**МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**КАФЕДРА** **КОМП’ЮТЕРИЗОВАНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ**

ДОПУСТИТИ ДО ЗАХИСТУ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_\_\_\_ А.В. Ільєнко

«\_\_\_\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_ р.

На правах рукопису

УДК 004.056.5:510.22(043.3)

**МАГІСТЕРСЬКА АТЕСТАЦІЙНА РОБОТА**

**ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ**

**«МАГІСТР»**

**Тема**:Система захисту комп’ютерної мережі засобами віртуалізації

|  |  |
| --- | --- |
| **Автор:** | І.Ю. Юрчук |
| **Науковий керівник:** к.т.н., доц. | А.Б. Єлізаров |
| **Нормоконтролер:** асист. | С.В. Єгоров |

**Київ 2020**

**НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ**

**Факультет:** Кібербезпеки, комп’ютерної та програмної інженерії

**Кафедра:** Компютеризованих систем захисту інформації

**Освітній ступінь:** Магістр

**Спеціальність:** 125 «Кібербезпека»

**Освітньо-професійна програма**: «Безпека інформаційних і комунікаційних систем»

ЗАТВЕРДЖУЮ

Завідувач кафедри

\_\_\_\_\_\_\_\_\_\_\_ С.В. Казмірчук

«\_\_» \_\_\_\_\_\_\_\_\_ 20\_\_ р.

**ЗАВДАННЯ**

**на виконання магістерської атестаційної роботи**

**магістранта Юрчук Ірини Юріївни**

1. Тема: *Система захисту комп’ютерної мережі засобами віртуалізації*

затверджена наказом ректора від «02» жовтня 2019 року № 2265/ст*.*

1. Термін виконання з 14.10.2019 р. по 09.02.2020 р*.*
2. Вихідні дані: дані про систему захисту засобами віртуалізації.
3. Зміст пояснювальної записки: аналіз технології віртуалізації, розробка плану відновлення після катастроф, аналіз та розробка загальної політики ІТ-безпеки на підприємстві, розробка правил захисту баз даних, розробка політики резервного копіювання, розробка системи захисту засобами віртуалізації.

**КАЛЕНДАРНИЙ ПЛАН**

**виконання магістерської роботи**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Етапи виконання магістерської роботи** | **Термін виконання етапів** | **Примітка** |
|  | Уточнення постановки задачі | 14.10.2019 | *Виконано* |
|  | Аналіз літературних джерел | 15.10.2019 -21.10.2019 | *Виконано* |
|  | Обґрунтування вибору рішення | 22.10.2019 -28.10.2019 | *Виконано* |
|  | Збір інформації | 29.10.2019 -11.11.2019 | *Виконано* |
|  | Аналіз технології віртуалізації | 12.11.2019 -18.11.2019 | *Виконано* |
|  | Розробка загальної політики ІТ-безпеки на підприємстві, політики резервного копіювання | 18.11.2019 -09.12.2019 | *Виконано* |
|  | Розробка системи захисту засобами віртуалізації | 10.12.2019 -19.01.2020 | *Виконано* |
|  | Перевірка на антиплагіат | 20.01.2020-28.01.2020 | *Виконано* |
|  | Оформлення і друк пояснювальної записки | 29.01.2020-02.02.2020 | *Виконано* |
|  | Оформлення презентації | 03.02.2020 | *Виконано* |
|  | Отримання рецензій від рецензента | 04.02.2020 | *Виконано* |
|  | Захист в ЕК | 05.02.2020 | *Виконано* |

Магістрант І. Юрчук

(підпис, дата)

Науковий керівник А. Єлізаров

(підпис, дата)

**РЕФЕРАТ**

Магістерська атестаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел, додатків і має 80 сторінок основного тексту, 17 рисунків, 8 таблиць, 3 сторінки додатків. Список використаних джерел містить 17 найменувань і займає 2 сторінки. Загальний обсяг роботи 83 сторінки.

Метою роботи є розробка віртуалізації мережі для оптимізації ІТ-інфраструктури компанії.

В роботі представлено рішення, в рамках якого створені віртуальні сервери і робочі станції, які заміняють робочі станції з індивідуальною операційною системою Windows і програмним забезпеченням на сервісі, доступним усім користувачам.

В роботі розроблено план відновлення після катастроф, проведено аналіз та розроблено загальну політику ІТ-безпеки на підприємстві, правила захисту баз даних, політику резервного копіювання і розроблено систему захисту засобами віртуалізації задля оптимізації.

Розроблена система відноситься до галузі інформаційної безпеки і може бути використана як для оптимізації і підвищення рівня захищеності існуючої інфраструктури, так і для нових компаній при побудові власного корпоративного хмарного середовища.

Можливі напрямки розвитку цієї роботи пов’язані із розширенням можливостей програмного забезпечення, які дозволять створювати більш ефективні платформи віртуалізації, як для серверних систем, так і для настільних комп'ютерів.

Ключові слова: захист, віртуалізація, технологія віртуалізації, комп’ютерна мережа, інформаційна безпека.

**ЗМІСТ**

[**ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ** 7](#_Toc30454842)

[**ВСТУП** 8](#_Toc30454843)

[**РОЗДІЛ 1. ТЕХНОЛОГІЯ ВІРТУАЛІЗАЦІЇ** 10](#_Toc30454844)

[**1.1.** **Основні визначення та історія виникнення** 10](#_Toc30454845)

[**1.2.** **Як працює віртуалізація?** 11](#_Toc30454846)

[**1.3.** **Переваги віртуалізації** 12](#_Toc30454847)

[**1.4.** **Типи віртуалізації** 13](#_Toc30454848)

[**1.5.** **Як працює віртуалізація серверу?** 15](#_Toc30454849)

[**1.6.** **Типи віртуалізації серверу** 19](#_Toc30454850)

[**1.7.** **Обмеження віртуалізації сервера** 21](#_Toc30454851)

[**1.8.** **Центр обробки даних** 22](#_Toc30454852)

[**1.9.** **Віртуалізація серверу VMWare** 25](#_Toc30454853)

[**1.10.** **Висновки до розділу** 28](#_Toc30454854)

[**РОЗДІЛ 2. РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ** 29](#_Toc30454855)

[**2.1.** **План відновлення після катастроф** 29](#_Toc30454856)

[**2.1.1.** **Мета та сфера застосування цього плану** 29](#_Toc30454857)

[**2.1.2.** **Цілі планування** 29](#_Toc30454858)

[**2.1.3.** **Команди відновлення та їх обов'язки** 30](#_Toc30454859)

[**2.1.3.1.** **Команда з управління катастрофами** 30](#_Toc30454860)

[**2.1.3.2.** **Операційна команда** 32](#_Toc30454861)

[**2.1.3.3.** **Комунікаційна команда** 34](#_Toc30454862)

[**2.1.3.4.** **Команда безперервної діяльності** 34](#_Toc30454863)

[**2.1.4.** **Дії у випадку катастрофи** 35](#_Toc30454864)

[**2.1.4.1.** **Сценарій відновлення** 36](#_Toc30454865)

[**2.2.** **Загальна політика ІТ безпеки на підприємстві** 36](#_Toc30454866)

[**2.2.1.** **Фізичний захист** 36](#_Toc30454867)

[**2.2.2.** **Інформаційна безпека** 39](#_Toc30454868)

[**2.3.** **Правила захисту баз даних** 42](#_Toc30454869)

[**2.3.1.** **Порядок правил** 43](#_Toc30454870)

[**2.3.1.1.** **Визначення загроз** 43](#_Toc30454871)

[**2.3.1.2.** **Заходи попередження загроз** 46](#_Toc30454872)

[**2.3.1.3.** **Дослідження системи безпеки баз даних** 56](#_Toc30454873)

[**2.4.** **Політика резервного копіювання** 59](#_Toc30454874)

[**2.4.1.** **Частота і види копіювання** 60](#_Toc30454875)

[**2.4.2.** **Резервне копіювання на магнітну стрічку (backup)** 60](#_Toc30454876)

[**2.4.3.** **Контроль резервного копіювання** 61](#_Toc30454877)

[**2.5.** **Висновки до розділу** 63](#_Toc30454878)

[**РОЗДІЛ 3. СИСТЕМА ЗАХИСТУ ЗАСОБАМИ ВІРТУАЛІЗАЦІЇ** 64](#_Toc30454879)

[**3.1.** **Опис і мета проекту віртуалізації робочих станцій** 64](#_Toc30454880)

[**3.1.1.** **Конфігурація** 67](#_Toc30454881)

[**3.1.2.** **Програмне забезпечення** 67](#_Toc30454882)

[**3.1.3.** **Citrix XenDesktop** 68](#_Toc30454883)

[**3.1.3.1.** **Конфігурація** 71](#_Toc30454884)

[**3.1.4.** **Citrix XenApp** 72](#_Toc30454885)

[**3.1.4.1.** **Конфігурація** 78](#_Toc30454886)

[**3.1.5.** **Citrix XenServer** 78](#_Toc30454887)

[**3.1.5.1.** **Конфігурація** 79](#_Toc30454888)

[**3.1.6.** **NetApp** 79](#_Toc30454889)

[**3.1.6.1.** **Технічні характеристики** 79](#_Toc30454890)

[**3.2.** **Висновки до розділу** 81](#_Toc30454891)

[**ВИСНОВКИ** 82](#_Toc30454892)

[**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ** 83](#_Toc30454893)

[**Додаток А** 86](#_Toc30454894)

[**План дій при сценарії «Незначні пошкодження»** 86](#_Toc30454895)

[**Додаток Б** 87](#_Toc30454896)

[**План дій при сценарії «Значні пошкодження»** 87](#_Toc30454897)

# **ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ**

ІТ – Information Technology – інформаційні технології.

ПК – персональний комп’ютер.

ОС – операційна система.

CD – Compact Disc – компакт-диск.

IP – Internet Protocol – унікальний мережевий адрес.

SQL – Structured Query Language – мова програмування в базах даних.

ПЗ – програмне забезпечення.

ICA – Independent Computing Architecture–закритий протокол для сервера додатків, розробленого компанією Citrix Systems.

AMD –Advanced Micro Devices–один з найбільших виробників центральних процесорів, графічних процесорів і адаптерів**.**

XML – Extensible Markup Language – розширювана мова розмітки.

DC – Data Center – дата-центр.

CPU – Central Processing Unit – центральний процесор.

HDD – Hard Disk Drive – жорсткий диск.

SAN – Storage Area Network – мережа зберігання даних.

VPN – Virtual Private Network – віртуальна приватна мережа.

WWW – World Wide Web – всесвітня мережа.

**ВСТУП**

**Актуальність**. Значний розвиток ринку технологій віртуалізації за останні декілька років відбувся завдяки збільшенню потужності апаратного забезпечення, який дозволив створювати по-справжньому ефективні платформи віртуалізації, як для серверних систем, так і для настільних комп'ютерів.

Технології віртуалізації вже давно існують у світі обчислювальної техніки. Однак ця технологія стала лише ключовим компонентом постійно зростаючого центру обробки даних. За останній час організації почали помічати, що прогрес серверних процесорів та пам'яті випереджає ОС. Багато компаній виявили, що використання процесора та пам'яті регулярно становило менше 20%.

Наразі складно уявити побудову нового серверного вузла компанії без використання технології віртуалізації. Визначальними факторами такої популярності є економія грошей і часу, а також високий рівень безпеки та забезпечення безперервності бізнес-процесів.

**Відомі підходи до вирішення поставленої задачі.** Сьогодні вже можна знайти рішення для віртуалізації серверів, що підтримують широкий спектр систем у середовищі розробки, забезпечення якості та виробництва. Віртуалізація сервера - це технологія, яка надає можливість запускати кілька ізольованих ОС на одній частині серверного обладнання, що дозволяє більш високий рівень використання ресурсів і дозволяє створити захищене, налаштоване та ізольоване середовище виконання для запущених програм, навіть якщо вони не мають довіри, не впливаючи на додатки інших користувачів.

**Метою роботи є** розробка віртуалізації мережі для оптимізації існуючої ІТ-інфраструктури компанії.

Для досягнення поставленої мети вирішуються такі **задачі:**

1. аналіз технології віртуалізації.
2. розробка плану відновлення після катастроф.
3. аналіз та розробка загальної політики ІТ-безпеки на підприємстві.
4. розробка правил захисту баз даних.
5. розробка політики резервного копіювання.
6. розробка системи захисту засобами віртуалізації.

**Галузь застосування**. Розроблена система захисту відносяться до галузі інформаційної безпеки і може бути використана як для оптимізації і підвищення рівня захищеності існуючої інфраструктури, так і для нових компаній при побудові власного корпоративного хмарного середовища.

**Об’єктом дослідження** є технологія віртуалізації.

**Предметом дослідження** є система віртуалізації мережі.

**Методи дослідження** базуються на аналізі технології віртуалізації, розробці політик безпеки, системи захисту та проектування мережі.

**Новизна одержаних результатів полягає в наступному:**

Вдосконалено систему комп’ютерної мережі, в рамках якої створюються віртуальні сервери і робочі станції, що дозволять замінити робочі станції з індивідуальної операційною системою Windows і програмним забезпеченням.

**Практичне значення отриманих результатів:**

* розроблено План відновлення після катастроф, правила захисту баз даних, політику резервного копіювання.
* проведено аналіз та розроблено загальну політику ІТ-безпеки на підприємстві.
* розроблено систему захисту засобами віртуалізації.

**Апробація.** Основні положення роботи доповідалися та обговорювалися на XV Міжнародній науково-практичній конференції «Наукові горизонти – 2019», том 15. («Scientific Horizons – 2019», volume 15) – 30.09.2019 – 7.10.2019.

# **РОЗДІЛ 1. ТЕХНОЛОГІЯ ВІРТУАЛІЗАЦІЇ**

## **Основні визначення та історія виникнення**

Віртуалізація - це технологія, яка дозволяє створювати корисні ІТ-сервіси, використовуючи ресурси, які традиційно пов'язані з обладнанням [1]. Це дозволяє використовувати повну потужність фізичної машини, розподіляючи її можливості між багатьма користувачами чи середовищами.

У віртуалізації використовується програмне забезпечення, яке імітує функціональність обладнання для створення віртуальної системи [3]. Ця практика дозволяє ІТ-організаціям керувати кількома ОС, більш ніж однією віртуальною системою та різними програмами на одному сервері. Переваги віртуалізації включають підвищення ефективності та економії масштабу.

Попри те, що технологія віртуалізації винайдена до 1960-х років, вона не була широко прийнята й до початку 2000-х. Технології, що давали можливість віртуалізації - як гіпервізори - були розроблені десятиліттями тому, щоб надати декільком користувачам одночасний доступ до комп'ютерів, які виконували пакетну обробку. Пакетна обробка була популярним стилем обчислень у бізнес-секторі, який виконував рутинні завдання тисячі разів дуже швидко (наприклад, заробітна плата).

Та протягом наступних декількох десятиліть популярність інших рішень проблем користувачів росла, тоді як віртуалізація – ні [5]. Одним з таких інших рішень був розподіл часу («time-sharing»), який відокремлював користувачів в ОС - ненавмисно призводив до інших ОС, таких як UNIX, які в підсумку поступилися місцем Linux. Весь час віртуалізація залишалася в основному неприйнятою, нішевою технологією.

При швидкому переході до 1990-х більшість підприємств мали фізичні сервери та ІТ-стеки для одного постачальника, що не дозволяло застарілим додаткам запускатись на іншому обладнанні постачальника [8]. Оскільки компанії оновлювали своє ІТ-середовище менш дорогими товарними серверами, ОС та додатками від різних постачальників, вони були зв'язані з недостатньо використовуваним фізичним обладнанням - кожен сервер міг виконувати лише одне завдання, яке стосується одного постачальника.

Ось тут віртуалізація справді почалася. Це було природним рішенням двох проблем: компанії могли розділити свої сервери та запустити застарілі програми на декілька типів та версій ОС [6]. Сервери почали використовуватись більш ефективно, тим самим зменшивши витрати, пов'язані з придбанням, налаштуванням, охолодженням та технічним обслуговуванням. Сьогодні вона настільки поширена на підприємствах, що часто потрібно спеціалізоване програмне забезпечення для управління віртуалізацією, яке допомагає відстежувати все це.

* 1. **Як працює віртуалізація?**

Програмне забезпечення, яке називається гіпервізори (див. рис. 1.1), відокремлює фізичні ресурси від віртуальних середовищ - речей, які потребують ці ресурси [1]. Гіпервізори можуть бути над ОС (наприклад, на ноутбуці) або встановлюватися безпосередньо на апаратне забезпечення (наприклад, на сервер), саме тому більшість підприємств віртуалізуються. Гіпервізори забирають ваші фізичні ресурси та ділять їх так, щоб віртуальне середовище могло ними користуватися.

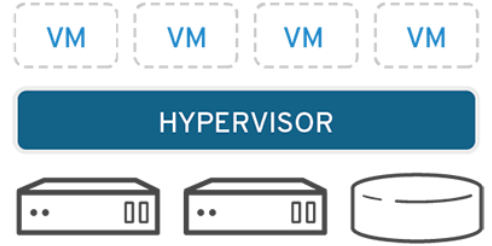


Рис.1.1. Схема гіпервізору

Ресурси розподіляються за потребою від фізичного середовища до багатьох віртуальних середовищ. Користувачі взаємодіють з обчисленнями та виконують обчислення у віртуальному середовищі (зазвичай це називається гостьова машина або віртуальна машина). Віртуальна машина функціонує як єдиний файл даних. І як і будь-який цифровий файл, його можна переміщувати з одного комп'ютера на інший, відкривати в одному з них і впевнитись, що працює так само.

Коли віртуальне середовище працює і користувач або програма видає інструкцію, яка вимагає додаткових ресурсів від фізичного середовища, гіпервізор переносить запит у фізичну систему та кешує зміни, що відбувається майже на власній швидкості (особливо, якщо запит надсилається через гіпервізор з відкритим кодом на базі віртуальної машини на основі ядра).

* 1. **Переваги віртуалізації**

Віртуалізація надає компаніям можливість максимізувати їх виробництво [2]. Додатковими перевагами для бізнесу та центрів обробки даних є:

* Цілеспрямовані сервери. Віртуалізація забезпечує економічно ефективний спосіб розділення електронної пошти, баз даних та веб-серверів, створюючи більш комплексну та надійну систему.
* Швидке розгортання та перерозподіл. Коли фізичний сервер виходить з ладу, резервний сервер може не завжди бути готовим або оновленим. Також може бути недоступним зображення або клон сервера. Якщо це так, то процес передислокації може бути трудомістким і виснажливим. Однак якщо центр обробки даних віртуалізований, то процес швидкий і досить простий. Віртуальні засоби резервного копіювання, доступні для прискорення процесу на кілька хвилин.
* Зменшення тепла та покращення енергозбереження. Компанії, які використовують багато апаратних серверів, ризикують перегріти свої фізичні ресурси. Найкращий спосіб запобігти цьому - зменшити кількість серверів, що використовуються для управління даними, і найкращий спосіб зробити це шляхом віртуалізації.
* Краще для навколишнього середовища. Компанії та центри обробки даних, які використовують багато обладнання, залишають великий слід вуглецю; вони повинні брати на себе відповідальність за забруднення, яке вони створюють. Віртуалізація може допомогти зменшити ці ефекти, значно зменшивши необхідну кількість охолодження та потужності, тим самим допомагаючи очистити повітря та атмосферу. Як результат, компанії та центри обробки даних, які здійснюють віртуалізацію, покращать свою репутацію, а також підвищують якість їх відносин із клієнтами та планетою.
* Легша міграція до хмари. Віртуалізація наближає компанії до повного використання хмарного середовища. Віртуальні машини можуть бути навіть розгорнуті з центру обробки даних для створення хмарної інфраструктури. Можливість використовувати хмарове мислення за допомогою віртуалізації робить міграцію до хмари ще простішою.
* Відсутність залежності від постачальника. Віртуальні машини не залежать від апаратної конфігурації. Як результат, віртуалізація апаратного та програмного забезпечення означає, що компанії не потрібно залежати від постачальника цих фізичних ресурсів.
  1. **Типи віртуалізації**

Віртуалізація даних (див. рис.1.3.1). Дані, які поширюються по всьому світу, можна об'єднати в єдине джерело. Віртуалізація даних дозволяє компаніям ставитися до даних як до динамічного постачання - надаючи можливості обробки, які можуть об'єднувати дані з різних джерел, легко розміщувати нові джерела даних та трансформувати дані відповідно до потреб користувачів.

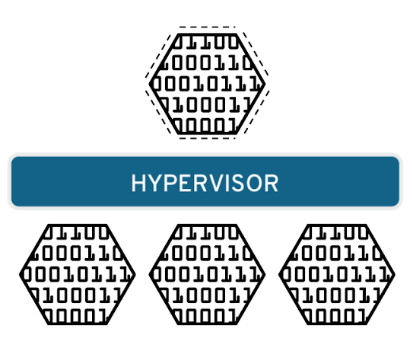


Рис. 1.3.1. Віртуалізація даних

Інструменти віртуалізації даних є перед декількома джерелами даних і дозволяють їм розглядатися як єдине джерело, доставляючи потрібні дані - у необхідній формі - в потрібний час будь-якій програмі чи користувачеві.

Віртуалізація настільних ПК (див. рис.1.3.2). Легко плутати з віртуалізацією ОС, яка дозволяє розгортати кілька ОС на одній машині, віртуалізація на робочому столі дозволяє центральному адміністратору (або автоматизованому інструменту адміністрування) розгортати імітовані робочі середовища на сотні фізичних машин одночасно. На відміну від традиційних середовищ робочого столу, які фізично встановлюються, налаштовуються та оновлюються на кожній машині, віртуалізація настільних ПК дозволяє адміністраторам проводити масові конфігурації, оновлення та перевірку безпеки на всіх віртуальних робочих столах.

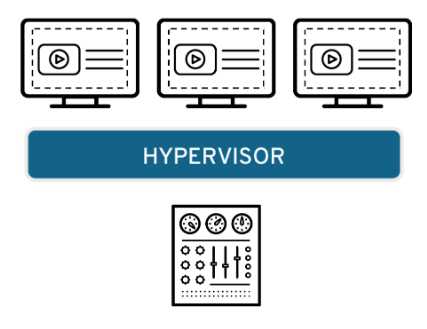


Рис. 1.3.2. Віртуалізація ПК

Віртуалізація сервера (див. рис.1.3.3). Сервери - це комп’ютери, призначені для дуже ефективної обробки великої кількості конкретних завдань, тому інші комп’ютери, як-от ноутбуки та настільні комп’ютери, можуть виконувати різні завдання.

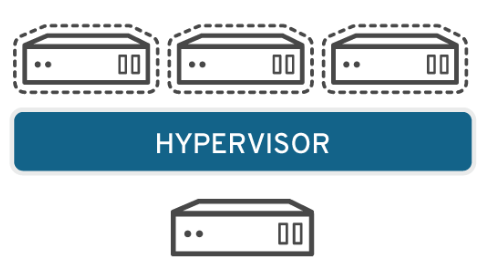


Рис. 1.3.3. Віртуалізація сервера

Віртуалізація сервера дозволяє йому виконувати більше цих специфічних функцій і включає розділення, щоб компоненти могли використовуватися для обслуговування декількох функцій.

Віртуалізація операційної системи (див. рис.1.3.4). Віртуалізація операційної системи відбувається в ядрі - центральних менеджерах завдань операційних систем. Це корисний спосіб запускати середовища Linux та Windows одночасно. Підприємства можуть також передавати віртуальні операційні системи на комп'ютери, які:

* Знижують об'ємні витрати на обладнання, оскільки комп’ютери не потребують таких високих можливостей.
* Підвищують безпеку, оскільки всі віртуальні екземпляри можна відстежувати та ізолювати.
* Обмежують час, витрачений на ІТ-сервіси, такі як оновлення програмного забезпечення.

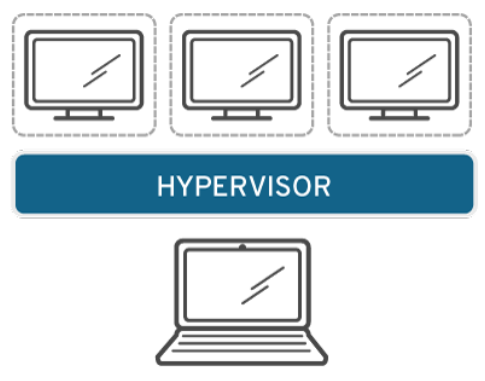


Рис. 1.3.4. Віртуалізація ОС

* 1. **Як працює віртуалізація серверу?**

Серверні комп'ютери - машини, на яких розміщуються файли та програми в комп'ютерних мережах - повинні бути потужними [7]. Деякі мають центральні процесори з декількома процесорами, які дають цим серверам можливість легко виконувати складні завдання. Адміністратори комп'ютерної мережі зазвичай виділяють кожному серверу певну програму або завдання. Багато з цих завдань погано поєднуються з іншими - кожному потрібна своя окрема машина. Одна програма на сервері також допомагає відстежити проблеми у мірі їх виникнення. Це простий спосіб впорядкувати комп'ютерну мережу з технічної точки зору.

Однак з цим підходом є кілька проблем. Одна з них полягає в тому, що він не використовує обчислювану потужність сучасних серверних комп'ютерів. Більшість серверів використовують лише невелику частину своїх загальних можливостей обробки. Ще одна проблема полягає в тому, що комп’ютерна мережа стає все більшою і складнішою, сервери починають займати багато фізичного простору. Центр обробки даних може переповнитися стелажами серверів, що споживають багато енергії та виробляють тепло.

Віртуалізація сервера намагається вирішити обидві проблеми за раз (див. рис. 1.5.1). Використовуючи спеціально розроблене програмне забезпечення, адміністратор може перетворити один фізичний сервер у кілька віртуальних машин. Кожен віртуальний сервер діє як унікальний фізичний пристрій, здатний запускати власну ОС. Теоретично можна створити достатньо віртуальних серверів, щоб використовувати всю обчислювану потужність машини, хоча на практиці це не завжди найкраща ідея.

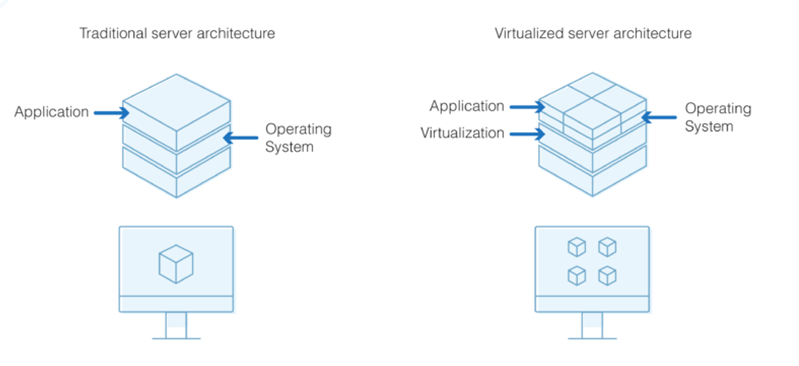


Рис. 1.5.1. Віртуалізація серверу

Віртуалізація не нова концепція. Вчені десятиліттями створювали віртуальні машини на суперкомп'ютерах. Але пройшло лише кілька років, як віртуалізація стала можливою для серверів. У світі ІТ віртуалізація серверів - гаряча тема. Це все ще молода технологія, і кілька компаній пропонують різні підходи.

Існує багато причин, через які компанії та організації інвестують у віртуалізацію серверів. Деякі причини є фінансово мотивованими, а інші вирішують технічні проблеми:

1. Віртуалізація сервера економить простір завдяки консолідації. Загальною практикою є виділяти кожен сервер одному додатку.

Якщо кілька додатків використовують лише невелику кількість процесорної потужності, адміністратор мережі може об'єднати кілька машин на одному сервері, де працює кілька віртуальних середовищ. Для компаній, які мають сотні чи тисячі серверів, потреба у фізичному просторі може значно зменшитися.

1. Віртуалізація сервера надає компаніям можливість практикувати надмірність без придбання додаткового обладнання.

Надлишок відноситься до запуску одного і того ж додатка на декількох серверах. Це міра безпеки - якщо сервер не працює з будь-якої причини, інший сервер, який працює з тим же додатком, може зайняти його місце. Це мінімізує будь-які перебої в обслуговуванні. Не було б сенсу будувати два віртуальних сервери, що виконують одну і ту ж програму на одному фізичному сервері. Якби фізичний сервер вийшов з ладу, обидва віртуальних сервера також не змогли б вийти з ладу. У більшості випадків адміністратори мережі створюватимуть надлишкові віртуальні сервери на різних фізичних машинах.

1. Віртуальні сервери пропонують програмістам ізольовані, незалежні системи, в яких можуть протестувати нові програми або ОС.

Замість придбання спеціальної фізичної машини адміністратор мережі може створити віртуальний сервер на існуючій машині. Оскільки кожен віртуальний сервер є незалежним по відношенню до всіх інших серверів, програмісти можуть запускати програмне забезпечення, не переживаючи про вплив інших програм.

1. Серверне обладнання згодом застаріє, і перехід від однієї системи до іншої може бути важким.

Для того щоб надалі пропонувати послуги, що надаються цими застарілими системами, адміністратор мережі може створити віртуальну версію обладнання на сучасних серверах. З точки зору програми, нічого не змінилося. Програми виконуються так, ніби вони все ще працюють на старому обладнання. Це може дати компанії час на перехід до нових процесів, не турбуючись про збої обладнання, особливо якщо компанія, яка виробляла застаріле обладнання, вже не існує і не може виправити зламане обладнання.

1. Новий тренд віртуалізації серверів називається міграцією.

Міграція стосується переміщення серверного середовища з одного місця в інше. Завдяки правильному апаратному та програмному забезпеченню можливо переміщення віртуального сервера з однієї фізичної машини в мережу до іншої. Спочатку це було можливо, лише якщо обидва фізичні машини працювали на одному і тому ж апаратному забезпеченні, ОС та процесорі. Зараз можна мігрувати віртуальні сервери з однієї фізичної машини на іншу, навіть якщо обидві машини мають різні процесори, але тільки від одного виробника.

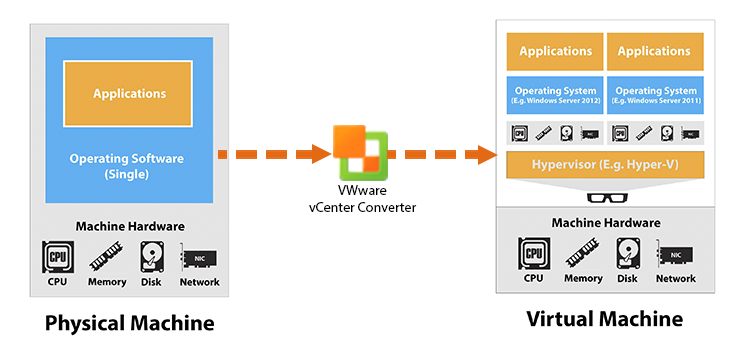
Physical to Virtual (див. рис. 1.5.2) - це тип міграції, в основі якої лежить перетворення існуючого фізичного серверу на віртуальний [20].

Рис. 1.5.1. Міграція типу Physical to Virtual

* 1. **Типи віртуалізації серверу**

Існує три способи створення віртуальних серверів: повна віртуалізація, пара-віртуалізація та віртуалізація на рівні ОС. Всі вони мають декілька загальних рис. Фізичний сервер називається хостом. Віртуальні сервери називаються гостями. Віртуальні сервери ведуть себе як фізичні машини. Кожна система використовує свій підхід для розподілу фізичних ресурсів сервера під потреби віртуального сервера.

Для повної віртуалізації використовується спеціальний вид програмного забезпечення, який називається гіпервізор (див. рис. 1.6.1). Гіпервізор взаємодіє безпосередньо з процесором та дисковим простором фізичного сервера. Він служить платформою для ОС віртуальних серверів. Гіпервізор зберігає кожен віртуальний сервер повністю незалежним і не знає про інші віртуальні сервери, що працюють на фізичній машині. Кожен гостьовий сервер працює на власній ОС - у вас навіть може бути один гість, який працює на Linux та інший в Windows.

Рис. 1.6.1. Повна віртуалізація

Гіпервізор контролює ресурси фізичного сервера. Коли віртуальні сервери запускають програми, гіпервізор ретранслює ресурси з фізичної машини на відповідний віртуальний сервер. Гіпервізори мають власні потреби в обробці, а це означає, що фізичний сервер повинен зарезервувати деяку потужність і ресурси для запуска програми гіпервізора. Це може вплинути на загальну продуктивність сервера і сповільнити програми.

Підхід паравіртуалізації трошки відрізняється (див. рис. 1.6.2.). На відміну від повної технології віртуалізації, гостьові сервери в системі паравіртуалізації знають один про одного.

Рис. 1.6.2. Паравіртуалізація

Гіпервізору паравіртуалізації не потрібно стільки потужностей для управління гостьовими ОС, оскільки кожна ОС вже усвідомлює вимоги, які інші ОС пред'являють на фізичний сервер. Вся система працює разом як єдине ціле.

Підхід до віртуалізації на рівні ОС взагалі не використовує гіпервізор (див. рис. 1.6.3). Натомість можливість віртуалізації є частиною операційної системи хосту, яка виконує всі функції повністю віртуалізованого гіпервізора.

Рис. 1.6.3. Віртуалізація на рівні ОС

Основним обмеженням цього підходу є те, що всі гостьові сервери повинні працювати в одній ОС. Кожен віртуальний сервер залишається незалежним від усіх інших, але ви не можете змішувати та співставляти між ними операційні системи. Оскільки всі гостьові ОС повинні бути однаковими, це називається однорідним середовищем.

Який метод найкращий? Це багато в чому залежить від потреб адміністратора мережі. Якщо всі фізичні сервери адміністратора працюють на одній операційній системі, то підхід на рівні ОС підійде найкраще. Системи на рівні ОС, як правило, більш швидкі та ефективні, ніж інші методи. З іншого боку, якщо адміністратор працює на серверах у кількох різних ОС, кращим вибором може бути пара-віртуалізація. Одним з потенційних недоліків систем паравіртуалізації є підтримка - метод є відносно новим, і лише кілька компаній пропонують програмне забезпечення для пара-віртуалізації. Більше компаній підтримує повну віртуалізацію, але інтерес до пара-віртуалізації зростає і може вчасно замінити повну віртуалізацію.

* 1. **Обмеження віртуалізації сервера**

Переваги віртуалізації сервера можуть бути настільки привабливими, що легко забути, що методика має обмеження. Перш ніж намагатися розробити рішення, для адміністратора мережі важливо дослідити віртуалізацію сервера та його власну архітектуру та потреби.

Для серверів, призначених для додатків з високими вимогами до обчислюваної потужності, віртуалізація не є гарним вибором. Це пов’язано з тим, що віртуалізація суттєво розділяє обчислювану потужність серверу між віртуальними серверами. Коли потужність цієї серверу не може відповідати вимогам програм, все сповільнюється. Задачі, які не займають багато часу, можуть тривати годинами. Гірше того, можливо, що система може вийти з ладу, коли сервер не може задовольнити необхідні вимоги обробки. Мережеві адміністратори повинні дуже гарно ознайомитись із процесором, перш ніж розділяти фізичний сервер на декілька віртуальних машин.

Також нерозумно перевантажувати центральний процесор, створюючи занадто багато віртуальних серверів на одній фізичній машині. Чим більше віртуальних машин повинен підтримувати фізичний сервер, тим меншу потужність може отримувати кожен сервер. Крім того, на фізичних серверах є обмежений обсяг дискового простору. Занадто багато віртуальних серверів може вплинути на здатність сервера зберігати дані.

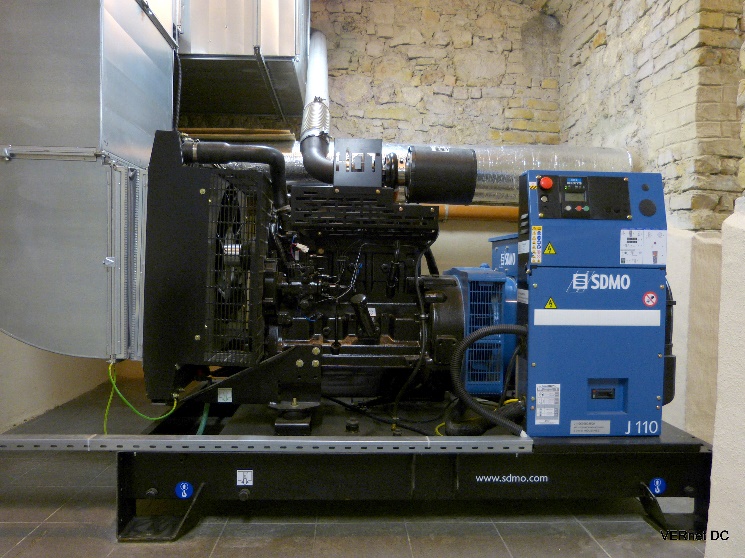
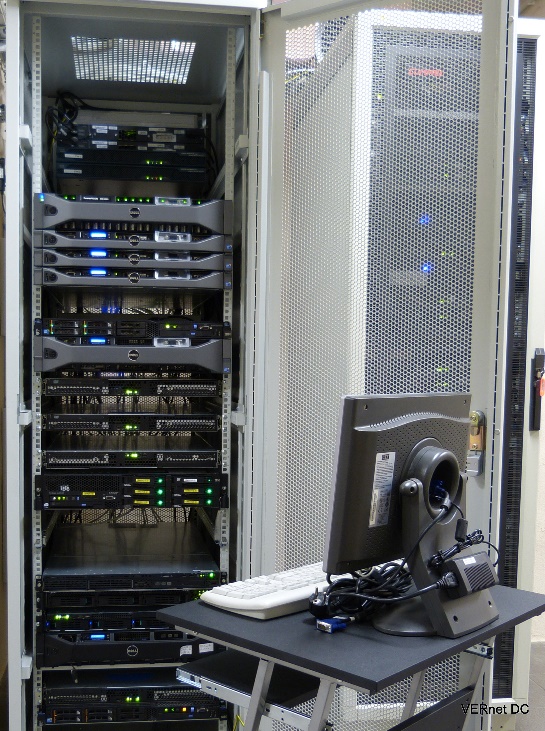
Ще одне обмеження - міграція. Зараз перенести віртуальний сервер з однієї фізичної машини на іншу можна лише тоді, коли обидва фізичні машини використовують процесор одного і того самого виробника. Якщо в мережі використовується один сервер, який працює на процесорі Intel, а інший, який використовує процесор AMD, неможливо перенести віртуальний сервер з однієї фізичної машини на іншу.

Навіщо адміністратору в першу чергу переміщувати віртуальний сервер? Якщо фізичний сервер вимагає обслуговування, перенесення віртуальних серверів на інші машини може скоротити час простою програми. Якщо міграція не є можливою, під час обслуговування всі програми, що працюють на віртуальних серверах, розміщених на фізичній машині, будуть недоступні.

* 1. **Центр обробки даних**

Центр обробки даних (datacenter) - це об'єкт, що складається з мережевих комп'ютерів та сховищ, які підприємства та інші організації використовують для організації, обробки, зберігання та поширення великої кількості даних [15]. Зазвичай бізнес значною мірою залежить від додатків, сервісів та даних, що містяться в центрі обробки даних, що робить його центром і важливим ресурсом для щоденних операцій.

Дані центри - це не єдина річ, а скоріше сукупність елементів[16]. Як мінімум, центри обробки даних служать основними сховищами для всіх типів ІТ-обладнання, включаючи сервери, підсистеми зберігання даних, мережеві комутатори, маршрутизатори та брандмауери, а також кабельні та фізичні стійки, що використовуються для організації та взаємозв'язку ІТ-обладнання (див.рис.1.8). Центр обробки даних також повинен містити належну інфраструктуру, таку як роз**поділ електроенергії та додаткові підсистеми живлення.

*а) б)*

*в) г)*

Рис. 1.8. Дата-центр VERnet DC фірми Versija: *а)* архітектоніка приміщення; *б)* елемент системи кондиціонування повітря; *в)* клієнтська стійка в дата-центрі; *г)*

електропостачання – дизельгенератор.

Сюди також відноситься електричне перемикання; джерела безперебійного живлення; резервні генератори; системи охолодження вентиляції та центрів обробки даних, наприклад конфігурації ряду охолодження та кондиціонери комп'ютерної кімнати; та адекватне забезпечення підключення до мережевого оператора. Все це вимагає фізичного обладнання з фізичною захищеністю та достатньою площею для зберігання всієї колекції інфраструктури та обладнання.

Немає вимоги до єдиного центру обробки даних, а сучасний бізнес може використовувати два чи більше встановлення центрів обробки даних у багатьох місцях для більшої стійкості та кращої продуктивності додатків, що знижує затримку, розміщуючи навантаження наближене до користувачів.

І навпаки, бізнес з кількома центрами обробки даних може вирішити консолідувати центри обробки даних, зменшивши кількість локацій, щоб мінімізувати витрати на ІТ-операції. Консолідація зазвичай відбувається під час злиття та поглинання, коли мажоритарному бізнесу не потрібні центри обробки даних, що належать підпорядкованому бізнесу.

Оператори центрів обробки даних також можуть сплачувати плату за оренду серверного простору в приміщенні для розміщення. Колокація - це привабливий варіант для організацій, які хочуть уникнути великих капітальних витрат, пов’язаних із створенням та підтримкою власних центрів обробки даних. Сьогодні постачальники колокації розширюють свої пропозиції, включаючи керовані сервіси, такі як взаємопов'язаність, що дозволяє клієнтам підключатися до публічної хмари.

Оскільки сьогодні багато провайдерів пропонують керовані послуги разом із засобами їх розміщення, визначення керованих послуг стає розмитим, оскільки всі постачальники продають цей термін дещо по-іншому. Важлива відмінність:

1. Колокація - організація оплачує продавця, щоб розмістити їх обладнання в приміщенні. Клієнт оплачує простір самостійно.
2. Керовані сервіси - організація сплачує постачальнику за те, щоб якимсь чином активно підтримувати або контролювати обладнання, будь то через звіти про ефективність, взаємозв’язок, технічну підтримку чи відновлення після аварій.

Проекти центрів обробки даних повинні також реалізувати надійні методи забезпечення безпеки. Наприклад, безпека часто відображається на плануванні дверних прорізів та коридорів для доступу, які повинні розміщувати рух великого ІТ-обладнання, а також дозволяти працівникам отримувати доступ до інфраструктури.

У центрах обробки даних часто використовуються екологічно чисті хімічні системи пожежогасіння, які ефективно поглинають вогонь кисню, пом'якшуючи побічні пошкодження обладнання. Оскільки центр обробки даних також є основним активом бізнесу, комплексні заходи безпеки, як-от доступ до бейджів та відеоспостереження, допомагають виявити та запобігти жорстокому поводженню службовців, підрядників та зловмисників.

Дата-центри все частіше впроваджують приватне хмарне програмне забезпечення, яке базується на віртуалізації, щоб додати рівень адміністрування, самообслуговування користувачів та оплату / повернення платежів адміністрації центру обробки даних. Мета полягає в тому, щоб дозволити індивідуальним користувачам забезпечити робочі навантаження та інші обчислювальні ресурси на вимогу без втручання ІТ.

* 1. **Віртуалізація серверу VMWare**

Продукти VMware включають віртуалізацію, мережеві інструменти та засоби управління безпекою, програмне забезпечення для дата-центру та зберігання[9].

VMware - найкраща платформа для великих даних. Можна мінімізувати час простою за допомогою рівномірного, економічно ефективного захисту від відмови, можна легко організовувати, визначати пріоритети та використовувати ресурси дата-центру[10].

За допомогою віртуалізації сервера VMware, на фізичному сервері встановлюється гіпервізор, що дозволяє на одному фізичному сервері працювати декільком віртуальним машинам. Кожна віртуальна машина може запускати власну операційну ОС, що означає, що декілька ОС можуть працювати на одному фізичному сервері [17]. Усі віртуальні машини на одному фізичному сервері діляться ресурсами, такими як мережа та оперативна пам’ять.

Лінійка серверного програмного забезпечення VMware включає:

* Сервер VMware ESX: Це рішення корпоративного рівня, яке створено для забезпечення кращої функціональності порівняно з безкоштовним сервером VMware. VMware ESX інтегрований з VMware vCenter, що надає додаткові рішення для поліпшення керованості та послідовності впровадження сервера.

VMware ESX Server - це програмне забезпечення віртуальної інфраструктури для розділення, консолідації та управління системами як віртуальними машинами в критично важливих середовищах [19]. Вузли віртуальної інфраструктури сервера ESX перетворюють фізичні системи в пул логічних ресурсів обчислень, де операційні системи та додатки повністю ізольовані в межах декількох віртуальних машин, розташованих на фізичних серверах.

Системні ресурси динамічно розподіляються між віртуальними машинами в залежності від потреб та гарантій рівня обслуговування, забезпечуючи використання потужностей мейнфрейм-класу та контроль серверних ресурсів.

ESX Server працює безпосередньо на системному обладнанні, щоб забезпечити безпечну, єдину платформу для розгортання, управління та віддаленого керування кількома віртуальними машинами. Віртуалізація сервера ESX має три ключові особливості для забезпечення динамічного та гнучкого центру обробки даних: розділення, ізоляція та інкапсуляція.

* Сервер VMware ESXi: Цей сервер схожий на сервер ESX, за винятком того, що сервісна консоль замінена установкою BusyBox і для роботи в ній потрібне дуже мало дискового простору.
* Сервер VMware: безкоштовне програмне забезпечення, яке можна використовувати в існуючих операційних системах, таких як Linux або Microsoft Windows.

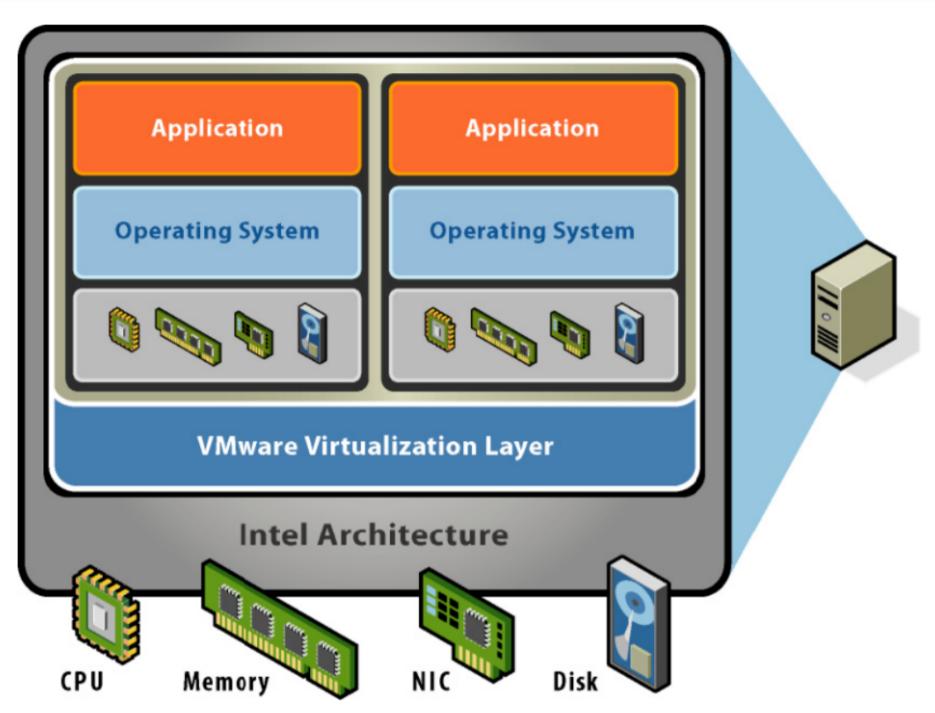
ESX Server використовує унікальну архітектуру гіпервізора (див. рис. 1.9.), яка вставляє невеликий і дуже надійний шар віртуалізації між апаратним забезпеченням сервера і віртуальними машинами. Такий підхід дає ESX Server повний контроль над ресурсами сервера, що виділяються для кожної віртуальної машини, і дозволяє уникнути накладних витрат, проблем із доступністю та витрат архітектури віртуалізації сервера, побудованої на хостній операційній системі.

Рис. 1.9. Архітектура віртуалізації

Цей рівень віртуалізації виконує всі необхідні перетворення для маскування фізичних апаратних ресурсів гостьової операційної системи.

Гостьова операційна система бачить послідовний набір віртуального обладнання, незалежно від того, який тип фізичної апаратури містить сервер. Це означає, наприклад, що незалежно від конкретного мережевого контролера, який використовує фізичний сервер, гостьова операційна система побачить лише мережевий контролер, визначений стандартизованим віртуальним обладнанням, встановленим на сервері ESX. Оскільки програми взаємодіють лише з пов'язаною гостевою операційною системою, а не з базовим віртуальним обладнанням, після встановлення сумісності операційної системи з віртуальним обладнанням сумісність програм не є проблемою.

Ця незалежність обладнання підвищує надійність завдяки невеликій кількості драйверів пристроїв, необхідних для віртуального обладнання та для кожної операційної системи віртуальної машини.

* 1. **Висновки до розділу**

Отже, було розглянуто поняття «віртуалізація», її історія, проаналізовано, як саме працює технологія віртуалізації, її переваги. У першому розділі представлено основні типи віртуалізації: віртуалізація даних, віртуалізація ПК і віртуалізація сервера. Також, більше детально описано віртуалізацію сервера і як саме це працює, її типи і обмеження. У виді рисунків, було представлено оптимальний та робочий варіант дата-центру, мета якого, полягає в тому, щоб дозволити індивідуальним користувачам забезпечити робочі навантаження та інші обчислювальні ресурси на вимогу без втручання ІТ.

Багато компаній інвестують у віртуалізацію сервера, незважаючи на обмеження. У міру розвитку технологій віртуалізації серверів потреба у величезних центрах обробки даних може знизитися. Споживання енергії та тепловіддача сервера також може зменшитися, що зробить використання сервера не тільки фінансово привабливим, але й екологічно чистою ініціативою. Оскільки мережі використовують сервери у повному обсязі, вони можуть побачити більші, ефективніші комп'ютерні мережі. Не буде перебільшенням сказати, що віртуальні сервери можуть призвести до повної революції в обчислювальній галузі.

Можливо, що більшість наших щоденних обчислювальних потреб будуть оброблятися через мережеве з'єднання, оскільки віртуальні сервери надають програми та сховище. В результаті ринок споживчих товарів може змінитися. Вам не знадобиться найшвидший ПК для запуску найновішого програмного забезпечення. Віддалена мережа віртуальних серверів може обробити обробку, і все, що вам знадобиться, - це простий мережевий термінал для доступу до нього.

# **РОЗДІЛ 2. РОЗРОБКА ПОЛІТИКИ БЕЗПЕКИ**

* 1. **План відновлення після катастроф**
     1. **Мета та сфера застосування цього плану**

Цей план був розроблений та написаний для використання у випадку катастрофи, що стосується підприємства[11]. Цей план побудований навколо команд, причому кожна команда має певні обов'язки.

Рішення про ініціювання процедур по відновленню аварій буде прийнято керівником групи з ліквідації наслідків катастроф або його заступником після оцінки ситуації після катастрофи чи кризи.

Якщо керівник групи з ліквідації наслідків стихійних лих вирішить розпочати процедури відновлення після аварій, то всі члени команд відновлення дотримуватимуться процедур, що містяться у цьому плані, до завершення відновлення.

Цей план містить всю інформацію, необхідну для відновлення працездатності служби у разі серйозних збоїв у роботі комп'ютерних сервісів.

Цей план повинен бути оновлений. Відповідальність ІТ-менеджера зобов'язана забезпечити проведення процедур для актуалізації цього плану[12]. Якщо під час використання плану ви виявите невірну інформацію, відсутню інформацію, або якщо у вас є проблеми в розумінні будь-якої частини цього плану, зверніться до ІТ-менеджера, щоб він був виправлений.

* + 1. **Цілі планування**

Катастрофа визначається як інцидент, який призводить до втрати комп'ютерної обробки на сайті підприємства, настільки, наскільки необхідно враховувати переміщення у режим очікування. Катастрофа може статися внаслідок ряду випадкових, шкідливих чи екологічних подій, таких як пожежа, повені, терористична атака, помилки людини та збої в роботі програмного забезпечення або обладнання.

Основна мета цього Плану по відновленню наслідків стихійних ситуацій - забезпечити продовження роботи визначених критично важливих для бізнесу систем у разі катастрофи.

Конкретними цілями плану є:

* Працювати у режимі очікування протягом 1-2 робочих днів після виклику режиму очікування.
* Відновити об'єкти підприємства в приміщеннях протягом максимального періоду роботи в режимі очікування.
* Звести до мінімуму перешкоди для діяльності підприємства.
  + 1. **Команди відновлення та їх обов'язки**

Цей розділ визначає функціональні обов'язки кожної команди з відновлення.

* + - 1. **Команда з управління катастрофами**

Команда з ліквідації наслідків катастроф відповідає за загальне керівництво операціями відновлення центру обробки даних. Вона визначає ступінь збитку, активує організацію відновлення та повідомляє керівників команд. ЇЇ головна роль полягає у моніторингу та спрямуванні зусиль на відновлення. Вона має подвійну структуру. до його складу якої входять керівники інших команд.

Керівник групи з ліквідації наслідків стихійних лих несе відповідальність за прийняття рішення про те, чи вимагає ситуація введення процедур відновлення наслідків аварій. Якщо він вирішить, що це так, то організація, визначена в цьому розділі, набирає чинності і на час катастрофи заміняє будь-які існуючі структури управління.

Команда з ліквідації наслідків катастроф несе відповідальність за:

* Прийняття рішень щодо відновлення комп’ютерного середовища з метою забезпечення визначеного рівня оперативного обслуговування користувачів.
* Управління всіма групами з відновлення та зв'язком з керівництвом підприємства, штаб-квартирою компанії та користувачами, за необхідністю.
* Збереження аудиту та контролю безпеки під час одужання після катастрофи.
* Контроль та облік надзвичайних витрат.

Обов’язки команди з ліквідації наслідків катастроф:

* Оцінка масштабу проблеми та потенційних наслідків.
* Повідомлення керівництву про стихійні лиха, процесу відновлення та проблеми.
* Ініціювання процедур відновлення після аварій.
* Координація операцій з відновлення.
* Моніторинг операцій з відновлення та забезпечення дотримання графіку.
* Координація та організація всіх необхідних бізнес-процесів, необхідних для забезпечення вихідного функціонування підприємства.
* Інформування про всі необхідні функції утримання групи.
* Документування операцій відновлення.
* Взаємодія з управлінням користувачів.
* Прискорення авторизації витрат іншими командами.
* Облік надзвичайних витрат.
* Проведення детального обліку збитків для допомоги у страхових вимогах.
* Забезпечення того, що перехід на резервні пристрої та остаточне відновлення операцій у центрі обробки даних перебувають під достатнім аудиторським контролем для забезпечення надійності та послідовності облікових записів.
* Моніторинг стандартів комп'ютерної безпеки.
* Забезпечити прийняття відповідних заходів щодо відновлення у строки, передбачених для обробки режиму надзвичайних ситуацій.
* Затвердження результатів аудиторських тестів на додатки, які обробляються в режимі очікування незабаром після їх виготовлення.
* Проведення детального аудиту критичних облікових файлів після першого циклу резервного копіювання було завершено.
* Проведення детального аудиту критичних облікових файлів після завершення першого циклу резервного копіювання.
* Повідомляти, що План відновлення після стихійних лих більше не діє при відновленні комп'ютерної обробки на первинному місці.
  + - 1. **Операційна команда**

Операційна команда відповідає за комп'ютерне середовище (комп'ютерний зал та інші життєво важливі місця комп'ютера) та за виконання завдань у цих середовищах. Ця команда несе відповідальність за відновлення комп'ютерної обробки та за виконання діяльності в комп'ютерній кімнаті.

Операційна група несе відповідальність за:

* Забезпечення того, щоб резервне обладнання відповідало графікам відновлення.
* Встановлення апаратного забезпечення комп'ютера та налаштування останньої версії ОС в режимі очікування.
* Отримання всіх відповідних історичних / поточних даних з місця зберігання та відновлення сучасного середовища прикладних систем.
* Забезпечення відповідного управління та укомплектованість резервного комп'ютерного обробного центру, управління даними, довідковою службою та контролем медіа / стрічки з метою задоволення визначеного рівня потреб користувачів.
* Підтримка функціонуючих версій всіх критичних додатків, необхідних для задоволення мінімальних експлуатаційних вимог.
* Виконання резервного копіювання на резервному сайті.
* Впорядкування нових локальних та глобальних засобів передачі даних та мережі комунікацій, яка пов'язує резервний пристрій з критично важливими користувачами.
* Встановлення мінімальної голосової мережі, яка дозволить ідентифікованим критично важливим користувачам телефонів підключатись до загальнодоступної мережі.

Обов’язки операційної команди:

* Надання технічної підтримки в режимі очікування.
* Співпраця з Мережевою групою для відновлення локальних і глобальних служб передачі даних для задоволення мінімальних вимог обробки.
* Отримання всіх необхідних резервних копій із зовнішнього сховища.
* Початок роботи в режимі очікування.
* Відновлення бібліотеки програмного забезпечення та бази даних до останнього резервного копіювання.
* Координація груп користувачів для відновлення будь-яких не відновлюваних даних.
* Забезпечення достатньої кількості персоналу для підтримки операцій у режимі очікування.
* Відновлення функцій довідки, управління даними та контроль медіаконтенту.
* Керування резервними пристроями для задоволення потреб користувачів.
* Встановлення графіку обробки та інформування контактів користувачів.
* Організація придбання та / або наявності необхідних комп'ютерних матеріалів.
* Забезпечення того, щоб вся документація щодо стандартів, операцій, забезпечення життєдіяльності записів, прикладних програм тощо зберігалася в безпечному середовищі та повторно збиралася в режимі очікування, якщо це необхідно.
* Оцінити ступінь пошкодження мережі передачі голосу та даних та обговорити альтернативні механізми щодо зв’язку з провайдерами телекомунікаційних послуг.
* Установити мережу на резервний об’єкт, щоб здійснити необхідні операції.
* Визначити пріоритети відновлення мережі в зонах користувача.
* Замовляти голосовий зв’язок / передачу даних та обладнання за потребою.
* Контроль за встановленням лінії та обладнання для нової мережі.
* Надання необхідної мережевої документації.
* Надання постійної підтримки мереж на резервному об’єкті.
* Відновити мережі на первинному сайті після завершення відновлення після аварій.
  + - 1. **Комунікаційна команда**

Команда з питань комунікацій відповідає за отримання директив комунікацій від Команди з ліквідації наслідків катастроф та передачу інформації під час стихійних лих та відновлення фази для працівників, постачальників та замовників.

Обов’язки комунікаційної команди:

* Взаємодія з Командою з ліквідації наслідків стихійних лих для отримання директив за повідомленнями для зв’язку.
* Інформування постачальників та покупців про можливі затримки.
* Інформування працівників про хід відновлення графіків.
* Переконання у відсутності помилок, які могли б пошкодити імідж компанії.
* Будь-які інші зв'язки з громадськістю.
  + - 1. **Команда безперервної діяльності**

Команда з питань безперервної діяльності несе відповідальність за підтримку основних бізнес-процесів під час катастрофи.

Обов’язки команди безперервної діяльності:

* Забезпечення мінімальних бізнес-процесів у компанії.
* Забезпечення та організація всіх обов'язкових вимог звітності перед органами влади.
* Забезпечення потоку інформації до клієнтів, постачальників.
  + 1. **Дії у випадку катастрофи**

Найбільш важливою і складною частина управління ресурсами є планування та організація необхідного персоналу під час виклику плану.

Персонал повинен бути добре відпрацьований, ознайомлений з Планом відновлення стихійних лих та бути впевненим у своїх завданнях.

Першим пріоритетом у ситуації стихійного лиха є забезпечення безпечної евакуації всього персоналу. У разі великих фізичних порушень необхідно дотримуватися стандартних аварійних процедур. Це означає негайно активізувати стандартні процедури тривоги для цієї частини будівлі, щоб відділи охорони здоров'я, безпеки та охорони і аварійні органи будуть правильно попереджені. У разі необхідності евакуація приміщень за встановленими процедурами евакуації та збирання на вулиці у визначеному місці, якщо це безпечно зробити.

Команда з ліквідації наслідків катастроф оцінює характер та масштаби проблеми. Якщо це безпечно, оперативна група вимикає все обладнання в комп'ютерній залі, включаючи кондиціонери. Охорона будівлі (орендодавець) попереджає керівника групи з ліквідації наслідків катастроф. Команда з ліквідації наслідків стихійних лих дає первинну оцінку керівнику групи з ліквідації наслідків стихійних лих, який повинен знати ступінь пошкодження будівель та обладнання та стан персоналу. Також повідомте про те, які дії були вжиті.

Керівник групи з ліквідації наслідків катастроф вирішує, чи активувати План відновлення після катастроф та який сценарій відновлення буде дотримуватися.

Потім команди з відновлення виконують визначені заходи з відновлення та виконують обов'язки кожної команди, як визначено в цьому Плані відновлення після катастроф.

* + - 1. **Сценарій відновлення**

У розділі описані різні сценарії відновлення, які можна реалізувати, залежно від характеру катастрофи та ступеня шкоди. Керівник групи з ліквідації наслідків стихійних лих вирішує, який сценарій відновлення використовувати, коли він активує План відновлення.

У сценарії «Незначні ушкодження» лише частина середовища обчислювальної машини не працює, але лінії зв'язку та мережа все ще працюють. Метою процесу відновлення в цьому випадку є переміщення програм із недоступних систем до резервного інструменту.

У цьому сценарії будівля все ще доступна, і користувачі можуть використовувати звичайні офісні приміщення, щоб дочекатися перезавантаження комп'ютерної обробки. План дій дивитись у Додатку А.

У сценарії «Значні ушкодження» все обчислювальне середовище комп'ютерної обробки (або більшість його) виходить з ладу. Лінії зв'язку та мережа не працюють. Метою процесу відновлення в цьому сценарії є переміщення всіх визначених програм у режим резерву.

Цей сценарій вимагає повної процедури відновлення, як це зафіксовано в цьому Плані відновлення після катастроф. План дій дивитись у Додатку Б.

* 1. **Загальна політика ІТ безпеки на підприємстві**

Загальна Політика ІТ Безпеки встановлює мінімальні обов'язкові для виконання всіма співробітниками, інструкції щодо ІТ безпеки в компанії[13].

Політика описує вимоги до використання корпоративних ІТ ресурсів з метою захисту цих ресурсів, а також інформації, яка обробляється та зберігається в інформаційних системах компанії від несанкціонованого доступу, зміни або знищення.

* + 1. **Фізичний захист**

Фізичний захист приміщення компанії забезпечується такими засобами;

* Відеоспостереження;
* контроль доступу в приміщення компанії;
* служба охорони;
* контроль входів та виходів.

Для внутрішнього контролю пересування сторонніх осіб та співробітників компанії, в приміщеннях встановлені камери відеоспостереження:

* у коридорах;
* архіві відділу адміністрування договорів;
* комутаційній;
* у відділі продажів лізингових послуг.

Процес здійснення відеозаписів контролюється системою відеоспостереження, що знаходиться в комутаційній.

Записи зберігаються на окремому сервері продовж 6 місяців. За відеоспостереження відповідають співробітники ІТ відділу.

Контроль доступу сторонніх осіб забезпечується за допомогою встановлених на основних входах до приміщення компанії (на 2-му та 3-му поверсі) відео-домофонів.

Кнопки для відкриття магнітного замку знаходяться на Рецепції, відповідно, 2-го та 3-го поверху. Крім того, на вхідних дверях встановленні доводчики, за допомогою яких двері після відвідувачів зачиняються на магнітний замок автоматично.

Служба охорони забезпечує безпеку компінії на рівні охорони приміщення під сигналізацією та швидкого реагування при натисканні кнопки тривожного виклику.

Кнопка тривожного виклику призначена для усунення непередбачуваних ситуацій, вторгнення третіх осіб, що поводяться неадекватно або небезпечно для співробітників та у випадку неможливості самостійного усунення співробітниками небажаних осіб.

В компанії знаходиться 2 кнопки тривожного виклику, одна - у ІТ відділі, інша - на Рецепції.

Сигналізація. Для управління охороною приміщення, офіс розділений на 4 зони:

* 1 зона - 2 поверх;
* 2 зона - коридори та сходи між 2 та 3 поверхом;
* 3 зона - 3 поверх до ІТ відділу;
* 4 зона - пожежний вихід.

Пульт управління сигналізацією 1 та 2 зони знаходиться біля виходу у внутрішній двір будівлі 3-ї зони - на 3 поверсі, 4-ї зони - біля пожежного виходу.

4 зона постійно знаходиться під сигналізацією, а пожежний вихід завжди закритий на ключ.

В неробочий час, все приміщення компанії знаходиться під сигналізацією. Крім того, центральний вхід до офісу (через 3 поверх) у вихідні та неробочі дні охороняється підприємством. Другий вхід блокується.

В компанії визначені наступні точки контролю доступу

* + пожежний вихід (2 поверх);
  + двері входу з 2 на 3 поверх;
  + відділ адміністрування договорів;
  + бухгалтерія;
  + відділ персоналу;
  + відділ ІТ;
  + комутаційна;
  + кабінети директорів.

На вказаних точках контролю доступу встановлені магнітні замки. Для відкриття замків використовується магнітна картка.

Управляння точками контролю здійснюється на апаратному рівні за допомогою програмного забезпечення Fort Net. Відповідне устаткування знаходиться в комутаційній. В разі відключення електропостачання, до кожного зчитувача з магнітних замків встановлені батареї, що забезпечують працездатність замків продовж 24 годин.

Відповідно до рівню доступу, співробітникам під підпис в Журналі реєстрації перепусток видаються електронні магнітні картки (перепустка).

За допомогою програми Fort Net відбувається:

* + програмування/ перепрограмування на перепустці рівня доступу
  + блокування перепустки, в разі втрати
  + контроль часу та проходження точок доступу.

Рівні доступу:

1. загальний рівень доступу «Всюди» - доступ для всіх співробітників, надає доступ в загальні приміщення офісу (відділів, де встановлені окремі магнітні замки);
2. рівень доступу «Повний» - рівень доступу, який надає доступ у всі точки контролю (мають співробітники ІТ відділу та прибиральниці (крім комутаційної));
3. окремі рівні доступу (напр., відділ персоналу + «всюди», бухгалтерія + «всюди»).
   * 1. **Інформаційна безпека**

Жоден файл не може бути скопійований співробітником на робочу станцію із зовнішніх носіїв без перевірки на наявність вірусів.

На всіх серверах та робочих станціях має бути встановлене відповідне анти-вірусне програмне забезпечення.

Комутаційна кімната повинна бути весь час закрита. Доступ до комутаційної обмежений і дозволений лише співробітникам ІТ відділу для виконання своїх службових обов'язків Відповідальність за збереження наданого ІТ обладнання несе співробітник, в користуванні якого воно знаходиться. Захист даних компанії від втрати забезпечується засобами резервного копіювання.

В компанії впроваджена система контролю за паролями доступу на робочі станції та основне програмне забезпечення для підтримки бізнесу. Встановлені наступні мінімальні вимоги для паролів:

* + пароль має буди не коротше ніж 8 символів;
  + складатися з цифр (0-9), літер (а-г) та великих літер (А-Z) або символів (@#$%&\* тощо);
  + повинен бути відмінним від раніше використовуваних паролів;
  + повинен бути згенерований користувачем;
  + не повинен складатися з прізвища чи ім’я користувача або складатися із іншомовних слів із словника.

Доменом контролюється зміна паролів кожні 40 днів. Користувачам забороняється розголошувати свої паролі доступу третім особам, іншим співробітникам компанії, а також записувати паролі та зберігати їх на відкритому для огляду місці (наприклад, на робочому столі, на моніторах, під клавіатурою тощо).

Системні паролі для доступу на сервери компанії знаходяться у відповідальних співробітників ІТ відділу та мають надійно зберігатися від третіх осіб.

Робоча станція має бути заблокована, якщо працівник виходить з свого кабінету. Якщо режим очікування триває більше 5 хв, робоча станція буде блокуватись автоматично. Всі робочі станції працівників повинні бути виключені в неробочий час.

Робочі станції, що знаходяться у місцях, доступних громадськості (наприклад, робочі кабінети, куди можуть заходити клієнти компанії), повинні бути розташовані таким чином, щоб інформація на моніторі не була доступна третім особам.

В разі необхідності передачі даних компанії стороннім організаціям, необхідно використовувати нові носії (СD-диски) або відформатовані USB-накопичувачі.

Співробітники компанії несуть відповідальність за контроль потоків інформації компанії.

Необхідно забезпечити наступне:

* заборонено залишати документи в принтері, сканері, котрі чи факсі. Документи, що містять конфіденційну інформацію і які роздруковуються на принтері/факсі. скануються на сканерах, що. знаходиться поза межами робочого кабінету (коридори, інші кабінети) були відразу вилучені з принтера/сканера/факсу користувачем, що здійснював друк/сканування.
* заборонено зберігати документи на робочому столі у відкритому вигляді під час робочого дня у присутності сторонніх осіб та по закінченню робочого дня;
* неякісні копії повинні бути одразу знищені;
* документи, що містять конфіденційну інформацію і підлягають знищенню, забороняється викидати у смітник загального призначення. Такі документи мають бути зібрані відповідним користувачем конфіденційної інформації та знищенні у шредері;
* уся електронна інформація та документи повинні зберігатись на сервері:
  + документи на стадії розробки - Диск Z;
  + документи для спільного використання - Диск K;
  + завершені документи та документи для внутрішнього використання в відділі - Диск M;
  + офіційні завершені документи, до яких повинен бути доступ у всіх працівників - в бібліотеці Lotus Notes.

Рекомендується надсилати електронні повідомлення з посиланням на документ, а не сам документ (тільки якщо у всіх адресатів є доступ до відповідної папки).

Help Desk не несе відповідальності за збереження документів та іншої інформації, що зберігається локально на робочій станції.

Працівникам заборонено інсталювати та деінсталювати будь-які програми на робочих станціях. Про всі проблеми з робочими станціями, іншим офісним обладнанням та мережею потрібно повідомляти через Систему Управління Запитами.

Якщо проблема з робочою станцією вимагає більше ніж 30 хв для вирішення, Help Desk замінює неробочу робочу станцію запасною.

Співробітникам компанії без обмежень дозволяється користуватися мережею Інтернет з професійною метою.

Також, дозволяється користування мережею Інтернет в особистих цілях, але тільки у вільний від виконання службових завдань час. Несприятливо витрачати ресурси, зокрема, робочий час на завантаження та здійснення пошуку в мережі Інтернет без змісту та мети. Відвідування веб-ресурсів розважального характеру заборонено.

Список заборонених веб-ресурсів регулярно поновлюється ІТ відділом або за запитом Керівництва.

Користувачам забороняється завантажувати із мережі Інтернет файли, що не пов'язані із їх роботою та такі що перевищують розмір 20 Mb. В разі професійної необхідності, файл, що перевищує вказаний розмір, на запит користувача може бути завантажений відповідальними співробітниками ІТ відділу.

* 1. **Правила захисту баз даних**

Метою цих Правил є визначення засобiв захисту та контролю iнформацiї, що зберiгається в базах даних бiзнес-додаткiв компанiї[14]. Правила створенi для використання адмiнiстраторами баз даних та розробникiв.

Правила обов'язковi для виконання всiма спiвробiтниками компанiї. Контроль за виконання Правил покладається на керівників відділів.

Власником бізнес-процесу щодо органiзацii методологiї захисту баз даних визначається Відділ інформаційних технологій та методологічної підтримки. Власником (Розробником) Правил визначається Відділ інформаційних технологій та методологічної підтримки.

База даних - це програмне забезпечення, призначене для управління даними та дає можливість зберігати, здійснювати пошук та змінювати ці данні.

Безпека баз даних - захист баз даних від несанкціонованого доступу та модифікації.

Бізнес-додаток - програмне забезпечення, що використовується для забезпечення бізнес процесів компанії. Для цілей цього Порядку, бізнес-додатками визначаються Lease Manager/lnsurance Manager, 1С .

Бізнес-процес - являє собою набір пов'язаних між собою та структурованих ді й чи задач, що створюють відповідний продукт чи послугу для конкретного клієнта (внутрішнього чи зовнішнього).

Загроза - будь-яка подія, що може скомпрометувати конфіденційні дані, їх цілісність та/або доступність.

* + 1. **Порядок правил**
       1. **Визначення загроз**

В контексті безпеки баз даних, Правилами визначаються відповідні загрози та необхідні контролі для їх попередження.

Загроза складається з комбінації наступних елементів:

* роль учасника, який є джерелом загрози;
* інформація , що має бути захищена від загрози;
* метод несанкціонованого доступу;
* безпосередньо несанкціоновані дії.

Особи, що залучені в операції з базами даних, їх ролі та учасники, що можуть стати джереломзагрози мають бути визначені.

Для цілей компанії визначені наступні учасники:

1. Зовнішній користувач - кінцевий користувач, який не належить до компанії.
2. Внутрішній користувач - кінцевий користувач, який належить до компанії.
3. Системний розробник - розробляє веб додатки та бізнес-додатки; створює та налаштовує веб-сервери та сервери бізнес-додатків (в т.ч., операційну систему та програмне забезпечення проміжного рівня); створює та налаштовує мережу для серверу баз даних; створює та налаштовує сервер баз даних (в т.ч., ОС та програмне забезпечення проміжного рівня ).
4. Системний адміністратор - управляє та підтримує веб-сервери та сервери бізнес-додатків (в т.ч. ОС та програмне забезпечення проміжного рівня); управляє сервером баз даних (в т.ч., ОС та програмне забезпечення проміжного рівня); управляє мережевим обладнанням .
5. Адміністратор баз даних - створює та налаштовує бази даних; адмініструє бази даних бізнес-додатків .
6. Оператор бази даних - користувач бази даних, що вносить бізнес-дані в базу даних.

В контексті даної Політики, інформація, що має бути захищена - це інформація, що знаходиться на сервері баз даних.

До інформації, що зберігається на сервері баз даних відноситься :

1. Інформація , що відноситься до системи управління базою даних :
   * інформація щодо конфігурації бази даних (наприклад, логіни та паролі користувачів);
   * журнали баз даних (журнал доступів в базу даних).
2. Інформація , що не відноситься до системи управління базою даних:
   * бізнес-дані;
   * бізнес-додатки.
3. Інформація щодо адміністрування ОС:
   * інформація щодо конфігурації ОС;
   * журнали ОС (журнал трасування, журнал попереджень).
4. Системна інформація :
   * файли , що пов'язані з базою даних (журнали, резервні копії).

Метод - спосіб, у який учасником здійснюється несанкціонована діяльність з інформацією. Визначивши методи, є можливість створити ефективні контролі для зниження вірогідності загрози.

Нижче наведений перелік потенційних методів:

* несанкціонований перехват інформації, шляхом прослуховування каналів зв'язку;
* парольні атаки шляхом підбору паролів по словнику;
* крадіжка логінів та паролів шляхом промислового шпигунства;
* несанкціонований доступ у бази даних завдяки помилкам в налаштуванні бази даних;
* несанкціонований доступ у бази даних завдяки уразливості бази даних;
* несанкціонований доступ у бази даних через модифікування в файли бази даних;
* неправомірний доступ до логінів та паролів, використовуючи службову інформацію баз даних;
* несанкціонований доступ у бази даних через створення несанкціонованих облікових записів адміністраторів баз даних або операторів баз даних;
* створення засобів обходу системи безпеки бази даних;
* несанкціоноване видалення інформації з баз даних через несанкціоновану маршрутизацію;
* несанкціонований доступ у бази даних через зміну управлінської інформації;
* запити SQL з метою виведення з ладу служби.

Несанкціонованими діями визначаються неправомірна діяльність учасника щодо інформації.

Зазначені методи відповідають методам , за допомогою яких здійснюються несанкціоновані дії.

Нижче наведений перелік прогнозованих несанкціонованих дій:

* несанкціоноване використання інформації (шляхом видалення);
* несанкціонована модифікація або знищення інформації;
* виведення з ладу служби (шляхом виснаження ресурсів);
* несанкціонована модифікація або знищення інформації в базі даних;
* несанкціонований доступ до інформації у базі даних.
  + - 1. **Заходи попередження загроз**

З метою ефективного попередження несанкціонованого доступу та мінімізації наслідків від несанкціонованого доступу, визначаються наступні заходи:

* Початкова конфігурація

Бази даних, що не оновлювалися, або такі, що використовуються і з активованим непотрібним функціоналом створюють численні загрози та уразливість системи. Крім того, використання портів за замовченням або забороняючих паролів для мережевого доступу збільшує вірогідність неавторизованного доступу.

1. Інсталяція

* використання останньої версії. Для того, щоб останні заходи безпеки були доступні, необхідно впровадити наступні контролі:
  + - обов'язково встановити останні оновлення для системи безпеки (security patches);
    - рекомендується визначити та використовувати останню версію бази даних .
* встановлювати тільки мінімальний функціонал. Для попередження неавторизованого використання, а також марнотратне використання ресурсів, необхідно впровадити наступні контролі:
  + - обов'язково вибирати та встановлювати тільки необхідний функціонал;
    - непотрібний, але встановлений за замовченням функціонал обов'язково потрібно видалити або деактивувати.
* зміна налаштувань портів. Для попередження неавторизованого використання, необхідно впровадити наступні контролі:
  + - обов'язково змінити розповсюджені номери портів або такі, що присвоюються за замовченням під час інсталяції.
* обмеження мережевого доступу. Для попередження неавторизованого використання мережевого функціоналу, необхідно впровадити наступні контролі :
  + - обов'язково обмежити доступ до мережевого доступу до баз даних.

1. Авторизація

Діюча система авторизації бази даних використовує парольну авторизацію під час входу в систему. Для попередження доступу неавторизованих користувачів, що ви користовують авторизовані облікові записи для просочення інформації або зміни даних, зміни інформації щодо облікового запису необхідно впровадити жорсткий контроль. Крім того, оскільки облікові записи адміністраторів баз даних дають можливість користувачам здійснювати будь-які дії в базі даних. Інформація щодо таких облікових записів має контролюватися ще жорсткіше. ніж щодо звичайних користувачів. Нижче запропоновані контролі для підтримки високого рівня безпеки.

* 1. управління обліковими записами:
* створення необхідних облікових записів. Для попередження маскування неавторизованого використання інформації щодо облікових записів, необхідно впровадити наступні контролі:
  + - створювати обов'язково тільки необхідні облікові записи ;
    - обов'язково визначити права доступу для кожного облікового запису;
    - обов'язково створити окремий обліковий запис для користувача та адміністратора із відповідними правами доступу.
* видалення зайвих облікових записів. Для попередження маскування неавторизованого використання інформації щодо облікових записів, необхідно впровадити наступні контролі:
  + - обов'язково видалити облікові записи, які не використовуються (наприклад , співробітників, які більше не працюють в компанії);
    - обов'язково видалити облікові записи , створені за замовченням, що не використовуються .
* блокування невикористовуваних облікових записів користувачів. Для попередження маскування неавторизованого використання інформації щодо облікових записів, необхідно впровадити наступні контролі:
  + - обов'язково блокувати облікові записи користувачів, які не використовуються визначений період часу;
    - обов'язково підтвердити як часто (кількість разів) обліковий запис останнім часом використовувався.
* блокування облікових записів через невдалу спробу входу в систему. Для попередження маскування неавторизованого використання інформації щодо облікових записів, необхідно впровадити наступні контролі:
  + - рекомендується визначити кількість спроб входу в систему, після яких обліковий запис буде заблокований.
* управління обліковим записом адміністратора баз даних. Для мінімізації операційних помилок та неавторизованого користування адміністратором баз даних, необхідно впровадити наступні контролі:
  + - обов'язково обліковий запис адміністратора баз даних має бути наданий тільки необхідній особі;
    - обов'язково обліковий запис адміністратора баз даних не повинні використовувати для діяльності, що не потребує адміністративних прав доступу;
    - обов'язково для кожного адміністратора має бути створений окремий обліковий запис адміністратора баз даних.
* логін/пароль для ОС та середовища для розробки. Для попередження неавторизованого використання облікових записів розробників, необхідно впровадити наступні контролі:
  + - обов'язково, навіть якщо однаковий логін використовується для входу в операційну систему та середовища для розробки, необхідно використовувати різні паролі для кожного облікового запису;
    - рекомендується використовувати різні логіни та паролі для входу в о ОС та середовища для розробки.
* тимчасові облікові записи. Для попередження неавторизованого користування тимчасовими користувачами, необхідно впровадити наступні контролі:
  + - обов'язково або надавати загальні/анонімні логіни із змінними паролями, або надавати тимчасові облікові записи .
  1. управління паролями:
* складність паролів. Для попередження того, що будуть такі паролі, до яких легко здогадатися необхідно впровадити наступні контролі:
  + - обов'язково не давати користувачам можливості встановлювати паролі до яких легко здогадатися.
* періодична зміна паролів. Навіть в ситуації, коли пароль розсекречений та для попередження використання паролю для неавторизованого доступу, необхідно впровадити наступні контролі:
  + - обов'язково періодично змінювати пароль адміністратора баз даних;
    - обов'язково завжди змінювати початковий пароль;
    - рекомендується забезпечити неможливість повторного використання паролів;
    - рекомендується періодично змінювати паролі користувачів.
* встановлення закінчення терміну дії паролю. Для забезпечення того, що користувачі та адміністратори періодично змінюють паролі, необхідно

впровадити наступні контролі:

* обов'язково встановити дату закінчення терміну дії паролю адміністраторів баз даних ;
* рекомендується встановити дату закінчення терміну дії паролів користувачів.

1. Контроль доступу

Навіть якщо сервер баз даних захищений від зовнішніх загроз, якщо не встановлені ефективні контролі доступу, сервер стає уразливим до внутрішніх загроз (неавторизований доступ через викрадення інформації щодо авторизованого облікового запису).

* визначення прав доступу. Для відповідного визначення прав доступу, необхідно впровадити наступні контролі:
  + - обов'язково класифікувати облікові записи відповідно до їх цілей та користування;
    - обов'язково визначити права доступу для кожної групи облікових записів;
    - обов'язково розподілити облікові записи відповідно до прав доступу;
    - обов'язково для кожного з цих розподілених облікових записів визначити мінімальний набір даних, необхідних для доступу в базу даних та мінімальний набір прав (читати, писати, створювати, видаляти), які необхідно становити в вимогах доступу в базу даних.
* встановлення прав доступу. Для обмеження небажаного доступу до даних, необхідно впровадити наступні контролі :
  + - обов'язково надавати мінімум прав доступу для кожного облікового запису , визначеного в вимогах доступу в базу даних;
    - обов'язково права адміністратора можуть бути надані тільки обмеженій кількості облікових записів.
* визначення вимог до прав доступу в бази даних:
  + - обов'язково - неможна створювати користувацькі облікові записи, що дають необмежений доступ усім користувачам;
    - обов'язково - неможна створювати користувацькі облікові записи, що дозволяють звичайним користувачам мати можливість надавати права доступу звичайним користувачам;
    - рекомендується блокувати та деактивувати прямий доступ власнику облікового запису, що відрізняється від права створення, видалення та підтримки об'єктів.
* перегляд облікових записів користувачів. Для того. щоб зміни до вимог до прав доступ у в бази даних були застосовані до налаштувань прав

доступу , необхідно впровадити наступні контролі:

* + - обов'язково здійснювати періодичні перевірки, щоб пересвідчитись , що непотрібні права доступу не надані;
    - обов'язково при внесенні змін до системи перевірити , чи не встановились непотрібні права доступу;
    - обов'язково при виявлені встановлених непотрібних прав доступу, внести необхідні зміни.

1. Шифрування

Частіше інформація може бути скомпрометована усередині компанії (наприклад, крадіжка співробітниками або втрата ноутбуку, який використовувався за межами офісу), ніж зовнішніми атаками. Тому, важлива інформація має бути захищена від компрометації.

Нижче наведені засоби шифрування, призначені для захисту баз даних від зовнішніх та внутрішніх загроз.

* передача за шифрованих даних. Для захисту каналів передачі даних між серверами баз даних та клієнтами від прослуховування, необхідно впровадити наступні контролі:
  + - рекомендується шифрувати дані, за допомогою спеціального програмного забезпечення.
* шифрування даних:
* засоби шифрування даних баз даних. Для того, щоб захистити дані, що зберігаються в базах даних від крадіжки. необхідно впровадити наступні контролі:
  + - рекомендується шифрувати дані за допомогою спеціального програмного забезпечення.
* шифрування фізичних файлів. Для того, щоб захистити фізичні дані (наприклад. паперові) від крадіжки, необхідно впровадити наступні контролі:
  + - рекомендується шифрувати дані за допомогою спеціального програмного забезпечення.
* шифрування резервних копій. Для того, щоб захистити резервні копії даних від крадіжки, необхідно впровадити наступні контролі:
  + - рекомендується шифрувати дані за допомогою спеціального програмного забезпечення.
* шифрування процедур. Для того, щоб захистити процедури від крадіжки, необхідно впровадити наступні контролі:
  + - рекомендується шифрувати процедури за допомогою спеціального програмного забезпечення.
* управління ключами шифрування. Для того , щоб захистити за шифровані дані від неавторизованого користування, необхідно впровадити наступні контролі:
  + - рекомендується впровадити систему управління ключами шифрування.

1. Обмеження користуванням знімними носіями

Для попередження просочування інформації, шляхом підключення до серверів баз даних знімних носіїв, таких як дисковод, СD-R/RW, DVD-R/RW/ROM, флеш-накопичувачів та подібне, користування такими приладами має мути обмеженим. Також , підключення принтерів та їх використання має бути належним чином обмежене.

* обмеження під'єднання знімних носіїв до серверу баз даних:
* обмеження під'єднання знімних носіїв. Щоб пересвідчитись, що знімні носії не під'єднані до серверу баз даних, необхідно впровадити наступні контролі:
* обов'язково вилучити всі непотрібні знімні носії;
* обов'язково від'єднати всі непотрібні принтери.
  + обмеження користуванням знімними носіями. Для забезпечення того, що конфіденційна інформація не переноситься на знімні носії, необхідно впровадити наступні контролі:
* обов'язково доступ до знімних носіїв необхідно контролювати;
* обов'язково під'єднання до принтерів має контролюватись;
* рекомендується контролювати під'єднання до знімних носіїв.
  + логування під’єднань до знімних носіїв. Для створення засобу стримання просочування інформації та отримати докази на випадок просочування інформації, необхідно впровадити наступні контролі:
* рекомендується логувати під'єднання до знімних носіїв;
* рекомендується фіксувати доступ до знімних носіїв;
* рекомендується логувати під 'єднання користувачів до знімних носіїв.
* обмеження термінального доступу до серверів баз даних. Для попередження викрадення інформації через термінальний доступ, необхідно впровадити наступні контролі:
  + обов'язково доступ до знімних носіїв (через термінали) має контролюватися;
  + обов'язково необхідно посилити термінальне під'єднання до сервер і в баз даних до того, як буде наданий доступ;
  + обов'язково ПК користувачів мають бути авторизовані до того, як буде наданий доступ;
  + обов'язково програмне забезпечення встановлене на ПК та використання має контролюватися;
  + обов'язково доступ до принтерів (з ПК) має контролюватися.

1. Інше

Безпека баз даних може бути посилена шляхом впровадження серверного доступу та контролю ресурсів. Нижче наведені заходи для зниження вірогідності неавторизованого доступу до серверу баз даних та крадіжки значного масиву даних.

* обмеження термінального доступу (через ІР-адресу). Для обмеження доступу в бази даних, необхідно впровадити наступні контролі:
  + обов'язково використовувати Firewall для захисту серверів баз даних від неавторизованого термінального доступу;
  + обов'язково обмежити термінальний доступ до серверів баз даних, що авторизований; підключатися до серверу або терміналу, що належать до однакового сегменту мережі (наприклад, ІР-адреса фільтрує використання роутерів, використання налаштування бази даних, що обмежує мережевий доступ).
* обмеження доступу до ресурсів на кожного користувача. Для попередження втручання в систему та крадіжки значного масиву даних необхідно впровадити наступні контролі:
  + - рекомендується уникати перевантаження процесору звичайними користувачами.
* тестування уразливості:
  + - * тестування уразливості до виробничого етапу. Для того, щоб пересвідчитись, що усі заходи безпеки були впроваджені відповідно до вимог політики безпеки баз даних, необхідно впровадити наступні контролі:
    - обов'язково здійснювати тестування уразливості до виробничого етапу.
      * періодичне сканування уразливості. Для того, щоб підтримувати ефективність заходів безпеки, необхідно впровадити наступні контролі:
    - обов'язково періодично здійснювати сканування уразливості, приймаючи до уваги останні загрози.
* захист від лазівок:
  + - * посилення серверів. З метою попередження неавторизованого доступу та пошкодження серверів баз даних, необхідно впровадити наступні контролі:
    - обов’язково застосувати безпечні налаштування ОС та мережі на сервері баз даних.
      * захист від таємних каналів просочування інформації. З метою попередження неавторизованого доступу в систему через таємні канали. Необхідно впровадити наступні контролі:
    - обов'язково призначити відповідального за створення та зміну вихідного програмного коду та його перевірку/тестування для того, щоб пересвідчитись , що програмний код не був модифікований .
* обмеження каналу доступу до файлів:
  + - * обмеження доступу в файли конфігурації баз даних. З метою попередження пошкодження баз даних, необхідно впровадити наступні контролі:
    - обов'язково тільки адміністратори можуть мати доступ до файлів конфігурації баз даних;
    - обов'язково тільки адміністратори можуть мати доступ до скриптів;
    - обов'язково необхідно періодично переглядати права доступу до файлів конфігурації баз даних.
      * обмеження каналів доступу. Для попередження операційних помилок та неавторизованого користування базами даних необхідно впровадити наступні контролі:
* обов'язково програмне забезпечення, що використовується для доступу в бази даних можуть бути встановлені тільки на робочі станції тих користувачів, які мають авторизований доступ до баз даних;
* рекомендується обмежити мережеві канали доступу, які можуть бути використані для доступу в бази даних/сервер.
  + - 1. **Дослідження системи безпеки баз даних**

Файл реєстрації входів в систему (логи), що містить відповідну інформацію, має створюватись, щоб забезпечити, що вони наявні для моніторингу та використання в якості доказів для швидкого вирішення проблем.

1. Управління логами

Якщо в базі даних не створюються логи, розслідування та відслідковування щодо просочування інформації, а також, неавторизованого доступу, може виявитися дуже складним.

* Логування:
  + - * отримання журналу входу в систему. З метою відслідковування логінів, необхідно впровадити наступні контролі:
* обов'язково створювати журнал входу в систему;
  + - * отримання інформації щодо логів доступу в базу даних. Для здійснення моніторингу доступу до персональної, конфіденційної та іншої інформації, необхідно впровадити наступні контролі:
* обов'язково створювати логи, пов'язані із доступом/внесенням змін до персональної, конфіденційної, управлінської та іншої важливої інформації;
  + - * отримання логів щодо внесення змін до бази даних. Для здійснення моніторингу внесення змін до об'єктів бази даних, необхідно впровадити наступні контролі:
* обов'язково створювати журнали перевірки безпеки об'єктів баз даних (облікових записів баз даних, таблиць тощо) створення та внесення змін .
* Захист логів:
  + - * відновлення логів. Для того , щоб логи могли бути відновлені, коли це необхідно , потрібно впровадити наступні контролі:
* обов'язково копіювати логи на зовн ішні носії (стрічки , диски , зовнішні бази даних тощо);
* обов'язково зберігати зовнішні носії у місці, що зачиняється;
* обов'язково застосувати контроль доступу до логів;
  + - * попередження внесення змін до логів:
* обов'язково попереджувати неавторизований доступ до логів (використовувати цифровий підпис із зазначенням часу, зберігати декілька копій логів, зберігати логи на носіях, з яких можливо тільки читати інформацію)
  + - * шифрування логів:
* рекомендується застосування шифрування логів.

1. Визначення неавторизованого доступу

Навіть якщо база даних захищена від неавторизованого доступу, все одно існує вірогідність здійснення таких спроб. Тому, необхідно мати механізм за допомогою якого можна виявити такі спроби.

* механізм визначення. Для визначення неавторизованого доступу , потрібно впровадити наступні контролі:
* обов' язково впровадити механізм повідомлення про спроби неавторизованого доступу (наприклад, електронною поштою).
* перевірка часу доступу:
  + - * визначення доступу до управлінської інформації бази даних. Для визначення підозрілого доступу до управлінської інформації бази даних під час та після робочого часу, необхідно впровадити наступні контролі:
* обов' язково перевіряти та визначати логи входу в базу даних в неробочий час;
* перевірка іншого неавторизованого доступу. Для визначення інших способів неавторизованого доступу, необхідно впровадити наступні контролі:
* рекомендується визначити атаки через підбір по словнику, шляхом перевірки , що кількість невдалих спроб в систему менше ніж визначено для даного періоду часу;
* рекомендується здійснювати моніторинг логів запитів в SQL;
* рекомендується здійснювати моніторинг логів створення та модифікації об'єктів баз даних;
* припинення неавторизованого доступу. Для мінімізації збитків від виявленого неавторизованого доступу, необхідно впровадити наступні контролі:
* рекомендується впровадити механізм (програмне забезпечення) для припинення та переривання неавторизованого доступу.

1. Аналіз логів

Для того, щоб визначити, що відповідна подія є порушенням безпеки, необхідно аналізувати логи:

* механізм аналізу логів:
* обов'язково впровадити механізм аналізу логів (встановлення програмного забезпечення для аналізу логів);
* періодичний аналіз логів.

Для визначення лагів, необхідно впровадити наступні контролі:

* обов'язково аналізувати сесії.

Для визначення доступів в базу даних. необхідно впровадити наступні контролі:

* обов'язково аналізувати інформацію бази даних SQL.
  1. **Політика резервного копіювання**

Дана політика визначає порядок резервного копіювання даних, які підлягають обов'язковому копіюванню, згідно з внутрішніми вимогами компанії.

Резервна копія (backup) - зберігання файлів на магнітних стрічках або інших офлайнових носіях з метою запобігання втрати даних у разі збою роботи обладнання.

Політика створена з метою захисту даних в компанії, щоб забезпечити їх збереження і можливість відновлення в разі збою обладнання, навмисного і ненавмисного знищення даних, або аварії. Резервне копіювання дозволяє завжди отримувати доступ до інформації, і забезпечує безперервність бізнесу.

Політика відноситься до всього обладнання і даних, що належить компанії або перебувають в її користуванні.

Резервному копіюванню підлягають дані, які зберігаються на наступних серверах компанії:

* Server1 (зберігаються робочі папки і документи користувачів);
* MailServer (Lotus Notes);
* FileServer (документи);
* DBServer (база SQL);
* 1cserver (база 1С);
* DC\_server (додатковий домен-контролер, папки з відсканованими документами).

Сервера, на яких зберігається важлива для компанії інформація, знаходяться в віртуальному середовищі VMware. Резервне копіювання серверів здійснюється VMware протягом дня з частотою, визначеною для кожної групи в залежності від пріоритетності:

* Сервера першого приорітету: MailServer, DBServer, DС\_server.
* Сервера другого приорітету: Share, FileServer, 1cserver.
* Сервера третього приорітету: App\_Server, test.
  + 1. **Частота і види копіювання**

Snapshots – це моментальна копія стану даних у системі зберігання, або програмі, зафіксована на конкретний момент часу. Копіювання здійснюються щодня кілька разів і зберігаються в сховищі даних компанії – NetАрр 2050. Крім того, дані серверів MailServer, DBServer, FileServer, на яких знаходиться критично важлива інформація, копіюється в сховище NetАрр 2020, яке знаходиться в відділенні компанії і є резервним сервером, на випадок аварії в офісі компанії.

Snapmirror – щоденне копіювання у сховище даних NetАрр 2020.

У таблиці 2.4.1 зображено частоту (копіювань у день) і види копіювання.

*Таблиця 2.4.1*

|  |  |  |
| --- | --- | --- |
| **Ім’я серверу** | **Snapshot** | **Snapmirror** |
| MailServer | 3 | 1 (20:00) |
| DBServer | 3 | – |
| DC\_server | 2 | – |
| Share | 1 | – |
| FileServer | 3 | 1 (20:00) |
| App\_Server | 3 | – |

Також, щодня о 20:00 здійснюється резервне копіювання баз даних SQL сервера, яке проводиться цим же сервером. Копії баз даних розміщуються на файловому сервері.

* + 1. **Резервне копіювання на магнітну стрічку (backup)**

Резервне копіювання здійснюється на стрічковий магнітний накопичувач, ємністю 400 ГБ.

На стрічковий накопичувач (див. рис. 2.4.2.) копіюються дані домен-контроллера Server1 і важливі файли інших серверів, необхідних для безперебійної роботи компанії, в разі збою основних файлових серверів.

Рис. 2.4.2. Стрічковий накопичувач

На серверах Server1, MailServer, FileServer, DBServer, 1cserver встановлений агент віддаленого доступу, який за розкладом (один раз вночі в 00:00) здійснює резервне копіювання (backup) на магнітний накопичувач наступні папки і бази:

* із 1 cserver - папку Workbase;
* із DBServer - базу SQL (Lease Manager);
* із FileServer - папку Shared Docs;
* із MailServer - папку D: (Lotus Notes);
* із Server1 - папку Users і С:.
  + 1. **Контроль резервного копіювання**

Контроль резервного копіювання здійснюється:

* автоматично;
* відповідальним ІТ-спеціалістом.

Автоматичний контроль резервного копіювання на магнітний носій здійснюється за допомогою програми Backup Ехес, яке знаходиться на DC\_server, що виконує роль додаткового домен-контроллера.

Відповідальний ІТ-спеціаліст:

* здійснює заміну стрічок: вставляє стрічку напередодні запису (відповідно до розкладу додатку Backup Ехес (див рис. 2.4.3) і вилучає записану стрічку);
* зберігає магнітні стрічки;
* контролює успішність завершення процесу резервного копіювання;
* усуває збої при резервному копіюванні;
* підтримує файл реєстрації резервного копіювання (backup log).

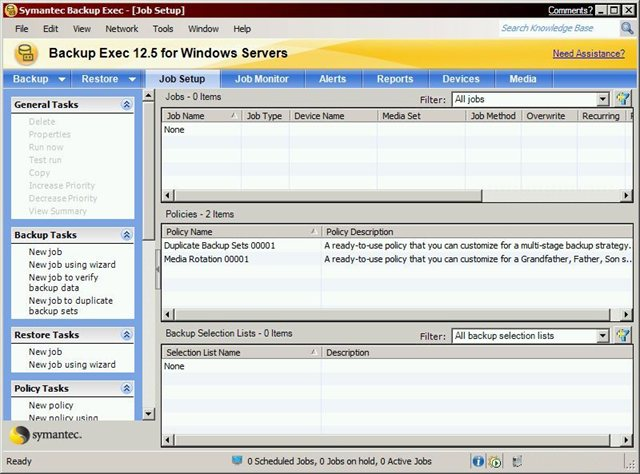


Рис. 2.4.3. Backup Exec - система резервного копіювання та відновлення даних серверів і робочих станцій.

У разі планової або незапланованої відсутності відповідального ІТ-фахівця, його обов'язки з управління резервним копіюванням виконує керівник ІТ відділу.

Місцем зберігання магнітних стрічок визначено в компанії, де згідно з Процедурою відновлення після аварії, буде розташовуватися тимчасовий офіс. Магнітні стрічки доставляються в банк один раз в тиждень, по п'ятницях.

Відповідальний ІТ-фахівець повинен перевіряти статус резервного копіювання в системі щоранку і повідомляти про будь-яких збоях керівнику ІТ відділу.

Щоденне фіксування інформації про резервне копіювання в файл Backup Log здійснюється з метою повідомлення про копіювання, його статус, використовуваних магнітних накопичувачах, підтримки системи резервного копіювання. Файл резервного копіювання зберігається в комутаторній.

У разі збою резервного копіювання, відповідальний ІТ-фахівець зобов'язаний

негайно:

* звернути увагу на будь-які повідомлення/інформацію на моніторі сервера;
* повідомити керівника ІТ відділу про збої;
* зафіксувати про збої в файлі резервного копіювання (backup log) і прийнятих заходів;
* очистити магнітний накопичувач;
* перевірити термін використання магнітного накопичувача. Знищити і замінити його на інший, якщо перевищено термін експлуатації;

1. якщо збій резервного копіювання повторюється, можливо, потрібно буде виконати ручне резервне копіювання. В такому випадку, необхідно, щоб всі користувачі вийшли із системи.
   1. **Висновки до розділу**

У другому розділі представлено розробку документів, необхідних для ефективної безпеки підприємства у разі втрати, знищення чи пошкодження даних. Важливо було розробити саме план відновлення, щоб вчасно відновити апаратне забезпечення, програми та дані, щоб задовольнити потреби відновлення бізнесу. Деякі дані є дуже важливими для виживання та подальшої діяльності. Вплив втрати даних або пошкодження внаслідок відмов обладнання, помилок людини, злому або зловмисного програмного забезпечення може бути суттєвим. Тому, політика резервного копіювання даних та відновлення електронної інформації є необхідною.

Пріоритети відновлення ІТ повинні відповідати пріоритетам відновлення бізнес-функцій та процесів. Політика безпеки баз даних розроблена задля уникнення несанкціонованого доступу. Це означає тримати сервер бази даних у захищеному та заблокованому середовищі з контролем доступу. Сервер баз даних захищений брандмауером від загроз безпеці баз даних, який також захищає базу даних від ініціювання вихідних з'єднань.

**РОЗДІЛ 3. СИСТЕМА ЗАХИСТУ ЗАСОБАМИ ВІРТУАЛІЗАЦІЇ**

* 1. **Опис і мета проекту віртуалізації робочих станцій**

Citrix XenDesktop - це рішення, в рамках якого створюються віртуальні робочі станції, які замінять робочі станції з індивідуальної операційною системою Windows і програмним забезпеченням на сервіс, доступний всім користувачам.

Робочі столи є віртуальними і працюють на віддалених серверах. З точки зору користувача, процедура входу на віртуальний робочий стіл аналогічна входу на робочу станцію з індивідуальної операційною системою Windows. Користувачі вводять свої облікові дані один раз і підключаються до своїх робочих столів.

Віртуальні робочі столи компонуються динамічно за запитом, при кожному вході користувачів в систему.

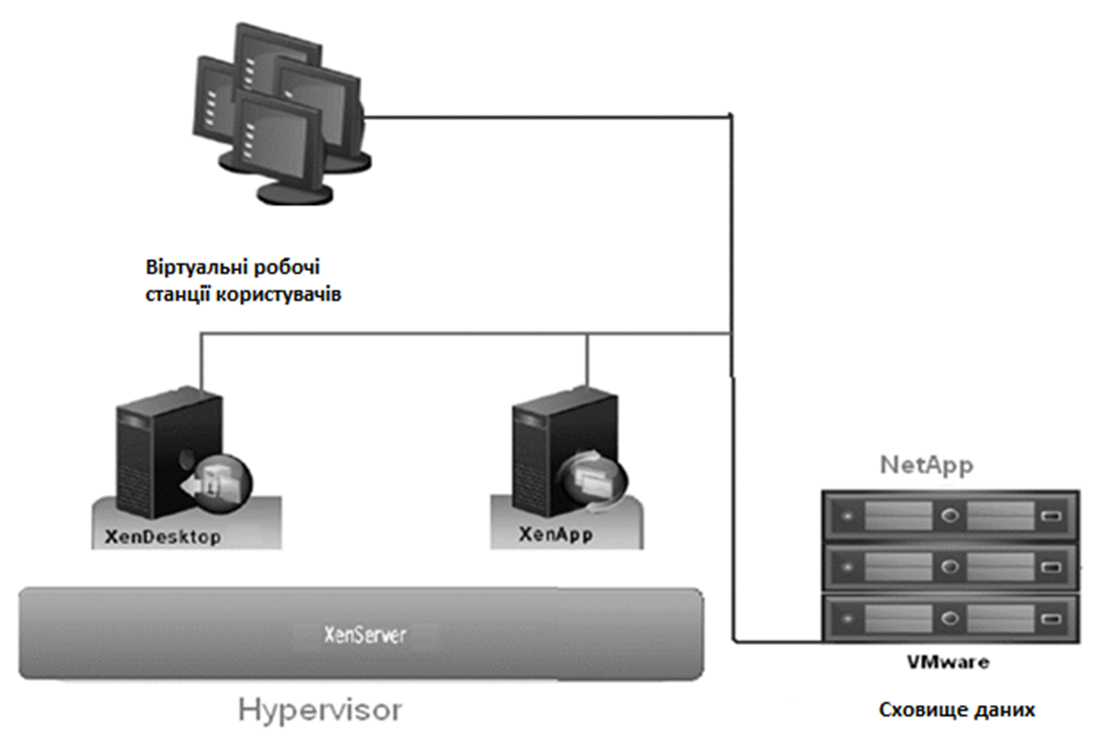
Вся інформація з віртуального комп'ютера зберігається в спеціальних дата-центрах. Це забезпечує її гарантований захист від втрати (всі дані проходять процедуру автоматичного резервного копіювання), випадкового або навмисного видалення, а також від доступу до неї сторонніх осіб.

Обслуговування віртуальних робочих місць (зокрема установка ПЗ, оновлення ПЗ й т.д.) проводиться централізовано.

У додатку XenDesktop вирішується завдання створення і управління віртуальними робочими столами, а також забезпечення ними користувачів. Формується головний образ робочого столу («золотий образ») і потім за допомогою програми XenDesktop з цього образу створюються робочі столи користувачів.

«Золотий образ» робочого столу дає можливість доступу до всіх, необхідним для роботи користувачів з додатками, які були в нього додані. Наведено перелік додатків, доступних в «золотом образі»: Microsoft Office 2010, Chrome, LM, Mozzila, BLANA, Adobe Reader, MeDoc, PDF transformer, Лига, Java, Lingvo, FleshPlayer, Kasperskiy. Групи віртуальних робочих столів створюються і управляються як одне ціле.

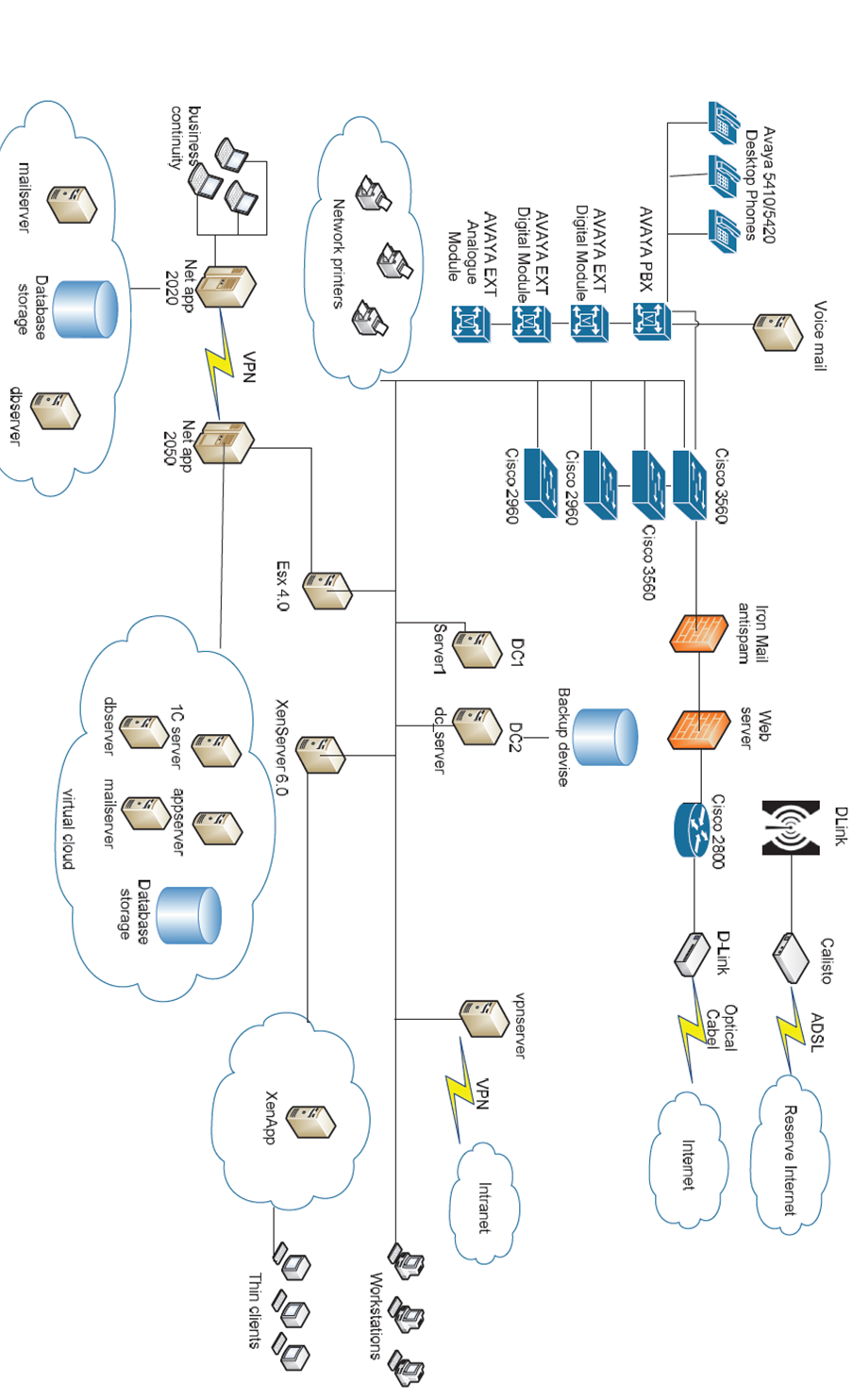
Архітектура рішення зображена на рис. 3.1.1.

Рис. 3.1.1. Архітектура рішення

Переваги проекту:

* спрощення ІТ-інфраструктури;
* економія грошових ресурсів на закупівлю ліцензій на операційні системи, комп'ютерного обладнання та за рахунок зниження споживання електрики;
* зниження тимчасових витрат на підготовку робочого місця співробітникам;
* зниження тимчасових витрат на відновлення робочого процесу внаслідок аварії;
* безпеку і захист інформації від втрати і доступу до неї сторонніх осіб;
* можливість централізованого управління і контролю.

Загальний вигляд топології мережі на підприємстві див. на рис. 3.1.2.

Рис. 3.1.2. Топологія мережі на підприємстві

* + 1. **Конфігурація**

Представлено опис обладнання, яке задіяне в віртуалізації робочих станцій (див. табл. 3.1.1).

*Таблиця 3.1.1*

|  |  |  |  |
| --- | --- | --- | --- |
| **Обладнання** | **Кількість** | **Конфігурація** | **Коментарі** |
| HP ProLiant DL 380 G7 | 1 | CPU -2  (Procesador Intel Xeon X5690)  16 Ядер  Memo – 78 Gb  HDD – 500Gb  ОС – (XenServer) ESX 5.0 | Сервер управління віртуальним середовищем Citrix. |
| HP ProLiant DL 380 G6 | 1 | CPU -2  (Procesador Intel Xeon E5520)  8 Ядер  Memo – 30 Gb  HDD – 150Gb  ОС – ESX 4.0 | Сервер управління віртуальним середовищем VMware. |
| NetApp | 1 | FAST 2050  HDD – 3,7 Tb | Сховище даних. |

* + 1. **Програмне забезпечення**

Представлено опис програмного забезпечення, яке задіяне в віртуалізації робочих станцій (див. табл. 3.1.2).

*Таблиця 3.1.2*

|  |  |
| --- | --- |
| **Програмне забезпечення** | **Конфігурація** |
| **XenDesktop/XenApp virtualization** | |
| Citrix XenDesktop Controller | Version 5.5 Platinum Edition |

*Продовження табл.3.1.2*

|  |  |
| --- | --- |
| Citrix XenApp Server | Version 6.5 |
| ОС для XenDesktop Controller | Windows Server 2008 R2 SP2 64 bit |
| Citrix XenServer | 6.0 |
| **Віртуальний робочий стіл «золотий образ»** | |
| ОС | MS Windows XP Profession (en) (32-bit) SP 3 |
| Microsoft Office | Office Standard 2010 |
| Chrome | – |
| Mozzila | – |
| Adobe Reader | 9.0 |
| PDF transformer | 3.0 |
| Java | 7.0 |
| Flash Player | 10.0.22.87 |
| Ліга Закон | 9.0 |
| Lease Manager | – |
| Lingvo | X3 |
| BLANA | – |
| Kasperskiy | 6.0 |
| .MeDoc | 11.01.025 |

* + 1. **Citrix XenDesktop**

Citrix XenDesktop пропонує повну систему доставки віртуальних десктопів, інтегруючи декількох розподілених компонентів з розширеними засобами настройки, які спрощують створення інфраструктури віртуальних десктопів і управління нею в режимі реального часу.

Основними компонентами (див. рис. 3.1.3) XenDesktop є:

Контролер.

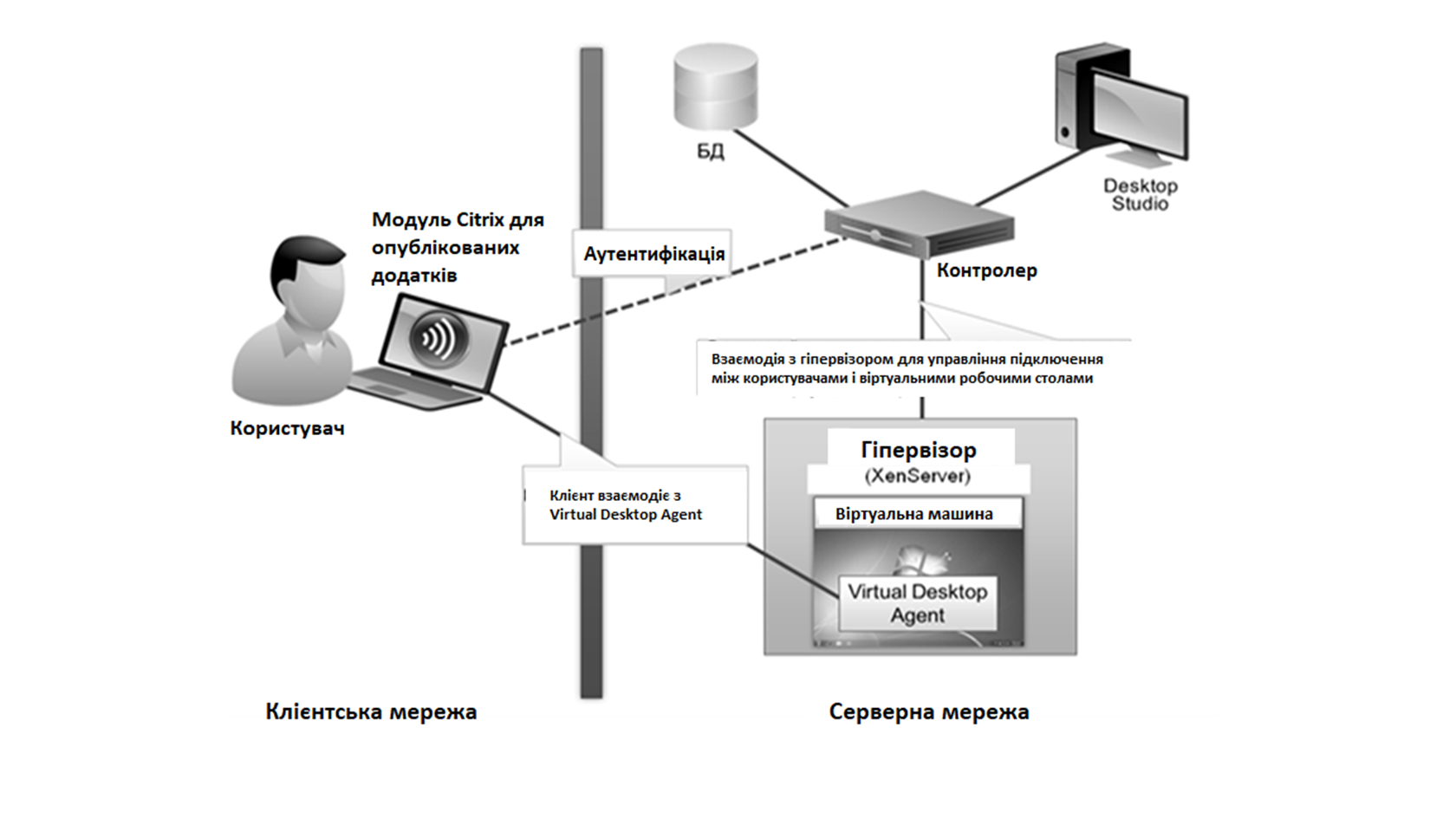
Контролер, який встановлюється на серверах в центрі обробки даних, складається з служб, які перевіряють справжність користувачів, керують складанням середовищ їх віртуальних робочих столів і є брокером підключень користувачів до їх віртуальним робочих столів. Він контролює стан робочих столів, запускаючи і зупиняючи їх на вимогу і в залежності від адміністративної конфігурації. У деяких редакціях контролер дозволяє встановити компонент управління профілем, щоб управляти параметрами персоналізації користувача в віртуалізованних або фізичних середовищах Windows.

Рис. 3.1.3. Компоненти XenDesktop

Агент віртуального робочого столу.

Встановлений на віртуальних десктопах, цей агент забезпечує прямі підключення ICA між віртуальним десктопом і користувацькими пристроями.

Citrix online plug-in.

Онлайн-модуль Citrix, що встановлюється на призначених для користувача пристроях, забезпечує їх безпосередні ICA-підключення до віртуальних робочих столів.

Служби створення машин.

Набір служб, що працюють спільно для створення за запитом віртуальних робочих столів на основі головного образу робочого столу. Це дозволяє оптимізувати використання сховища і надати кожному користувачеві чистий віртуальний робочий стіл при кожному його вході в систему.

Desktop Studio.

Забезпечує настройку і управління розгортанням XenDesktop. Desktop Studio пропонує різні майстри для виконання процесу настройки середовища, створення робочих столів і їх призначення користувачам.

Desktop Director.

Дозволяє ІТ-персоналу з підтримки рівня 1 і 2 відстежувати розгортання XenDesktop і виконувати повсякденні завдання з обслуговування. Крім того, для усунення неполадок можна переглядати і взаємодіяти з сеансом користувача за допомогою віддаленого помічника (Microsoft).

Citrix XenApp.

У розгортанні XenDesktop можна використовувати XenApp для отримання вигод від ефективних процесів, пов'язаних з потоковим доступом до додатків і виртуализацией. XenApp забезпечує як користувачам, так і адміністраторам умови роботи з додатками, кращі ніж з встановленими. Додатки швидше запускаються, значно підвищено якість умов роботи користувача, і істотно знижені витрати на управління додатками.

Citrix XenServer.

XenServer - це рішення інфраструктури віртуальних машин корпоративного класу, що створює основи для доставки віртуальних десктопів і пропонує розширені можливості управління. На XenServer можна запустити безліч віртуальних машин завдяки перевазі розширених функцій віртуалізації в останніх процесорах Intel і AMD з підтримкою віртуалізації.

* + - 1. **Конфігурація**

Конфігурацію XenDesktop див. у табл. 3.1.3.1.1. – управління віртуальними робочими столами.

IP адреса віртуальної машини: IP-10.244.55.42.

*Таблиця 3.1.3.1.1*

|  |  |
| --- | --- |
| **Характеристика обладнання** | **Програмне забезпечення** |
| CPU 1  Memo 4Gb  HDD 40Gb | Windows 2008 R2 SP2 64 bit  Windows SQL Server 2008 R2 64 bit  Windows via C/C++ 2008 64 bit  Windows Net Framework 4  Citrix XenDesktop  Citrix Web Interface  Citrix Tools for virtual machines  Citrix Broker service  Citrix Powershell snap-in |

Конфігурація XenDesktop, продубльованого на NetApp в віртуальному середовищі VMware див. у табл. 3.1.3.1.2.

IP адреса віртуальної машини: IP-10.244.55.44

*Таблиця 3.1.3.1.2*

|  |  |
| --- | --- |
| **Характеристика обладнання** | **Програмне забезпечення** |
| CPU 1  Memo 1Gb  HDD 25Gb | Windows 2008 R2 SP2 64 bit  Windows SQL server 2008 R2 64 bit  Windows via C/C++ 2008 64 bit  Windows Net Framework 4 |

*Продовження таблиці 3.1.3.1.2.*

|  |  |
| --- | --- |
|  | Citrix XenDesktop  Citrix Web Interface  Citrix Tools for virtual machines  Citrix Broker service  Citrix Powershell snap-in |

* + 1. **Citrix XenApp**

XenApp - це основний програмний компонент інфраструктури Citrix для надання Windows-додатків (див. рис. 3.1.4.1). Завдання XenApp та інфраструктури Citrix для надання Windows-додатків полягає в наданні додатків на вимогу, як на фізичних, так і на віртуальних робочих столах.

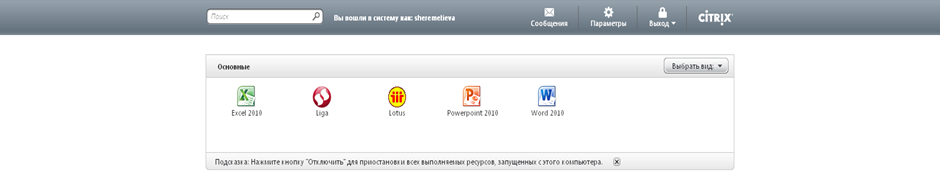


Рис. 3.1.4.1. Загальний вигляд Citrix XenApp

XenApp пропонує три методи надання додатків на користувача пристроях, серверах і робочих столах:

* Віртуалізація додатків на стороні сервера: додатки працюють в центрі обробки даних. XenApp надає інтерфейси всіх додатків на користувача пристроях і транслює дії користувача, такі як натискання клавіш і дії миші, в додаток.
* Віртуалізація додатків на стороні клієнта: XenApp виконує потокову передачу додатків на призначені для користувача пристрої з центру обробки даних на вимогу і виконує ці програми в інтерфейсі користувача.
* Віртуалізація додатків, розміщених на віртуальній машині: проблемні програми та програми, що вимагають певних операційних систем, працюють на робочому столі в центрі обробки даних. XenApp надає інтерфейси всіх додатків на користувача пристроях і передає дії користувача, такі як натискання клавіш і операції миші, в додаток.

Наприклад, якщо натиснути на програму Lotus Notes, то отримаємо наступні етапи підключення (див. рис. 3.1.4.2).

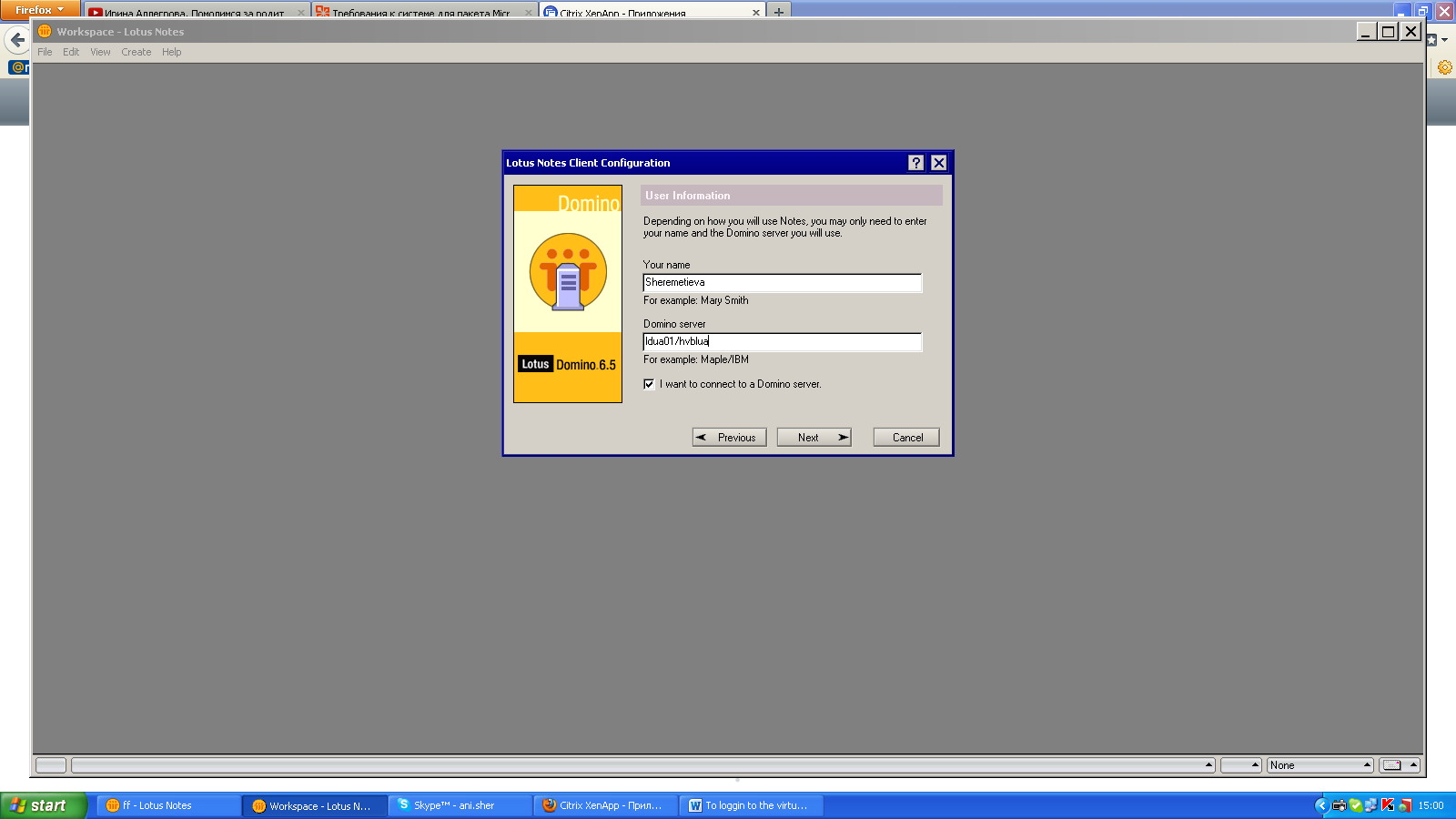


Рис. 3.1.4.2. Підключення до Lotus Notes

У полі "Your name" необхідно ввести своє ім'я та прізвище, а в полі "Domino Server" - ldua01/hvblua і натиснути Next.

Далі, вибрати «Налаштувати з'єднання з локальною мережею (LAN)» та натиснути Next (див. рис. 3.1.4.3).

Рис. 3.1.4.3. Налаштування з’єднання з Domino Server

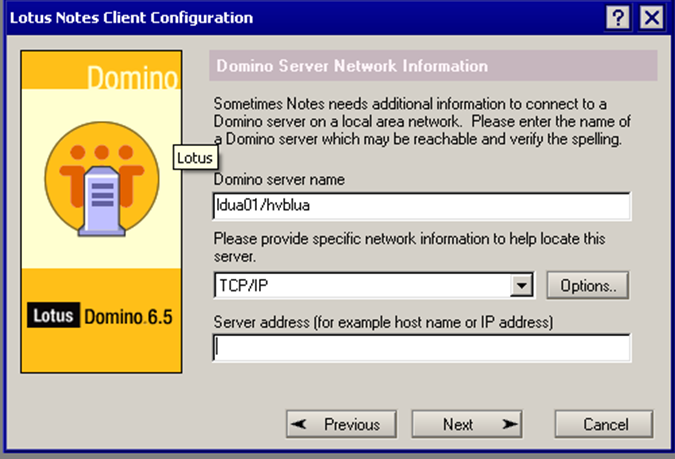
У наступному вікні необхідно вибрати із випадаючого списку - протокол TCP\IP, а у полі Server address ввести 10.244.55.21 і натиснути Next (див. рис. 3.1.4.4).

Рис. 3.1.4.4. Налаштування Network Information

Далі, ввести свій пароль та натиснути кнопку ОК (див. рис. 3.1.4.5).

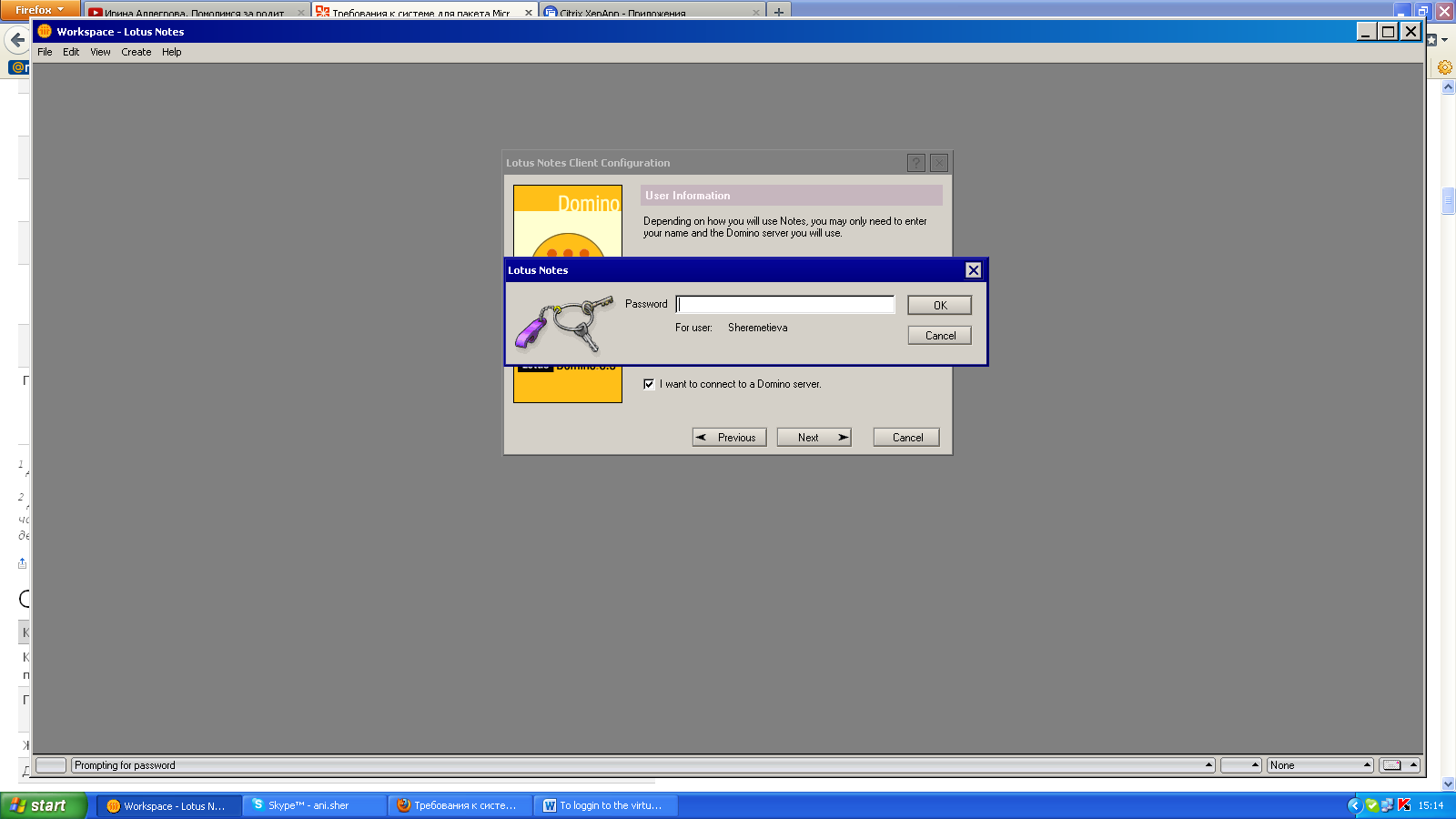


Рис. 3.1.4.5. Введення паролю

І вибрати зі списку – Office (Network) та натиснути OК (див. рис. 3.1.4.6).

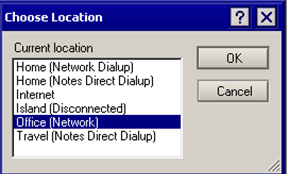


Рис. 3.1.4.6. Підключення до мережі

Після всіх вищезазначених кроків програма готова до роботи.

На рис. 3.1.4.7. зображено процес надання додатків в середовищі XenApp.

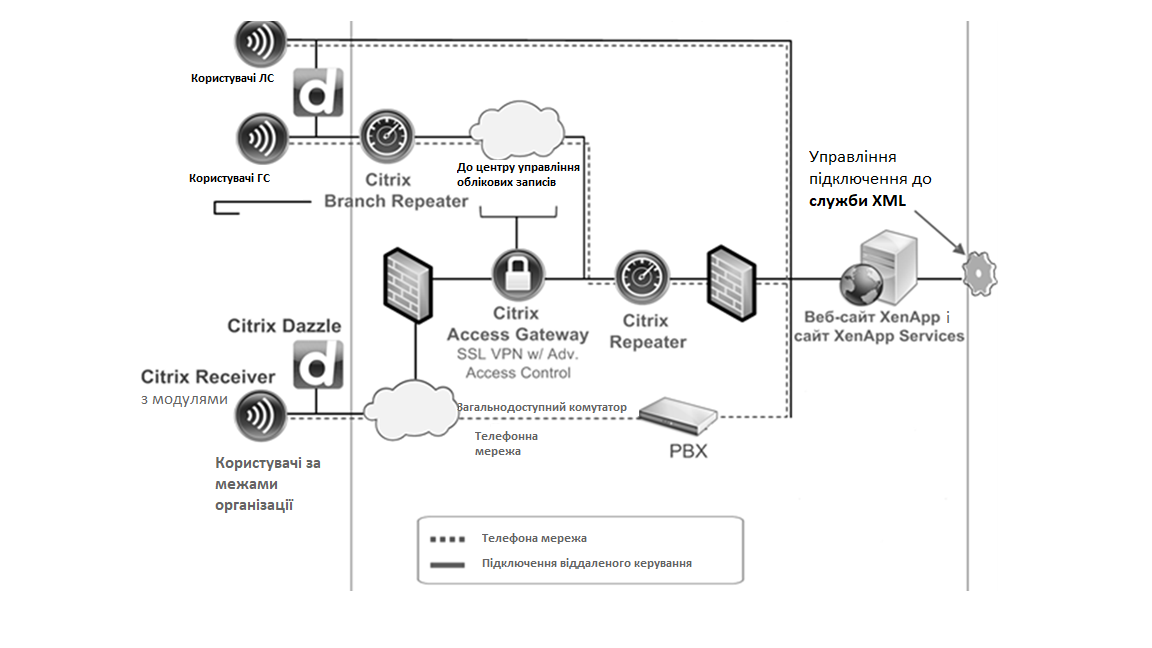
Рис. 3.1.4.7. Процес надання додатків

Середа XenApp включає три групи компонентів: призначені для користувача пристрої (на схемі представлені компонентами Citrix Receiver і Citrix Dazzle), інфраструктура доступу і інфраструктура віртуалізації.

У лівій частині схеми знаходяться компоненти Citrix Dazzle і Citrix Receiver, що представляють набір пристроїв, на яких можна встановлювати клієнтське програмне забезпечення. Citrix Dazzle надає користувачам набір додатків, доступ до яких був дозволений ІТ відділом. Citrix Receiver управляє клієнтськими програмними модулями, які забезпечують взаємодію користувачів з віртуалізованими додатками.

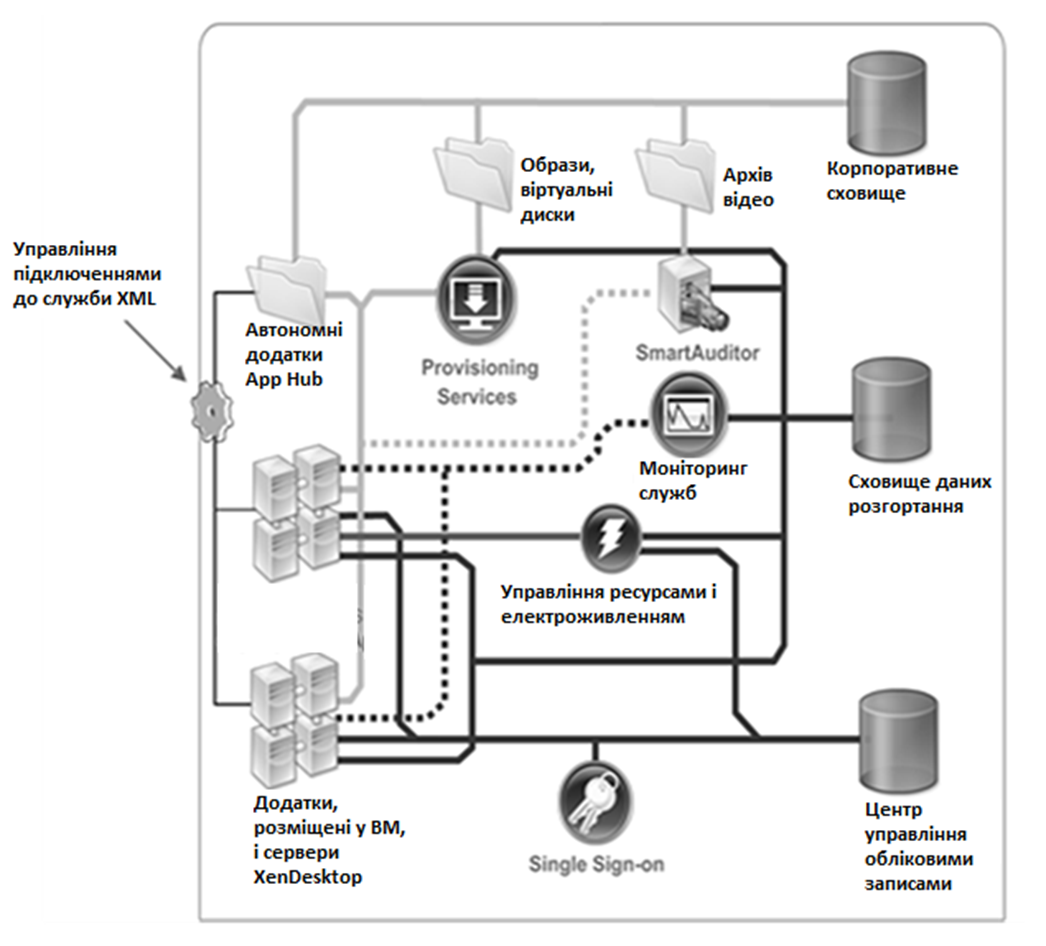
Інфраструктура доступу надає безпечні точки входу, розгорнуті в ДМЗ (демілітаризована зона), і забезпечує доступ до ресурсів, опублікованими на серверах XenApp.

Інфраструктура віртуалізації представляє групу серверів, що забезпечують моніторинг середовищ додатків і управління ними. Всі користувачі використовують Citrix Dazzle для вибору потрібних додатків. Модулі Citrix Receiver застосовуються для їх запуску. Локальні користувачі в межах брандмауера можуть працювати з веб-сайтом XenApp і сайтом XenApp Services безпосередньо. Користувачі на віддалених майданчиках отримують доступ до додатків через сайти, реплікованих за допомогою Citrix Branch Repeater, а користувачі за межами компанії отримують доступ до системи за допомогою рішень для безпечного доступу, таких як Access Gateway (див.рис. 3.1.4.2).

Рис.3.1.4.2. Інфраструктура доступу

Служба XML передає запити і дані між інфраструктурами доступу і віртуалізації (див. рис. 3.1.4.3). Використовуючи профілі і політики Active Directory, сервери XenApp ініціюють потрібний тип подання додатка користувачеві. Сервери XenApp забезпечують віртуалізацію додатків на стороні сервера і управління сеансами. Відомості про сеансах і конфігурації зберігаються в модулях збору даних і центральне сховище (сховище даних середовища). Компонент App Hub надає профілі потокових додатків (додатки, віртуалізовані на стороні клієнта і розміщені в корпоративному сховище). Сервер додатків, розміщених на віртуальній машині, ізолює проблемні додатки в безшовному робочому столі, який може бути віртуалізувати на сервері або призначеному для користувача пристрої в залежності від профілю користувача.

Образи робочих столів надаються за допомогою Provisioning Server. Дані конфігурації сеансів і серверів зберігаються в корпоративній базі даних.

Рис. 3.1.4.3. Інфраструктура віртуалізації 

Provisioning Services надає робочі столи, які зберігаються у вигляді образів в корпоративній базі даних, на серверах.

SmartAuditor забезпечує моніторинг сеансів. Записані сеанси знаходяться в корпоративному сховищі, а дані конфігурації - в сховище даних середовища.

Моніторинг служб дозволяє тестувати робочі навантаження серверів для оцінки кількості серверів, необхідних для середовища, і їх відстеження після розгортання. Управління ресурсами і електроживленням забезпечує скорочення енергоспоживання та адміністрування ресурсів сервера шляхом динамічного зміни числа активних серверів.

Служба Single Sign-on забезпечує управління паролями віртуалізованих додатків. Паролі зберігаються в наборі повноважень облікового запису.

* + - 1. **Конфігурація**

Конфігурація XenApp див. у табл. 3.1.4.1. Управління додатками.IP адреса віртуальної машини: IP-10.244.55.43.

*Таблиця 3.1.4.1.1.*

|  |  |
| --- | --- |
| **Характеристика обладнання** | **Програмне забезпечення** |
| CPU 1  Memo 2Gb  HDD 40Gb | Windows 2008 R2 SP2 64 bit  Windows SQL Server 2008 R2 64 bit  Windows Via C/C++ 2008 64 bit  Windows Net Framework 4  MS Office 2010  Lotus  Liga  Lingvo X-3  Citrix XenApp Server 6.5  Citrix XenAapp Migration center  Citrix XenApp Management  Citrix Xenapp Receiver  Citrix License Configuration tool |

* + 1. **Citrix XenServer**

Citrix XenServer є повною платформою для віртуалізації серверів Citrix. Пакет XenServer містить всі необхідні компоненти для створення і управління розгортанням віртуальних робочих станцій.

XenServer працює безпосередньо на серверах без операційної системи, що збільшує ефективність і масштабованість системи.

XenServer працює відокремлюючи елементи, притаманні фізичній машині (наприклад, жорсткі диски, ресурси і порти) і розподіляючи їх на віртуальні машини, що працюють на ньому.

Citrix XenCentre - додаток, за допомогою якого здійснюється управління віртуальним середовищем. Так, в цьому додатку можна створити «золотий образ» віртуальної машини, з встановленими додатками, які не будуть публікуватися на сервері додатків XenApp. XenCentre можна встановити на будь-яку робочу станцію.

* + - 1. **Конфігурація**

На XenServer встановлено два віртуальних сервера під керуванням Windows 2008 R2 XenDesktop і XenApp, які керують доступом користувачів до віртуальних столів і програм. Обладнання:

* HP ProLiant DL 380 G7
* CPU -2 (Procesador Intel® Xeon® X5690 )
* 16 Ядер
* Memo- 78 Gb
* HDD- 500Gb
* ОС - XenServer
  + 1. **NetApp**

NetApp являє собою дискову систему зберігання даних і програмне забезпечення, які забезпечує зберігання, обслуговування, захист та архівування даних.

У компанії задіяно 2 пристрої для зберігання даних: FAS2020 і FAS2050, які забезпечують управління складними розподіленими і зростаючими середовищами зберігання даних.

* + - 1. **Технічні характеристики**

Технічні характеристики мережевої системи зберігання даних NetApp FAS2020 / 2050 див. у табл. 3.1.6.1.

*Таблиця 3.1.6.1*

|  |  |
| --- | --- |
| **Підтримка протоколів SAN** | Протокол Fibre Channel для SCSI (4/2/1 Гбит/с); FAS и DAS; IP SAN (iSCSI) |
| **Поддержка мережевих протоколів** | NFS V2/V3/V4 поверх UDP або TCP, PCNFSD V1/V2  для перевірки автентичності NFS (PC), Microsoft CIFS, HTTP 1.0, віртуальні хости HTTP 1.1 |
| **Число логічних пристроїв** | До 1 024 |
| **Тома FlexVol** | До 200 на 1 контролер для моделей FAS2020 и FAS2050.  До 500 на 1 контролер для моделі FAS2050. |
| **Копії Snapshot** | До 51,000 на 1 контролер для моделей FAS2020 и FAS2050. До 127,000 на 1 контролер для моделі FAS2050. |
| **Підтримуване число хостів** | До 2 зовнішніх (хостових) портів підключення на 1 контролер до 4 серверів прямого підключення на одну конфігурацію "активний-активний"  До 24 серверів з підключенням через SAN для FAS2020.  До 32 серверів з підключенням через SAN для FAS2050. |
| **Підтримувані конфігурації** | Контролерні конфігурації.  Один контролер, конфігурація "активний-активний" з кластерниим аварійним перемиканням (CFO).  Внутрішні (дискові) конфігурації.  Сховище високої готовності з двома або кількома альтернативними шляхами передачі даних (PDF). |
| **Надійність** | Контролери, вентилятори і джерела живлення з резервуванням і можливістю гарячої заміни. |
| **Менеджмент** | Вбудована повнодуплексна консоль 10/100 Base-T Ethernet, діагностичні світлодіодні індикатори, Maintenance Center, |

*Продовження таблиці 3.1.6.1.*

|  |  |
| --- | --- |
| **Менеджмент** | SNMP, telnet, SSH, HTTP, SSL, сценарії хостів, розсилка повідомлень по електронній пошті. |
| **Безпека** | Захист від вірусів, SecureAdmin, IPSec, перевірка достовірності CHAP, контроль доступу на базі ролей (RBAC). |

* + - 1. **Конфігурація**

Конфігурацію NetApp відображено у табл. 3.1.6.2.

*Таблиця 3.1.6.2*

|  |  |  |
| --- | --- | --- |
| **Масштабованість** | **FAS2020** | **FAS2050** |
| Макс. номінальна ємність | 68 ТБ | 104 Тб |
| Макс. число внутрішніх дисків | 12 | 20 |
| Макс. число зовнішніх дисків | 56 | 84 |
| Макс. загальне число дисків (внутрішніх і зовнішніх) | 68 | 104 |
| Макс. число дисків на внутрішню петлю FC | 56 | 84 |
| Пам'ять ECC | 2 Гб | 4 Гб |
| Реальна кількість дисків | 6 | 20 |
| Ємність диска | 420 Гб | 300 Гб |
| Фактична ємність загального простору (RAID - DP) | 2,6 Тб | 7,4 Тб |
| Фактична ємність використовуваного простору | 1,3 Тб | 3,7 Тб |

* 1. **Висновки до розділу**

Отже, у третьому розділі описано проект віртуалізації робочих станцій - Citrix XenDesktop. Зокрема, представлено опис нової ІТ-інфраструктури, архітектури рішення, основних компонентів, конфігурації, а також визначення «золотого образа».

Мета впровадження проекту віртуалізації робочих на підприємство полягає в оптимізації існуючої ІТ-інфраструктури на базі Citrix XenDesktop, Citrix XenApp, Citrix XenServer.

Тому, Citrix XenDesktop - це новітнє рішення, в рамках якого створюються віртуальні робочі станції, які замінять робочі станції з індивідуальної операційною системою Windows і програмним забезпеченням на сервіс, доступний всім користувачам. Робочі столи є віртуальними і працюють на віддалених серверах. Вся інформація з віртуального комп'ютера зберігається в спеціальних дата-центрах. Це забезпечує її гарантований захист від втрати, випадкового або навмисного видалення, а також від доступу до неї сторонніх осіб.

# **ВИСНОВКИ**

Результатом виконаної роботи є рішення задачі оптимізації, в рамках якої створені віртуальні робочі станції, які замінили робочі станції з індивідуальної операційною системою Windows і програмним забезпеченням на сервіс, доступний всім користувачам. Розроблена система захисту може бути використана як для оптимізації і підвищення рівня захищеності існуючої інфраструктури, так і для нових компаній при побудові власного корпоративного хмарного середовища.

Завдяки віртуалізації обладнання та його розподілення на основі реальних потреб користувачів та додатків, наявна обчислювальна потужність, простір пам’яті та пропускна здатність мережі можуть використовуватися набагато ефективніше.

У процесі виконання роботи були отримані наступні результати:

Проаналізовано технологію віртуалізації, її функції і переваги, представлено основні типи віртуалізації, більш детально описано віртуалізацію серверу, її функції, типи і обмеження. У виді рисунків, було представлено оптимальний та робочий варіант дата-центру.

На основі проведеного аналізу було важливим розробити план відновлення після катастроф, загальну політику ІТ-безпеки на підприємстві, правила захисту баз даних і політику резервного копіювання, задля уникнення втрат, пошкоджень і несанкціонованого доступу.

Розроблено систему віртуалізації на базі VMware і Citrix, перевагами якої є спрощення ІТ-інфраструктури, економія грошових ресурсів на закупівлю ліцензій на операційні системи, комп'ютерного обладнання за рахунок зниження споживання електрики, зниження тимчасових витрат на підготовку робочого місця співробітникам, на відновлення робочого процесу внаслідок аварії, безпеку і захист інформації від втрати і доступу до неї сторонніх осіб, можливість централізованого управління і контролю.

# **СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ**

1. What is virtualization? [Electronic resource] / Red Hat, 2018 – Режим доступу: WWW. – URL: <https://www.redhat.com/en/topics/virtualization/what-is-virtualization>.

Exploring data virtualization tools and technologies [Electronic resource] / Margaret Rouse // Techtarget network, 2019 – Режим доступу: WWW. – URL: <https://searchservervirtualization.techtarget.com/definition/virtualization>.

Статья «Анализ современных технологий виртуализации» [Электронный ресурс] / Иван Тужилкин – Режим доступу: WWW. – URL: <https://habr.com/ru/company/southbridge/blog/212985/>.

Hyper-V feature focus [Electronic resource] / Dustin Hannifin // ScienceDirect, 2010 – Режим доступу: WWW. – URL: <https://www.sciencedirect.com/topics/computer-science/virtualization-technology>.

Virtualization [Electronic resource] / Rajkumar Buyya // ScienceDirect, 2013 – Режим доступу: WWW. – URL: <https://www.sciencedirect.com/topics/computer-science/virtualization-technology>.

Future Trends: Virtualization Technology [Electronic resource] / Nihad Ahmad Hassan // ScienceDirect, 2017 – Режим доступу: WWW. – URL: <https://www.sciencedirect.com/topics/computer-science/virtualization-technology>.

How Server Virtualization Works? [Electronic resource] / Jonathan Strickland // HowStuffWorks, 2008 – Режим доступу: WWW. – URL: <https://computer.howstuffworks.com/server-virtualization.htm>.

An Introduction to Virtualization? [Electronic resource] / Amit Singh // Kernelthread, 2008 – Режим доступу: WWW. – URL: <http://www.kernelthread.com/publications/virtualization/>.

Виртуализация [Электронный ресурс] / VMware, 2018 – Режим доступу: WWW. – URL: <https://www.vmware.com/ru/solutions/virtualization.html>.

The Top 7 Uses For VMware Workstation [Electronic resource] / Vegibit, 2014 – Режим доступу: WWW. – URL: <https://vegibit.com/the-top-7-uses-for-vmware-workstation/>.

Disaster Recovery Plan (DRP) [Electronic resource] / Margaret Rouse // Techtarget network, 2017 – Режим доступу: WWW. – URL: <https://searchdisasterrecovery.techtarget.com/definition/disaster-recovery-plan>.

10 mistakes to avoid in your disaster recovery planning process [Electronic resource] / Jon Toigo // Techtarget network, 2014 – Режим доступу: WWW. – URL: <https://searchdisasterrecovery.techtarget.com/feature/10-mistakes-to-avoid-in-your-disaster-recovery-planning-process>.

Writing an Information Security Policy [Electronic resource] / Grace Carter // DataVersity, 2018 – Режим доступу: WWW. – URL: <https://www.dataversity.net/writing-information-security-policy/>.

7 Database Security Best Practices [Electronic resource] / Paul Rubens // eSecurityPlanet, 2016 – Режим доступу: WWW. – URL: <https://www.esecurityplanet.com/network-security/6-database-security-best-practices.html>.

Дата-центр VERnet DC [Электронный ресурс]/ SIA VERSIJA, 2020 – Режим доступу: WWW. – URL: <https://www.vernet-dc.lv/rus/data-centr/>.

Data center [Electronic resource] / Margaret Rouse // Techtarget network, 2017 – Режим доступу: WWW. – URL: <https://searchdatacenter.techtarget.com/definition/data-center>.

VMware [Electronic resource] / Margaret Rouse // Techtarget network, 2017 – Режим доступу: WWW. – URL: <https://searchvmware.techtarget.com/definition/VMware>.

VMware ESX Server [Electronic resource] // VMWare, 2005 – Режим доступу: WWW. – URL: <https://www.vmware.com/pdf/esx_vin_eval.pdf>.

Міграція у хмару [Електронний ресурс] / Березніков Андрій // Denovo, 2018 – Режим доступу: WWW. – URL: <https://www.de-novo.biz/blog/migraciya-u-hmaru-osnovni-instrumenti-ta-shlyahi-perenosu-5>.

**Додаток А**

# **План дій при сценарії «Незначні пошкодження»**

|  |  |
| --- | --- |
| **Завдання** | **Група** |
| Оцінити шкоду | Управління та ліквідація наслідків стихійних лих |
| Визначення відповідних програм | Управління та ліквідація наслідків стихійних лих |
| Запросити відповідні ресурси у резерві | Управління стихійними лихами |
| Отримати відповідні резервні копії | Операційна |
| Перезавантажити відповідні програми в режимі резерву | Операційна |
| Надання доступу до основних ресурсів та послуг для критичних позицій | Операційна |
| Інформуйте користувачів про нові процедури | Зв'язку |
| Замовити обладнання для заміни пошкоджених комп'ютерів | Операційна |
| Встановіть заміну обладнання та перезавантажте додатки | Операційна |
| Інформуйте користувачів про нормальну роботу | Зв'язку |

# **Додаток Б**

# **План дій при сценарії «Значні пошкодження»**

|  |  |
| --- | --- |
| **Завдання** | **Група** |
| Оцінка шкоди | Управління та ліквідація наслідків стихійних лих |
| Визначити відповідні програми | Управління стихійними лихами та Операційна |
| Розподілити всі групи відновлення після збоїв | Управління стихійними лихами |
| Інформування всіх зацікавлених сторін та клієнтів | Зв'язку |
| Увімкнути переадресацію дзвінків, поштового серверу, автовідповідач | Операційна |
| Повідомлення користувачів, що офіс буде недоступний протягом визначеного часу | Зв'язку |
| Запросити відповідні ресурси у резерві | Управління стихійними лихами |
| Перевірка документів, необхідних на об'єкті | Команда безперервної діяльності |
| Організація переїзду до об'єкта Stand bay | Команда безперервної діяльності |
| Отримати відповідні резервні копії | Операційна |
| Перезавантажити відповідні програми в резерві | Операційна |
| Надати доступ до ресурсів і послуг для критичних позицій | Операційна |

**Продовження додатку Б**

**Додаток А**

|  |  |
| --- | --- |
| Виділити нові варіанти офісного обладнання | Управління та ліквідація наслідків стихійних лих |
| Замовити замінне обладнання для заміни пошкодженого обладнання. | Операційна |
| Встановити мережу та обладнання для заміни та перезавантажити програми | Операційна |
| Інформувати користувачів про нормальну роботу | Зв'язку |