недоліки існуючих засобів захисту даних інформаційних систем.
- Визначити основні поняття та визначення забезпечення доступності.

3 МЕТОДИ ЗАБЕЗПЕЧЕННЯ ДОСТУПНОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

Доступність даних – принцип забезпечення доступу до інформації та зв’язаними з нею діями тим користувачам, що авторизовані в інформаційній системі. Також під поняттям доступності розуміється стан інформації, при якому користувачі, що мають право, можуть її отримати безперервно.

Основні заходи та механізми, що забезпечують доступність інформації, це:

- дублювання каналів зв’язку;
- дублювання шлюзів та між мережевих екранів;
- резервне копіювання;
- відновлення середи роботи.

Засоби забезпечення від несанкціонованого доступу:

- засоби авторизації;
- мандатне та вибіркове керування доступом;
- керування доступом на основі ролей;
- журналювання.

Програмні засоби:

- системи виявлення вторгнень;
- аналізатори протоколів;
- антивірусні засоби;
- між мережеві екрани;
- системи резервного копіювання;
- системи аутентифікації;

Фактори, що впливають на доступність інформаційних систем:

- атака типу «відмова в обслуговуванні»;
- атаки програм-здирників;

- саботаж.

- людиний фактор та не професіоналізм

Основним завданням забезпечення доступності є виконання вимог до інформаційних систем щодо доступності їх ресурсів. Вимоги, як правило, формулюються в термінах часу доступності ресурсів на рік.

Загальна модель забезпечення доступності з урахуванням вимог виглядає наступним чином

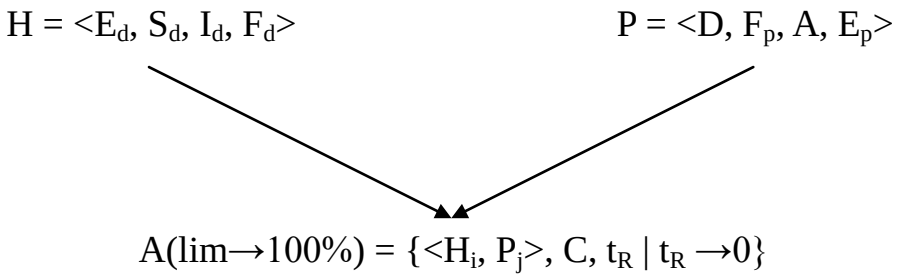

Рисунок 3.1 — Модель забезпечення доступності ІС

Основними складовими моделі є програмні та апаратні засоби інформаційних систем. Для апаратної частини (H):

– множина кінцевих пристроїв E_d визначає кількість точок доступу до інформаційних ресурсів на серверах S_d. Даний параметр важливий з точки зору навантаження на сервера, а також ймовірних джерел атак;

– множина S_d визначає кількість інформаційних ресурсів системи. Це дозволяє визначити множину ресурсів, для яких потрібно забезпечити доступність;

– множина мережевих пристроїв I_d визначає пристрої, які забезпечують трафік для ресурсів інформаційної системи;

– множина захисних систем F_d визначає наявність засобів забезпечення безпеки інформації в процесі її передачі та зберігання.

Програмні засоби забезпечення доступності визначають локальні системи захисту на хостах інформаційної системи:

– множина систем запобігання D на кінцевих пристроях визначає наявність та ефективність захисту втрати інформації з кінцевих пристроїв та серверів інформаційної системи;

– множина F_d визначає наявність та ефективність персональних програмних мережевих екранів кінцевих пристроїв і, особливо, серверів;

– параметр A визначає множину застосувань, які розгорнуті та використовуються на кінцевих пристроях, що, в свою чергу, визначає наявність вразливості в системі безпеки;

– параметр E_p визначає наявність та множину сервісів, які використовуються кінцевими пристроями, серверами та мережевими пристроями інформаційної системи.

Кооперація даних підмоделей дозволяє визначити систему виявлення рівня доступності інформаційних ресурсів на основі наступних параметрів:

– пара $<H_i, P_j>$ визначає вплив програмно-апаратних ресурсів інформаційної системи на доступність даних;

– множина C яка описує надлишковість зв’язків між мережевими об’єктами визначає наявність резервування каналів зв’язку в інформаційній системі;

– значення t_R визначає множину параметрів відновлення кожного об’єкту інформаційної системи в разі виходу з ладу.

Слід зазначити, що час відновлення об’єктів інформаційної системи повинен прагнути нулю, що, в свою чергу, визначає зворотню залежність доступності системи, яка повинна досягати визначеного порогового значення часу доступності.

3.1 Організаційні заходи забезпечення доступності даних

Організаційні заходи призначені для забезпечення доступності інформації для користувачів:

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

– визначення відповідальності користувачів за порушення правил використання системи;

– визначення ролей для користувачів;

У відповідності до представленої раніше загальної моделі забезпечення доступності, структура апаратного забезпечення може бути представлена наступною схемою (рисунок 3.2)

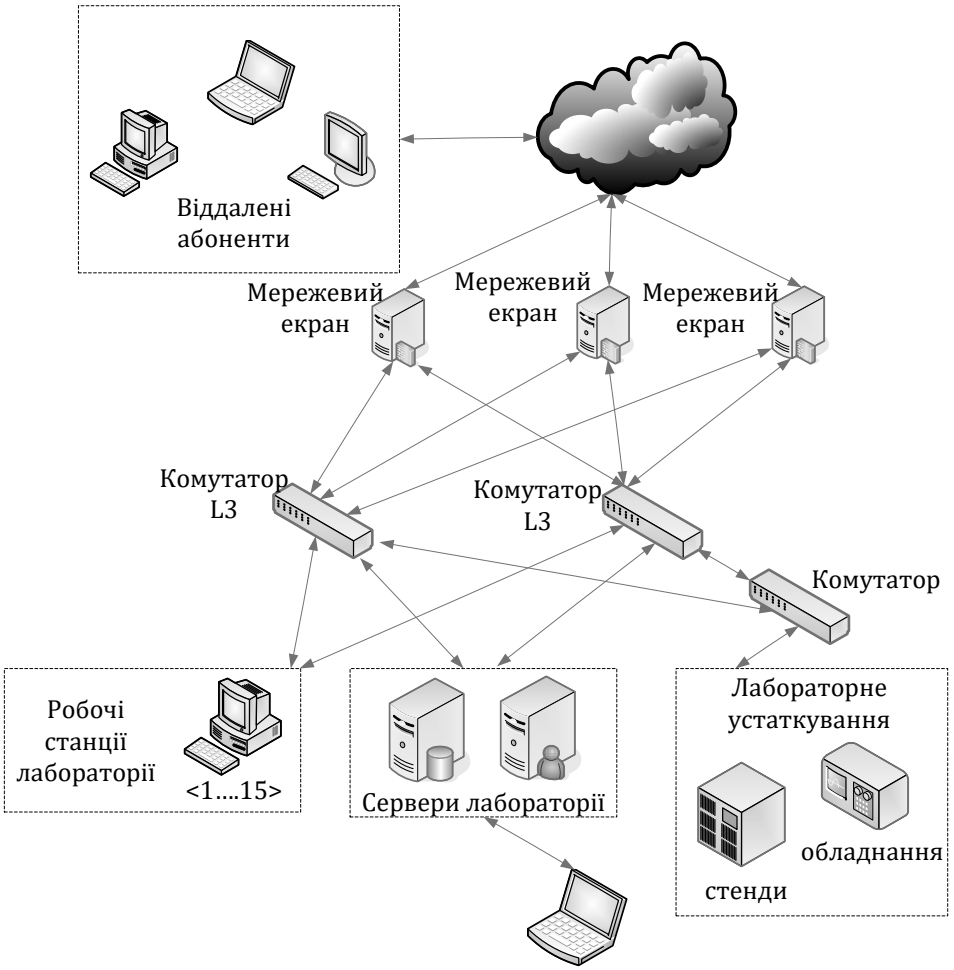

Рисунок 3.2 - Апаратна модель забезпечення доступності інформації

Апаратна модель доступності 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);
– маршрутизатори (опціонально).

Кожний з цих елементів інфраструктури має певні властивості, які стосуються загальної безпеки системи та, зокрема, доступності. Таким чином, кожний елемент можна описати вектором параметрів його впливу на доступність інформаційної системи, а сукупність цих значень визначає загальний вплив апаратної моделі на доступність лабораторії.

$$H = <E_d, S_d, I_d, F_d>$$

де $E_d = \{e_1, e_2, ..., e_i\}$ - множина значень доступності для кінцевих пристроїв,

$S_d = \{s_1, s_2, ..., s_j\}$ - множина значень доступності для серверів,

$I_d = \{i_1, i_2, ..., i_k\}$, - множина значень доступності мережевих пристроїв,

$F_d = \{f_1, f_2, ..., f_z\}$ - множина значень захищеності мережевого шлюзу.

Фактично, дана множина параметрів реалізується у вигляді вектора параметрів, які характеризують оцінку впливу пристроїв на доступність системи.

Серед програмних модулів, які реалізують захист інформації використовуються наступні:

– вбудовані засоби операційних систем серверів (мережеві екрани, 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;
– система запобігання витоку даних;

– антивірусне програмне забезпечення.

Модульність даної структури дозволяє, за необхідністю, вилучати певні системи захисту і замінювати їх іншими без втручання в загальну роботу, а модель, котра реалізує структурований опис параметрів програмної моделі визначається наступним чином:

$$P = <D, F_p, A, E_p>$$

де $D = \{d_1, d_2, ..., d_i\}$ - вектор впливу наявних систем запобігання витоку інформації,

$F_p = \{f_{p1}, f_{p2}, ..., f_{pj}\}$ - вектор значень впливу налаштувань персональних екранів кінцевих пристроїв,

$A = \{a_1, a_2, ..., a_k\}$, - множина застосувань, які наявні в системі та можуть впливати наявністю вразливості,

$E_d = \{e_1, e_2, ..., e_z\}$ - множина сервісів, які використовуються в системі.

Основними складовими інформаційної системи лабораторії з віддаленим доступом є наступні:

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

– 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 3.3 - Програмна модель забезпечення доступності інформації

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

– 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 системи зберігання;

– 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.

3.2 Модель захисту від атаки «відмова в обслуговуванні»

На початку розділу було визначено, що одним з факторів порушення доступності даних це коли окремі компоненти інформаційної системи лабораторії 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.

Таким чином, можна запропонувати модель, яка враховує характеристики трафіку, котрий використовується інформаційною системою. Робота віддаленої учбової лабораторії, на 75% будується на наявності та контролю трафіку в системі. Тому дана модель є дуже важливою для побудови методу захисту доступності.

$$Tr = <In_c, Out_c>,$$

Параметр In визначає множину параметрів, які характеризують доступність системи з використанням внутрішніх інтерфейсів, а параметр Out, відповідно, параметри доступності з використанням зовнішніх інтерфейсів. При цьому,

$$In_c = \{S_{int}, A_{int}, Sw_{int}\}$$
$$Out_c = \{Tr_{out}, Fw_{int}\}$$

де S_{int} - внутрішні інтерфейси серверів системи;

A_{int} - програмні інтерфейси застосувань, які використовуються для взаємодії в системі;

Sw_{int} - інтерфейси комутаторів, які здійснюють передачу даний в рамках системи;

Tr_{out} - інтерфейси, які забезпечують зв'язок із зовнішніми системами;

Fw_{int} - інтерфейси, які використовуються системами фільтрації трафіку.

3.2.1 Контроль внутрішніх інтерфейсів

Якщо в внутрішній мережі лабораторії організувати комплексний підхід до запровадження аналізу інтерфейсів та трафіку, який через них проходить, то ці заходи забезпечать доступність даних та захистять

внутрішні ресурси від DDoS-атак. Забезпечить контроль на 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 сервера зберігання даних;

– контроль (вибірковий) застосувань, які реалізовані на сервері;

– контроль інтерфейсів на комутаторах.

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

– утиліта TCPDump, яка дозволяє збирати інформацію з інтерфейсу серверу;

– 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 співвідностити 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.

3.2.2 Контроль зовнішніх інтерфейсів

Якщо контроль внутрішніх інтерфейсів, в першу чергу, зосереджений на запобіганні виникнення атак відмов в обслуговуванні всередині мережі лабораторії, то контроль зовнішніх інтерфейсів мережевого обладнання забезпечує захист від зовнішніх атак. При організації заходів захисту даних від зовнішніх атак можна використовувати частково механізми для захисту внутрішніх інтерфейсів.

Основний захист від зовнішніх атак відмов в обслуговуванні зосереджений на межі мережі:

– 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 мережі:

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

– 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 адміністратора.

Відповідно до цього, контроль межі 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 по певних сервісах, які розгорнуті на обладнанні).

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 адміністратором системи та іншими відповідальними особами в разі виявлення загроз безпеці.

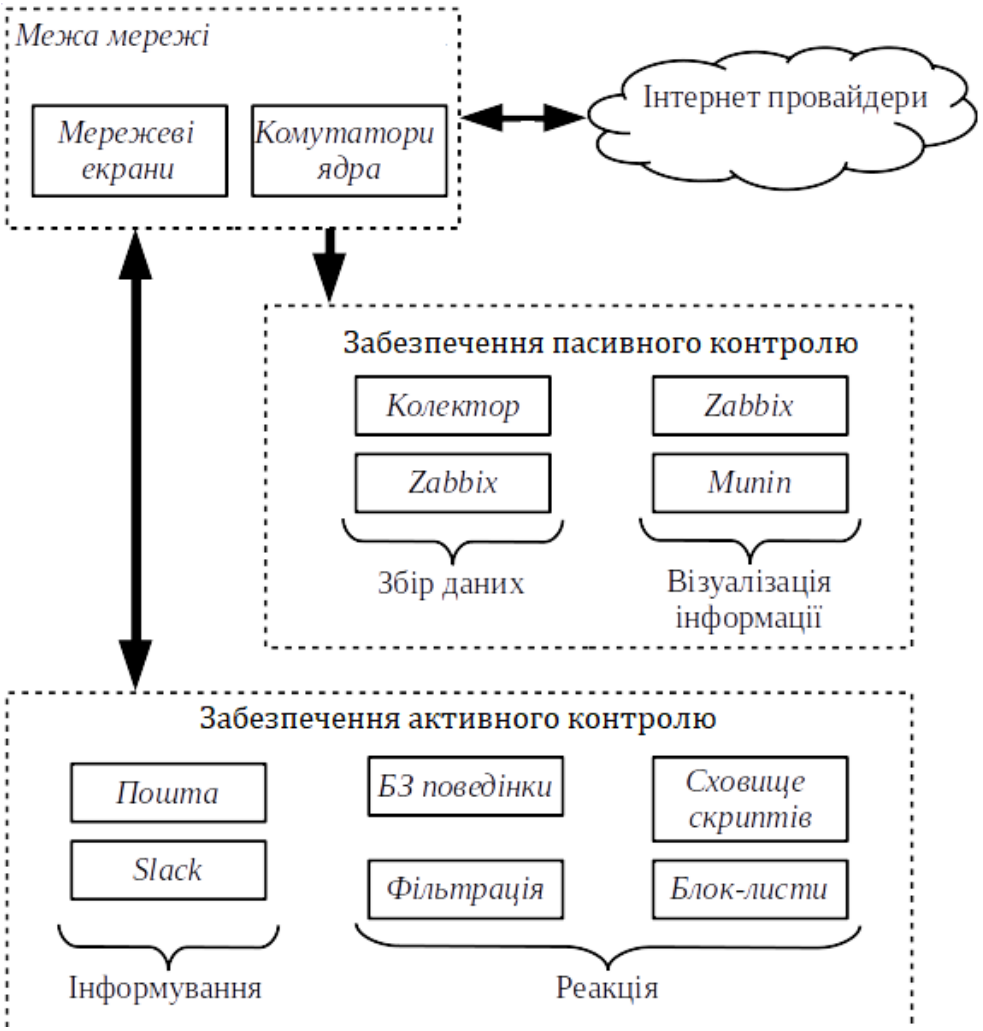

Рисунок 3.4 - Система міжмережного контролю трафіку

3.3 Забезпечення доступності використовуючи заходи захисту від небажаної розсилки

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

– розсилка поштового спаму;

– спам-атаки на веб-сервіси;

– 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.

3.3.1 Захист поштового сервісу

Поштова система працює як додатковий сервіс та приймає участь в аутентифікації користувачів:

– кожний користувач отримує унікальну адресу, яка асоціюється з його обліковим записом при регістрації на інформаційній платформі лабораторії;

Виходячи з особливостей роботи поштової системи, існує ризик використання її як базу для спам розсилки, що може призвести до певних загроз та ризиків. Для запобігання цих загроз використовується ряд заходів, які дозволяють контролювати черги поштових повідомлень, аналіз змісту поштових повідомлень та інше. 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.

3.3.2 Захист веб-системи

Веб система інформаційної системи лабораторії використовується для підтримки веб сайту надання графічних сервісів для користувачів системи. Використання веб системи суттєво спрощує використання сервісів за рахунок інтерфейсно - орієнтованого підходу роботи з даними, проте створює додаткові ризики для загальної безпеки мережевої та інформаційної структури.

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 даних наступні:

– DDoS атака на веб-сервер системи;

– злам системи доступу до серверу;

– зміна інформації на сервері;

– зміна прав доступу користувачів.

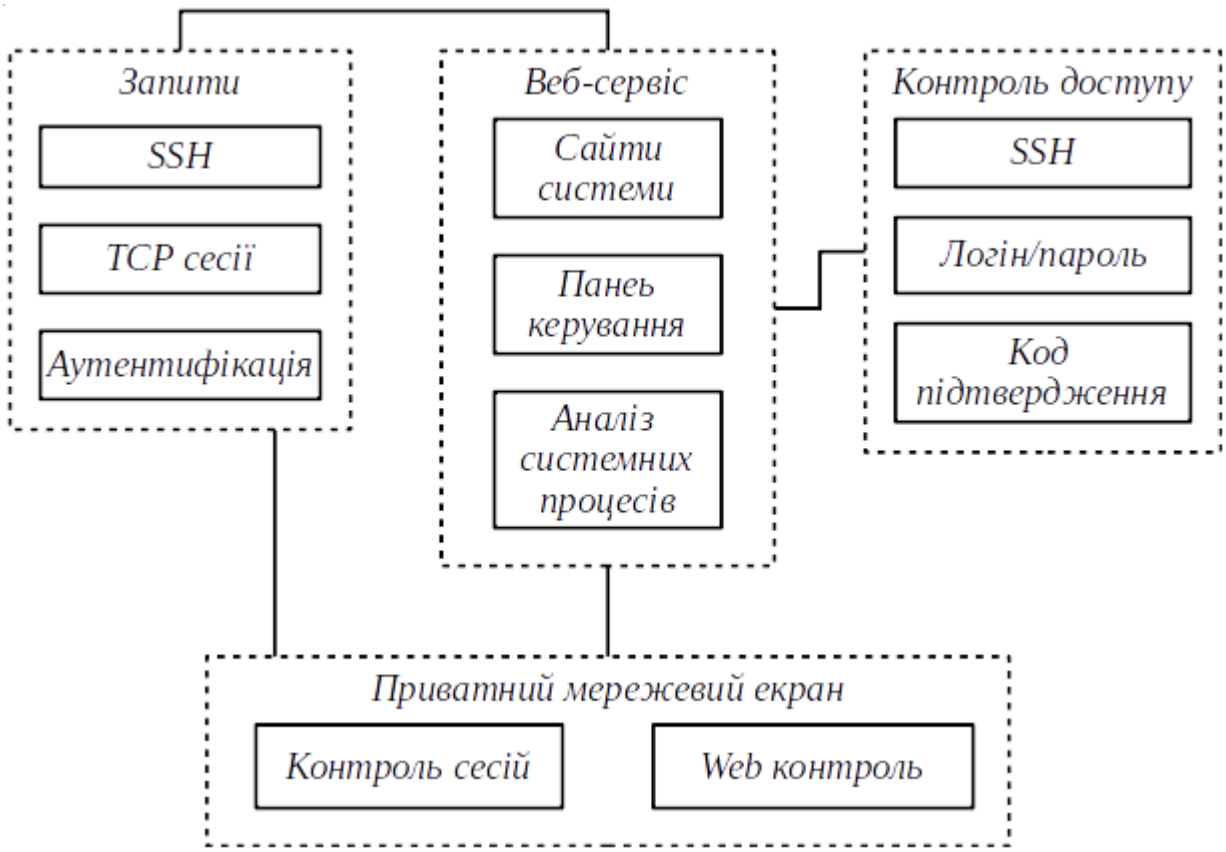

Рисунок 3.5 – Модель забезпечення доступності як захист веб-системи мережі

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

3.3.3 Захист сховищ

Враховуючи, що основна функція системи, це обмін файлів, її робота пов’язана з інтенсивними потоками даних з сервером 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.

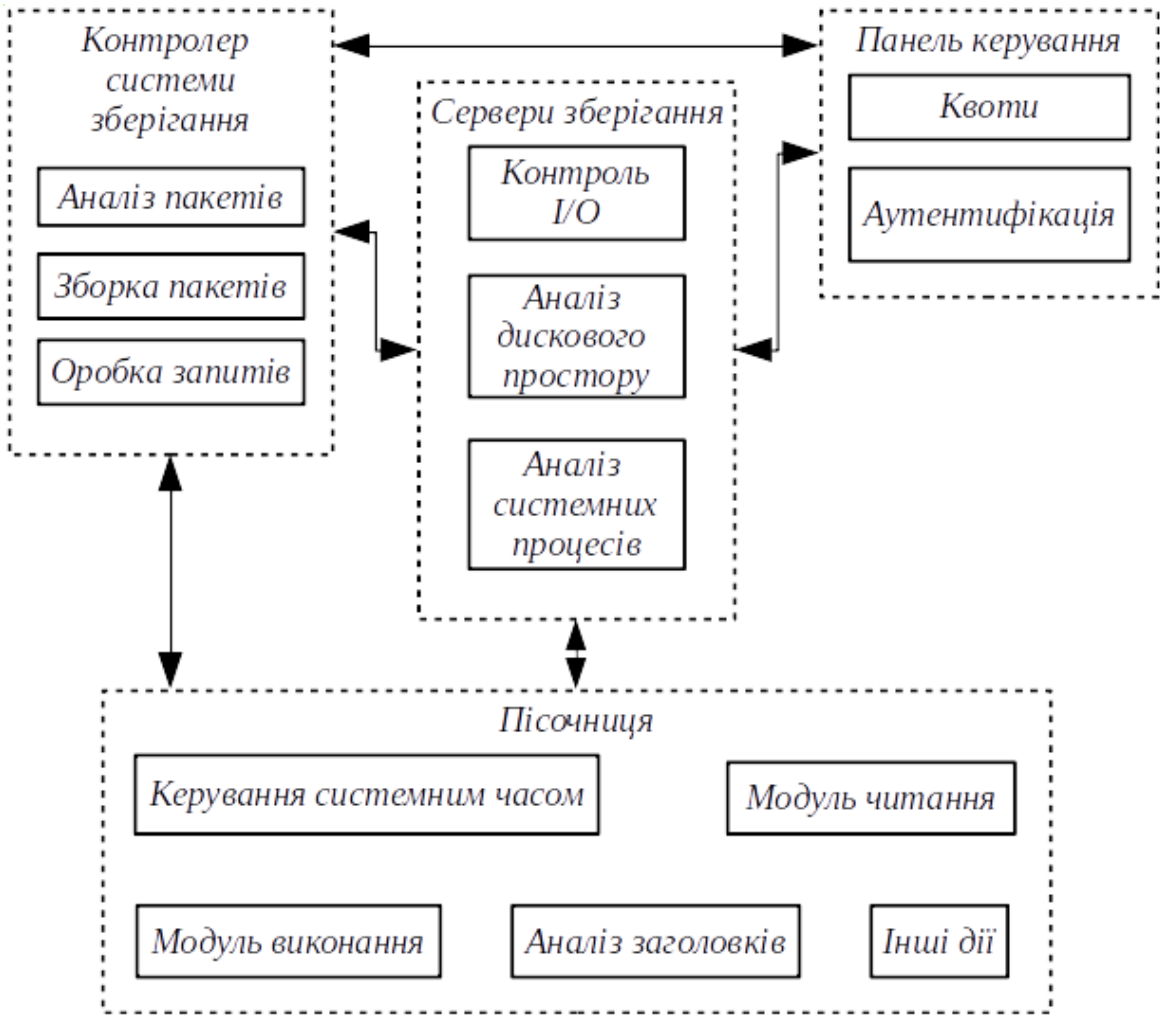

Рисунок 3.6 – Модель заходів забезпечення захисту сховища

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 Виявлення зловживань

В мережі віддаленої лабораторії зберігаються і обробляються дані користувачів, які мають доступ до підсистем мережі, необхідно забезпечити захист від зловживань в мережі її користувачами. До зловживань в мережі віднесено наступні дії:

- завантаження виконавчих файлів (віруси, скрипти та ін.);
- завантаження файлів не доречних до завдань;
- 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 забезпечено 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 мережі зберігання даних

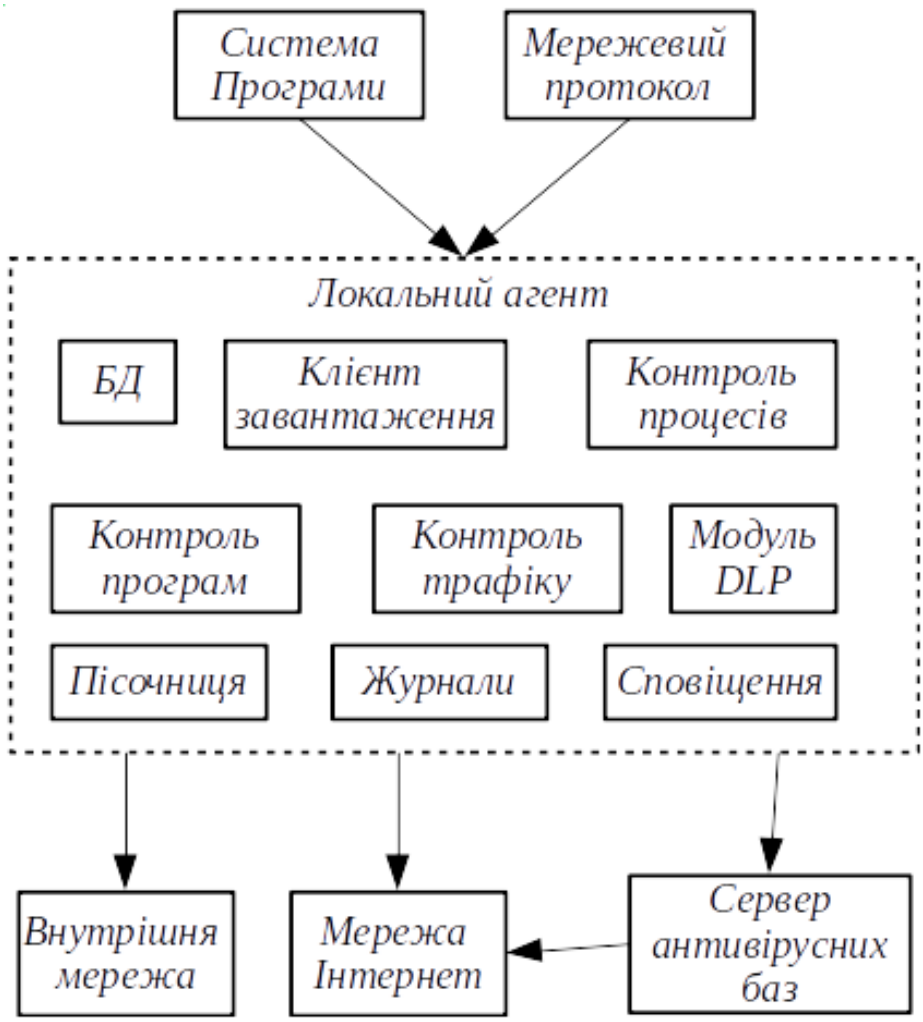

Рисунок 3.7 – Модель антивірусного захисту кінцевих станцій

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

Антивірусний захист здійснюється з 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.

3.5 Принцип резервування як метод забезпечення доступності інформації

Резервування – метод підвищення надійності систем та об’єктів. Використовується в галузях техніки та технологіях.

Види резервування:

– апаратне резервування – механізми дублювання;
– інформаційне резервування – методи виявлення та корекції помилок;
– тимчасове резервування – методи альтернативної логіки;
– програмне резервування – методи використання незалежних функціонально рівнозначних програм.

Класифікація резервування за ознаками – рівень резервування, кратність резервування, стан резервних елементів, способи з’єднання основних та резервних елементів.

Відмова вважається тоді, коли втрачають робото здатність основного та резервного елементів.

Кратність резервування – відношення числа резервних елементів до основних. Однократне резервування – це дублювання.

При використанні методу резервування інтенсивність відмов зростає з потоком часу.

Ефективність резервування оцінюють за допомоги коефіцієнта зростання надійності, що визначається за показником безвідмовності:

$$\gamma_p = P(t)_p / P(t)$$

$$\gamma_Q = Q(t) / Q(t)_p$$

де $P(t)_p$, $Q(t)_p$, — ймовірність безвідмовної роботи та ймовірність відмови для резервної системи.

$P(t)$ и $Q(t)$ — ймовірність безвідмовної роботи та ймовірність відмови для не резервної системи.

3.5.1 Загальне резервування

При загальному типі резервуванню підлягає уся система цілком. Також розділяють загальне постійне резервування, де усі резервні пристрої підключені до основного та працюють в одному режимі з потоком часу, та резервне заміщення, де резервні пристрої підключаються тільки після відмови основного.

Переваги постійного загального резервування:

- відносно проста побудова схем;

- відсутність навіть короткої перерви в роботі при відмові;

- відсутність додаткових підключених елементів, що знижують загальну надійність схем.

3.5.2 Резервування із заміщенням

Принцип використання резервування із заміщенням передбачає, що резервний пристрій додається до роботи системи після відмови, включається автоматично, або при участі людини. Якщо налаштування автоматичне, то необхідно передбачити надійність перемикаючих елементів, в іншому випадку надійність може знизитись в порівнянні з надійністю нерезервованої системи. Також до недоліків резервування із

заміщенням відноситься час, витрачений на перемикання до резервних пристроїв, якщо використовувати ручне перемикання, то перерва збільшується, але таке перемикання більш надійне.

3.5.3 Роздільне резервування

Використання такого типу резервування потребує індивідуальний резерв для кожної надлишкової частини. При розділеному заміщенні відмова системи може бути тільки тоді, коли відмова два рази поряд станется в одному тому ж пристрої, що малоймовірно. При проведенні математичних розрахунків можна зробити висновок, що найнадійнішою системою буде система, де використовується роздільне резервування з заміщенням ненавантаженим резервом.

3.6 Резервне копіювання для забезпечення доступності інформації

Принцип резервного копіювання є процес створення копій даних системи на носіях для того, щоб мати змогу відновити їх у випадку.

При даному принципі захисту даних використовується два виду операцій: резервне копіювання даних або дублювання даних тобто сам процес створення копій даних, та відновлення даних – процес відновлення.

Необхідність в можливості швидкого та дешевого відновлення інформації у випадку втрати.

Вимоги до систем резервного копіювання:

1. Надійність збереження інформації.
2. Багатоплатформеність.
3. Простота використання.
4. Швидке підключення.

Надійність можна забезпечити використовуючи відмово стійке обладнання системи зберігання, дублювання інформації та зміною пошкоджених або втрачених даних. Багатоплатформеність забезпечується

використанням на серверній частині різних ОС. Простоти в використанні можна досягнути якщо мінімізувати вплив людини використанням систем автоматизації. Швидке підключення – ця вимога відображає економію часу, тому проста інсталяція та налаштування є ключовими також моментами.

Параметри, що визначають резервне копіювання – це момент відката - встановлення точки, моменту в прошлому часі на який будуть встановлені дані (RPO), та час необхідний для відновлення даних з резервної копії.

Типи резервного копіювання:

1. повне копіювання – створення повної копії усіх даних;

2. диференційне копіювання – копіювання файлів даних, що були змінені з моменту останнього повного резервного копіювання, копіюється кожний раз по новому. Дуже важливе при загроз та атак на систему;

3. інкрементне (додаткове) копіювання – копіювання тільки тих елементів , що були змінені з останнього разу коли виконувалось повне або додаткове резервне копіювання. Усі наступні додаткові додають тільки змінені файли. Таке копіювання займає менше часу, але процес відновлення навпаки більше часу;

4. клонування – копіює розділ або носій цілком з усіма файлами на інший носій або розділ;

5. створення образу – створення точної копії розділу або носія, що зберігається в одному файлі;

6. холодне резервування – використання ненапруженого резерву;

7. гаряче резервування – використання напруженого резерву;

3.6.1Апаратне резервування

Апаратне резервування це найнадійніший засіб забезпечення надійності систем.

Резервування даних дозволяє забезпечити цілісність та доступність даних, які зберігаються в системі. Резервування даних в мережі лабораторії забезпечується:

– резервуванням дискової системи на основному сервері мережі;

– використання додаткового комп’ютера, на якому зберігаються копії даних;

– резервування конфігурацій мережевого обладнання.

Таким чином, для забезпечення резервування даних, необхідно використання надлишкових дискових масивів на сервері зберігання даних та організація внутрішньої ізольованої мережі для передачі даних між основним сервером та резервним.

Розрахунок дискової системи. Враховуючи, що необхідно, в першу чергу, організувати резервування на кожному критичному хості (сервері), було розроблено схеми RAID масивів, як на основному сервері, так і на резервному.

Резервування на основному сервері здійснено шляхом організації дзеркалювання даних, що дозволяє мати повну копію кожного диску системи, проте надлишковість апаратного забезпечення.

Для функціонування системи зберігання, на момент організації мережі, було визначено забезпечення загального дискового простору не менш 500 Гб.

Для забезпечення відмовостійкості серверів резервування, було визначено використання більш дешевих дисків з організацією в дисковий масив п’ятого типу

Дана конфігурація виконана в більш дешевому форматі:

– використання HDD дисків суттєво знизило вартість резервної системи;

– організація дисків в групи RAID 5 дозволило зменшити кількість дисків;

– організація дисків в групи RAID 5 дозволило підвищити швидкість читання та запису даних.

Враховуючи особливості даного формату RAID, запис можна здійснювати одночасно на кожний диск, що дозволяє організовувати кілька потоків запису та зменшити час резервування.

Внутрішня мережа резервування. Для того щоб здійснювати резервування даних в мережі, було визначену окрему фізичну підмережу, якій властиві наступні переваги:

– відсутність впливу на основний трафік мережі зберігання даних;

– окремі мережеві інтерфейси для передачі даних до серверів резервування;

– безпека передачі даних, за рахунок ізольованого сегменту.

3.7 Метод забезпечення захисту доступності

На основі запропонованих моделей можна впровадити модифікований метод забезпечення доступності, який передбачає ряд етапів, які реалізують оцінку захищеності інформаційної системи від загроз доступності.

Більшість етапів вимагають реалізації у вигляді програмних модулів та функцій.

На першому етапі проводиться автоматизована інвентаризація мережевих пристроїв віддаленої лабораторії:

– персональні комп’ютерні лабораторії;

– контролери;

– SCADA системи;

– комутатори;

– маршрутизатори;

– шлюзи;

На другому етапі проводиться аналіз програмного забезпечення, яке використовується на мережевому обладнанні. Використовуються спеціальні шаблони на основі фільтрів, що дозволяє створювати такі списки, які цікавлять адміністраторів виключно в контексті цільової системи.

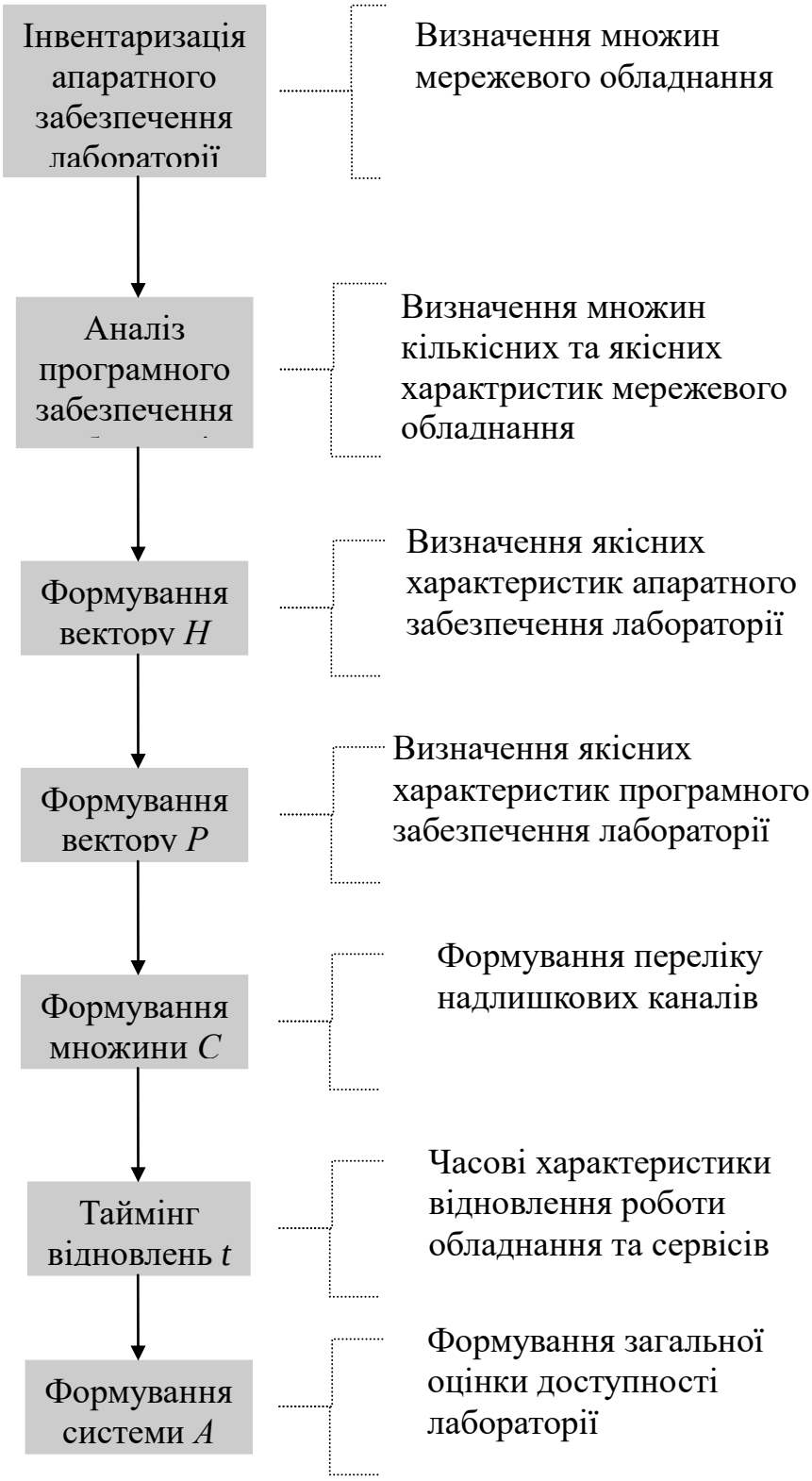

Рисунок 3.8 — Метод захисту доступності віддаленої лабораторії

На третьому етапі визначаються вектори оцінки апаратної складової інформаційної системи лабораторії. Оцінка базується на кількості інтерфейсів пристрою,

На четвертому етапі визначається вектор оцінки програмного забезпечення

На п’ятому етапі визначається множина комунікаційних каналів, які використовуються в системі та об’єднують кінцеві пристрої лабораторії.

На шостому етапі визначаються часові характеристики відновлення елементів лабораторії, таких як сервери, комутатори та їх інтерфейсів, контролери, та інше ключове обладнання.

На сьомому етапі визначається модель доступності віддаленої лабораторії на основі визначених векторів апаратних та програмних моделей та часових характеристик відновлення ресурсів.

3.8 Висновки до розділу

В третьому розділі кваліфікаційної дипломної роботи представлені методи забезпечення доступності інформаційних систем. Проведено дослідження основних заходів та механізмів, що забезпечують доступність інформації. На основі раніше зазначених вимог до роботи розроблена загальна модель забезпечення доступності та представлені усі складові її частини.

Проведено дослідження основних заходів забезпечення захисту та розроблено їх моделі. Представлені моделі програмного та апаратного забезпечення доступності інформації. Проведена параметризація елементів та складових частин цих моделей.

На основі проведеного дослідження різних видів зловживань та атак на інформаційні системи були розроблені моделі захисту від атак, що загрожують доступності до даних. Перша з моделей – це модель захисту від атаки «відмова в обслуговуванні». Наступні розроблені моделі забезпечують доступність використовуючи заходи захисту від небажаної розсилки. Це такі

заходи, як захист поштового сервісу, захист веб-систем, захист сховищ даних.

Останнє завдання в досліджені забезпечення доступності було визначення процесів та функцій резервування, як одного з найвикористовуючих засобів забезпечення доступності. Розглянуті та розроблені методи резервування на прикладі обладнання лабораторії.

Згідно з усіма розробленими моделями захисту даних запропонований метод захисту доступності віддаленої лабораторії.

ВИСНОВКИ

В результаті проведеного дослідження запропоновано разширення стандартних методів забезпечення доступності інформаційних систем та мереж за рахунок введення оціки надлишковості комунікаційних каналів та екстраполяції даних методів на систему дистанційного навчання.

Також, для більшості етапів реалізації методу, було розроблено моделі опису, аналізу та оцінки відповідних складових інформаційної навчальної системи:

- загальна модель забезпечення доступності визначає початковий набір характристик елементів системи для оцінки її доступності, яка описує прагнення досягти доступність до 100%;
- моделі апаратних та програмних складових учбової системи, які описують оцінки їх елементів, котрі визначають стійкість до порушення доступності інформації або складових систем;
- модель захисту від атак “відмова в обслуговуванні”, описує інтерфейсні харатеристики обладнання та його сервісів з боку визначення здатності проведення подібних атак;
- структурні моделі визначають організаційне застосування запропонованих моделей на реальних об’єктах віддаленої лабораторії та визначають організаційні, апаратні та програмні рішення для інформаційного захисту системи.

Усі запропоновані моделі визначають ієрархічну структуру захисту інформаційної системи та її мереж від атак, які спрямовані на порушення доступності системи. Метод захисту, який базується даних моделях, дозволяє оцінити систему перед вводом до експлуатації та під час неї, но покриває більшість життєвого цикли цільової інформаційної системи.

Впровадження даного методу супроводжується створенням множини скриптів, які необхідні для збору даних про стан елементів системи та сервісів, які необхідні для реалізації учбових активностей. Основними перевагами впровадження результатів даного дослідження є наступне:

- використання даного методу на етапі введення системи до роботи дозволило зменшити кількість відмов в обслуговувані на 13,4% в порівнянні з стандартними методами захисту;
- використання даного методу по відношенню існуючої інформаційної учбової системи дозволило скоротити кількість відмов на 9,3%;
- ефективність наявних атак в обслуговуванні на систему дистанційної освіти (віддалену лабораторію) зменшилася на 26,6%.

В якості існуючої системи віддаленої лабораторії використовувалася лабораторія мережевих технології кафедри комп'ютерні інтелектуальні системи та мережі. Під ефективністю наявних атак в обслуговувані розуміється тривалість недоступності системи в разі здійснення такої атаки.

До недоліків запропонованого методу можна віднести необхідність формування скриптів збору інформації, які повинні створювати програмісти або системні адміністратори з досвідом. Також, в ході дослідження були виявлені певні складнощі в проведенні оцінки параметрів інформаційної системи віддаленої лабораторії, зокрема трактовка отриманих результатів може залежати від досвіду аналітика та типу мережевого обладнання.

До подальшого розвитку даного дослідження пропонується розширення переліку параметрів які можуть впливати на доступність систем віддаленої лабораторії та збільшення рівня автоматизації збору інформації про елементів системи на основі графічного інтерфейсу.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. А.А. Барсегян, М.С. Купріянов, В.В. Степаненко, І.І. Холод. Методи і моделі аналізу даних: OLAP і DataMining, Пітер, 2015. – 1090 с.

2. M. Just. Designing authentication systems with challenge questions. In L. F. Cranor and S. Garfinkel, editors, Security and Usability: Designing Secure Systems that People Can Use, сторінки 143–155, Sebastopol, CA, 2005. O'Reilly Media, Inc. [Електронне джерело] Режим доступу: ttps://pdfs.semanticscholar.org/fbfb/c601e 582f904decf2f739a4e1d41ee86ec0d.pdf

3. K. D. Mitnick and W. L. Simon. The Art of Deception: Controlling the Human Element of Security. Wiley, 2012. [Електронне джерело]Режим доступу: http://sbisc.ut.ac.ir/wp-content/uploads/2015/10/mitnick.pdf

4. Social Authentication. Alex Rice[Електронне джерело] Режим доступу: blog.facebook.com/blog.php?post=486790652130.

5. J. Podd, J. Bunnell, and R. Henderson. Cost-effective computer security: Cognitive and associative passwords. In OZCHI '96: Proceedings of the 6th Australian Conference on Computer-Human Interaction (OZCHI '96), page 304, Washington, DC, USA, 1996. IEEE Computer Society. [Електронне джерело] Режим доступу: http://ieeexplore.ieee.org /document/560026/?reload=true

6. M. Zviran and W. J. Haga. User authentication by cognitive passwords: an empirical assessment. In JCIT: Proceedings of the Fifth Jerusalem Conference on Information technology, pages 137–144, Los Alamitos, CA, USA, 1990. IEEE Computer Society Press. [Електронне джерело]Режим доступу: https://www.researchgate.net/publication/3505320_User_authentication_by_cognitive_passwords_an_empirical_assessment

7. CREDANT Technologies. Mountains of mobiles left in the back of New York cabs, 16, 2008. [Електронне джерело]Режим доступу: www.credant.com/mountains-of-mobiles-left-in-the-back-of-new-york-cabs.html.

8. T. Bridis. Hacker impersonated Palin, stole e-mail password, Sept. 18, 2008. Associated Press. Режим доступу: http:// www.ycorpblog.com/2008/10/08/ impersonated.zip.

9. S. Schechter, S. Egelman, and R. W. Reeder. It’s not what you know, but who you know: A social approach to last-resort authentication. In CHI ’09: Proceedings of the ACM SIGCHI Conference on Human Factors in Computing Systems, Boston, MA, 2009. ACM. [Електронне джерело]Режим доступу: http://www.guanotronic.com/serge/ papers/chi09b.pdf