Міністерство освіти і науки України
Національний технічний університет
«Дніпровська політехніка»

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеня бакалавра

студента *Чурсіна Олександра Олександровича*

академічної групи *гр. 125-18-1*

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему: *Комплексна система захисту інформації ТОВ «Супутник С» з детальною розробкою підсистеми зберігання та обробки конфіденційних данних*

Керівники	Прізвище, ініціали	Оцінка за шкалою		Підпис
		рейтинговою	інституційною	
кваліфікаційної роботи				
розділів:				
спеціальний	Ст.викл.Святошенко В.О.			
економічний	к. е. н., доц. Пілова Д.П.	65	задовільно	

Рецензент				

Нормоконтролер	ст. викл. Тимофєєв Д.С.			

Дніпро
2022

ЗАТВЕРДЖЕНО:
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу ступеня бакалавра

студенту *Чурсіну О.О.* **академічної групи** *125*
(прізвище та ініціали) (шифр)

спеціальності *125 Кібербезпека*

спеціалізації

за освітньо-професійною програмою *Кібербезпека*

на тему ***Комплексна система захисту інформації ТОВ «Супутник С» з детальною розробкою підсистеми зберігання та обробки конфіденційних данних***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від _____
№ 268-с

Розділ	Зміст	Термін виконання
1	Загальні відомості та опис структурі підприємства; Обгрунтування постановки задачі	15.05.2022
2	Розробка моделі порушника, загроз та вибір профілю захищеності.	28.05.2022
3	Економічне обґрунтування доцільності розробки.	08.06.2022

Завдання видано _____ _____
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: _____

Дата подання до екзаменаційної комісії: _____

Прийнято до виконання _____ _____
(підпис студента) (прізвище, ініціали)

РЕФЕРАТ

Пояснювальна записка: 79с., 12 рис., 13 табл., 30 джерел.

Метою дипломної роботи є пошук захищеної системи хмарного сховища.

Об’єктом дослідження є процес забезпечення захищеності даних хмарного сховища.

Предметом дослідження є засоби забезпечення захищеності даних хмарного сховища.

Перший розділ представляє собою огляд основних понять предметної області.

У другому розділі проведено проектування і розробку моделей загроз і порушників, створено профіль захищеності, виявлено основні загрози і на основі порівняльного аналізу обрано хмарне рішення. .

Третій розділ присвячено економічному аналізу доцільності впровадження хмарного рішення підвищеного рівня безпеки.

КІБЕРБЕЗПЕКА, КІБЕРЗАГРОЗА, НЕСАНЦІОНОВАНИЙ ДОСТУП, ХМАРНІ СХОВИЩА, РОЗПОДІЛЕНІ ОБЧИСЛЕННЯ.

ABSTRACT

Explanatory note: 79p., 12 fig., 13 tables., 30 sources.

The purpose of the thesis is to find a secure cloud storage system.

The object of research is the process of ensuring the security of cloud storage data.

The subject of the study is the means of ensuring the protection of cloud storage data.

The first section is an overview of the basic concepts of the subject area.

The second section designed and developed models of threats and violators, created a security profile, identified the main threats and based on a comparative analysis selected a cloud solution. .

The third section is devoted to the economic analysis of the feasibility of implementing a cloud solution of increased security.

CYBER SECURITY, CYBER THREAT, UNAUTHORIZED ACCESS, CLOUD STORAGE, DISTRIBUTED CALCULATIONS.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ОС — Операційна система

NIST — National Institute of Standards and Technology

GPL — General Public License

API — Application Programming Interface

SAAS — програмне забезпечення як сервіс

PAAS — програмне забезпечення як сервіс

IAAS — програмне забезпечення як сервіс

КС – комп'ютерна система

ОС – операційна система

ОІД — Об’єкт інформаційної діяльності

АРМ — Автономне робоче місце

КЗ — Контрольована зона

КЗЗ — Комплекс засобів захисту

ПЗ — Програмне забезпечення

ЗМІСТ

ВСТУП

Оскільки хмарні сховища стають все більш поширеними, безпека даних стає більш серйозною проблемою для користувачів таких сервісів. Компанії та школи вже деякий час розширюють використання таких послуг, як Google Drive, і багато окремих користувачів також зберігають свої персональні файли в Dropbox, Box, Amazon Drive, Microsoft OneDrive тощо. Вони, без сумніву, стурбовані збереженням своєї інформації, а особливо питанням захищеності їх особистих даних.

Безумовно, використання хмарного сховища має багато переваг, але воно несе з собою деякі серйозні загрози безпеки, які можуть послабити ваш бізнес.

Дані, що зберігаються в хмарному сховищі, майже завжди зберігаються в зашифрованому вигляді, який необхідно зламати, перш ніж зловмисник зможе прочитати інформацію. Але як показує практика, зазвичай разом на сервері зберігаються також і самі ключі шифрування, що підвищує небезпеку використання таких сервісів.

Тому актуальним є пошук захищеної системи хмарного сховища яка дозволить здійснювати захищене зберігання даних у зашифрованому вигляді на хмарному сервісі без використання процедур збереження ключів, що дозволить підвищити рівень захищеності даних користувачів при вивантажені їх на віддалене хмарне сховище.

Метою дипломної роботи є пошук захищеної системи хмарного сховища.

Об’єктом дослідження є процес забезпечення захищеності даних хмарного сховища.

Предметом дослідження є засоби забезпечення захищеності даних хмарного сховища.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ І СТАНУ ПИТАННЯ

1.1 Поняття хмарних сховищ

В останні роки ефективного застосування набувають хмарні технології або хмарні обчислення (англ. Cloud computing). В [1] дається визначення хмарних обчислень як моделі забезпечення повсюдного та зручного доступу через мережу до спільного пулу обчислювальних ресурсів, що підлягають налаштуванню (наприклад, до комунікаційних мереж, серверів, засобів збереження даних, прикладних програм та сервісів), які можуть бути оперативно надані та звільнені з мінімальними експлуатаційними затратами або зверненням до провайдера. До хмарних технологій проявляють зацікавленість як великі компанії, які намагаються оптимізувати свої витрати на IT-інфраструктуру підприємства, так і малі компанії, які не мають можливості відразу розгорнути свою власну інфраструктуру. Також зацікавлені звичайні користувачі, що можуть отримати такі послуги як зберігання даних, використання програм тощо.

Зростання інтересу до технології хмарних обчислень пов’язано з економічним ефектом від їх використання. В ході їх використання споживачі можуть істотно знизити капітальні витрати на побудову центрів обробки даних (ЦОД), закупівлю серверного та мережного обладнання, апаратних і програмних рішень, забезпечення безперервності і працездатності, а також час побудови та введення в експлуатацію великих об’єктів інфраструктури інформаційних технологій. Всі ці проблемні питання за даних умов перекладаються з користувачів на провайдерів хмарних послуг, а користувач лише оплачує фактично надані послуги.

Також хмарні сервіси надають користувачам гнучкість у налаштуванні таких параметрів, як обчислювальна потужність, обсяг файлового сховища, склад програмного забезпечення тощо. Однак, незважаючи на явні переваги, під час використання хмарних обчислень необхідно вирішувати і ряд проблемних питань.

Основними з них є довіра до постачальника сервісу, забезпечення конфіденційності, цілісності та доступності інформації на усіх етапах її існування, безперебійність в роботі, захист від несанкціонованого доступу (НСД) та збереження особистих даних користувачів, які передаються та обробляються в хмарі [2].

Хмарне сховище даних – це назва моделі, в якій дані зберігаються на розподілених в мережі серверах, які надаються в основному третьою стороною. На відміну від моделі, коли дані знаходяться на власних серверах, внутрішня структура організації зберігання даних скрита від користувача [3].

Згідно документу IEEE опублікованому в 2008 році, «хмарна обробка даних – це парадигма, в рамках якої інформація постійно зберігається на серверах в мережі Інтернет і тимчасово кешується на клієнтській стороні, наприклад, на персональних комп'ютерах, ігрових приставках, ноутбуках, смартфонах і т. п.» [4].

Хмарно-орієнтоване середовище даних – це група серверів, на яких дані користувачів зберігаються у режимі онлайн. Тобто всі дані можуть зберігатись і опрацьовуватись у хмарі, що є віртуальним сервером і може розташовуватись у різних куточках планети [5].

Всі існуючі моделі хмарних обчислень можна розділити на три основні типи: приватні, загального користування та гібридні.

При зберіганні даних у хмарі через робочий комп'ютер можна отримати доступ до них з будь-якого іншого пристрою, наприклад, з планшета, смартфона або ноутбука. Всі зміни з файлами (редагування, копіювання, сортування або вилучення) будуть автоматично відображені на всіх пристроях. Спільний доступ можна надавати окремим файлам і папкам. Це дуже зручно у випадку, коли група осіб працює над спільним проектом. Наприклад, якщо один з членів команди завантажує файли в спільну папку, то інші учасники одразу ж отримують до нього доступ. При цьому не потрібно відправляти файл кожному з членів проекту персонально [6].

Переваги хмарних сховищ даних:

1. Можливість доступу до даних з будь-якого пристрою (ПК, планшету, смартфону тощо), в будь-який час (при наявності виходу в Інтернет).

2. Можливість організації спільної роботи з даними.

3. Економія дискового простору на жорсткому диску комп'ютера, що дозволяє підвищити продуктивність операційної системи комп'ютера.

4. Висока ймовірність збереження даних навіть у разі апаратних збоїв.

5. Клієнт платить тільки за те місце в сховищі, яке фактично використовує, а не за оренду сервера, всі ресурси якого він може і не використовувати.

6. Клієнту немає необхідності займатися придбанням, підтримкою і обслуговуванням власної інфраструктури зберігання даних, що в результаті зменшує загальні витрати виробництва.

7. Всі процедури по резервуванню і збереженню цілісності даних виконуються провайдером «хмарного» центру, який не втягує в цей процес клієнта.

8. Можливість використання будь-якої операційної системи.

9. Оновлення програм відбувається автоматично та своєчасно.

Недоліки хмарних сховищ даних:

1. Небезпека у процесі зберігання та пересилання даних.

2. Загальна продуктивність при роботі з даними в «хмарі» може бути нижчою, ніж при роботі з локальними копіями даних.

3. Необхідність наявності стабільного та швидкісного під'єднання до мережі Інтернет.

4. Обмежений перелік програмного забезпечення, яке може використовуватися.

5. Обладнання для побудови власного хмарного сховища є досить дорогим.

З точки зору постачальника, завдяки об'єднанню ресурсів та непостійному характеру споживання з боку користувачів, хмарні технології дозволяють економити на масштабах, використовуючи менші апаратні ресурси, ніж при виділенні апаратних потужностей для кожного користувача, а за рахунок

автоматизації процедур модифікації виділення ресурсів істотно знижуються витрати на абонентське обслуговування.

З точки зору користувача, ці характеристики дозволяють отримати послуги з високим рівнем доступності і низькими ризиками непрацездатності, забезпечити швидке масштабування обчислювальної системи завдяки еластичності без необхідності створення, обслуговування і модернізації власної апаратної інфраструктури [8].

Згідно згаданого принципу «4-3-2», друга цифра характеризує три основних методи постачання хмарних сервісів: Infrastructure-As-A-Service (IaaS), Platform-As-A-Service (PaaS) та Software-As-A-Service (SaaS):

IaaS (інфраструктура як послуга) надається як можливість використання хмарної інфраструктури для самостійного управління ресурсами обробки та зберігання, мережами та іншими фундаментальними обчислювальними ресурсами. Наприклад, споживач може встановлювати і запускати довільне програмне забезпечення, контролювати операційні системи, віртуальні системи зберігання даних і встановлені програми, а також володіти обмеженим контролем над набором доступних мережевих сервісів. Контроль і управління основною фізичною і віртуальною інфраструктурою хмари (в тому числі мережі, серверів, типів використовуваних операційних систем, систем зберігання) здійснюється хмарним провайдером [9]. У цьому випадку постачальник послуги надає в оренду обчислювальні ресурси. Це може бути сукупність віртуальних машин, сховищ даних, мережевих елементів різних типів. За допомогою IaaS користувач отримує можливість швидко розгортати копії ОС, запускаючи віртуальні копії ряду програмних пакетів. У цьому випадку немає необхідності розгортати власну мережеву інфраструктуру. Все необхідне можна отримати у постачальника IaaS. При цьому таке середовище практично завжди є гнучким і масштабованим.

Найбільшими постачальниками інфраструктури як послуги є Amazon, Microsoft, VMWare, Rackspace та Red Hat. Хоча деякі з них пропонують більше, ніж просто інфраструктуру, їх об’єднує мета продавати базові обчислювальні ресурси.

PaaS (платформа як послуга) – модель надання хмарних обчислень, при якій споживач отримує доступ до використання інформаційно-технологічних платформ: операційних систем, систем управління базами даних, засобів розробки і тестування, розміщеним у хмарного провайдера. В цій моделі вся інформаційно-технологічна інфраструктура, включаючи обчислювальні мережі, сервери, системи зберігання, цілком керується провайдером. Провайдер так само визначає набір доступних для споживачів видів платформ і їх керованих параметрів. Споживач може використовувати платформи на свій розсуд, створюючи їх віртуальні екземпляри, встановлюючи, розробляючи і тестуючи на них прикладне програмне забезпечення. При цьому існує можливість динамічної зміни кількості споживаних обчислювальних ресурсів [10]. Найчастіше PaaS використовується програмістами, які спільно працюють над різними проектами. В цьому випадку всі або частина розробників отримують доступ до єдиного середовища розробки віддалено.

З PaaS розробники абстрагуються від нище лежачої інфраструктури. Наприклад, Google Apps надає платформи для бізнесу в режимі онлайн, доступ до яких відбувається за допомогою Інтернет-браузера тоді як програмне забезпечення і дані зберігаються на серверах Google.

SaaS (програмне забезпечення як послуга) – одна з форм хмарних обчислень, модель обслуговування, при якій передплатникам надається готове прикладне програмне забезпечення, яке повністю обслуговується провайдером. Постачальник в цій моделі самостійно управляє додатком, надаючи замовникам доступ до функцій з клієнтських пристроїв, як правило через мобільний додаток або веб-браузер [11]. Основна перевага моделі SaaS для споживача послуги полягає у відсутності затрат, пов’язаних з установкою, оновленням та підтримкою працездатності обладнання і працюючого на ньому програмного забезпечення

Прикладами SaaS можуть служити MicrosoftOffice 365, Gmail та Google docs.

Рівневе представлення хмарних сервісів наведено на рис. 1.1.

Зі зростанням рівня методу постачання хмарних послуг зростає й оглядова цінність для кінцевого користувача, і, відповідно, кількості абонентів даного виду послуг (рис. 1.2).

Хоча на сьогодні й існує широка таксономія термінів, які звужують контекст, але в цілому все зводиться до цих трьох сервісів. Ці три типи сервісів можуть працювати окремо або в комбінації один з одним.

Остання цифра в принципі «4-3-2» характеризує тип хмари: приватний чи публічний. Хоча тип хмари впливає на розміщені в ній сервіси достатньо опосередковано – для кінцевого користувача використання сервісу, який розміщений в приватній хмарі чи в публічній, може не нести жодної різниці – використання практично завжди повністю прозоре. Аналогічно до методів постачання, існують додаткові терміни, що характеризують тип хмари, наприклад, Community Cloud, але дані типи так чи інакше є або розвитком, або симбіозом приватного чи публічного типів.

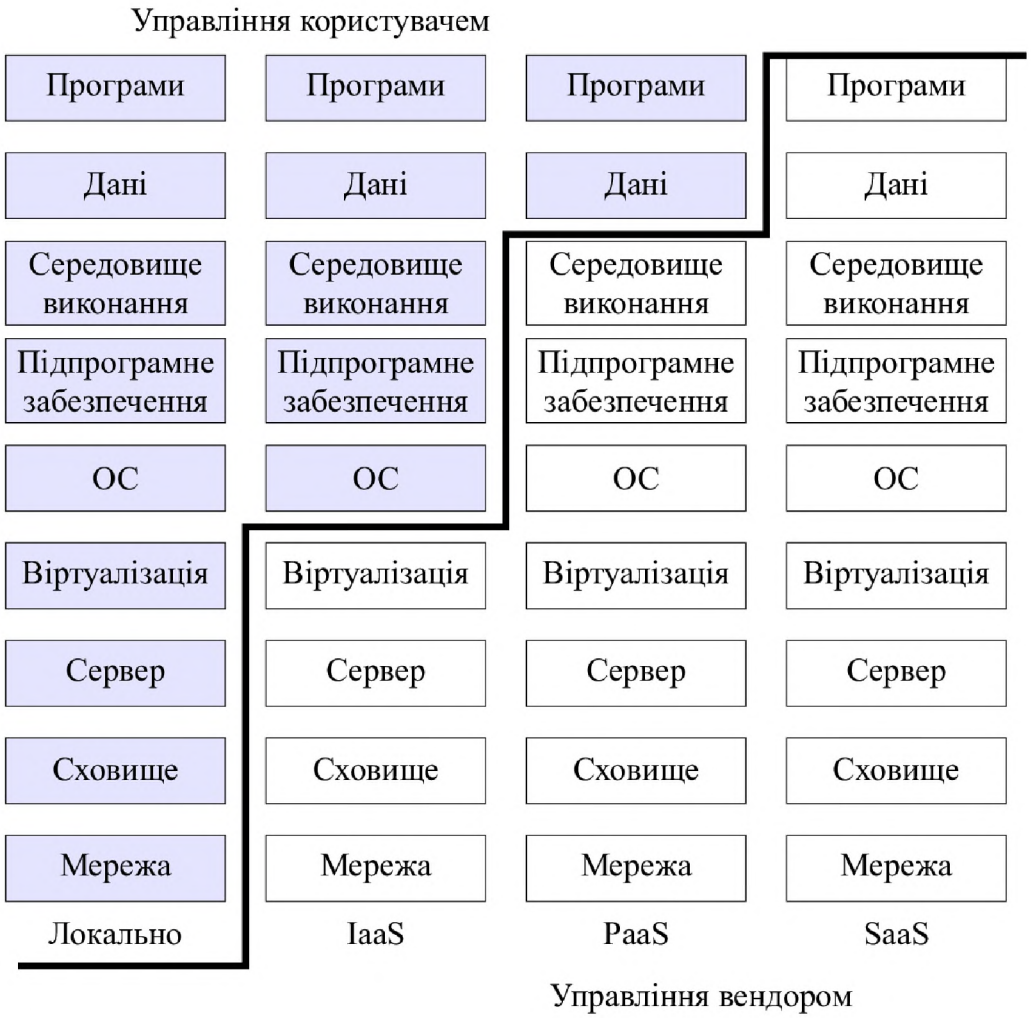


Рисунок 1.1 — Рівневе представлення хмарних сервісів

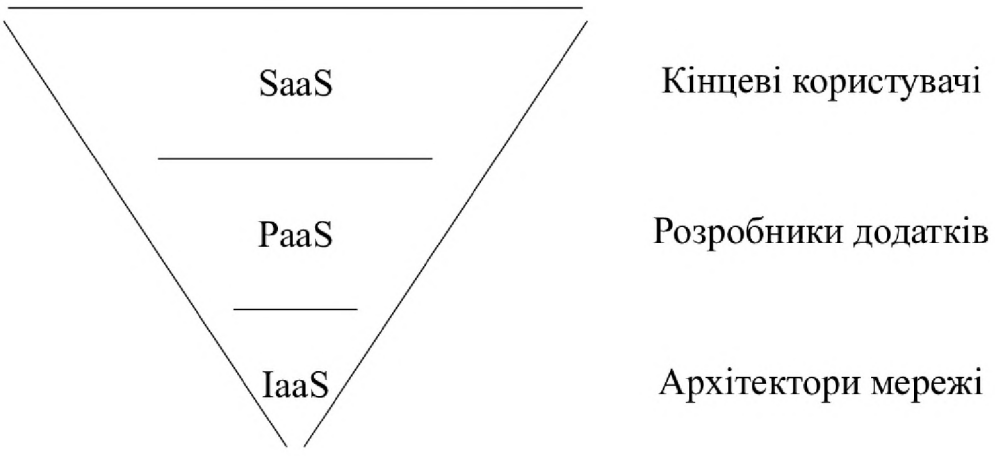


Рисунок 1.2 — Моделі роботи з хмарою для різних груп користувачів

Таким чином, хмарні технології охоплюють окрім самих обчислень, такі області, як зберігання даних, інформаційні послуги, інтеграцію, безпеку,

організацію певних процесів і управління. Причому один і той же провайдер може пропонувати будь-який перелік послуг. Користувач же може отримувати весь спектр послуг у одного провайдера, а може скористатися і різними провайдерами для певних різновидів сервісів. Наявне різноманіття провайдерів і сервісів істотно ускладнює процес вибору для користувача.

Одним з основних підходів до реалізації хмарної інфраструктури є технологія віртуалізації – надання обчислювальних ресурсів, абстраговане від їх реальної апаратної реалізації. Наприклад, одночасне використання декількох, ізольованих одна від одної, операційних систем і додатків на одному комп'ютері. Сукупність комп'ютерних ресурсів, які емулюють роботу окремих компонентів апаратного або програмного забезпечення, або навіть цілого комп'ютера, прийнято називати віртуальною машиною. Наявність декількох віртуальних машин на одному реальному комп'ютері забезпечує можливість незалежної роботи на одному фізичному сервері (вузлі) кількох операційних систем і додатків.

Віртуалізація може поліпшити адаптивність, гнучкість і масштабованість IT-середовища і суттєво знизити витрати. Віртуалізація дозволяє більш ефективно використовувати обчислювальні потужності і спільно використовувати ресурси різних апаратних пристроїв при обслуговуванні багатокористувацьких клієнтів. Крім того, віртуалізація прискорює розгортання робочих навантажень, підвищує їх продуктивність і доступність, а також дає можливість автоматизувати багато процесів.

В даний час існують дві основні технології створення систем хмарних обчислень, засновані на віртуалізації серверів: віртуалізація на основі гіпервізора та контейнерна віртуалізація (рис. 1.3).

У першому підході віртуалізація здійснюється за допомогою гіпервізора – програмної надбудови над основною ОС, яка відділяє віртуальні машини від сервера і в міру необхідності динамічно виділяє обчислювальні ресурси кожної ВМ (Amazon, Azure, VMWare) [12]. Використання такого підходу не є суворою

вимогою і існує інший спосіб, який використовує ізольовані контейнери (OpenVZ, LXC (Linux Containers), Docker) [13-16].

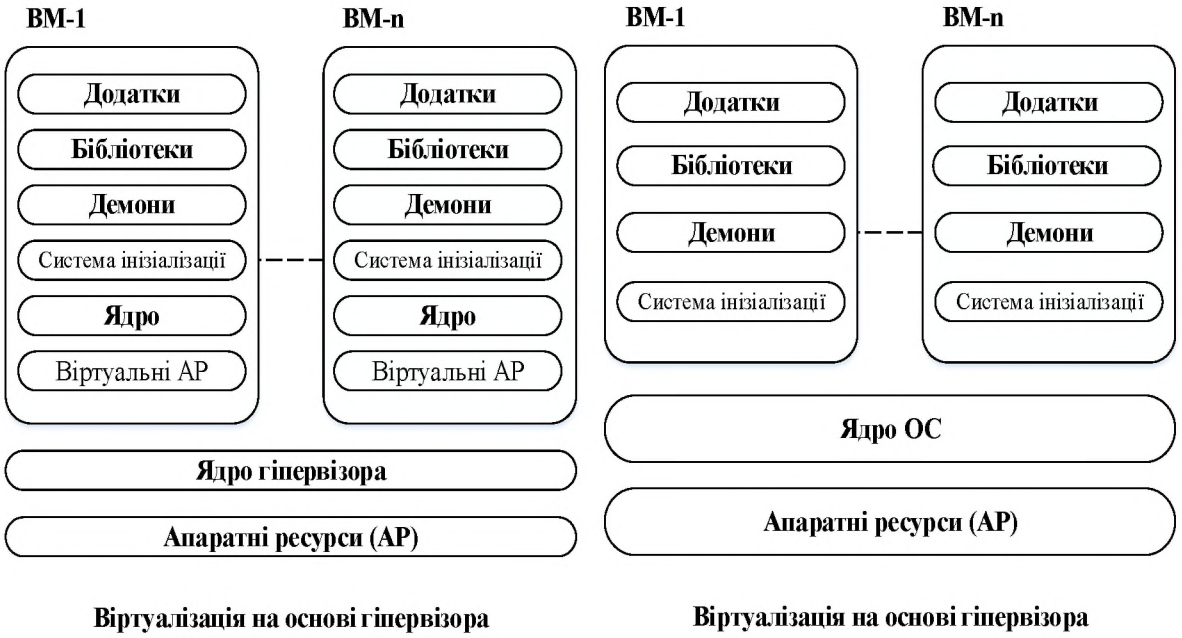


Рисунок 1.3 — Порівняння двох технологій віртуалізації

У кожному з цих підходів є як свої переваги, так і недоліки. Підхід з використанням віртуалізації дозволяє запускати в хмарі ОС будь-яких виробників, але втрачаючи при цьому в продуктивності від 8 до 12 відсотків в порівнянні з використанням фізичного сервера. Другий підхід вигідніше з точки зору обчислювальної продуктивності системи і економії дискових ресурсів, тому що контейнери використовують ядро основної системи. При цьому користувачі обмежені у виборі ОС тільки збірками сімейства GNU/Linux, що в більшості випадків розглядається як істотний недолік контейнерної віртуалізації. У той же час, суттєва перевага в продуктивності дозволяє в цьому випадку використовувати ресурси хмари навіть для високопродуктивних обчислень [13]. В останні роки і такі великі гравці на ринку хмарних послуг, як Amazone і Azure, крім традиційної віртуалізації на основі гіпервізора стали надавати послуги на основі контейнерних технологій [17]. Google використовували дану технологію спочатку як основну [18].

Другим недоліком до недавнього часу були серйозні проблеми в безпеці: так як кожен контейнер має доступ до ядра основної системи, то потенційний зловмисник міг отримати привілейовані права в основній системі зламавши один з контейнерів в хмарі. Однак IT-технології не стоять на місці і, наприклад, в останніх розробках системи віртуалізації LXC з'явилася можливість запускати непривілейовані контейнери, зламавши які, зловмисник отримає тільки обмежені права користувача в основній системі [19].

1.2 Захищеність хмарних сховищ

За даними Cloud Security Alliance (CSA), більше 70 відсотків підприємств в світі зараз працюють – по крайній мірі, частково в хмарі.

З такими перевагами, як зниження фіксованих витрат, більш висока гнучкість, автоматичне оновлення програмного забезпечення, розширення спільної роботи і свобода роботи з будь-якого місця, 70 відсотків не є великим сюрпризом.

Проте, у хмарних сховищ є своя частка проблем безпеки.

Нещодавно «Звіт про безпеку хмарних обчислень» показав, що «90 відсотків організацій дуже або помітно стурбовані безпекою загальнодоступних хмар». Ці проблеми охоплюють широкий спектр питань: від уразливості до злому облікових записів, від зловмисників і до повномасштабних порушень даних [1].

Хоча хмарні сервіси відкрили нову епоху передачі і зберігання даних, багато компаній все ще вагаються чи роблять кроки без чіткого плану забезпечення безпеки.

Розглянемо проблеми забезпечення безпеки хмарних сховищ.

1. Порушення даних

Хмарні обчислення і сервіси є відносно новими, проте порушення даних у всіх формах існують роками. Залишається питання: «Якщо конфіденційні дані зберігаються в Інтернеті, а не в приміщенні, чи є хмарне сховище за своєю природою менш безпечним?»

Дослідження, проведене Інститутом Ponemon під назвою «Атака людини в хмарі», повідомляє, що понад 50 відсотків опитаних IT-фахівців і фахівців в області безпеки вважають, що заходи безпеки їх організацій із захисту даних в хмарних службах є низькими. У цьому дослідженні використовувалися дев'ять сценаріїв, де відбулося порушення даних, щоб визначити, чи було це переконання дійсно обґрунтованим [1].

Після оцінки кожного сценарію в звіті був зроблений висновок про те, що загальне порушення даних було в три рази більше ймовірним для компаній, що використовують хмарні сховища даних, ніж для компаній, які цього не роблять. Простий висновок полягає в тому, що хмарне сховище має унікальний набір характеристик, які роблять його більш уразливим.

2. Злом акаунтів

Зростання і впровадження хмарних сховищ в багатьох організаціях відкрили цілий ряд нових проблем із захопленням акаунтів.

Зловмисники тепер можуть використовувати інформацію для входу в систему ваших (або ваших співробітників) для віддаленого доступу до конфіденційних даних, що зберігаються в хмарі; Крім того, зловмисники можуть підробляти інформацію і маніпулювати нею за допомогою зламаних облікових даних [2].

Інші способи викрадення включають помилки сценаріїв і повторно використовувані паролі, які дозволяють зловмисникам легко і часто без виявлення крадіжки облікових даних. У квітні 2010 року Amazon зіткнулася з помилкою міжсайтового скриптингу, яка також була спрямована на облікові дані клієнтів. Фішинг, кейлоггінг і переповнення буфера – всі вони представляють подібні загрози. Однак найбільш помітна нова загроза, відома як атака «Людина в хмарі», включає в себе крадіжку призначених для користувача токенів, які хмарні платформи використовують для перевірки окремих пристроїв без необхідності входу в систему при кожному оновленні та синхронізації.

3. Інсайдерська загроза

Атака зсередини організації може здатися малоймовірною, але внутрішня загроза існує. Співробітники можуть використовувати свій авторизований доступ до хмарним службам організації для неправомірного використання або доступу до такої інформації, як облікові записи клієнтів, фінансові форми і інша конфіденційна інформація.

Крім того, ці інсайдери можуть навіть не мати злих намірів.

Дослідження, проведене Imperva «Внутрішній контроль загроз з боку інсайдерів», показало, що загрозою зсередини є зловживання інформацією в результаті зловмисних дій, нещасних випадків або шкідливих програм. В ході дослідження також були вивчені чотири передових практики, які компанії могли б використовувати для реалізації безпечної стратегії, такі як ділові партнерства, встановлення пріоритетів ініціатив, контроль доступу і впровадження технологій.

4. Ін'єкція шкідливих програм

Ін'єкції шкідливого ПО – це скрипти або код, вбудовані в хмарні сервіси, які діють як «допустимі екземпляри» і запускаються як SaaS для хмарних серверів. Це означає, що шкідливий код може бути впроваджений в хмарні служби і розглядатися як частина програмного забезпечення або служби, яка працює на самих хмарних серверах [2].

Коли ін'єкція виконується і хмара починає працювати разом з нею, зловмисники можуть підслуховувати, порушувати цілісність конфіденційної інформації і красти дані. Загрози безпеці в вразливості хмарних обчислень, звіт Університету Східної Кароліни, аналізує загрози впровадження шкідливих програм в хмарні обчислення і стверджує, що «атака впровадження шкідливих програм стала основною проблемою безпеки в системах хмарних обчислень» [2,3].

5. Зловживання хмарними сервісами

Розширення хмарних сервісів дозволило як малим, так і корпоративним організаціям легко розміщувати величезні обсяги даних. Однак хмарна безпрецедентна ємність сховища також дозволила як хакерам, так і авторизованим

користувачам легко розміщувати і поширювати шкідливі програми, нелегальне програмне забезпечення та інші цифрові властивості.

У деяких випадках ця практика зачіпає як постачальника хмарних послуг, так і його клієнта. Наприклад, привілейовані користувачі можуть прямо або побічно збільшувати ризики безпеки і в результаті порушувати умови використання, що надаються постачальником послуг.

Ці ризики включають в себе обмін піратським програмним забезпеченням, відео, музикою та книгами і можуть привести до юридичних наслідків у вигляді штрафів і розрахунків відповідно до законів. Залежно від шкоди, ці штрафи можуть бути ще більш позамежними. Можна зменшити схильність до ризику, контролюючи використання і встановлюючи керівні принципи для розміщення співробітників в хмарі. Постачальники послуг і юридичні особи, такі як CSA, визначили, що є образливим або недоречним поведінкою, поряд з методами виявлення такої поведінки.

6. Небезпечні API

Інтерфейси прикладного програмування (API) дають користувачам можливість налаштовувати свій функціонал роботи в хмарному сховищі.

Однак API-інтерфейси можуть становити загрозу для хмарної безпеки через їх природу. Вони не тільки дають компаніям можливість налаштовувати функції своїх хмарних сервісів відповідно до потреб бізнесу, але і аутентифікувати, надавати доступ і шифрувати дані [4].

У міру того, як інфраструктура API-інтерфейсів зростає для забезпечення кращого обслуговування, збільшуються і ризики безпеки. API надають програмістам інструменти для створення своїх програм для інтеграції їх додатків з іншим критично важливим для роботи програмним забезпеченням. Популярним і простим прикладом API є YouTube, де розробники можуть інтегрувати відео YouTube в свої сайти або додатки.

Уразливість API полягає в зв'язку між додатками. Хоча це може допомогти програмістам і підприємствам, вони також залишають вразливі ризики безпеки.

7. Відмова в обслуговуванні

На відміну від інших видів кібератак, які зазвичай запускаються для встановлення довгострокової точки опори і захоплення конфіденційної інформації, атаки типу «відмова в обслуговуванні» не намагаються порушити ваш периметр безпеки. Швидше, вони намагаються зробити сайт і сервери недоступними для законних користувачів. Однак в деяких випадках DoS також використовується в якості димової завіси для інших зловмисних дій і для усунення пристроїв безпеки, таких як брандмауери веб-додатків.

8. Недостатня юридична перевірка

Більшість проблем, які розглянуті в цьому пункті, носять технічний характер, проте цей конкретний пробіл у безпеці виникає, коли організація не має чіткого плану своїх цілей, ресурсів і політик для хмари. Іншими словами, це фактор людей.

Крім того, недостатня юридична перевірка може створити загрозу безпеці, коли організація швидко мігрує в хмару, не чекаючи, що служби не будуть відповідати очікуванням клієнта.

Це особливо важливо для компаній, чиї дані підпадають під регулюють закони, такі як PII, PCI, PHI і FERPA, або тих, які обробляють фінансові дані для клієнтів.

9. Загальні уразливості

Безпека в хмарі – це спільна відповідальність між постачальником і клієнтом.

Це партнерство між клієнтом і постачальником вимагає від клієнта вживання профілактичних заходів для захисту своїх даних. У той час як основні провайдери, такі як Box, Dropbox, Microsoft і Google, мають стандартизовані процедури для захисту свого боку, точний контроль зерна залежить від вас, клієнта [5, 6].

Як зазначає Skyfence в своїй статті «Безпека та спільне використання Office 365», це залишає в ваших руках ключові протоколи безпеки, такі як захист

паролів користувачів, обмеження доступу до файлів і пристроїв і багатофакторна аутентифікація.

Суть полягає в тому, що клієнти і постачальники мають загальні обов'язки, і якщо їх не виконувати, це може привести до компрометації ваших даних.

10. Втрата даних

Дані в хмарних службах можуть бути втрачені в результаті зловмисної атаки, стихійного лиха або видалення даних постачальником послуг. Втрата важливої інформації може мати руйнівні наслідки для підприємств, які не мають плану відновлення. Amazon є прикладом організації, яка постраждала від втрати даних в результаті постійного знищення даних багатьох своїх клієнтів в 2011 році.

Google була ще однією організацією, яка втратила дані, коли її енергосистема була вражена блискавкою чотири рази.

Захист ваших даних означає ретельний аналіз процедур резервного копіювання вашого постачальника, оскільки вони пов'язані з фізичним розташуванням сховищ, фізичним доступом і фізичними лихами.

Згідно з останніми новинами в області інформаційної безпеки досить багато хмарних сховищ даних не забезпечують надійного захисту інформації. Атаки на шляху передачі інформації ускладняються і набирають швидкість.

Корпорація Microsoft в квітні 2020 року опублікувала звіт про загрози інформаційної безпеки Security Intelligence Report за період з лютого 2019 року. Він базується на даних, отриманих захисними програмами і сервісами компанії (дані про кількість виявлених загроз, а не про випадки зараження).

Кількість пристроїв в Україні, що зіткнулися з кіберзагрозами в період з лютого 2019 року по січень 2020 року, досягло 25-30% в середньому в місяць, тоді як аналогічний показник у першому кварталі 2019 року був майже в два рази менше – 15%. Найвищі показники були зафіксовані в Пакистані, Непалі, Бангладеш і Україні (33,2% або вище), найнижчі – в Фінляндії, Данії, Ірландії та США (11,4% або нижче).

В ході дослідження з'ясувалося, що хмарні додатки з низьким рівнем безпеки є мішенню для зловмисників. 79% SaaS-додатків для хмарного зберігання

даних і 86% SaaS-додатків для спільної роботи не забезпечують шифрування ні інформації що зберігається, ні переданої інформації.

Отже, до основних проблем хмарних сховищ даних належать:

– недостатня безпека при зберіганні і пересиланні даних;

– залежність надійності, своєчасності отримання і доступності даних від багатьох проміжних параметрів, таких як: канали передачі даних на шляху від клієнта до хмари, якість роботи інтернет-провайдера клієнта, доступність самої хмари в даний момент часу;

– загальна продуктивність при роботі з даними в «хмарі» може бути нижче, ніж при роботі з локальними копіями даних [20].

У зв'язку з технологічними особливостями, використовуваними для побудови структури хмарних обчислень, до стандартних типів загроз, які є наслідком розміщення ресурсів на фізичних серверах, додалися складності, пов'язані з контролем хмарного середовища віртуалізації, трафіку між клієнтськими машинами та розмежуванням прав доступу. Більш того, розподілена і відкрита структура хмарних обчислень з мультидоменною і розрахованою на багато користувачів структурою стала дуже привабливою мішенню для потенційних зловмисників.

Як відмічалося вище, архітектура хмарних сервісів складається з трьох взаємозалежних рівнів: інфраструктура, платформа і додатки. Кожен з цих рівнів може бути уразливий до програмних і конфігураційних помилок, допущених користувачами або провайдерами сервісу. Система хмарних обчислень може піддаватися декільком видам загроз безпеки – включаючи загрози цілісності, конфіденційності та доступності її ресурсів, даних і віртуальної інфраструктури, які можуть бути використані нецільовим чином, наприклад, в якості майданчика для поширення нових атак [21].

Зберігання даних в хмарі означає, що ці дані містяться на загальнодоступних серверах. Якщо компанія переведе в хмару, без урахування непередбачених наслідків, критичні корпоративні дані, такі, як, наприклад, інформація про клієнтів або інтелектуальна власність, то вони зазнають

підвищеного ризику. При цьому юридична відповідальність за збереження інформації як і раніше лежить на організації, що розмістила ці дані в хмарі, а не на провайдері хмарних послуг.

Інша серйозна проблема з захистом даних в хмарі – це відсутність можливості для клієнта хмарних послуг самому проводити аудит і контролювати події служби безпеки, наприклад, за допомогою перевірки лог-файлів, що може серйозно обмежити можливості по пошуку подій, які призвели до порушення безпеки системи.

У хмарних обчисленнях важливу роль відіграє технологія віртуалізації. Однак принципи віртуалізації містять потенційні загрози інформаційній безпеці хмарних обчислень, наприклад, пов'язані з використанням загальних сховищ даних різними ВМ. Кожна ВМ зберігається у вигляді образу, який являє собою окремий файл. Розміри цих файлів можуть бути змінені в залежності від поточних потреб користувача сервісу. Зменшення розміру розділу однією з ВМ хмари і збільшення розділу іншої, можуть привести до того, що фізичні сектора, що містять інформацію про віддалені файли, перемістяться з однієї ВМ на іншу. В результаті користувач іншої ВМ може отримати доступ і відновити дані, які раніше належали іншій організації.

Одним з можливих рішень є шифрування всієї інформації. В цьому випадку зашифрована інформація не зможе бути відновлена без відповідних ключів [22], однак слід враховувати, що шифрування може зажадати додаткових обчислювальних ресурсів і значно уповільнювати процес читання і запису даних.

Віртуальні машини динамічні, вони клонуються і можуть переміщатися між фізичними серверами. Дана мінливість впливає на розробку цілісності системи безпеки. Однак уразливості ОС або додатків у віртуальному середовищі поширюються безконтрольно і часто проявляються після довільного проміжку часу (наприклад, при відновленні з резервної копії). У середовищі хмарних обчислень важливо надійно зафіксувати стан захисту системи, незалежно від її місця розташування.

Уразливості всередині віртуального середовища. Сервери хмарних обчислень і локальні сервери використовують одні і ті ж ОС і додатки. Для хмарних систем загроза віддаленого злому або зараження шкідливим ПЗ висока. Система виявлення та запобігання вторгнень повинна бути здатна виявляти шкідливу активність на рівні віртуальних машин, незалежно від їх розташування в хмарному середовищі.

Навіть коли віртуальна машина вимкнена, вона також наражається на небезпеку зараження. Доступу до сховища образів віртуальних машин через мережу для цього цілком достатньо, при цьому на виключеній віртуальній машині неможливо запустити захисне програмне забезпечення. В даному випадку повинен бути реалізований захист не тільки всередині кожної віртуальної машини, а й на рівні гіпервізора.

1.3 Постановка задачі

Виходячи з описаних вище недоліків систем хмарного зберігання даних можна зробити висновок про необхідність пошуку рішень, які будуть покривати основні загрози підприємства.

Отже, основна задача полягає в побудові моделі загроз для підприємства і знаходження хмарного рішення, яке буде гарантувати безпеку відносно виявлених загроз.

1.4 Обстеження на об’єкті інформаційної діяльності

Об’єктом інформаційної діяльності являється товариство з обмеженою відповідальністю «Супутник С».

Вид діяльності: діяльність у галузі комп'ютерного програмування, консультаційні послуги у галузі комп'ютерних технологій інші види діяльності в галузі інформаційних технологій та комп'ютерних систем, інша професійна, наукова та технічна діяльність, не включена до інших категорій.

Характеристика складових ОІД

Контрольована зона обмежена стінами будівлі центрального офісу, та стінами серверних приміщень віддалених відділень підприемства. Забезпечуеться приватним охоронним агентством на підставі укладеного договору.

Характеристики будівлі центрального офісу:

- центральний офіс ТОВ «Супутник С» розташований в двох поверховій будівлі на першому поверсі, в будівлі маєтьcя підвальне приміщення, загальна площа офісного приміщення —приблизно 320 м^2.
- стіни, та несучі конструкція монолітна залізобетонна конструкція, товщина 350 мм.
- перекриття між поверхами виконане з пустотних залізобетонних плит
- внутрішні перестінки виконані з гіпсокартону на металевому каркасі, товщиною 150 мм.
- стеля підвісна, загальна висота від підлоги 320 см., висота міжстелевого проміжку 20 см. (на першому поверсі), 50 см. (на другому та третьому поверхах).
- підлога в приміщеннях офісу покрита кахельною плиткою.
- вікна — металопластикові пакети з двійним склом.
- фасадні двері виконані з металопластику з подвійним склом, тильні виконані з металу та дерева.
- Системи електропостачання, водопостачання, опалення та каналізації централізовані. Входять до будівлі через підвальне приміщення, виходять за межі КЗ.

Таблиця 1.1 — Специфікація приміщень будівлі ТОВ «Супутник С»

№ приміщення	Назва відділу, який займає кабінет
1	Хол. На 1-му поверсі. Рецепція
2	Коридорне приміщення
3	Гардеробна
4	Столове приміщення
5	Тамбур, тильний вихід

6	Міжповерховий перехід
7	Кабінет розробників
8	Санітарний вузол
9	Кімната охорони
10	Технічне приміщення
11	Відділ HR
12	Велика зала(2-й поверх)
13	Кабінет директора
14	Менеджер
15	Серверна

Режими роботи підприємства:

На підприємстві п’яти денний робочий тиждень. Два вихідних (субота, неділя). Понеділок — п’ятниця: 9:00 — 18:00, Обідня перерва: 12:00 — 13:00

Фізичне середовище

ТОВ «Супутник С» має підключення до телефонної лінії компанії

«Укртелеком», має три номери. Для організації телефонної мережі використовується офісна АТС на 16 номерів. Телефонна лінія має вихід за межі КЗ.

Система електропостачання підключена до централізованої мережі, до підстанції котра знаходиться в 200 м. від будівлі. Має трьох фазний ввід, в підвальному приміщенні встановлено лічильник, шафу автоматики, та шафу запобіжників. Електропроводка розведена по всій будівлі кабелем типу «ШВВП 3х2.5». Лінія електропостачання має вихід за межі КЗ.

Система заземлення виконана згідно норм.

Водопостачання до офісу підводиться з центральної лінії через підвал будівлі, в підвалі на вводі розташований кран зменшення тиску. Лінія системи водопостачання виходить за межі КЗ.

Система стічної каналізації підключена до централізованої мережі, система виконана з пластикових труб, та переходів діаметром 100 мм. Має вихід за межі КЗ.

В приміщеннях будівлі існує система вентиляції та кондиціонування повітря. В приміщеннях встановлено вентиляційні канали, які підключено до витяжок, також в кожному приміщенні в якому працюють люди встановлено кондиціонери.

В будівлі встановлено пожежну сигналізацію, у відповідності з проектної документації. Систему пожежної сигналізації виведено на моніторинг до приватного централізованого пульту пожежної охорони «Венбест». Підприємства співпрацюють на базі укладеного договору.

В будівлі встановлено охоронну сигналізацію. Систему виведено на централізований пульт охорони.

Інформаційне середовище

Всі робочі станції об'єднані в комп'ютерну мережу з сервером. Вся інформація яка оброблюється на робочих станціях зберігається на сервері. Робочі станції підключені до мережі через мережеві комутатори. До серверу підключено модем, за допомогою якого мається можливість виходу до глобальної мережі Internet. Комп'ютерна мережа побудована на базі технології Fast Ethernet, має топологію «зірка».

Таблиця 1.2 — Характеристики апаратного забезпечення

Параметр	Значення (не Нижче)
АРМ	
Процесор	Intel Core i5 3.50 GHz
ОЗУ	16 Гб
Об'єм жорсткого диску	1000Gb
Материнська плата	Gigabyte H-81
Блок живлення	600Wt BeQuiet
Привід	Відсутній
Відео	Nvidia GTX 1070
Порти	4xUSB 2.0, PS/2, Card reader
Мережа	1000 mbps

Додатково	Клавіатура + мишка в комплекті.
Монітор	27" Samsung
Сервер	
Процесор	Intel Xeon 3420
ОЗУ	64Gb
Об'єм жорсткого диску	П'ять SATA ДНска
Порти	Два порти Gigabit Ethernet
Привід	DVD
Блок живлення	1 блок живлення 800Wt FSP
Комутаційне обладнання	
Комутатор	D-Link DGS-1100-24, D-Link DGS-1210-16, TP-L1NK TL-SG2109WEB
Маршрутизатор	TP-LINK TD-9917

Кожна РС має свою унікальну IP адресу, своє мережеве ім'я, інвентарний номер, відповідального за РС. Перелік РС станцій наведено в таблиці 1.3.

Таблиця 1.3 — Перелік РС

IP адреса	Мережеве ім'я	Відповідальна особа
192.168.5.101	Director	Відповідальна особа 1
192.168.5.102	Manager	Відповідальна особа 2
192.168.5.103	Teamlead	Відповідальна особа 3
192.168.5.104	HR	Відповідальна особа 4
192.168.5.105	Buh	Відповідальна особа 5
192.168.5.106	Developer2	Відповідальна особа 6
192.168.5.107-192.168.5.108	Developer3	Відповідальна особа 7

В інформаційній системі ТОВ «Супутник С» використовується програмне забезпечення декількох типів (загальносистемне ПЗ, прикладне ПЗ, спеціалізоване ПЗ). Програмне забезпечення також можна розподілити на те яке встановлене на АРМ та сервері. Характеристики ПЗ представлені в таблиці 1.4.

Таблиця 1.4 — Характеристики програмного забезпечення

Назва ПО	Тип	Ліцензія	Призначення	Термін дії	Встановлено
Windows 11 Pro	Системне	Commercial	Операційна система	Безстроковий	PC1…PC7
Eset NOD 32	Прикладне	Commercial	Антивірус	Безстроковий	PC1…PC7
Microsoft Office 2020	Прикладне	Commercial	Редактор текстових файлів	Безстроковий	PC1…PC3, PC5, PC7
Adobe Photoshop 2020	Прикладне	Commercial	Графічний редактор	Безстроковий	PC4…PC7
Unity	Прикладне	Commercial	Ігровий двигун	Безстроковий	PC6…PC7
Visual Studio 2022 Professional	Прикладне	Commercial	Інтегроване середовище розробки	Безстроковий	PC6…PC7
IntelliJ IDEA 2022 Professional Edition	Прикладне	Commercial	Інтегроване середовище розробки	Безстроковий	PC6…PC7

На підприємстві працюють робітники різних відділів. Список робітників наведено в таблиці 1.5.

Таблиця 1.5 — Список робітників ТОВ «Супутник С»

№ п\п	Відділ	Посада
1	Керівники	Директор
2	Відділ HR	HR
3	Менеджери	Менеджер
4	Відділ розробки	Тімлід
5	Бухгалтерія	Бухгалтер
6	Відділ розробки	Розробник
7	Відділ розробки	Розробник

Таблиця 1.6 — Класифікація інформації, яка циркулює на ІТС

Вид інформації		Режим доступу	Правовий режим	Вид представ-лення в ІТС	Вимоги до захисту		
					К	Ц	Д
Інформація про клієнтів (персональна)		ІзОД	Конфіден-ційна інформація	ТекстовийЕлектрон-ний	3	2	3
Інформація про працівників (персональна)		ІзОД	Конфіден-ційна інформація	ТекстовийЕлектрон-ний	4	4	4
Продукти роботи підприємства	Вхід./Вихід. документи	ІзОД	Конфіден-ційна інформація	Текстовий Електрон-ний	4	3	4
	Матеріали про проект				4	5	4
	Дизайн				4	5	4
Фінансова звітність (банківські рахунки, виручка)		ІзОД	Службова інформація	Електрон-ний	3	4	4

Рівні конфіденційності:

– К1 - рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не є конфіденційною;

– К2 - рівень конфіденційності інформації, при якому компанія зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї;

– К3 - рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;

– К4 - рівень конфіденційності інформації, що може призвести до значних;

– матеріальних втрат у разі розкриття інформації особам, що не мають допуску до неї;

– К5 - критичний рівень конфіденційності інформації, що може призвести до краху

– компанії у разі втрати конфіденційності інформації. Рівні цілісності:

– Ц1 - рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;

– Ц2 - рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;

– Ц3 - рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;

– Ц4 - рівень цілісності інформації, що може призвести до значних матеріальних втрат у разі втрати цілісності інформації;

– Ц5 - критичний рівень цілісності інформації, що може призвести до краху компанії у разі втрати цілісності інформації.

Рівні доступності:

– Д1 - рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;

– Д2 - рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;

– Д3 - рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;

– Д4 - рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;

– Д5 - критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

Всі ресурси обробляються працівниками підприємства - 1 менеджер, 3 розробника, 1 тімлід, 1 HR, 1 директор.

Вся текстова документація зберігається у складському приміщенні під ключ, до якого доступ має тільки директор. Електронна інформація записується та зберігається на 5 різних полицях (зачинені на ключ), у вигляді 2Тб жорстких дисків. Резервування всієї інформації виконується кожен день на ці диски.

Інформація про клієнтів (персональна) менеджер домовляється з клієнтом про проект (замовлення), після чого вносить його в систему замовлень (CRM, ERP, Printoffice24) та передає інформацію до директора, вона може бути роздрукована. Зберігається на полицях в закритому сейфі.

Інформація про працівників (персональна) обробляється директором та, може бути роздрукована. Зберігається на полицях в складському приміщенні.

Продукти роботи підприємства - вхідні та вихідні документи (правки, розрахунки, аналітика і т.д.), матеріали про проекти, дизайнерські рішення та розробки - при роботі над проектом, тімлід та розробники постійно зберігають результати на певному етапі і передають на перевірку менеджеру та директору. Після внесення всіх правок, готовий проект передається замовнику, а також зберігається в електронному вигляді на полицях в складському приміщенні на дисках.

Клієнти самі звертаються до компанії (реклама) або менеджери самі знаходять потенційних клієнтів (спеціальні платформи, аналіз та опрацювання нових компаній та підприємств); клієнт звертається до компанії з своїм проектом/ідеєю до менеджера компанії з яким ведуться переговори з приводу проекту (мета, ціль, розвиток, потенціал та прибуток) та його можливостей. Клієнта вносять в програми (CRM, ERP, Printoffice24). Всю допоміжну інформацію по проекту та свої персональні данні клієнти пересилають на корпоративну пошту. Після ознайомленням з проектом директор, його приймає в роботу тімлід, розробляється план робіт та визначаються терміни (період вивчення ринку, період створення моделі проекту, корективи, графічна робота, корективи, побудова фінальної моделі та виведення результатів на ринок). З клієнтом також зв'язуються директор та менеджер та створюють договір, після якого клієнт вносить повну оплату проекту (під час проекту можуть виникати додаткові витрати, про які інформують клієнтів). Менеджери працюють над проектом, використовуючи певне ПЗ. При кожному етапі відтворення проекту, директор та тімлід вносять корективи. Для конкретного проекту створюють свої терміни для кожного етапу, під час яких з клієнтом підтримується зв'язок (інформується по виконанню певного етапу та його результатів) через менеджера (Google Meet). Клієнти також можуть вносити свої корективи. Для коректівів проекту на кожній стадії він може друкуватися принтерами, які локально підключені до кожного директор та HR. Після завершення проекту директор тримає зв’язок із клієнтом для підтвердження результатів та у ролі допомоги для правильного просування проекту у ринок.

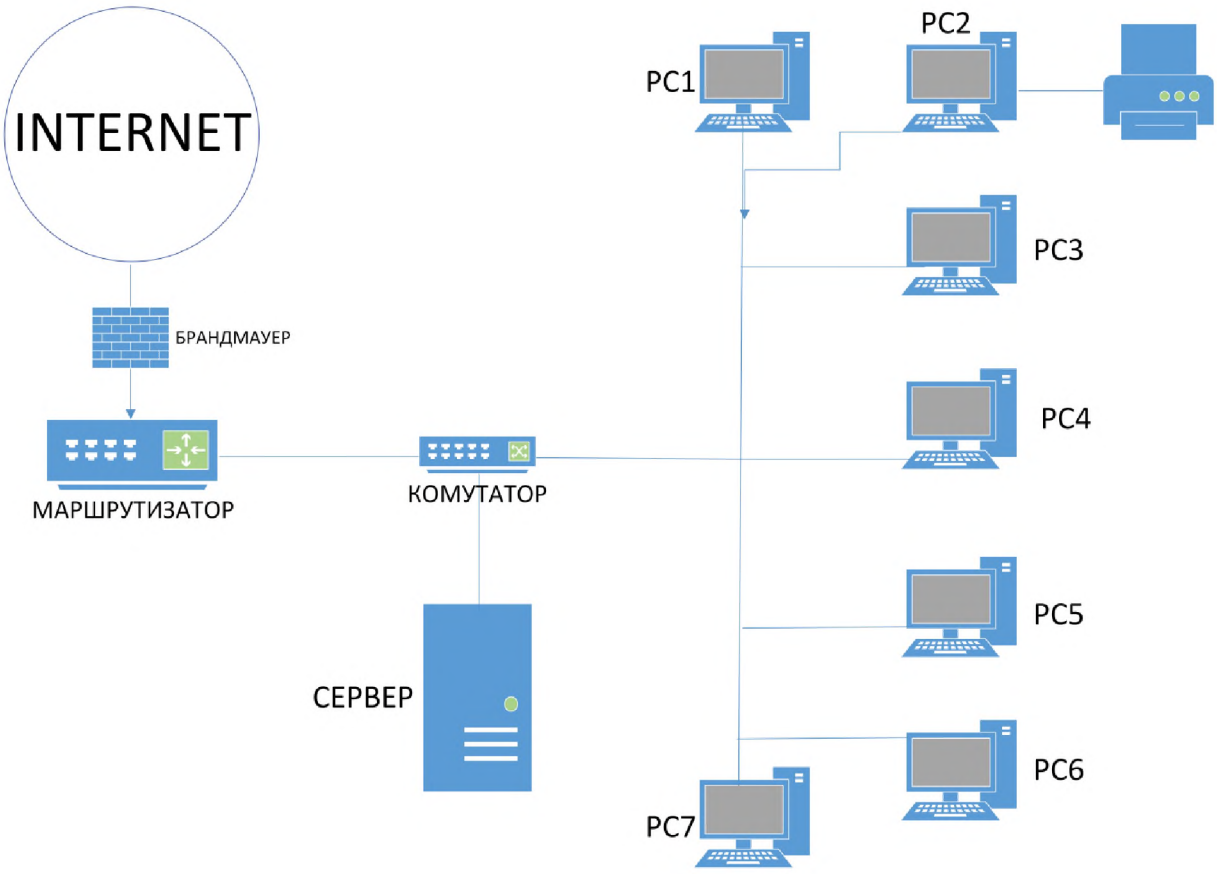


Схема інформаційних потоків надана на рисунку 2.1.

Інформаційні потоки:

1. Обробка інформації про клієнтів
2. Обробка інформація про працівників
3. Обробка продуктів роботи підприємства
4. Обробка договорів

PC1	Директор
PC2	HR
PC3	Менеджер
PC4	Тімлід
PC5	Бухгалтер
PC6-7	Розробник

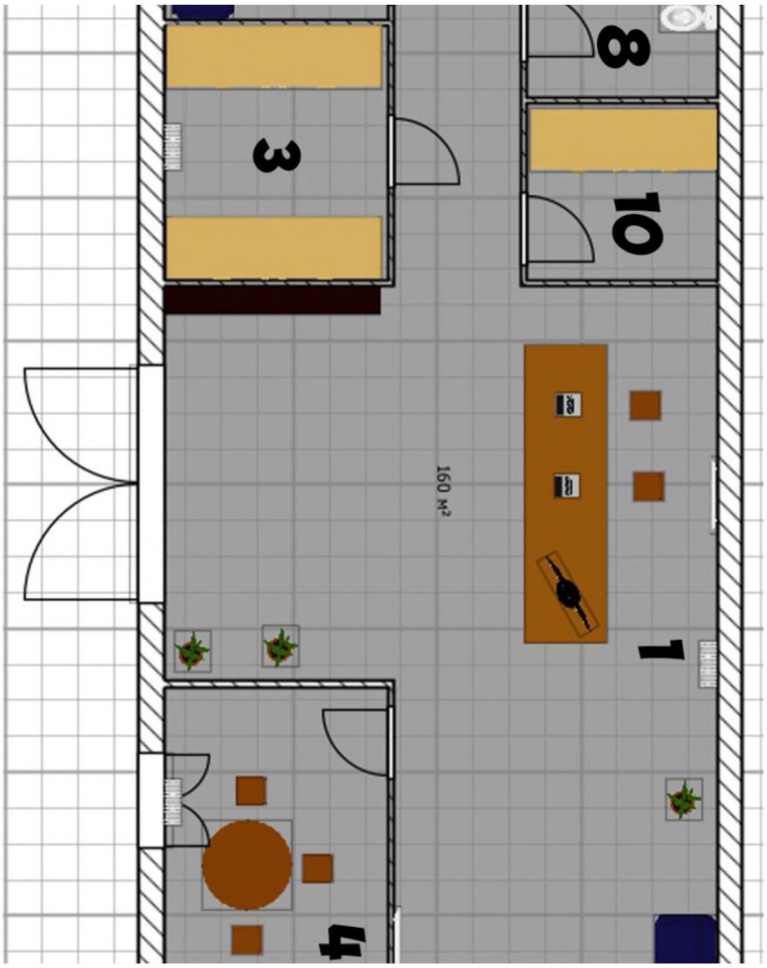


Рис.2.2 — Генеральный план 1 поверху

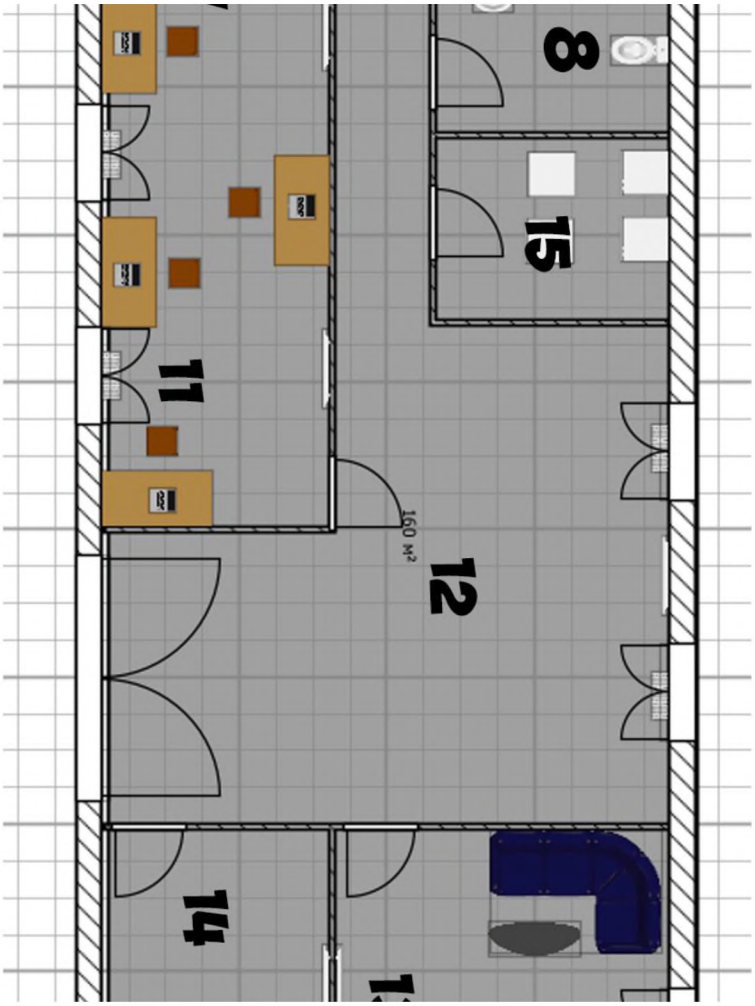


Рис 2.3 — Генеральный план 2 поверху

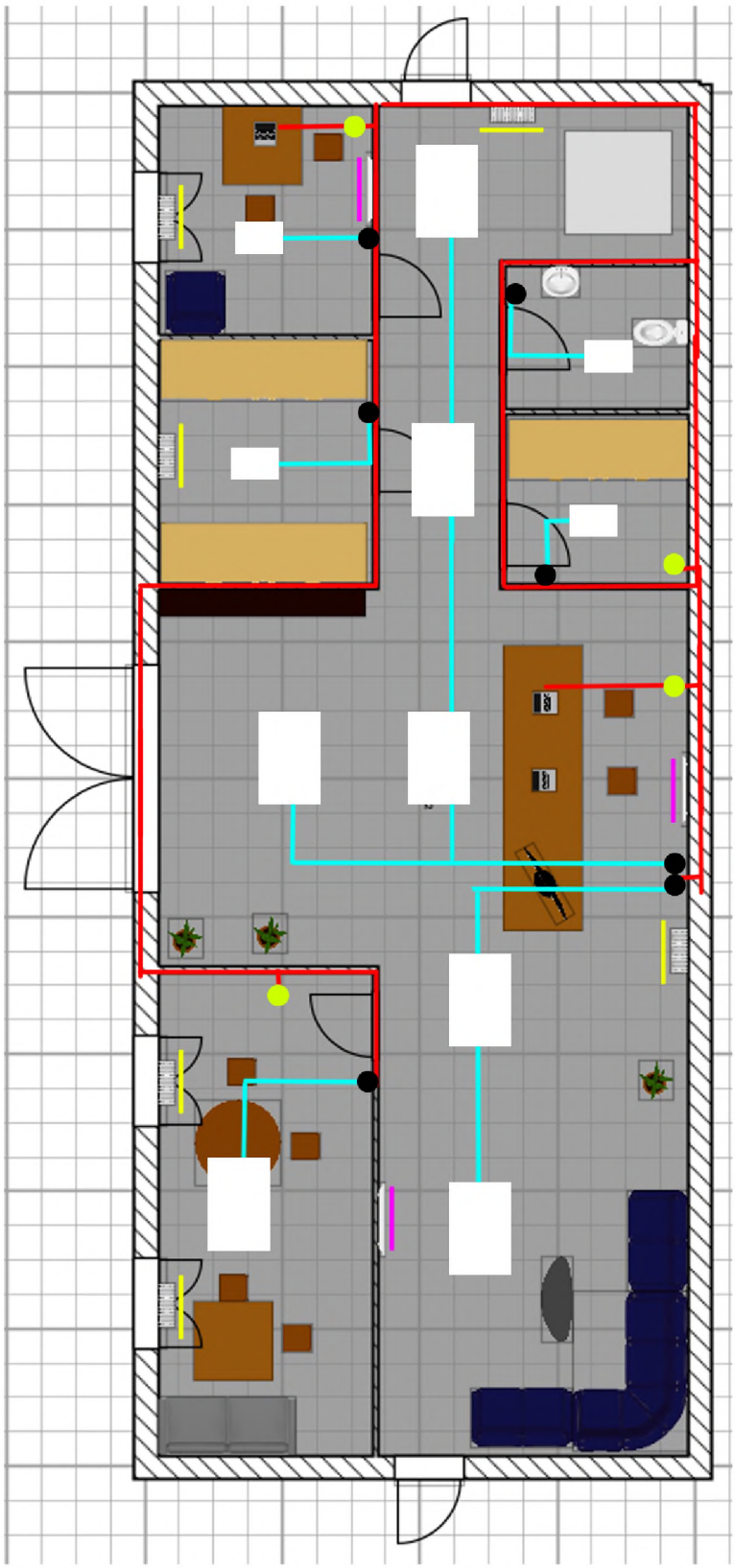


Рис 2.4 — Схема електроживлення та опалення 1 поверху

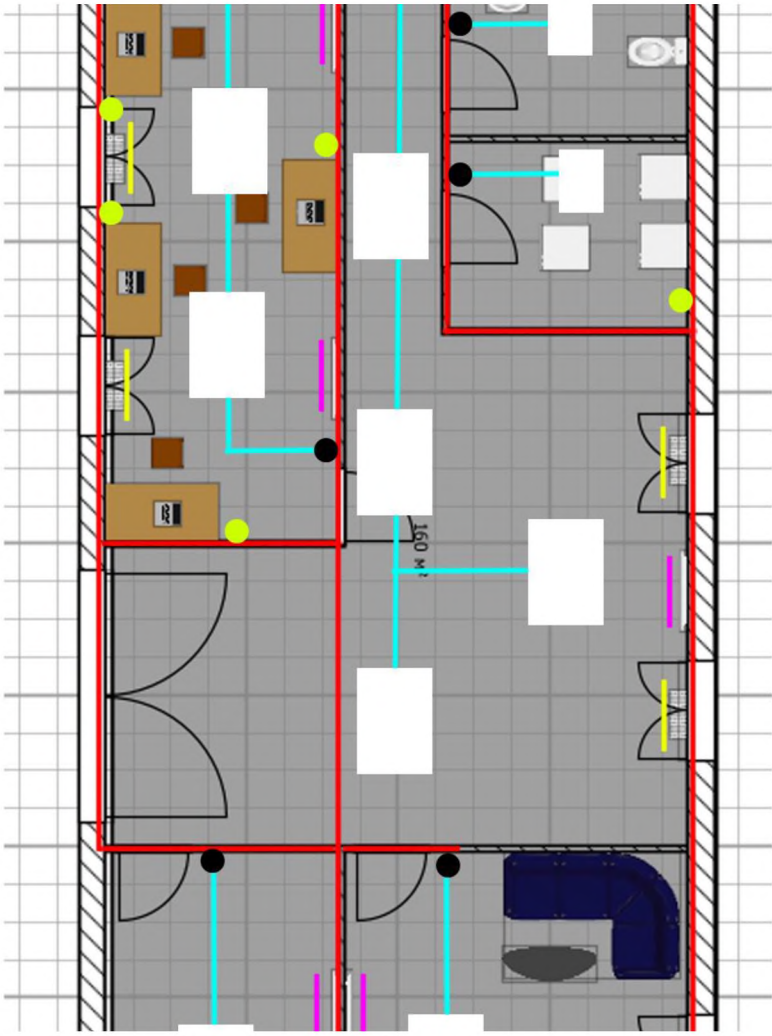


Рис 2.5 — Схема електроживлення та опалення 2 поверху

Умовні позначення:

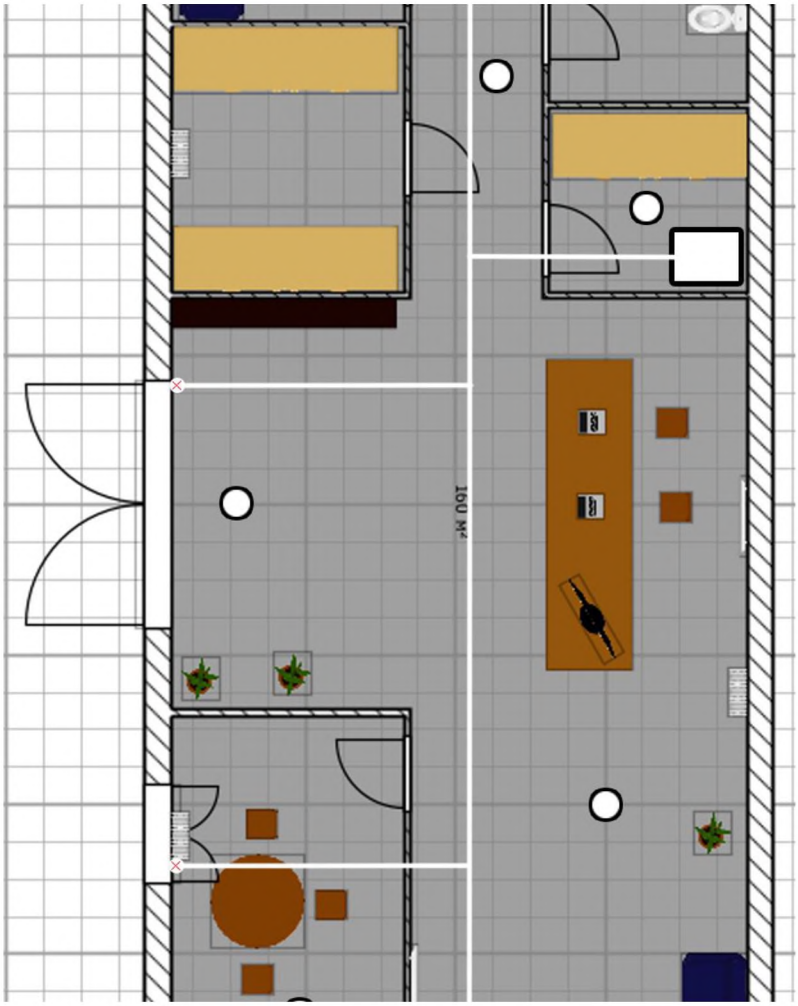


Рис 2.6 — Схема охоронної системи 1 поверху

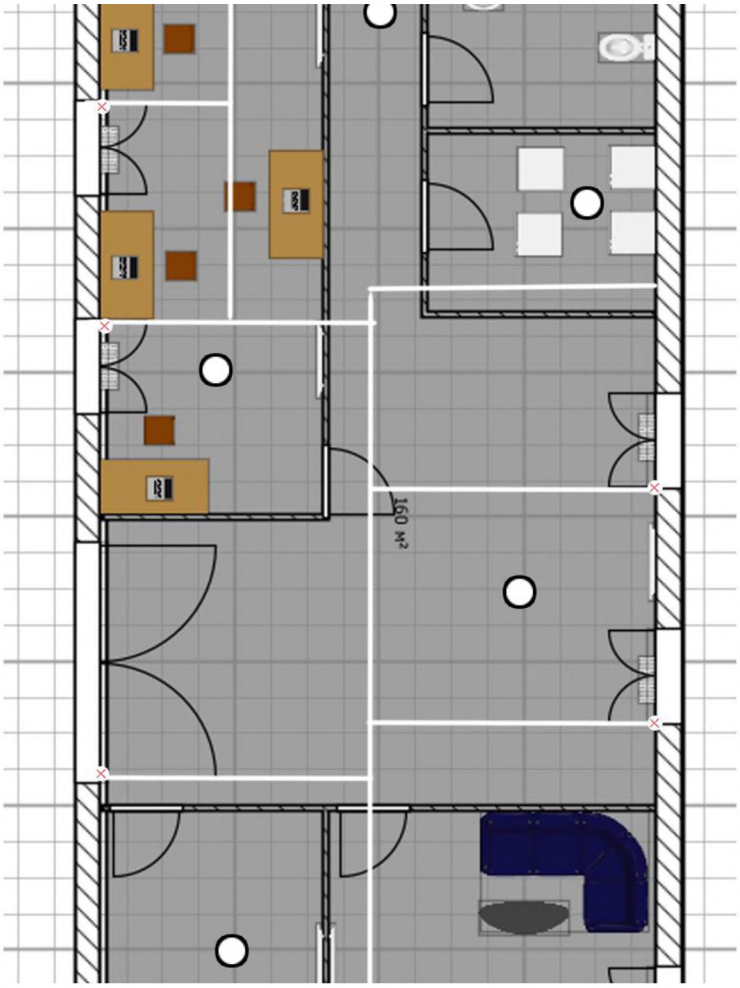
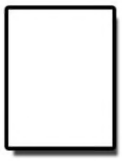


Рис 2.7 — Схема охоронної системи 2 поверху

Умовні позначення:



ППКП ОМЕГА

лінія сигналізації

Датчик розбиття скла

Датчик розмикання дверей

Датчик диму

1.5 Висновок

Розглянувши схему побудови КСЗІ, одним із найважливіших етапів є зберігання корпоративних даних у безпечному та масштабованому сховищі. Дані вимоги можна реалізувати за допомогою технології хмарних сховищ. Ця технологія має широкі можливості при реалізації, має велику сукупність налаштувань та принципів реалізації. Дозволяє зберігати велику кількість секретної корпоративної інформації з високим рівнем безпеки.

Хмарні технології розробляються протягом багатьох років та є поєднанням декількох ключових технологій, які багатьма розглядаються як наступний етап розвитку IT-архітектури підприємств.

Впровадження хмарних технологій дозволяє відмовитися від застарілого локального інфраструктурного підходу до запуску сервісів у сфері інформаційно-комунікаційних технологій та мають практичні переваги:

– швидкість отримання доступу до необхідних додатків; – динамічна зміна обчислювальної потужності залежно від потреб споживача;

– стандартизовані платформи для розробки власних додатків та сервісів;

– зменшення потреби у збільшенні обчислювальної потужності власних серверів.

РОЗДІЛ 2
СПЕЦІАЛЬНА ЧАСТИНА

2.1 Модель загроз

Загрози безпеці даних, що зберігаються в хмарному сховищі, в цілому, можна розділити на 4 класи:

1 Порушення конфіденційності інформації (К) - отримання інформації користувачами або процесами всупереч встановленим правилам.

2 Порушення цілісності інформації (Ц) - повне або часткове знищення, викривлення, модифікація інформації, нав'язування хибної інформації тощо.

3Порушення доступності інформації (Д) - часткова або повна втрата працездатності системи, блокування доступу до інформаці.

4 Втрата спостережності (керованості системою) (С) - порушення процедур ідентифікації та автентифікації.

Потенційно загрози можуть завдати шкоди інформації, працівникам, кліентам, технічним засобам і процесам. Загрози також можна поділити на:

- навмисні (Н);
- випадкові (В);
- природні (П).

Потрібно ідентифікувати як випадкові, так і навмисні джерела загроз.

Загрози можуть бути ідентифіковані в загальному вигляді або за типами.

Таблиця 2.1

Шкала оцінки ймовірності реалізації загрози

Оцінка ймовірності	Характеристика
1	Практично неможливо
2	Малоймовірне (не частіше ніж 1 раз на 1 рік)
3	Ймовірне до 1 разу на 3 місяці
4	Ймовірне до 1 разу на тиждень

5	Ймовірне до 1 разу на добу

Зроблено якісну оцінку ймовірності реалізації загрози та визначено сукупний рівень загрози. Результати аналізу викладені в таблиці 2.1.

Таблиця 2.2

Результати аналізу загроз та разливостей інформації в ІТС.

Вразливість	Загроза	Ймовірність	Порушення	Природа
Вразливості системи авторизації та аутентифікації.	Несанціонований доступ до системи	3	КЦДС	Н
Вразливості системи шифрування даних.	Отримання чи пошкодження (знищення) даних	3	КЦДС	Н
Вразливості системи на рівні зберігання даних	Копіювання конфіденційних даних	3	КЦДС	Н
Відсутність механізму автентифікації	Отримання доступу до облікового запису користувача без права на це	2	КЦДС	Н
Вразливості сервера зберігання	Використання вірусів для отримання або	2	КЦДС	Н

даних.	пошкодження даних			
Вразливість серверу до мережевих атак	Втрата даних в наслідок несправностей сервера	2	ЦДС	Н
Розвідка, аналіз трафіка	Перехоплення інформації, що пересилається. Збої у роботі механізмів забезпечення шифрування	3	КЦД	Н
Неавторизоване переглядання документів на пристрої віддаленого чи мобільного співробітника	Втрата чи викрадення мобільного пристрою	2	К	В

Більша частина загроз в списку є критичною, оскільки кожна веде до втрати, пошкодження або розповсюдження конфіденційних і важливих даних.

Значні загрози

Найзначнішими загрозами я вважаю втрати даних в наслідок несправностей сервера та отримання чи пошкодження (знищення) даних, тому що інфраструктура компанії якщо вона знаходиться лише всередині офісу може бути дуже вразлива у випадку цілеспрямованих дій зловмисників та у випадку виходу з лагоду локальних серверів. Через це корпоративні дані можуть бути або викрадені, або безповоротно загублені.

Щоб вирішити цю проблему необхідно звернутися до технологій хмарних сховищ, бо так конфіденційні дані будуть збережені у інфраструктурі яка не залежить від локальних перебоїв у офісі, а хмарна інфраструктура сервісів які дають користуватись своїми хмарними сховищами дозволяє не загубити доступу до своїх даних навіть у надзвичайному випадку.

Також хмарні сховища у деякому випадку допомагає зекономити на закупці жорстких дисків, SSD, тощо для зберігання даних компаніях якщо вони будуть генеруватись дуже великому обсязі.

2.2 Модель порушника

У кожному конкретному випадку, виходячи з технології обробки інформації, необхідно розробити модель порушника, яка повинна бути адекватна реальному порушнику для даної автоматизованої системи.

Модель порушника – абстрактний формалізований або неформалізований опис дій порушника, який відображає його практичні та теоретичні можливості, апріорні знання, час та місце тощо.

Модель порушника повинна визначати:

– можливу мету порушника та її градацію за ступенями небезпечності для автоматизованої системи;

– категорії осіб, з числа яких може бути порушник.;

– припущення про кваліфікацію порушника;

– припущення про характер його дій.

Метою порушника можуть бути:

– отримання необхідної інформації у потрібному обсязі та асортименті;

– мати можливість вносити зміни в інформаційні потоки у відповідності зі своїми намірами (інтересами, планами);

– нанесення збитків шляхом знищення матеріальних та інформаційних цінностей.

Рекомендується класифікувати порушників за рівнем можливостей, що надаються їм засобами автоматизованої системи, наприклад, поділити на чотири рівні цих можливостей.

Класифікація є ієрархічною, тобто кожний наступний рівень включає в себе функціональні можливості попереднього:

– перший рівень визначає найнижчий рівень можливостей ведення діалогу з автоматизованій системі – можливість запуску фіксованого набору завдань (програм), що реалізують заздалегідь передбачені функції обробки інформації;

– другий рівень визначається можливістю створення і запуску власних програм з новими функціями обробки інформації;

– третій рівень визначається можливістю управління функціонуванням автоматизованої системи, тобто впливом на базове програмне забезпечення системи і на склад і конфігурацію її устаткування;

– четвертий рівень визначається повним обсягом можливостей осіб, що здійснюють проектування, реалізацію, впровадження, супроводження програмно-апаратного забезпечення автоматизованої системи, аж до включення до складу автоматизованої системи власних засобів з новими функціями обробки інформації.

За рівнем знань про автоматизовану систему усіх порушників можна класифікувати як таких, що:

– володіють інформацією про функціональні особливості автоматизованої системи, основні закономірності формування в ній масивів даних та потоків запитів до них, вміють користуватися штатними засобами;

– володіють високим рівнем знань та досвідом роботи з технічними засобами системи та їхнього обслуговування; – володіють високим рівнем знань у галузі обчислювальної техніки та програмування, проектування та експлуатації автоматизованої системи;

– володіють інформацією про функції та механізм дії засобів захисту.

2.2 Профіль захищеності

Вибраний профіль захищеності комп'ютерної системи, що входить до складу АС класу 3, з вимогами до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації:

3.КЦД.2 = { КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }

Критерії конфіденційності:

КД-2 — базова довірча конфіденційність;

КА-2 — базова адміністративна конфіденційність;

КО-1 повторне використання об’єктів;

КВ-2 — базова конфіденційність при обміні.

Критерії цілісності:

ЦД-1 — мінімальна довірча цілісність;

ЦА-2 — базова адміністративна цілісність;

ЦО-1 — обмежений відкат;

ЦВ-2 — базова цілісність при обміні.

Критерії доступності:

ДР -1— використання ресурсів;

ДВ-1 — ручне відновлення після збоїв.

Критерії спостережності:

НР-2 — реєстрація;

НИ-2 — одиночна ідентифікація и автентифікація; НК-1 однонаправлений достовірний канал;

НО-2 — розподіл обов'язків; НЦ-2 — цілісність КЗЗ;

НТ-2 — самотестування;

НВ-1 автентифікація при обміні.

КД-2. Базова довірча конфіденційність. Реалізовано. Політика довірчої конфіденційності, що реалізується КЗЗ, визначає множину об'єктів КС, до яких вона відноситься: продукти роботи підприємства. КЗЗ здійснює розмежування доступу на

підставі атрибутів доступу користувача і захищеного об'єкта. [НИ-1].

КА-2. Базова адміністративна конфіденційність. Реалізовано. Політика адміністративної конфіденційності, що реалізується КЗЗ, визначає множину об'єктів КС, до яких вона відноситься: продукти роботи підприємства, інформація про клієнтів та співробітників, рекламні данні, бухгалтерська та фінансова звітності. КЗЗ надає можливість адміністратору або користувачу, що має відповідні повноваження, для кожного захищеного об'єкта шляхом керування належністю користувачів, процесів і об'єктів до відповідних доменів визначити конкретних користувачів і/або групи користувачів, які мають право одержувати інформацію від об'єкта. [НИ-1, НО-1].

КО-1. Повторне використання об’єктів. Реалізовано. До того як користувач або процес зможе одержати в своє розпорядження звільнений іншим користувачем або процесом об’єкт, встановлені для попереднього користувача або процесу права доступу до даного об’єкту скасовуються, а також вся інформація, що міститься в даному об’єкті, стає недосяжною. [НИ-1, НО-1].

КК-1. Аналіз прихованих каналів - виявлення. Реалізовано. Канал по пам’яті може бути реалізований, якщо не буде реалізоване повторне використання об’єктів. Канал по часу може бути реалізований, оскільки з високою вірогідністю користувачі не будуть перевіряти схеми закриття і відкриття файлів, однак це можна попередити використовуючи наприклад «port knocking», який вимагає дотримання певних заданих послідовностей для відкриття портів. [КО-1].

КВ-2. Базова конфіденційність при обміні. Реалізовано. Множина об’єктів та інтерфейсних процесів - сервер документів, драйвер файлової системи, захищенні документи. Наявні протоколи захисту інформації при обміні (HTTPs - використовує додатковий шар шифрування/автентифікації, WPA2 - посилена безпека даних і посилений контроль доступу до бездротових мереж - підтримує шифрування відповідно до стандарту AES,...), оновлення ПО. [НО-1].

ЦД-1. Мінімальна довірча цілісність. Реалізовано. КЗЗ надає користувачу можливість для кожного захищеного об'єкта (продукти роботи підприємства), що належить його домену, визначити конкретних користувачів і/або групи користувачів, які мають право модифікувати об'єкт. [НИ-1].

ЦА-2. Базова адміністративна цілісність. Реалізовано. Політика адміністративної цілісності, що реалізується КЗЗ, визначає множину об'єктів КС, до яких вона відноситься: продукти роботи підприємства, інформація про клієнтів та співробітників, рекламні данні, бухгалтерська та фінансова звітності. КЗЗ розмежовує доступ на підставі атрибутів доступу - процесу і захищеного об'єкту. [НИ-1, НО-1].

ЦО-1. Обмежений відкат. Реалізовано. Множина об'єктів - захищенні документи, файли, технологічна інформація. Існують автоматизовані засоби, які дозволяють авторизованому користувачу або процесу відкатити або відмінити певний набір (множину) операцій - редагування інформації, наприклад в Word - Ctrl+z, видаленні файли можна відновити, система контролю версії, резервне копіювання..., виконаних над захищеним об'єктом за певний проміжок часу.

ЦВ-2. Базова цілісність при обміні. Реалізовано. Об'єкти - документи, файли, технологічна інформація (оновлення ПО, антивірусу). Хеш функція (функція, що здійснює перетворення масиву вхідних даних довільної довжини в (вихідну) бітову послідовність встановленої довжини, що виконується певним алгоритмом; не зворотний процес, фіксована довжина на виході, не значні зміни даних повинні значно змінювати результат функції, для різних вхідних даних може створитися один хеш; один з видів алгоритмів – MD-5), наявні протоколи передачі по мережі та комутаційні пристрої. [НО-1].

ДР-1. Використання ресурсів - квоти. Реалізовано. Відносяться до таких ресурсів системи: об'єм пам'яті, дисковий простір, пропускна спроможність каналів зв'язку... [НО-1].

ДС-1. Стійкість при обмежених відмовах. Реалізовано. Об'єкт - оперативна пам'ять. [НО-1].

ДЗ-І. Гаряча заміна - модернізація. Реалізовано. Відноситься не тільки до конструкції, а й до апаратного і програмного забезпечення. Оновлення антивірусу, системних файлів. [НО-1].

ДВ-1. Відновлення після збоїв - ручне відновлення. Реалізовано, (тільки після збоїв системи, а не інформації). Точки відновлення, резервне копіювання. [НО-1].

НР-2. Реєстрація - Зовнішній аналіз, захищений журнал. Реалізовано. [НИ-1,НО1].

НИ-2. Зовнішня ідентифікація і автентифікація, одиночна. Реалізовано. Вхід до локального запису відбувається з використанням пароля. Також є можливість скористатися фізичним ключом безпеки [НК-1].

НК-1. Одно-направлений достовірний канал. Реалізовано. З'єднання з системою проводить тільки людина(користувач) - введення паролю тільки з клавіатури.

НО-2. Розподіл обов'язків адміністраторів. Реалізовано. Політика розподілу обов'язків, що реалізується КЗЗ, визначає ролі адміністраторів і звичайного користувача і притаманні їм функції, визначає дві адміністративні ролі: адміністратора безпеки та іншого адміністратора. Однак на нашому об'єкті одна людина наділена функціями адміністратора безпеки та системного адміністратора. [НИ-1].

НЦ-2. Цілісність комплексу засобів захисту - КЗЗ з гарантованою цілісністю. Реалізована. Політика цілісності КЗЗ визначає домен КЗЗ та інші домени, а також механізми захисту, що використовуються для реалізації розподілення доменів. КЗЗ підтримує домен для свого власного виконання з метою захисту від зовнішніх впливів і несанкціонованої модифікації або втрати керування. Політика цілісності КЗЗ визначає склад КЗЗ і механізми контролю цілісності компонентів, що входять до складу КЗЗ: антивірус, вбудовані механізми у системі, хеш функція...

НТ-2. Самотестування за запитом - Самотестування при старті. Реалізовано. Система та антивірус автоматично починають перевірку при ініціалізації. [НО-1].

НВ-1. Автентифікація вузла. Реалізовано. Обмін даними може відбуватися через блютуз з'єднання, через USB...

НА-1. Базова автентифікація відправника. Реалізовано. Наявний цифровий підпис. [НИ-1].

НП-1. Базова автентифікація отримувача . Реалізовано. Наявний цифровий підпис. [НИ-1].

2.4 Реалізація підсистеми хмарного сховища

Задля зменшення бюджету підприємств на обслуговуванні дискових масивів локального знаходження впроваджуються системи хмарних сховищ.

Використання хмарного сховища полегшує доступ до даних, оскільки воно звільняє жорсткий диск і захищає файли від будь-яких збоїв на фізичній машині. При попередньому розгляді існуючих систем захищених хмарних сховищ, було підняте питання щодо визначення вимог захисту до таких систем.

Організації, що перейшли на хмарні сховища отримують такі переваги:

-використання всієї потужності сучасних інформаційних технологій без необхідності вкладатися в створення власної мережевої інфраструктури, розгортати і супроводжувати складне програмне забезпечення;

-можливість перекласти рутинні роботи щодо створення резервної копії даних, встановлення оновлень безпеки на корпорацію постачальника;

-оплата послуг за принципом оренди: перенесення витрат на програмне забезпечення з капітальних в операційні, прогнозованість платежів;

-знайомі користувачам інструменти роботи, швидке розгортання і використання співробітниками, низькі витрати на навчання кінцевих користувачів;

Розглянемо основні вимоги до захищених хмарних сховищ, та реалізуємо відповідні практичні рішення.

Вимоги до безпеки хмарних технологій

Характеристика	Для користувачів	Для операторів
Секретність інформації про користувачів	Переадресація даних, зонування мережі, автентифікація файлової системи, чистка дисків після звернення до них	Шифрування пристроїв і файлової системи
Секретність даних про користувачів під час виконання різних завдань	Відокремлення ОС та ВМ	Відокремлення ОС
Секретність під час	VPN, SSL, VLAN	VPN, SSL

передачі даних по мережі		
Авторизація та автентифікація користувачів для отримання даних	Автентифікація ОС, VPN-автентифікація, firewall	Автентифікація ОС, VPN-автентифікація

Постачальники, які використовують приватне шифрування, вирішують цю проблему, не зберігаючи ніде копію вашого пароля. Хоча технологія, що стоїть за цим, може ускладнитися, зводиться до того, що замість того, щоб передавати пароль, який потім перевіряється службою, ви передаєте підтвердження того, що ви знаєте пароль. Знову ж, математика стає складною, але на практиці вона працює так само, як і будь-який інший провайдер: ви вводите свій пароль і отримуєте доступ.

Відповідно, при побудові системи безпеки середовища хмар також можна виділити певні шари контролю і доступу. Хмара комбінує можливості користувача і постачальника, брандмауери і різновиди способів ізоляції. При цьому окремі елементи безпеки можуть контролюватися користувачем незалежно від провайдера.

Моделі хмарних обчислень:

-інфраструктура як сервіс (IaaS)

-платформа як сервіс (PaaS)

-програмне забезпечення як сервіс (SaaS).

У різних сервісах клієнтом контролюються різні верстви безпеки незалежно від провайдера.

Як можна побачити з рисунку 2.1, можливості користувача по управлінню системою безпеки залежать від вибору сервісної моделі. У моделі IaaS на стороні замовника можна побудувати свої власні технічні засоби забезпечення безпеки. Клієнт може мати повний контроль над реальною конфігурацією сервера, що гарантує йому більший контроль ризиків безпеки оточення і даних.

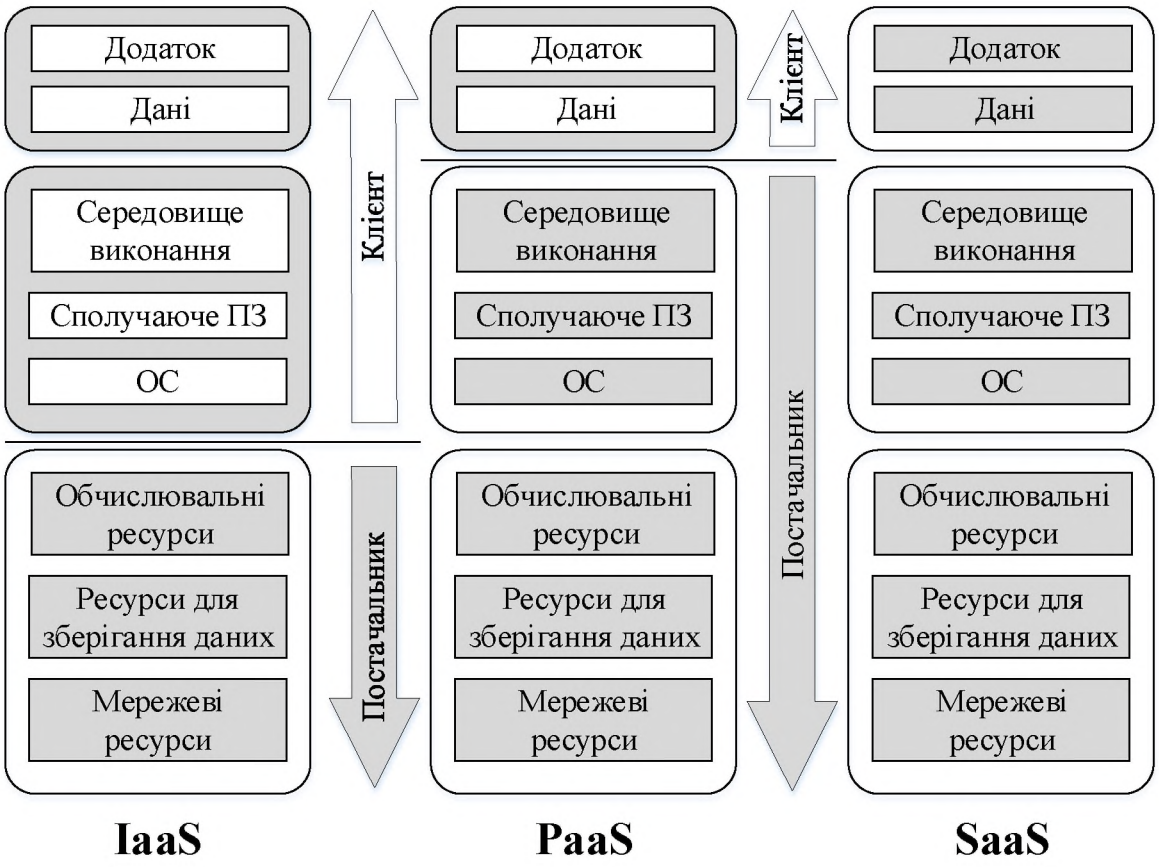


Рис — 2.8. Багаторівнева система безпеки хмар на прикладі трьох моделей хмарних сервісів

У PaaS постачальник управляє лише апаратною платформою і операційною системою, що обмежує можливості підприємства замовника в управлінні ризиками на цих рівнях.

У моделі SaaS як платформа, так і інфраструктура повністю управляється провайдером хмарних послуг. Це означає, що, якщо операційна система або сервіс не налаштовані належним чином, то дані на більш високому прикладному рівні можуть бути в небезпеці. Для користувачів у цьому випадку не обов'язково знати, як надаються ці послуги (які включають в себе мережу, сервери, операційні системи, сховища і навіть окремі функції додатків). Користувачеві важливо, щоб сервіс був досить дешевий і доступний тоді, коли він необхідний. Тому багато деталей функціонування сервісу і його інфраструктура виявляються прихованими для користувача. У можливостях управління клієнт виявляється обмеженим

тільки мінімальним набором налаштувань конфігурації програми під свої потреби.

Відповідальність постачальника хмарного сервісу починається з фізичної безпеки і безпеки середовища. Цей рівень безпеки – високорівневий, так як він пов'язаний з керованістю хмарою як єдиною інформаційною системою. Саме постачальник хмарного сервісу здійснює експлуатацію фізичних серверів центрів обробки даних, тому клієнт так само, як і у випадку зі звичайним ЦОД, повинен розглянути наступні ключові моменти: фізичний доступ персоналу до серверів і мережевої інфраструктури, засоби пожежної сигналізації та пожежогасіння, кліматичний і температурний контроль над серверами і іншими апаратними засобами, знищення виведених з експлуатації пристроїв зберігання даних.

Якщо SaaS та PaaS надають додатки клієнтам, то IaaS це не робить. Вона просто пропонує обладнання, щоб ваша організація могла поставити все, що захоче, та в основному забезпечує постачання віртуальних машин постачальникам IaaS замість програм, а машини можуть містити будь-які розробки, які хочуть отримувачі послуг.

Недоліки Хмарних сховищ:

Одну з основних загроз для хмарних середовищ зберігання даних становлять хакери і віруси. Перші можуть отримати доступ до конфіденційної інформації, розміщеної на сервері, зламати сайти і змінити їх вміст, а також вивести з ладу сервер за допомогою DDoS-атакы. Віруси ж, вражаючи хмарні середовища, перетворюють їх у один великий розсадник інфекції. Крім того, вони дуже сповільнюють їх роботу, а також займають інтернет-канал. Ці загрози за принципом роботи не сильно відрізняються один від одної. Багато вірусів використовують для розповсюдження вразливості в програмному забезпеченні. Так і хакери теж воліють застосовувати атаки, спрямовані на відомі вразливості в програмному забезпеченні. Використовуючи вразливості, і ті й інші одержують досить легкий доступ до віддаленого комп'ютера навіть у тому випадку, якщо останній добре захищений.

Огляд і вибір існуючих рішень

На сьогоднішній день існує більше п’ятдесяти компаній, які надають хмарні сервіси. В деяких з них забезпечено досить високий рівень захисту даних, а в деяких – ні. В даному пункті роботи будуть розглянуті найбільш затребувані рішення в сфері хмарних технологій і проведено їх порівняння.

В таблиці 2.1 приведено порівняння п’яти найпопулярніших хмарних сховищ по базовим критеріям.

Таблиця 2.3

Порівняльна характеристика найпопулярніших хмарних сховищ даних

Характеристика	Dropbox	Google Drive	iCloud drive	One Drive	CloudMe
1	2	3	4	5	6
Безкоштовний обсяг дискового простору, Гб	2	15	5	15	-
Максимальный об’єм(ГБ)	необмежений	2000	2000	1000	5000
Максимальний розмір файлу, Гб	10	200	256	10	2
Спільний доступ до даних	Так	Так	Так	Так	Так
Термін зберігання даних	Необмежений	Необмежений	Необмежений	Необмежений	Необмежений
Пряме посилання на завантаження	Так	Так	Так	Ні	Ні

Можливість редагування документів MS Office	Так	Так	Так	Так	Так
Наявність мобільної версії	Так	Так	Так	Так	Так
Ціна($/місяць)	50	10	10	12.5	15

Далі приведено аналіз найбільш популярних хмарних сховищ з приводу забезпечення в них інформаційної безпеки (ІБ).

Dropbox. У Dropbox розроблено кілька рівнів захисту: зокрема, використовується безпечна передача даних, шифрування, конфігурація мережі, а також елементи управління на рівні додатків.

У бізнес-версії Dropbox забезпечено більш високий рівень захисту. У ньому є додаткове шифрування при передачі даних і в додатках, зберігання утримуваних файлів у вигляді зашифрованих блоків, а також роздільне зберігання метаданих і блоків даних. Дані Dropbox захищаються за допомогою шифрування алгоритмом AES (256-розрядним). Під час пересилки даних використовується протокол SSL/TLS [20, 28].

Google Drive. Дані кожного користувача Google Drive захищені логічною схемою, як ніби вони зберігаються на окремому сервері. Доступ до даних надається по зашифрованим тунелях протоколу HTTPS. Цей протокол включений за замовчуванням для всіх користувачів, тому ніхто не зможе отримати доступ до даних, крім їх власника. В Google Drive використовується Perfect Forward Secrecy – алгоритм шифрування даних при обміні інформацією з серверами інших компаній. Завантажені на Google Drive відео не шифруються. Відновлення акаунту здійснюється за допомогою секретного питання. Сам сервіс перевіряє придуманий користувачем пароль на надійність і не дозволяє використовувати легко зламувані паролі. У Google Drive існує версія для бізнес-акаунтів, яка

дозволяє забезпечувати більш високий рівень захисту файлів. В ній відсутній аналіз інформації, що передається для показу реклами і присутня система єдиного входу.

iCloud drive. В iCloud дані шифруються за допомогою алгоритму AES (з довжиною ключа не менше 128 біт). Для зберігання зв'язки ключів використовується шифрування по 256-розрядному алгоритмом AES. Трафік між пристроями та Поштою iCloud шифрується з використанням протоколу TLS 1.2. Для певних типів конфіденційної інформації використовується наскрізне шифрування (сквозное шифрование / end-to-end).

OneDrive. Базова версія OneDrive забезпечує шифрування переданих між клієнтом і сервером даних; пароль від акаунта перевіряється на надійність. Бізнес-версія OneDrive має поліпшені функціями безпеки. В ній забезпечується фізична безпека центру обробки даних, мережева безпека, безпека доступу та безпека додатків і даних. Типи сховищ (сховище шифрованого контенту, база даних контенту і сховище ключів) фізично розділені, завдяки чому при зломі будь-якого з них можна скомпрометувати інформацію.

CloudMe. Дана система дозволяє створювати резервні копії файлів, забезпечує захищене з'єднання SSL, доступ по протоколу HTTPS та розмежування доступу до даних.

На базі аналізу джерел [29-38] побудовано таблицю 2.2, в якій проводиться аналіз найпопулярніших хмарних сховищ даних з приводу наявності в них різних методів ЗІ.

Таблиця 2.4

Критерії безпеки хмарних сховищ

Критерій безпеки	Dropbox	CloudMe	Google Drive	iCloud Drive	OneDrive
Двухфакторна автентифікація	+	-	+	+	+

Шифрування на стороні клієнта	-	-	-	-	-
Шифрування на стороні сервера	+	-	+	+	+
Розмежування доступу	-	+	+	+	+
Безпечна передача даних	+	+	+	+	+
Виявлення шкідливих програм	+	-	+	+	+
Контроль доступу для сторонніх додатків	+	-	+	+	+
Автоматичне резервне копіювання	+	-	-	+	+
Перевірка пароля на надійність	+	-	+	+	+
Можливість повернутися до попередньої версії документа	+	+	-	+	+

Отже, можна зробити висновок про те, що не всі з розглянуті хмарних сховищ забезпечують надійний захист даних, що в них зберігаються, проте, найнадійнішим і тим, що прокриє основні загрози компанії є OneDrive.

2.5 Реалізація системи збереження даних в хмарному сховищі

Сьогодні дуже раціональним рішенням щодо зберігання даних компанії (наприклад зберігання резервних даних) вважається зберігання даних у хмарних сховищах. Існує багато варіантів сервісів, які дозволяють реалізувати цю ідею. Результатом дослідження різних варіантів на ринку було виявлено найкращий сервіс під наші потреби, а саме OneDrive.

У хмарному сервісі повинні зберігатися результати роботи розробників, такі як розроблені дизайнерські рішення щодо архітектури розробленого ПЗ, інструментарій для його розробки, диздоки, технічну документацію під надійним шифруванням обраного сервісу хмарного сховища. Також було б раціональним дублювати туди копії документів які мають підвищений рівень конфіденційності, корпоративні таємниці, тощо.

Після закінчення робочого дня робота працівників повинна бути збережена у хмарному сховищі. Реалізувати автоматичне зберігання усіх необхідних даних можна за допомогою корпоративного клієнту та певних розширень для ОС, які дозволяють підвантажувати усі необхідні дані які створюються працівниками, розробниками тощо у хмару за допомогою корпоративного клієнту без необхідності власноруч кожному працівнику, розробнику тощо завантажувати дані у хмару.

Таким чином після під’єднання хмарних сховищ до системи, схему інформаційних потоків можна зобразити наступним чином:

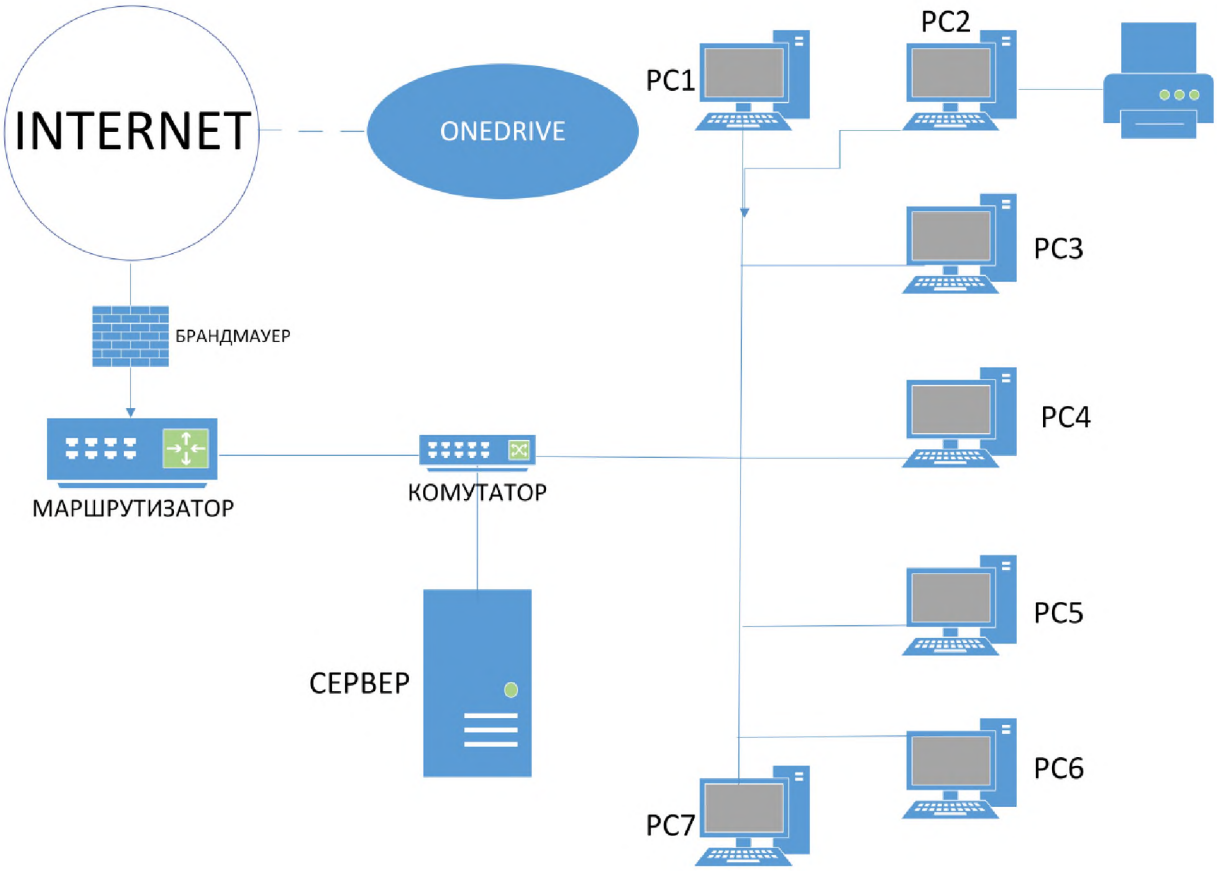


Рис. 2.9 Схема інформаційних потоків після додавання хмарного сховища

Плюсами використання хмарного сховища можна вважати незалежність від потенційного виходу з ладу обладнання в офісі, відсутність необхідності зберігати жорсткі диски у складському приміщенні, що дозволяє зекономити на утриманні приміщення та закупівлі дисків. Також це у деякій мірі автоматизує процес резервного копіювання усіх даних компанії.

Мінуси можна виділити наступні: необхідність платити за певні тарифі сервісу який надає послуги хмарного сховища, необхідність працювати саме у його інфраструктурі. І найголовнішим мінусом можна вважати те, що при відсутності доступу до Інтернету ви втрачаєте доступ до усіх своїх даних і це унеможливлює роботу над ними далі до моменту відновлення зв'язку.

Але цю проблему можна поліпшити.

Для гарної роботи системи необхідно мати альтернативні шляхи доступу до Інтернету. Одним із найкращих альтернативних шляхів можна вважати систему супутникового Інтернету Starlink. Плюсами цієї системи можна вважати те, що

вона не має проблем із потенційними перебитими дротами та потенційним блокуванням різними джерелами проблем для зв'язку. Система дозволяє отримати доступ до Інтернету навіть у досить важких умовах навколо офісу у надзвичайних ситуаціях. Також плюсом можна вважати що швидкість та затримки цього сервісу дозволять компанії без особливих проблем продовжити свою роботу та мати доступ до хмарного сховища без проблем.

Мінусами такого підходу можна вважати високу ціну обладнання, яке потрібно буде закуповувати компанії та вартість підписки на сервіс у розмірі 100 доларів США. Але компанія яка розглядається у роботі повинна без проблем потягнути цю плату за безперебійний доступ до мережі щоб продовжувати роботу у будь-яких ситуація.

Ще однім альтернаті них шляхом є підписання контракту з постачальником мабільного 4G інтернету. Цей варіант має привабливу ціну та просте налаштування для усього офісу.

2.6 Висновки до розділу 2

Провівши дослідження щодо потенційних загроз та недоліків у роботі системи компанії, було виявлено що дуже важливим рішенням буде використання сервісів хмарних сховищ для підвищення незалежності від локальних сховищ даних та спрощенні їх зберігання за допомогою ліквідації потреби у зберіганні дисків на складі. Було досліджено декілька сервісів хмарних сховищ та виявлено їх плюси та мінуси. Було обрано найкращий для досліджуваної компанії, а саме – OneDrive. Було описано можливості реалізації процесу вбудовування в систему хмарного сховища та розглянуто потенційні недоліки та плюси цього рішення. Розглянуто можливість вирішення головного недоліку використання хмарних сервісів, а саме потенційні проблеми з ними при перебоях з кабельним Інтернетом. Запропоновано рішення цієї проблеми у вигляді додаткової альтернативи кабельному Інтернету, а саме систему супутникового Інтернету Starilink.

РОЗДІЛ 3
ЕКОНОМІЧНЕ ОБГРУНТУВАННЯ ДОЦІЛЬНОСТІ ВПРОВАДЖЕННЯ ОБРАНОГО ХМАРНОГО РІШЕННЯ

3.1 Економічне обгрунтування доцільності впровадження обраного хмарного рішення

Для економічного обгрунтування доцільності огляду і вибору безпечного хмарного своviза потрібно провести розрахунки, щоб визначити економічну ефективність використання основних результатів, які будуть отримані після розрахунків.

Економічна доцільність визначається:

- розрахунками капітальних витрат;
- розрахунками експлуатаційних витрат;
- розрахунками річного економічного ефекту від впровадження обраного хмарного рішення.

3.1.1 Розрахунок суми витрат на впровадження обраного хмарного рішення

Спочатку розраховується трудомістшсть впровадження обраного хмарного рішення, для цього потрібно скласти час, який знадобиться для кожної робочої операції:

$$t = tmз + tв + ta + tвз + tозб + tовр + tд, \text{ годин, де}$$

- tmз - тривалість складання ТЗ= 50 годин;
- tв - тривалість розробки концепції безпеки інформації у організації = 30 годин;
- ta - тривалість процесу аналізу ризиків = 36 годин;
- tак - тривалість визначення вимог заходів, методів та засобів захисту = 18 годин;
- tозб - тривалість виробу основних рішень = 56 годин;

- tовр - тривалість організації виконання відновлювальних робіт і забезпечення неперервного функціонування організацій = 120 години;
- tд - тривалість документального оформлення впровадження обраного хмарного рішення = 20 годин.

$$t = 50 + 30 + 36 + 18 + 56 + 120 + 20 = 330 \text{ годин.}$$

3.1.2 Розрахунок суми витрат на впровадження обраного хмарного рішення.

Сума витрат на впровадження обраного хмарного рішення {Kpn) складається з витрат на:

- Заробітну плату спеціаліста з кібербезпеки — Ззп, грн;
- Вартості витрат машинного часу — Змч.

$$Kpn = Ззп + Змч = 27411 \text{ грн}$$

Заробітна плата спеціаліста складається з основної та додаткової заробітної плати, соціальних виплат та визначається за формулою:

$$Ззп = t * Зіб = 24750{,}00 \text{ грн}$$

де t — загальна тривалість впровадження обраного хмарного рішення = 330 годин;

Зіб — середньогодинна заробітна плата спеціаліста з інформаційної безпеки з нарахуваннями = 12000 / 160 = 75, грн/годину

Вартість машинного часу визначається за формулою:

$$Змч = t * Смч = 2661 \text{ грн}$$

де t — трудомістшсть підготовки документації на ІТК =4 години;

Смч — вартість 1 години машинного часу ПК, грн./година (5,6 грн).

Розрахована вартість впровадження обраного хмарного рішення інформації Kpn ь складовою одноразових капітальних витрат разом з витратами на придбання програмних засобів, як рекомендовані для використання.

Отже фіксована сума капітальних витрат на впровадження обраного хмарного рішення складає:

$$К = Крп + Кзпз + Каз + Кнавч + Кн = 61411 \text{ грн.}$$

$$К = 27411 + 11150 + 7850 + 9400 + 5600 = 61411 \text{ грн}$$

де *К* — вартість впровадження обраного хмарного рішення та залучення для цього зовнішніх спеціалістів, тис. грн;

Кзпз — вартість закупівлі ліцензійного основного і додаткового програмного забезпечення (ПЗ), тис. грн;

Крп — вартість впровадження обраного хмарного рішення, тис. грн;

Каз — вартість закупівлі апаратного забезпечення та допоміжних матеріалів,

Кнавч вартість витрати на навчання технічних фахівців і обслуговуючого персоналу = 5600 грн;

Кн — витрати на встановлення обладнання та налагодження системи, тис. грн.

3.2 Оцінка можливого збитку

Для розрахунку вартості такого збитку можна застосувати наступну спрощену модель оцінки для умовного підприємства.

Необхідні вихідні дані для розрахунку:

tn — час простою вузла або сегмента корпоративної мережі внаслідок атаки, 1 година;

tв — час відновлення після атаки персоналом, що обслуговує корпоративну мережу, 2 години;

tви — час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента корпоративної мережі 2 години;

Зо — заробітна плата обслуговуючого персоналу (адміністраторів та ін.), 5500 грн./міс.;

Зс — заробітна плата співробітників атакованого вузла або сегмента корпоративної мережі, 11000 грн./міс.;

Чо — чисельність обслуговуючого персоналу (адміністраторів та ін.), 1 особа;

Чс — чисельність співробітників атакованого вузла або сегмента корпоративної мережі, 7 осіб.;

О — обсяг прибутку атакованого вузла або сегмента корпоративної мережі, 2 млн грн. у рік;

Пзч — вартість заміни устаткування або запасних частин, грн; I — число атакованих сегментів корпоративної мережі, 1;

N — середнє число атак на рік, 10.

Упущена вигода від простою атакованого сегмента корпоративної мережі становить:

$$U=Пп +Пв +V=11740,4,$$

де Пп — оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента корпоративної мережі, грн;

Пв — вартість відновлення працездатності вузла або сегмента корпоративної мережі (переустановлення системи, зміна конфігурації та ін.), грн;

V — втрати від зниження обсягу продажів за час простою атакованого вузла або сегмента корпоративної мережі, грн.

Втрати від зниження продуктивності співробітників атакованого вузла або сегмента корпоративної мережі являють собою втрати їхньої заробітної плати (оплата непродуктивної праці) за час простою внаслідок атаки:

$$П_п = \frac{\sum Зс}{F} * t_n,$$

$$Пп = ((11000 *7)/176)*3 = 1312,5 грн,$$

де F — місячний фонд робочого часу (при 40-а годинному робочому тижні становить 176 ч).

Витрати на повторне введення інформації Пви розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента

корпоративної мережі Зс, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу tви:

$$Пви = ((11000 * 7)/176) * 4 = 1750 \text{ грн},$$

Витрати на заміни устаткування або запасних частин можуть скласти 3200

Тоді витрати на відновлення працездатності вузла або сегмента корпоративної мережі складуть:

$$Пв = 1312,5 + 1750 + 125 = 1875 \text{ грн.}$$

Таким чином, загальний збиток від атаки на сегмент корпоративної мережі організації складе:

$$В = 1 * 14 * 13764,4 = 192700 \text{ грн.}$$

3.3 Розрахунок економічного ефекту

Економічний ефект в сфері проектування рішення:

$$Е_{пр} = Ц_а - Ц_п \qquad (3.21)$$

$$Е_{пр} = 65000,0 - 61411,6 = 3588,4 \text{ грн.}$$

Річний економічний ефект в сфері експлуатації:

$$Е_{кс} = В_{еа} - В_{еп}$$

$$Е_{кс} = 24544,8 - 16354,8 = 8190 \text{ грн.}$$

Додатковий економічний ефект у сфері експлуатації:

$$\Delta E_{екс} = \sum_{t=1}^{T} E_{екс} (1 + R)^{T-t}$$

$$\Delta E_{екс} = \sum_{t=1}^{5} 8190 * (1 + 0,16)^{5-t} = 56323.7 \text{ грн.}$$

Сумарний ефект складає:

$$E = E_{\text{пр}} + \Delta E_{екс} = 414{,}4 + 56323.7 = 56738{,}1 \text{ гр}$$

Таблиця 3.1.

Показники економічної ефективності проектного рішення

	Найменування	Одиниці вимірювання	Значення показників	
			Базовий варіант	Новий варіант
	Капітальні вкладення	Грн.	-	3527,38
	Ціна придбання	Грн.	5000,0	4585,6
	Річні експлуатаційні витрати	Грн.	5922,0	3956,4
	Ціна споживання	Грн.	24544,8	16354,8
	Економічний ефект в сфері проектування	Грн.	-	3588,4
	Річний економічний ефект в сфері експлуатації	Грн.	-	8190
	Додатковий ефект в сфері експлуатації	Грн.	-	56738,1
	Сумарний ефект	Грн.	60362,5	

3.4 Визначення та аналіз показників економічної ефективності впровадження обраного хмарного рішення

Коефіцієнт повернення інвестицій ROSI показує, скільки гривень додаткового прибутку приносить одна гривня капітальних інвестицій на впровадження обраного хмарного рішення:

$$ROSI = E / K, \text{ частки одиниці}$$

де — Е загальний ефект від впровадження обраного хмарного рішення грн.; К — капітальні інвестиції за варіантами, що забезпечили цей ефект, грн.

Коефіцієнт повернення інвестицій ROSI:

$$60362,5 / 60423,5 = 0,99$$

Проект визнається економічно доцільним, якщо розрахункове значення коефіцієнта повернення інвестицій перевищує величину річної депозитної ставки з урахуванням інфляції:

Розрахункове значення коефіцієнта повернення інвестицій:

$0,99 > 0,95$

Термін окупності капітальних інвестицій То показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження обраного хмарного рішення:

$$T = 1/0,99 = 1.01 \text{ років.}$$

3.5 Висновки до розділу 3

Впровадження обраного хмарного рішення є економічно доцільним, оскільки коефіцієнт повернення інвестицій ROSI складає 0,99, що означає отримання 0,99 грн. економічного ефекту на кожну гривню капітальних вкладень на впровадження обраного хмарного рішення. Отримане значення коефіцієнту повернення інвестицій значно вище дохідності альтернативного вкладення коштів.

ВИСНОВКИ

В ході роботи було проаналізовано підприємство, розроблено плани інформаційних потоків і визначено вразливі місця системи.

Було проаналізовано існуючі загрози і створено моделі порушника і загрози.

В результаті було виявлено найбільш вразливі місця системи, на основі чого було проведено порівняльний аналіз і обрано хмарне рішення, яке дає достатній рівень захисту і покриває виявлені загрози.

Окрім цього було проведено аналіз економічної доцільності впровадження подібного роду рішення, який дав позитивний результат на користь необхідності даного заходу.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. "A History of Cloud Computing". ComputerWeekly.

2. Louden, Bill (September 1983). "Increase Your 100's Storage with 128K from Compuserve". Portable 100. New England Publications Inc. 1 (1): 22. ISSN 0738-7016.

3. Daniela Hernandez (May 23, 2014). "Tech Time Warp of the Week". Wired.

4. "Box.net lets you store, share, work in the computing cloud". Silicon Valley Business Journal. December 16, 2009. Retrieved October 2, 2016.

5. "On-premises private cloud storage description, characteristics, and options". Archived from the original on 2016-03-22. Retrieved 2012-12-10.

6. S. Rhea, C. Wells, P. Eaton, D. Geels, B. Zhao, H. Weatherspoon, and J. Kubiatowicz, Maintenance-Free Global Data Storage. IEEE Internet Computing , Vol 5, No 5, September/October 2001, pp 40–49. [1] Archived 2012-03-29 at the Wayback Machine [2] Archived 2011-06-23 at the Wayback Machine

7. Kolodner, Elliot K.; Tal, Sivan; Kyriazis, Dimosthenis; Naor, Dalit; Allalouf, Miriam; Bonelli, Lucia; Brand, Per; Eckert, Albert; Elmroth, Erik; Gogouvitis, Spyridon V.; Harnik, Danny; Hernandez, Francisco; Jaeger, Michael C.; Bayuh Lakew, Ewnetu; Manuel Lopez, Jose; Lorenz, Mirko; Messina, Alberto; Shulman-Peleg, Alexandra; Talyansky, Roman; Voulodimos, Athanasios; Wolfsthal, Yaron (2011). "A Cloud Environment for Data-intensive Storage Services". 2011 IEEE Third International Conference on Cloud Computing Technology and Science: 357–366. CiteSeerX 10.1.1.302.151. doi:10.1109/CloudCom.2011.55. ISBN 978-1-4673-0090-2. S2CID 96939.

8. Cardin, Jay. "Qumulo – Because Data Storage Is Not Created Equal". WEI Tech Exchange. WEI. Retrieved 5 August 2021.

9. Vernik, Gil, et al. "Data On-boarding in Federated Storage Clouds." Proceedings of the 2013 IEEE Sixth International Conference on Cloud Computing. IEEE Computer Society, 2013.

10. Kemme, Bettina, et al. "Consistency in Distributed Systems (Dagstuhl Seminar 13081)." (2013).

11. ZDNet, Nasuni Cloud Storage Gateway By Dan Kusnetzky, June 1, 2010, [3]

12. Gupta, P (20 October 2013). "The usage and adoption of cloud computing by small and medium businesses". International Journal of Information Management. 33 (5): 861–874. doi:10.1016/j.ijinfomgt.2013.07.001.

13. "Ochs, R. (2012). The New Decision-Makers. CRN (June 22, 2012). Retrieved on December 10, 2012". Archived from the original on August 5, 2016. Retrieved December 10, 2012.

14. "4 reasons why cloud and on-premises storage are different, but equally good for people data". 2013-09-09. Archived from the original on 2013-09-25. Retrieved 2013-09-09.

15. O'Brien, J. A. & Marakas, G. M. (2011). Computer Software. Management Information Systems 10th ed. 145. McGraw-Hill/Irwin

16. Wu C F, Wang Y S, Liu G N, Amies, A, 2012, Create solutions on IBM SmartCloud Enterprise: Transfer image assets between different accounts IBM developerWorks, June 6.

17. "The Attack Surface Problem". Sans.edu. Retrieved 2013-07-08.

18. "US-CERT ICS-TIP-12-146-01 Targeted Cyber Intrusion and Detection Mitigation Strategies".[permanent dead link]

19. Chu, Cheng-Kang; Chow, Sherman S.M.; Tzeng, Wen-Guey; Zhou, Jianying; Deng, Robert H. (2014-02-01). "Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage". IEEE Transactions on Parallel and Distributed Systems. 25 (2): 468–477. doi:10.1109/TPDS.2013.112. ISSN 1045-9219. S2CID 13030328.

20. Transfer files from one onedrive account to another.

21. Butler, Brandon (2 June 2014). "Cloud's worst-case scenario: What to do if your provider goes belly up". Network World. Retrieved 20 June 2015.

22. Gaudin, Sharon (12 January 2015). "Verizon gets 'black eye' in long cloud shutdown". ComputerWorld. Retrieved 20 June 2015.

23. Butler, Brandon (1 November 2013). "Free cloud storage service MegaCloud goes dark". Network World. Retrieved 20 June 2015.

24. "DoDD 5015.2 DOD Records Management Program, Section 5.1.3" (PDF). Archived from the original (PDF) on March 22, 2011.

25. Mello, John P. (20 March 2012). "National Security Agency Pressed to Reveal Details on Google Deal". PCWorld. Retrieved 2013-07-08.

26. Spring, Tom. "Google Ditches Microsoft's Windows Over Security Issues, Report Claims". PCWorld. Retrieved 2013-07-08.

27. Subashini, S.; Kavitha, V. (2011-01-01). "A survey on security issues in service delivery models of cloud computing". Journal of Network and Computer Applications. 34 (1): 1–11. doi:10.1016/j.jnca.2010.07.006.

28. Justin Pot (7 December 2011). "Codex Cloud: Upload Your Books & Read Them Online Along With Other People's Uploads". MakeUseOf. Archived from the original on 21 October 2016. Retrieved 12 December 2012.

29. Nancy Messieh (18 October 2011). "Publishers beware: Is CodexCloud the Grooveshark for ebooks?". NextWeb.

30. Jones, Hadley (16 January 2014). "When Online File Storage Gets Legal: Regulatory Compliance". CloudWedge. Retrieved 2014-01-16.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

	Формат	Наіменування	Кількість листів	Примітки
		Документація		
	А4	Реферат	1	
	А4	Список умовних скорочень	1	
	А4	Зміст	1	
	А4	Вступ	1	
	А4	Аналіз предметної області і постановка задачі	34	
	А4	Проектування і створення власної реалізації	19	
	А4	Економічне обґрунтування доцільності розробки	7	
	А4	Висновки	1	
	А4	Перелік посилань	3	
0	А4	Додаток А	1	
1	А4	Додаток Б	1	
2	А4	Додаток В	1	
3	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на фізичному носії.

1 Чурсін_ОО_125-18-1_.docx

2 Чурсін_ОО_125-18-1_.pdf

3 Чурсін_ОО_125-18-1_.pptx

4 Чурсін_ОО_125-18-1_.pdf.p7s

ДОДАТОК В. Відгук керівника економічного розділу.

Економічний розділ виконаний відповідно до вимог, які ставляться до кваліфікаційних робіт, та заслуговує на оцінку 65 б. («задовільно»).

Керівник розділу _____ доц. Пілова Д.П.

(підпис) (ініціали, прізвище)

ДОДАТОК Г. Відгук керівника кваліфікаційної роботи.

Відгук

На кваліфікаційну роботу студента групи 125-18-1

Чурсіна Олександра Олександровича

На тему: «***Комплексна система захисту інформації ТОВ «Супутник С» з детальною розробкою підсистеми зберігання та обробки конфіденційних данних.***»

Пояснювальна записка складається зі вступу, трьох розділів і висновків, розташованих на 83 сторінках.

Мета роботи є актуальною, оскільки вона спрямована на розробку підсистеми пам'яті, який забезпечить абсолютно безпечне зберігання інформації.

При виконанні роботи автор продемонструв добрий рівень теоретичних знань і практичних навичок. На основі аналізу основних понять предметної області, а також сучасного стану питання захищеності хмарних сховищ в ній сформульовано задачі, вирішенню яких присвячений другий розділ. У ньому було проведено проектування і розробку підсистеми пам'яті, який забезпечить абсолютно безпечне збереження інформації.

До недоліків роботи слід віднести недостатню проробку окремих питань.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог «Положення про систему виявлення та запобігання плагіату».

В цілому робота задовольняє усім вимогам, а її автораЧурсіна О.О. заслуговує на оцінку « » та присвоєння кваліфікації «Бакалавр з кібербезпеки» за спеціальністю 125 Кібербезпека.

Кваліфікаційна робота заслуговує оцінки «_____».

Керівник кваліфікаційної роботи ст.викл. Святошенко В.О