Міністерство освіти і науки України
Тернопільський національний технічний університет імені Івана Пулюя
(повне найменування вищого навчального закладу)
Факультет комп'ютерно-інформаційних систем і програмної інженерії
(назва факультету)
Кафедра кібербезпеки
(повна назва кафедри)

КВАЛІФІКАЦІЙНА РОБОТА

на здобуття освітнього ступеня

бакалавр
(освітній рівень)

на тему: *"Методи і засоби організації захисту даних у віртуалізованому середовищі підприємства "*

Виконав: студент (ка)

Спеціальності:
125 «Кібербезпека»
(шифр і назва напряму підготовки, спеціальності)

Метелешко М.І.
підпис (прізвище та ініціали)

Керівник *Стадник М.А.*
підпис (прізвище та ініціали)

Нормоконтроль *Кареліна О.В.*
підпис (прізвище та ініціали)

Завідувач кафедри *Загородна Н.В.*
підпис (прізвище та ініціали)

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2021

АНОТАЦІЯ

– Методи і засоби організації захисту даних у віртуалізованому середовищі підприємства // Кваліфікаційна робота ОР «Бакалавр» //Метелешко Микола Іванович// Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБсз-41 // Тернопіль, 2021 // С. , рис. – , табл. – , кресл. – , додат. – .

Ключові слова: БЕЗПЕКА ДАНИХ, ІНФОРМАЦІЙНА БЕЗПЕКА, АПАРАТНО-ПРОГРАМНИЙ КОМПЛЕКС ЗАХИСТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ.

Кваліфікаційна робота присвячена проектуванню і розробці системи безпеки на прикладі інтернет-магазину «ГІГАБАЙТ+». Розроблена система дозволила підвищити рівень захищеності персональних даних, які зберігаються і обробляються в інформаційній системі підприємства.

Метою дипломного проекту було розробка і реалізація політики інформаційної безпеки в мережі інтернет-магазину ІТ-послуг «ГІГАБАЙТ+».

Для досягнення поставленої мети були вирішення такі завдання:

– приведено короткий опис компанії;

– проведено аналіз ризиків інформаційної безпеки;

– приведено комплекс завдань, які підлягають подальшому вирішенню;

– проведено аналіз і обгрунтування вибору системи безпеки;

– описано впроваджувані програмно-апаратні засоби інформаційної безпеки, а також описано контрольний приклад застосування обраних засобів інформаційної безпеки.

ANNOTATION

Methods and facilities of data security at an enterprise virtualized environment // Thesis of educational level "Bachelor" // Meteleshko Mykola Ivanovych // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and software engineering, Department of Cybersecurity, СБсз-41 group // Ternopil, 2021 // P. , fig. -, table. - , chair. - , added. -.

Keywords: : DATA SECURITY, INFORMATION SECURITY, HARDWARE AND SOFTWARE PACKAGE FOR INFORMATION SECURITY PROTECTION.

The qualification thesis is devoted to to design and develop a security system on the example of the Gigabyte+online store. The developed system have increased the level of security of personal data that is stored and processed in the enterprise's information system.

The aim of the diploma project was to develop and implement an information security policy in the network of the «Gigabyte+» online IT services store.

To achieve this goal the following tasks have been solved:

- a brief description of the company is provided;

- an analysis of information security risks was carried out;

– a set of tasks that are subject to further solution is given;

- analysis and justification of the choice of security system was carried out;

-the implemented information security software and hardware tools are described, as well as a control example of using the selected information security tools.

The object of research is the activity of the online store of IT services "gigabyte+" in the framework of ensuring information security.

The subject of the research is the process of designing and developing a security system.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ, СИМВОЛІВ, ОДИНИЦЬ, СКОРОЧЕНЬ І ТЕРМІНІВ

ПЗ	Програмне забезпечення
ОС	Операційна система
ПДН	Персональні дані
КЗ	Контрольована зона
ЛОМ	Локальна обчислювальна мережа
СЗІ	Системи захисту інформації

ВСТУП

Комп’ютери стали невід’ємною частиною нашого повсякденного життя. Вони використовуються для зберігання і відправки листів особистого характеру, проведення різних банківських операції, і обробки інших, не менш важливих документів. У сучасному конкурентному світі, кожен бізнес змушений покращувати свою ефективність і продуктивність, щоб залишатися попереду конкурента або просто залишитися в бізнесі. Комп’ютерні мережеві технології – інтранет, екстранет, інтернет – дозволили зберігати, передавати інформацію, а найголовніше, зробили її доступною для ведення бізнесу з будь-якої точки світу. Інтернет-технології інтегрували в себе корпоративні програми, програми управління знаннями, системи підтримки прийняття рішень, інтернет-пошук і зберігання, а також таку частину зовнішньої системи, як системи для роботи з постачальниками, клієнтами (електронна комерція) і бізнес-партнерами (електронний бізнес). З усіма можливостями, які пропонують комп’ютери, мережі та інтернет-технології, організація отримує безліч переваг, включаючи швидкий доступ до інформації, більшу функціональність для користувачів, поліпшення обслуговування клієнтів, зниження витрат, а також збільшену видимість в інтернет. Ці переваги також підштовхують компанії в реалізації інтернет-технології без урахування загроз безпеки, які вони за собою тягнуть.

Забезпечення захисту даних компанії на практиці відбувається в умовах впливу різних чинників. Деякі з них систематизовані в стандартах, деякі заздалегідь невідомі і здатні знизити ефективність або навіть скомпрометувати передбачені заходи. Оцінка ефективності захисту повинна обов’язково враховувати, як об’єктивні обставини, так і ймовірні фактори.

Безпека інформації є актуальним завданням численних організацій з автоматизованими бізнес-процесами. Діяльність організації завжди знаходиться під загрозою, чи є ці загрози випадковими або навмисними. Їх поява може призвести до пошкодження даних з якими працює організація. Система інформаційної безпеки високого рівня збільшує довіру з боку клієнтів і партнерів,

і часто це одна з основ успіху компанії. Можна сформулювати три базові принципи інформаційної безпеки, яка повинна забезпечувати:

- цілісність даних;

- конфіденційність інформації;

- доступність інформації для всіх авторизованих користувачів.

Актуальність визначається необхідністю проектування і розробки системи безпеки на прикладі інтернет-магазину «ГІГАБАЙТ+». Розроблена система дозволить підвищити рівень захищеності персональних даних, які зберігаються і обробляються в інформаційній системі підприємства.

Метою дипломного проекту є розробка і реалізація політики інформаційної безпеки в мережі інтернет-магазину ІТ-послуг «ГІГАБАЙТ+».

Для досягнення поставленої мети потрібно вирішити такі завдання:

– привести короткий опис компанії;

– провести аналіз ризиків інформаційної безпеки;

– уточнити комплекс завдань, які підлягають подальшому вирішенню;

– провести аналіз і обгрунтування вибору системи безпеки;

– описати впроваджувані програмно-апаратні засоби інформаційної безпеки, а також описати контрольний приклад застосування обраних засобів інформаційної безпеки.

Об’єктом дослідження є діяльність інтернет-магазину ІТ-послуг «ГІГАБАЙТ+» в рамках забезпечення інформаційної безпеки.

Предметом дослідження є процес проектування і розробки системи безпеки.

1 ТЕОРЕТИЧНА ЧАСТИНА

1.1 Техніко-економічна характеристика предметної області та підприємства

Основна задача інтренет-магазину «ГІГАБАЙТ+»: продаж комп'ютерної техніки; надання комплекс робіт по ремонту комп'ютерної та офісної техніки починаючи від програмного налаштування вашого ПК, ноутбука чи планшета;– заправка та відновлення всіх типів лазерних та струменевих картриджів, профілактика та ремонт принтерів, БФП та копіювальних апаратів.

Захист інформації є комплексом заходів, які спрямовані на забезпечення захисту і збереження даних, які зберігаються і обробляються в інформаційній системі підприємства.

Відносно інтернет-магазину, то він працює з великою кількістю персональних даних (ПДН), таких як:

– Контактні дані покупців/замовників;

– Платіжні реквізити;

– Дані постачальників;

– Складський облік;

– Внутрішній документообіг.

Ці дані потребують особливої уваги в плані захисту. Тому система захисту інформації інтернет-магазину направлена на вирішення таких завдань:

– Контроль доступу до хостингу: доступи до панелі управління хостингом (шлях / ip, логін, пароль), FTP-доступи (шлях / хост, логін, пароль), доступи до баз даних (шлях, ім'я бази даних, ім'я користувача бази даних, пароль).

– Визначити відповідальних осіб, які мають доступ до адміністративної панелі Інтернет-магазину.

– Налаштувати корпоративну пошту для спілкування співробітників компанії і клієнтів.

– Контроль вхідної та вихідної пошти, використання особистих акаунтів в робочих процесах.

– Управління доступом до поштових акаунтів і адмін-панелі Інтернет-магазину.

– Контроль контенту Інтернет-магазину.

– Створення резервних копій файлів Інтернет-магазину, бази даних, листів, клієнтської бази, бази товарів, контенту.

Основними виходами бізнес-процесу захисту даних Інтернет-магазину є:

– Перелік даних для захисту;

– Перелік відповідальних осіб;

– Перелік заходів та засобів забезпечення захисту даних;

– Політика безпеки компанії.

До основних видів діяльності компанії «ГІГАБАЙТ+», пов’язаних зі зберіганням, обробкою даних відносяться:

– Робота з замовленнями клієнтів;

– Зберігання контактних даних покупців;

– Робота з платіжними реквізитами;

– Робота з даними постачальників;

– Складський облік;

– Внутрішній документообіг;

– Забезпечення безперервної роботи Web-порталу;

– Внутрішній аудит корпоративної інформаційної системи;

– Регламентація діяльності з обробки інформації;

– Доступ до інформаційних ресурсів;

– Контроль корпоративного трафіку.

Оцінка показників ефективності видів діяльності наведено в таблиці 1.1

Таблиця 1.1 – Основні характеристики (показники ефективності) видів діяльності

№	Наіменування характеристики (показника)	Значення показника місяць
1	Робота з замовленням клієнтів	100 замовлень в день
2	Зберігання контактних даних покупців	100 транзакцій в день
3	Робота з платіжними реквізитами	200 транзакцій в день
4	Робота з даними постачальників	150 транзакцій в день
5	Складський облік	200 транзакцій в день
6	Внутрішній документообіг	200 повідомлень в день
7	Забезпечення безперервної роботи Web-порталу	24/7
8	Внутрішній аудит корпоративної інформаційної системи	Щотижнево
9	Регламентація діяльності з обробки інформації	Щотижнево
10	Доступ до інформаційних ресурсів	24/7
11	Контроль корпоративного трафіку	Щоденно

Структура компанії «ГІГАБАЙТ+» включає в себе:

– відділ з роботи з клієнтами;

– відділ доставки;

– склад;

– відділ кадрів;

– бухгалтерія.

Організаційна структура підприємства представлена на рисунку 1.1.

Рисунок 1.1 – Організаційна структура підприємства

Відділ по роботі з клієнтами координує діяльність всіх відділів компанії, пов’язаних з продажем ІТ-послуг.

Основними функціями відділу є:

– Обробка персональних даних клієнтів.

– Координування роботи всіх відділів компанії з обслуговування клієнтів.

– Консультування клієнтів з різних аспектів закупівлі комп’ютерної техніки та надання послуг з ремонту та обслуговування техніки.

– Оформлення замовлень клієнтів, формування документів на оплату і доставку замовлень;

– Оповіщення клієнтів про процес виконання і доставки їх замовлень.

– Організація та підтримка документообігу між клієнтами та відділами компанії.

Головна мета відділу доставки – своєчасне, оптимальне і якісне транспортне забезпечення доставки замовлень клієнтів інтернет-магазину на високому сервісному рівні.

Завданнями відділу доставки є:

– Удосконалення культури обслуговування клієнтів інтернет-магазину;

– Оптимізація кур’єрської доставки замовлень клієнтів інтернет-магазину і скорочення витрат на їх перевезення;

– Розвиток і впровадження нових технологій планування маршрутів доставки;

– Вживання заходів з мінімізації ризиків при перевезенні замовлень;

– Планування і виконання бюджету за видатками на перевезення, супровід і страхування замовлень;

– Підвищення ефективності використання автотранспорту.

Основними функціями бухгалтерії підприємства полягають: в забезпеченні бухгалтерського обліку компанії, плануванні та обліку виконання кошторису витрат інтернет-магазину, проведення взаєморозрахунків з підприємствами, організаціями, установами та фізичними особами, формування персоналу компанії.

1.2 Аналіз ризиків інформаційної безпеки

Розробка правил політики безпеки дозволяє виконувати безліч завдання, а саме:

– захист персоналу та інформації;

– визначення правил поведінки користувачів, системних адміністраторів;

– забезпечення авторизації персоналу, відстеження його поведінки, дослідження можливих загроз;

– визначення і дозвіл наслідків від зовнішніх загроз безпеки;

– визначення базових концепцій безпеки компанії;

– розробка методів зниження ризику;

– забезпечення контролю за дотриманням політики безпеки.

Політика інформаційної безпеки забезпечує основу для управління безпекою компанії і правила роботи з конфіденційними даними всіх співробітників. Вона допомагає забезпечити мінімізацію ризиків, для інцидентів з порушення безпеки.

Політика безпеки визначає ставлення організації до інформації, визначає внутрішні і зовнішні дані, а також інформаційні активи компанії, які необхідно захищати від несанкціонованого доступу і зміни.

Аналіз бізнес-процесів інтернет-магазину дозволив виділити наступні дані, які обробляються і зберігаються в інформаційній системі підприємства:

1. Персональні дані клієнта. Містять особисту інформацію клієнта. Необхідно забезпечувати цілісність даних, доступність і конфіденційність.

2. Дані про постачальників компанії. Містять інформацію про постачальників товарів. Необхідно забезпечувати високу конфіденційність даних. Виток може призвести до фінансових втрат компанії.

3. Внутрішній документообіг компанії містить службове листування співробітників компанії, розпорядження, накази та інші документи компанії. Під час захисту даних необхідно забезпечити цілісність і конфіденційність.

4. Складський облік – містить інформацію про наявність товару на складі та його рух. Для захисту необхідно забезпечувати цілісність і доступність даних.

Ризики інформаційної безпеки або IT-ризики, пов’язані з будь-якою небезпекою для безпеки інформаційних технологій. Хоча інформація, вже давно вважається цінним активом, зростання економіки знань привів до того, що організації стають все більш залежними від інформації і результатів її обробки. Різні загрози або інциденти, які ставлять під загрозу інформацію, можуть привести, до несприятливих наслідків в організації, починаючи від несуттєвих проблем і закінчуючи катастрофічними.

Для оцінки і вимірювання IT-ризиків використовується імовірнісна оцінка різних типів загроз і/або інциденту з їх прогнозованим впливом або наслідками. Альтернативні методи вимірювання IT-ризиками включають оцінку інших сприяючих факторів, таких як загрози, вразливості, ризики і вартість активів.

Уразливості в безпеці мережі можна назвати «м’якими місцями», які присутні в кожній мережі й окремих мережевих пристроях.

Розрізняють три основних типи вразливостей [1]:

– недоліки мережевих технологій;

– недоліки конфігурацій;

– недоліки політики безпеки.

Недоліки технологій включають в себе недоліки протоколу TCP / IP, вразливості операційної системи, слабкі сторони і вразливості мережевого обладнання. У таблиці 1.2 надано опис цих вразливостей.

Таблиця 1.2 – Опис недоліків технологій

Ідентифікатор	**Недоліки**	**Опис**
В1.1	Вразливості протоколу TCP/IP	Протоколи TCP/IP, HTTP, FTP, ICMP за своєю суттю незахищенні.
В1.2	Вразливості ОС	ОС UNIX, Linux, Macintosh, Windows мають внутрішні проблеми безпеки, які не вирішені
В1.3	Вразливості мережевого обладнання	Різні типи мережевого обладнання, такі як маршрутизатори, між мережеві екрани і т.д. мають наступні недоліки: відсутність парольного захисту; відсутність аутентифікації; протоколи маршрутизації; недоліки в захисті Firewall.

Недоліки та вразливості конфігурації мережі надані в таблиці 1.3 та вразливості в політиці безпеки зведено до таблиці 1.4.

Таблиця 1.3 – Вразливості конфігурації

Ідентифікатор	**Недоліки**	**Опис**
B2.1	Незахищений дані користувачів	Передачі по мережі незахищених даних користувача (логін, пароль і т.д.)
B2.2	Помилки в конфігурації інтернет-сервісів	Дозвіл на використання JavaScript в браузерах, дозволяє виробляти атаки з підозрілих сайтів. Використання IIS, Apache, FTP і служби терміналів також створюють проблеми безпеки.
B2.3	Використання слабких паролів в призначених для користувача облікових записів	Використання слабких або легко вгадуваних паролів
B2.4	Використання попередньо встановлених налаштувань безпеки в ПП	Більшість програмних продуктів мають налаштування за замовчуванням безпеки, які часто не відповідають необхідному рівню безпеки.
B2.5	Використання стандартних налаштувань мережевого обладнання	Неправильна конфігурація мережевого обладнання може призвести до значних проблем безпеки. Наприклад, помилки в конфігурації списків доступу, помилки в налаштуванні протоколів маршрутизації. Відсутність шифрування і управління віддаленим доступом може також завдати значної шкоди безпеці.

Таблиця 1.4 – Вразливості в політиці безпеки

Ідентифікатор	**Недоліки**	**Опис**
В3.1	Незахищені дані користувачів	Передачі по мережі незахищенних даних користувача (логін, пароль і т.д.)
В3.2	Використання слабких паролів в призначених для користувача облікових записів	Використання слабких або легко вгадуються паролів
В3.3	Використання попередньо встановлених налаштувань безпеки в програмних продуктах	Більшість програмних продуктів мають встановлені параметри, параметри безпеки, які часто не відповідають необхідному рівню безпеки.
В3.4	Використання стандартних налаштувань мережевого обладнання	Неправильна конфігурація мережевого обладнання може призвести до значних проблем безпеки. Наприклад, помилки в конфігурації списків доступу, помилки в налаштуванні протоколів маршрутизації. Відсутність шифрування і управління віддаленим доступом може також завдати значної шкоди безпеці.

Недоліки політики безпеки можуть призвести до непередбачуваних загроз безпеки. Загрози мережевої безпеки можуть виникнути якщо користувачі не виконують політику безпеки. Таблиця 1.5 демонструє деякі загальні недоліки політики безпеки.

Таблиця 1.5 – Вразливості політики безпеки

Ідентифікатор	**Недоліки**	**Опис**
В4.1	Недоліки в існуючій політиці безпеки	Відсутність політики безпеки або наявність в ній помилок.
В4.2	Відсутність наступності	Слабкі паролі, паролі, які легко зламуються або паролі за замовчуванням, відкривають несанкціонований доступ до мережі.

Продовження таблиці 1.5

В4.3	Відсутність логічного контролю доступу	Недостатній контроль і аудит за доступом до мережі дозволить зловмисникам проводити атаку на мережеві ресурси.
В4.4	Установка і модернізація апаратного обладнання та ПЗ без урахування політики безпеки	Установки неавторизованого програмного забезпечення або апаратного обладнання без використання політики безпеки призводить до виникнення вразливостей в інформаційній безпеки компанії.

За наявності права постійного або разового доступу до контрольованої зони (КЗ) локальної обчислювальної мережі (ЛОМ) порушники поділяються на два типи:

1) порушники, які не мають доступу до ЛОМ, що реалізують загрози з зовнішніх мереж зв'язку загального користування і (або) мереж міжнародного інформаційного обміну – зовнішні порушники.

2) порушники, які мають доступ до ЛОМ, включаючи користувачів ЛОМ, що реалізують загрози безпосередньо в ЛОМ – внутрішні порушники.

Можливості зовнішнього порушника (для всіх типів):

1) здійснювати несанкціонований доступ до каналів зв'язку, які виходять за межі службових приміщень;

2) здійснювати несанкціонований доступ через автоматизовані робочі місця, підключені до мереж зв'язку загального користування і (або) мереж міжнародного інформаційного обміну;

3) здійснювати несанкціонований доступ до інформації з використанням спеціальних програмних впливів за допомогою програмних вірусів, шкідливих програм, алгоритмічних або програмних закладок;

4) здійснювати несанкціонований доступ через елементи інформаційної інфраструктури ЛОМ, які в процесі свого життєвого циклу (модернізації, супроводження, ремонту, утилізації) виявляються за межами контрольованої зони;

5) здійснювати несанкціонований доступ через інформаційні системи взаємодіючих відомств, організацій та установ при їх підключенні до ЛОМ.

Таким чином, проведені дослідження дозволили виділити 7 основних типів загроз безпеки інтернет-магазину:

– викрадення бази даних клієнтів (для зняття грошей з їх рахунків, передачі конкуренту та т.д.);

– шахрайство з електронними платежами;

– внесення зловмисних змін в каталог товарів (наприклад, зміна цін або описів товарних позицій);

– втручання в процес роботи магазину (перенаправлення потоку клієнтів на інші ресурси, дефейсінг (заміна головної сторінки інтернет-магазину на іншу сторінку, вигідну шахраєві і т.д.);

– впровадження шкідливого коду в сторінки магазину (для крадіжки реквізитів кредитних карт, створення мережі заражених комп'ютерів і т.д.);

– вивід магазину з ладу шляхом прямого втручання, здійснення DDoS-атак (напрямок численних запитів на сайт магазину, що призводять до зупинки його роботи) і т.д.;

– поява «сайту-паразита», що використовує ресурси і популярність магазину, яка призводить до уповільнення його роботи і зниження його місця в пошуковій видачі.

Для нейтралізації даних загроз потрібен серйозний аналіз захищеності інтернет-магазину, який більшість власників відносно невеликих магазинів не можуть собі дозволити.

Крім цього також необхідно брати до уваги крадіжки з боку персоналу і можливе проникнення на територію складу сторонніх.

Для оцінки ризиків інформаційної безпеки (ІБ) в компанії використовується розрахункова методика. Дана методика призначена для проведення оцінки ризиків ІБ в рамках побудови або вдосконалення системи ІБ.

Методика дозволяє визначити чисельний показник ризику ІБ з метою прийняття ефективних заходів щодо захисту інформації. Узагальнений алгоритм проведення оцінки ризиків ІБ представлений на рисунку 1.2.

Рисунок 1.2 – Алгоритм проведення оцінки ІБ

Процедури оцінки ризиків ІБ як комплексного підходу виконуються співробітниками підприємства спільно з керівною ланкою.

1.3. Оцінка існуючих і планованих засобів захисту

В інтернет-магазині ІТ-послуг «ГІГАБАЙТ+» використовуються всі види інформаційних технологій, апаратні, програмні та організаційні.

Апаратні технології представлені в компанії:

- серверним обладнанням зберігання і обробки даних;

- термінальним обладнанням, а саме персональними комп'ютерами для доступу до інформації;

- мережним устаткуванням, тобто мережевими комунікаціями, обладнанням для комп'ютерних і телефонних мереж (комутатори, маршрутизатори і т.д.);

Програмне забезпечення представлено в компанії величезним спектром програм. Використовуються операційні системи сімейств Windows і Linux. Застосовуються бази даних MySQL 5.6.5 M8. Для управління підприємством використовується платформа 1С: Підприємство 8.1. Так само використовується величезна кількість допоміжних програм і утиліт, таких як: MS Office, антивірусні програми, програми резервного копіювання, електронна пошта і т.д. Для підтримки роботи з клієнтами використовуються можливості CRM Бітрікс 24.

Організаційне забезпечення полягає, по-перше, в плануванні, розробці та впровадженні нових рішень, спрямованих на підвищення ефективності діяльності

підприємства. Так само сюди входять заповнення і обробка баз даних співробітниками фірми, підтримка сайту компанії в актуальному стані.

Таким чином, в даний час неможливо уявити жодної сфери діяльності людини без застосування інформаційних технологій.

У час стрімкого прогресу інформаційних технологій, збільшення швидкодії апаратури, оновлення та появи нових програмних засобів, а також удосконалення методів взаємодії з ними, потрібно бути постійно в курсі подій. У компанії «ГІГАБАЙТ+», ведеться постійний збір і аналіз інформаційних технологій, в результаті необхідні нововведення впроваджуються в робочий процес. Так само з розвитком компанії, і появою нових сфер діяльності, застосовуються нові технології.

Однією з найважливіших ролей в компанії грає апаратне забезпечення. Її основні складові: робочі станції співробітників, сервери, мережеве обладнання та телефонія (АТС, телекомунікації, телефонні апарати).

У компанії для роботи співробітників використовуються офісні персональні комп'ютери з операційними системами сімейства Windows, а саме Windows XP, 7, 10. Станції мають вихід в локальну мережу компанії, в глобальну мережу – Інтернет. Так само, за допомогою них здійснюється обробка документації, доступ до баз даних, робота з сайтом компанії, робота з електронною поштою і т.д.

Є два сервера, на операційних системах сімейства Windows і Linux, використовуваних для різних цілей компанії. Вони застосовуються як WEB-сервери, сервери баз даних, сервери зберігання інформації, поштові сервери, термінальні сервери.

Як мережеве обладнання використовуються комутатор компанії Cisco. Так само апаратним шляхом, через firewall-маршрутизатор Cisco локальна мережа компанії пов'язана з мережею Інтернет (рисунок 1.3).

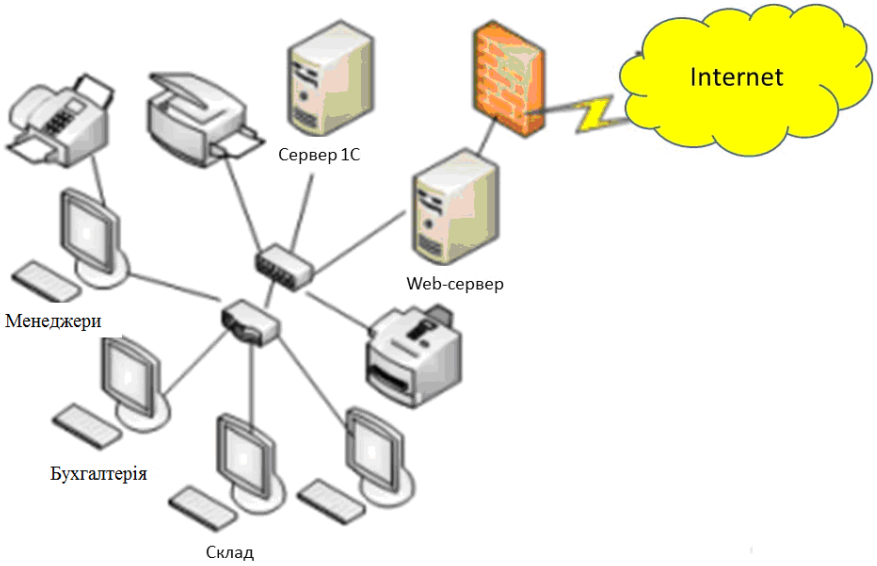

Рисунок 1.3 – Коротка схема мережі компанії

Для роботи в компанії використовується велика кількість як стандартного, так і спеціалізованого програмного забезпечення. Основним, базовим програмним забезпеченням є операційна система. На комп'ютерах користувачів використовуються ОС сімейства Windows, а саме Windows XP, 7 та 10. Так само на робочих станціях користувачів, встановлені основні програми для офісної роботи, а саме:

- Для роботи з електронними документами, презентаціями, таблицями використовується програми MS Office, AdobeReader.

- Для листування, як всередині офісу, так і з клієнтами компанії використовується програма для роботи з електронною поштою – TheBat! та Skype – програма, що забезпечує текстовий і голосовий зв'язок.

- Для роботи з бухгалтерською документацією та забезпечення складського обліку використовується система 1С Підприємство 8.1.

- Всі призначені для користувача комп'ютери захищені антивірусною програмою Kaspersky Endpoint Security for Windows workstations.

- Так само встановлені допоміжні утиліти типу: WinRAR, Ccleaner і ін.

Самим основним обладнанням є сервери. За допомогою них здійснюється вся основна робота фірми. На них зберігається і обробляється практично вся найважливіша інформація. Основою програмного забезпечення на серверах є

операційна система. У фірмі використовуються операційні системи сімейства Windows і Linux.

Linux представлений операційною системою Ubuntu Server. На сервері реалізовано резервне копіювання баз даних, встановлений FTP сервер, на якому зберігаються резервні копії документів працівників компаній. Він забезпечує користувачам доступ до документів як на робочому місці, так і в будь-якій точці, де є інтернет. На Ubuntu Server реалізований WEB-Server. Для цього, встановлено сервер Apache, PHP, база даних MySQL 5.6.5 M8. На даному WEB-сервері розташований сайт компанії.

На серверах Windows встановлена операційна система Windows 2003 Server. Там реалізовані сервери баз даних і сервери терміналів. Термінальний доступ на сервери здійснюється як за допомогою вбудованих засобів Windows, а саме windows remote desktop services, так і за допомогою програми стороннього виробника – Citrix MetaFrame. На серверах під Windows встановлені основні робочі програми 1С Підприємство 8.1.

Система програм «1С: Підприємство» є платформою і прикладним рішенням, яке використовується для автоматизації діяльності організацій і приватних осіб. Платформа забезпечує інструментарій для розробки та підтримки програмних рішень кінцевих користувачів. Такий підхід дає можливість створювати автоматизовані рішення для різних бізнес-процесів компаній і організацій, з використанням єдиної технологічної платформи. Платформа 1С: Підприємство є гнучким інструментом, який дозволяє створювати інформаційні системи в різних областях:

– автоматизація виробничих і торгових підприємств, бюджетних і фінансових організацій, підприємств сфери обслуговування і т.д .;

– підтримка оперативного управління підприємством;

–автоматизація організаційної і господарської діяльності;

– ведення бухгалтерського обліку з декількома планами рахунків і довільними вимірами обліку, регламентована звітність;

– широкі можливості для управлінського обліку і побудови аналітичної звітності, підтримка багатовалютного обліку;

– вирішення задач планування, бюджетування і фінансового аналізу;

– розрахунок зарплати і управління персоналом.

В компанії «ГІГАБАЙТ+» планується наступний набір заходів захисту:

– ІАФ (Ідентифікація та Аутентификация суб'єктів доступу і об'єктів доступу) – забезпечуються програмними засобами ОС: Windows XP, Windows 7, Windows 8, Ubuntu 14, Windows 2003 Server.

– УПД (Управління доступом суб'єктів доступу до об'єктів доступу) програмними засобами ОС: Windows XP, Windows 7, Windows 8, Ubuntu 14, Windows 2003 Server.

– ОПС (Обмеження програмного середовища) – здійснює штатний системний адміністратор організації.

– ЗМН (Захист машинних носіїв персональних даних) – забезпечуються відповідальним за організацію обробки даних.

– РПБ (Реєстрація подій безпеки).

– АВЗ (Антивірусний захист) – забезпечуються сертифікованим антивірусним засобом, встановленим штатним системним адміністратором організації. (Kaspersky Endpoint Security for Windows workstations)

– ВВ (Виявлення вторгнень) – забезпечуються обраними антивірусом (Антивірус Касперського).

– АЗ (Контроль (аналіз) захищеності персональних даних) – забезпечуються штатним адміністратором організації.

– ЗЦІ (Забезпечення цілісності інформаційної системи і персональних даних) – забезпечуються штатним адміністратором організації.

– ЗД (Забезпечення доступності персональних даних) – забезпечуються штатним адміністратором організації.

– ЗСВ (Захист середовища віртуалізації) – забезпечуються програмними засобами ОС: Windows XP, Windows 7, Windows 8, Ubuntu 14 і штатним адміністратором організації.

– ЗІС (Захист інформаційної системи, її засобів, систем зв'язку і передачі даних) – забезпечується захищеним каналом зв'язку з шифруванням інформації, яка передається за ним.

– ЗТС (Захист технічних засобів) – забезпечуються відповідальним за організацію обробки даних.

Один з найважливіших факторів, що впливають на ефективність системи захисту конфіденційної інформації, – сукупність сил і засобів підприємства, які використовуються для організації захисту інформації.

Сили і засоби різних підприємств відрізняються за структурою, характером і порядку використання. Так, як компанія працює з конфіденційною інформацією лише періодично, і захист інформації не є основною діяльністю компанії, то замість створення підрозділів в компанії включені окремі фахівці із захисту інформації. Дані підрозділи і посади є органами захисту інформації. Відповідальні особи компанії представлені в таблиці 1.6.

Таблиця 1.6 – Перелік довірених осіб

Довірені користувачі	Обґрунтування
Штатний програміст організації	Рекомендації з попередніх місць роботи Чи не був звільнений з попередніх посад через втрату довіри Достатній досвід роботи Підписав зобов'язання про нерозголошення конфіденційної інформації
Штатний адміністратор організації	Рекомендації з попередніх місць роботи Чи не був звільнений з попередніх посад через втрату довіри Достатній досвід роботи Підписав зобов'язання про нерозголошення конфіденційної інформації
Адміністратор безпеки	Рекомендації з попередніх місць роботи Чи не був звільнений з попередніх посад через втрату довіри Достатній досвід роботи Підписав зобов'язання про нерозголошення конфіденційної інформації
Оператор, що діє в рамках повноважень	Здійснення доступу до частини даних відповідно до посадових обов'язків Підписав зобов'язання про нерозголошення конфіденційної інформації

Діяльність підприємства забезпечується наступними технічними засобами, які надано в таблиці 1.7.

Таблиця 1.7 – Технічні характеристик апаратних засобів

Назва	Характеристика
Сервер баз даних	Сервер IBM x3500 Xeon Quad-Core E5430 2.66GHz/1333MHz 12MB L2 2X512MB O/Bay 2,5" HS SAS 8k DVD-ROM 835W p/s Процесор Express Quad-Core Intel Xeon Processor E5430 2.66GHz Модуль пам’яті 4 GB (2x2GB) PC2-5300 667 MHz ECC Chipkill DDR2 FBDIMM Жорсткий диск SAS 146GB HS 2.5" 10K RPM HDD
Веб-сервер	Сервер IBM x3650 1x Quad-Core Xeon E5430 2.66 GHz/1333 MHz 12MB L2 2x2GB PC2-5300 DDR2 Chipkill SDRAM, 0 GB HD (open bay) 2,5", SR 8k, CD-RW/DVD-ROM Combo, 2x Broadcom Gigabit Ethernet, ATI RN50 video (16 MB), 1x 835 W power supply 1 Модуль пам’яті 4 GB (2x2GB) PC2-5300 667 MHz ECC Chipkill DDR2 FBDIMM Жорсткий диск 146GB Hot-Swap 2.5" 10K RPM Ultra320 SAS HDD
Клієнтські комп’ютери	POWERMAN ES722BK Intel Celeron J1800 2400MHz DDR3 4 Гб Hynix 60 Gb SSD SB60 Відео-карта: Вбудована БП FSP 400W
Маршрутизатор	Dlink DSR-1000 2 порти WAN 10/100/1000Base-T 4 порти LAN 10/100/1000Base-T 2 порти USB 2.0 Консольний порт с роз'ємом RJ-45
Точка доступу	Точка доступу D-Link < DAP-2310 > AirPremier N Access Point (1UTP 10 / 100Mbps, 802.11b / g / n, 300Mbps) Характеристики: 2.4 ГГц N300 Мбит/сек Wireless 2 антени WDS-Bridge, Adapter, AP Фільтрація з MAC-адресами WPA2-Enterprise, WPA-Enterprise, WPA2-Personal, WPA-Personal, WEP-кодування с 64- або 128-бітним ключем
БФП	Лазерний БФП Panasonic KX-MB2000RUB Лазерний БФП Brother DCP-1510R
Джерело безперебійного живлення	БП Redundant power supply HS 835W БП Express Redundant Power and Cooling Option (39Y8487) x3400/x3500

Приклад технічної архітектури компанії наведено на рисунку 1.4.

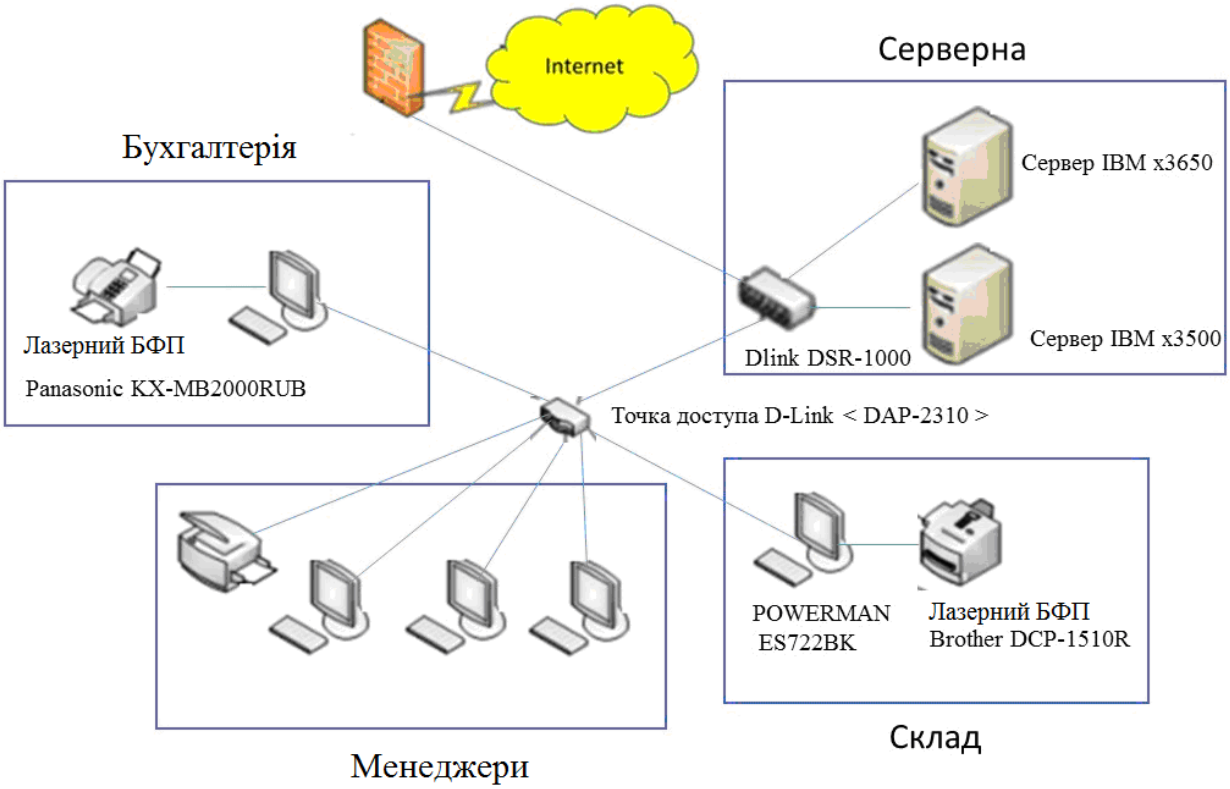

Рисунок 1.4 – Приклад технічної архітектури компанії

Технічні характеристики програмного забезпечення компанії зображено в на рисунку 1.5.

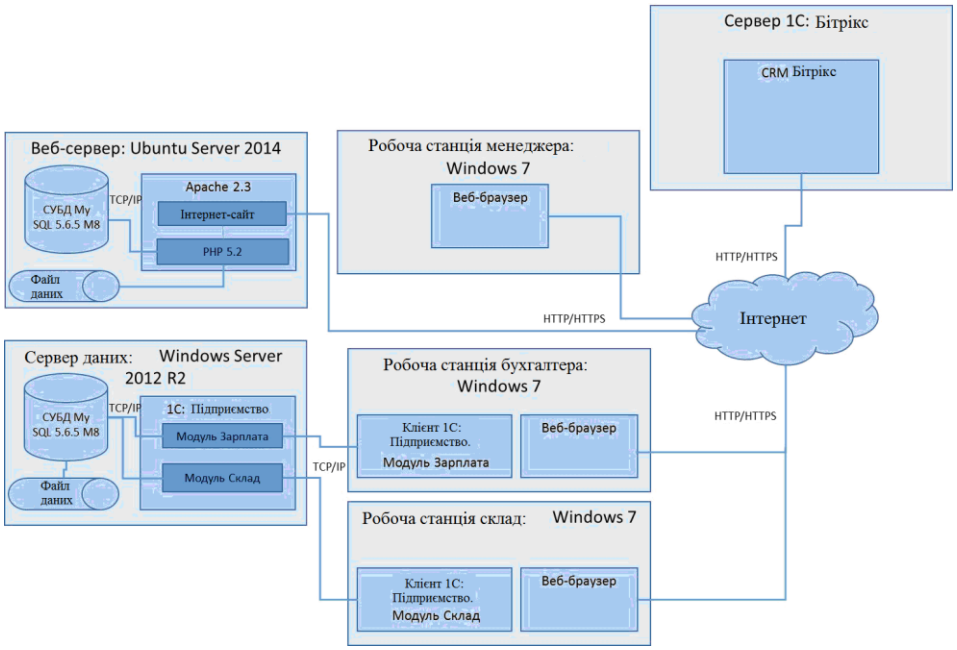

Рисунок 1.5 – Програмне забезпечення компанії

1.4 Оцінка ризиків інформаційної безпеки

Найбільш часто для розрахунку ризиків, використовується формула, яка включає в себе наступні параметри:

– вартість ресурсу (Asset Value, AV). Дана величина показує цінність ресурсу. При якісній оцінці ризиків вартість ресурсу найчастіше ранжується в діапазоні від 1 до 3, де 1 – мінімальна вартість ресурсу, 2 – середня вартість ресурсу і 3 – максимальна вартість ресурсу. У нашому випадку сервер баз даних і веб-сервер матимуть значення AV = 3, тоді як клієнтські комп'ютери мають AV = 1 по відношенню до інформаційної системи інтернет-магазину;

– міра вразливості ресурсу до загрози (Exposure Factor, EF). Цей параметр показує, в якому ступені той чи інший ресурс вразливий по відношенню до даної загрози. У нашому випадку ресурс інтернет-магазин має найбільшу доступність. Тому атаки, спрямовані на реалізацію відмови в обслуговуванні (Denial of Service, DoS) представляють для нього максимальну загрозу. При якісній оцінці ризиків дана величина також ранжуватись в діапазоні від 1 до 3, де 1 – мінімальна міра вразливості (слабкий вплив), 2 – середня (ресурс підлягає відновленню), 3 – максимальна (ресурс вимагає повної заміни після реалізації загрози);

– оцінка ймовірності реалізації загрози (Annual Rate of Occurrence, ARO) демонструє, наскільки ймовірна реалізація певної загрози за певний період часу (як правило, протягом року) і також ранжируется за шкалою від 1 до 3 (низька, середня, висока).

На підставі отриманих даних виводиться оцінка очікуваних втрат (рівень ризику):

– оцінка очікуваного можливого збитку від одиничної реалізації певної загрози (Single Loss Exposure, SLE) розраховується за формулою:

SLE = AV x EF;

– підсумкові очікувані втрати від конкретної загрози за певний період часу (Annual Loss Exposure, ALE) характеризують величину ризику і розраховується за формулою:

ALE = SLE x ARO.

Таким чином, кінцева формула розрахунку ризиків являє собою добуток:

ALE = ((AV x EF = SLE) x ARO).

Результати розрахунку зведено до таблиці 1.8.

Таблиця 1.8 – Результати оцінки ризиків інформаційних активів підприємства

Ризик	Актив					Ранг ризику
	База даних	Фінансова звітність	Веб-сервер (апаратна частина)	ПЗ сервера	ПЗ інтернет-магазину	
Викрадення БД	3	3	1	2	2	Високий
Шахрайство з платежами	2	3	1	1	1	Низький
Шкідливий код	2	2	1	2	2	Середній
DDoS атака	1	1	1	3	3	Середній
Сайт-паразит	1	1	1	2	3	Низький
Фізичне пошкодження обладнання	1	1	3	1	1	Низький

Проведений аналіз показав, що найбільш вразливими є база даних і програмне забезпечення інтернет-магазину і серверів баз даних і веб-сервера.

1.5 Висновки до розділу 1

У сучасному інформаційному просторі в умовах постійного нарощування обсягів атак через мережу стоїть особливо гостро.

З метою зниження ризиків безпеки передбачається використання віртуалізації. На сьогоднішній день віртуалізація є найперспективнішою технологією для технологій корпоративного сектора. Використання віртуального

середовища підприємства дає можливість знизити капітальні та експлуатаційні витрати. Це зниження досягається через економію витрат на обладнання, економії електроенергії і площ серверних приміщень, а також зниження людських ресурсів на адміністрування серверів. Сьогодні багато компаній у всьому світі переводять свої обчислювальні ресурси на віртуальну платформу. В роботі планується виконати побудова захищеної інформаційної системи з використанням програмного продукту VMware vSphere vStorage Appliance (VSA). Планується створення декількох мереж в межах одного хоста ESXi для інтернет-магазину.

2 ДОСЛІДЖЕННЯ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ І ЗАХИСТУ ІНФОРМАЦІЇ НА ПІДПРИЄМСТВІ

2.1 Характеристика комплексу задач, завдання та обґрунтування необхідності вдосконалення системи забезпечення інформаційної безпеки і захисту інформації на підприємстві

2.1.1. Вибір комплексу задач забезпечення інформаційної безпеки

Найбільш важливими засобами і методами щодо забезпечення заходів захисту даних є організаційні. Для найбільш повного і глибокого аналізу що відбуваються в сфері захисту конфіденційної інформації процесів є розуміння сутності планованих заходів. Перш за все необхідно розглянути одне з найважливіших напрямків захисту конфіденційної інформації – організаційний захист інформації.

Основою захисту інформації в організації є організаційний захист інформації. Зі створення нормативних документів і політики підприємства з організації захисту даних починаються усі заходи в організації захисту конфіденційної інформації підприємства.

Спільно з організаційним також необхідно забезпечити правовий та інженерно-технічний захист інформації на підприємстві.

Однак основою, ядром системи захисту інформації (СЗІ), на підприємстві, є організаційний захист.

Організаційний захист інформації визначає набір конкретних сил і засобів, які покликані реалізувати заходи щодо захисту даних на підприємстві, які сплановані і описані в політиці безпеки підприємства. Ці заходи вживаються в залежності від конкретної ситуації на підприємстві, пов’язаної з наявністю можливих загроз, що впливають на захист інформації і ведуть до її витоку.

Для розробки заходів, пов’язаних з політикою безпеки, є:

– планування заходів щодо захисту інформації;

– персональний контроль за їх виконанням;

– прийняття рішень за безпосереднім доступом до конфіденційної інформації своїх співробітників і представників інших організацій;

– розподіл обов'язків і завдань між посадовими особами та структурними підрозділами;

– аналітична робота і т.д.

Для визначення організаційного захисту даних використовуються два приблизно рівнозначних визначення.

Організаційний захист інформації – складова частина системи захисту інформації, яка визначає і виробляє порядок і правила функціонування об'єктів захисту і діяльності посадових осіб з метою забезпечення захисту інформації.

Організаційний захист інформації на підприємстві – регламентація виробничої діяльності та взаємовідносин суб'єктів (працівників підприємства) на нормативно-правовій основі, що виключає або послаблює нанесення збитку даному підприємству.

У першому визначенні визначається сутність організаційної захисту інформації. Друге визначає структуру СЗІ на рівні підприємства. До того ж обидва визначення визначають важливість нормативно-правового регулювання питань захисту інформації разом з комплексним підходом до використання в цих цілях наявних сил і засобів. Основними етапами організаційної захисту інформації є:

– організація роботи з персоналом;

– організація всередині об'єктового та пропускного режимів і охорони;

– організація роботи з носіями відомостей;

– комплексне планування заходів щодо захисту інформації;

– організація аналітичної роботи та контролю.

Основні принципи організаційного захисту інформації:

– принцип комплексного підходу – ефективне використання сил, засобів, способів і методів захисту інформації для вирішення поставлених завдань в залежності від конкретної ситуації, що складається з наявності факторів, що послаблюють або підсилюють загрозу захисту;

– принцип оперативності прийняття управлінських рішень (істотно впливає на ефективність функціонування та гнучкість системи захисту інформації та

відображає націленість керівництва і персоналу підприємства на вирішення завдань захисту інформації);

– принцип персональної відповідальності – найбільш ефективний розподіл завдань по захисту інформації між керівництвом і персоналом підприємства і визначення відповідальності за повноту і якість їх виконання.

Серед основних умов організаційного захисту інформації можна виділити наступні:

– безперервність всебічного аналізу функціонування системи захисту інформації в цілях прийняття своєчасних заходів по підвищення її ефективності;

– неухильне дотримання керівництвом та персоналом підприємства встановлених норм і правил захисту конфіденційної інформації.

Для забезпечення успішного вирішення завдань, пов’язаних із забезпеченням захисту інформації необхідно створити єдину систему захисту інформації. Така система є ядром безпеки підприємства, яка об’єднує всі ресурси і зусилля щодо запобігання загроз інформаційної безпеки підприємства та зменшення шкоди від цих загроз. Така система створюється з урахуванням діючих нормативно-правових документів та орієнтується на специфіку діяльності підприємства.

СЗІ – це об’єднання всіх компонентів підприємства, які відповідають за забезпечення захисту інформації: технічних засобів, методів захисту, нормативні документи і т.д.

Технічні засоби захисту інформації – пристрої (прилади), призначені для забезпечення захисту інформації, виключення її витоку, створення перешкод технічних засобів доступу до інформації, що підлягає захисту.

Криптографічні засоби захисту інформації – засоби (пристрої), що забезпечують захист конфіденційної інформації шляхом її криптографічного перетворення (шифрування).

Програмні засоби захисту інформації – системи захисту засобів автоматизації (персональних електронно-обчислювальних машин та їх комплексів) від зовнішнього (стороннього) впливу або вторгнення.

Ефективне вирішення завдань організації захисту інформації неможливо без застосування комплексу наявних у розпорядженні керівника підприємства відповідних сил і засобів. Разом з тим визначальну роль в питаннях організації захисту інформації, застосування в цих цілях сил і засобів підприємства відіграють методи захисту інформації, що визначають порядок, алгоритм і особливості використання даних сил і засобів в конкретній ситуації.

Методи захисту інформації – застосовуються з метою виключення витоку інформації універсальні і специфічні способи використання наявних сил і засобів (прийоми, заходи), що враховують специфіку діяльності захисту інформації.

Загальні методи захисту інформації поділяються на правові, організаційні, технічні та економічні.

Методи захисту інформації з точки зору їх теоретичної основи і практичного використання взаємопов’язані. Правові методи регламентують і всебічно нормативно регулюють діяльність щодо захисту інформації, виділяючи, насамперед, її організаційні напрямки. Тісний зв’язок організаційних і правових методів захисту інформації можна показати на прикладі рішення задач з виключення витоку конфіденційної інформації, зокрема це стосується комерційної таємниці підприємства, під час його взаємодії з різними державними та територіальними інспекторськими і наглядовими органами. Ці органи відповідно до наданих їм законом повноважень здійснюють діяльність з отримання, обробки та зберігання інформації про підприємства та громадян (що є його співробітниками).

Передача інформації, в установленому порядку віднесеної до комерційної таємниці або містить персональні дані працівника підприємства, повинна здійснюватися на основі договору, що передбачає взаємні зобов’язання сторін щодо нерозповсюдження (нерозголошення) цієї інформації, а також потребує заходи щодо її захисту.

2.1.2. Визначення місця проектованого комплексу завдань в комплексі завдань підприємства, деталізація завдань інформаційної безпеки і захисту інформації

Як показують дослідження темпи розвитку сучасних інформаційних технологій значно випереджають темпи розробки рекомендаційної і нормативно-правової бази керівних документів.

Використання сучасних методик оцінки інформаційної безпеки при проектуванні і супроводі корпоративних систем захисту інформації повинні забезпечувати діяльність компанії, пов’язану із забезпеченням захисту конфіденційної інформації [2].

Існуючі методики дозволяють:

– виконувати кількісну оцінку поточного рівня інформаційної безпеки компанії. Для цього необхідно визначити ризики в правовому, організаційно-управлінському, технологічному і технічному рівнях;

– розробляти і виконувати комплексний план з модернізації корпоративної системи захисту інформації. Удосконалення СЗІ дозволяє забезпечити задовільний рівень захищеності інформаційних активів компанії.

При розробці плану з модернізації корпоративної СЗІ необхідно вирішити такі завдання:

– визначити необхідні фінансові інвестиції, які використовуються для забезпечення безпеки. При цьому витрати повинні враховувати можливу шкоду від потенційних загроз і ймовірність їх виникнення;

– проінспектувати існуючий рівень безпеки компанії з метою блокування існуючих вразливостей;

– розробка необхідного комплексу організаційної документації для визначення зон відповідальності підрозділів і відповідальних осіб;

– розробити і узгодити з усіма зацікавленими службами і наглядовими органами проекту створення та розгортання СЗІ з урахуванням поточного рівня розвитку інформаційних технологій;

– забезпечити підтримку функціонування СЗІ з урахуванням зміни бізнес-процесів організації, змінами і виправленнями в організаційно-розпорядчої документації.

Розробка і впровадження комплексу заходів щодо захисту інформації дозволяє керівництву компанії:

– оцінювати поточну рівень інформаційної безпеки компанії;

– формувати єдиний набір правил і норм, які описують єдину концепцію безпеки;

– оцінити необхідні витрати на проектування, розробку і реалізацію захисту компанії.

Для керівників середньої ланки (начальники відділів і служб) цей план дозволить сформувати комплекс організаційних заходів, спрямованих на підвищення безпеки даних компанії.

Аналіз документообігу та комплектів організаційно-розпорядчої документації, виконується зазвичай в двох напрямках:

– аналіз документообігу компанії з грифом «конфіденційно»;

– розробка і поставка комплекту типової організаційно-розпорядчої документації з урахуванням вимог і рекомендацій корпоративної політики щодо інформаційної безпеки компанії.

Для виконання практичної реалізації заходів щодо впровадження політики інформаційної безпеки необхідно виконати наступні етапи:

– на підставі проведених досліджень корпоративної мережі, розробляється проект модернізації засобів захисту ІС;

– підготовка компанії до атестації

– оцінка документів компанії та розширення списку документів, які підлягають захисту;

– розробка набору нормативних документів, які відповідають рекомендаціям корпоративної політики інформаційної безпеки компанії.

Дуже великий вплив на рівень інформаційної безпеки компанії, надає кваліфікація співробітників, відповідальних за політику безпеки компанії багато в чому залежить від кваліфікації фахівців. Для підвищення рівня кваліфікації

співробітників необхідно проводити регулярні тренінги з використання СЗІ компанії, вивчення передового досвіду і технологій захисту даних і т.д.

Для підвищення рівня інформаційної безпеки компанії необхідно проводити регулярні дослідження поточного стану рівня захищеності.

Головна мета проектування та розробки СЗІ компанії полягають у забезпеченні сталого функціонування об'єкта:

– запобігання загроз його безпеки;

– захист законних інтересів власника інформації від протиправних посягань, у тому числі кримінально караних діянь у даній сфері відносин;

– забезпечення нормальної виробничої діяльності всіх підрозділів об'єкта.

Ще одне завдання, яке виконує СЗІ, є підвищення якості послуг, що надаються і гарантій безпеки майнових прав та інтересів клієнтів [3].

Для вирішення цих завдань необхідно:

– розподілити інформацію, яка використовується в бізнес-процесах підприємства, за відповідними категоріями обмеження доступу;

– виявити існуючі загрози і спрогнозувати можливі загрози безпеки інформаційних ресурсів компанії, виявити передумови та умови, які призводять до виникнення фінансового, матеріального і морального збитку, до порушення функціонування ІС компанії;

– забезпечити необхідні умови функціонування ІС з мінімізацією ймовірності виникнення загроз і зменшенням різних видів шкоди;

– розробити механізми і умови оперативного реагування на можливі загрози інформаційної безпеки;

– створити умови для максимально можливого відшкодування та локалізації збитку.

При виконанні робіт можна використовувати наступну модель побудови корпоративної системи захисту інформації, що наведена рисунку 2.1.

Рисунок 2.1 – Модель побудови корпоративної системи захисту інформації

2.2. Вибір захисних заходів

2.2.1. Вибір організаційних заходів

Організаційні механізми захисту інформації визначають порядок і умови комплексного використання наявних сил і засобів, ефективність якого залежить від застосовуваних методів технічного та економічного характеру.

Як підходу до створення системи захисту даних розглядається аналіз ризиків і вразливостей в захисті конфіденційної інформації. З цією метою складено список відповідальних осіб, а також перелік конфіденційних даних, які підлягають захисту.

Після проведеного аналізу до проектованої системі захисту інформації пред’являються такі вимоги:

– система повинна бути централізованою і забезпечувати ефективне управління системою з боку керівника і посадових осіб;

– система повинна дозволяти виконувати планування заходів в області захисту інформації;

– система повинна забезпечувати захист абсолютно конкретних інформаційних ресурсів, які є критичними для діяльності;

– система повинна забезпечувати активний захист конфіденційних даних;

– система повинна забезпечувати надійний і універсальний захист даних, які зберігаються і обробляються в ІС підприємства.

Керівник компанії і його заступник, який безпосередньо очолює роботу з організації захисту інформації, відіграють провідну роль у забезпеченні діяльності, спрямованої на організацію захисту персональних даних компанії.

Керівник компанії відповідає за діяльність, яка забезпечує організацію і проведення необхідних заходів, пов'язаних з блокуванням витоку відомостей, віднесених до конфіденційної інформації, і втрат носіїв інформації.

Керівник компанії повинен:

– мати уявлення про справжній стан справ в області захисту інформації;

– забезпечувати організаційні заходи, спрямовані на роботу з виявлення і закриття можливих каналів витоку конфіденційної інформації;

– складати посадові інструкції для відповідальних осіб і структурних підрозділів компанії, які відповідають за захист інформації;

– бути вимогливим по відношенню до персоналу в питаннях збереження конфіденційної інформації;

– мати можливість оцінити роботу відповідальних осіб і структурних підрозділів із забезпечення захисту персональних даних.

Заступник керівника підприємства повинен:

– постійно підвищувати свій професійний рівень в питаннях забезпечення захисту інформації;

– керувати роботою служби безпеки (інших структурних підрозділів, які вирішують завдання щодо захисту інформації);

– забезпечувати діяльність компанії, пов'язану з організацією захисту інформації.

У компанії для організації робіт із захисту інформації було створено підрозділ з технічного захисту інформації.

Функції підрозділу визначаються наказом керівника компанії і описуються у відповідних положеннях.

Підрозділ з технічного захисту інформації відповідає за вирішення завдань організації і проведення комплексу технічних заходів, спрямованих на виключення або суттєве ускладнення добування конкурентами відомостей, які є конфіденційною інформацією і які необхідно захищати.

Для забезпечення проведення робіт, пов'язаних з організацією захисту персональної інформації, можуть створюватися колегіальні органи (комісії), які створюються з метою вирішення окремих специфічних завдань із захисту даних. У компанії вже створені і функціонують такі комісії:

– технічна комісія;

– експертна комісія;

– комісія з розсекречення носіїв конфіденційної інформації;

– комісія з категорування об'єктів інформатизації та ін.

Для забезпечення максимального ефекту діяльності із захисту інформації необхідно використовувати всі наявні на підприємстві засоби захисту інформації.

До засобів захисту інформації відносяться:

– технічні;

– криптографічні;

– програмні та інші засоби і системи, розроблені і призначені для захисту конфіденційної інформації;

– засоби, пристрої та системи контролю ефективності захисту інформації.

Серед перерахованих методів захисту інформації особливо виділяються організаційні методи, спрямовані на вирішення наступних завдань:

– реалізація на підприємстві ефективного механізму управління, що забезпечує захист конфіденційної інформації та недопущення її витоку;

– здійснення принципу персональної відповідальності керівників підрозділів і персоналу підприємства за захист конфіденційної інформації;

– визначення переліків відомостей, що відносяться на підприємстві до різних категорій (видів) конфіденційної інформації;

– обмеження кола осіб, які мають право доступу до різних видів інформації в залежності від ступеня її конфіденційності;

– підбір і вивчення осіб, що призначаються на посади, пов’язані з конфіденційною інформацією, навчання та виховання персоналу підприємства, допущеного до конфіденційної інформації;

– організація і ведення конфіденційного діловодства;

– здійснення систематичного контролю за дотриманням встановлених вимог щодо захисту інформації.

2.2.2. Вибір інженерно-технічних заходів

Технічні засоби захисту інформації, які використовуються в комплексі з організаційними методами, відіграють велику роль в забезпеченні захисту інформації при її зберіганні, накопиченні і обробці з використанням засобів автоматизації. Технічні методи необхідні для ефективного застосування наявних в розпорядженні підприємства засобів захисту інформації, заснованих на нових інформаційних технологіях.

Мережева безпека складається з політик, яких було вжито для контролю авторизованого доступу, і запобігання несанкціонованого використання, зміни або блокування ресурсів комп’ютерної мережі. Мережева безпека включає в себе дозвіл на доступ до даних в мережі, контрольовані мережевим адміністратором [4]. Користувачі вибирають або їм призначають ідентифікатор і пароль, які дають їм доступ до інформації і програм в межах своїх повноважень. Мережева безпека охоплює різні комп’ютерні мережі, державні та приватні; політика мережевої безпеки забезпечує зв’язок і виконання сервісів підприємствами, державними установами та приватними особами. Мережі можуть бути приватні, такі як усередині компанії, і публічні, які відкриті для публічного доступу. Мережева безпека застосовується в організаціях, на підприємствах та інших установах. Найбільш поширеним і простим способом захисту мережевих ресурсів є присвоєння йому унікального імені та відповідного паролю доступу.

Мережева безпека починається з аутентифікації. Зазвичай для цього використовується ім’я користувача і пароль. Якщо при цьому потрібно тільки ім’я користувача та пароль, то така аутентифікація називається однофакторною. При двофакторній аутентифікації, користувач повинен підтвердити свою автентичність за допомогою маркера безпеки або «ключа», картки банкомату, коду, надісланого на мобільний телефон. Трифакторна аутентифікація використовується для підтвердження автентичності користувача його біометричні параметри (відбитки пальців або сканування сітківки ока).

Після аутентифікації, брандмауер забезпечує дотримання політик доступу до мережевих сервісів і ресурсів. Хоча брандмауер і є ефективним захистом від несанкціонованого доступу, але цей компонент може не перевірити потенційно небезпечний контент такий, як комп’ютерні хробаки або трояни, які передаються у мережі. Антивірусне програмне забезпечення або система запобігання вторгнень (IPS) допомагає виявити і пригнічити дію такого шкідливого програмного забезпечення. Виявлення аномалій, в мережевому трафіку, можуть допомогти такі програми, як аналізатор трафіку Wireshark. Ця програма може бути використана для цілей аудиту та подальшого аналізу трафіку.

Для збереження конфіденційності можна використовувати передачу зашифрованої інформації.

Для відволікання потенційних зловмисників можна створювати спеціальні приманки (Honeypots), які імітують доступні мережеві ресурси і слугують, як інструменти спостереження і раннього попередження вторгнення. При цьому методи, які використовуються зловмисниками, вивчаються вчасно і після нападу, для запобігання таких загроз в майбутньому. Такий аналіз може бути використаний для подальшого підвищення рівня безпеки в мережі. Прилади також можуть приховати від зловмисника робочі сервери. Прилади дають можливість зловмисникам витрачати свій час і енергію на помилковий сервер, а дані на реальному сервері не приваблюють їх увагу.

Управління безпекою в мережах відрізняється для всіх видів ситуацій. У домашній мережі або в мережі невеликого офісу достатньо тільки базової безпеки, тоді як великі підприємства можуть вимагати високого технічного

обслуговування і передових програмних і апаратних засобів для запобігання шкідливих атак від злому і спаму.

2.3 Висновки до розділу 2

Таким чином, у роботі для проектування та розробки СЗІ компанії полягають у забезпеченні сталого функціонування об’єкта та підвищення якості послуг, що надаються і гарантій безпеки майнових прав та інтересів клієнтів.

Для вирішення цих завдань необхідно:

– розподілити інформацію, яка використовується в бізнес-процесах підприємства, за відповідними категоріями обмеження доступу;

– виявити існуючі загрози і спрогнозувати можливі загрози безпеки інформаційних ресурсів компанії, виявити передумови та умови, які призводять до виникнення фінансового, матеріального і морального збитку, до порушення функціонування ІС компанії;

– забезпечити необхідні умови функціонування ІС з мінімізацією ймовірності виникнення загроз і зменшенням різних видів шкоди;

– розробити механізми і умови оперативного реагування на можливі загрози інформаційної безпеки;

– створити умови для максимально можливого відшкодування та локалізації збитку.

.

3 ПРАКТИЧНА ЧАСТИНА. ПРОЕКТУВАННЯ ПРОГРАМНО-АПАРАТНОГО КОМПЛЕКСУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ І ЗАХИСТУ ІНФОРМАЦІЇ ПІДПРИЄМСТВА

3.1 Комплекс проектованих програмно-апаратних засобів забезпечення інформаційної безпеки і захисту інформації підприємства

Віртуалізація відноситься до процесу створення віртуальної (замість фактичної) версії чого-небудь, в тому числі апаратних платформ віртуальних комп'ютерів, операційних систем, пристроїв зберігання даних, і комп'ютерних мережевих ресурсів.

Розглянемо модель (рис. 3.1) захищеної мережі на базі VMware vSphere 5.1 налаштованої на одному ESXi хості.

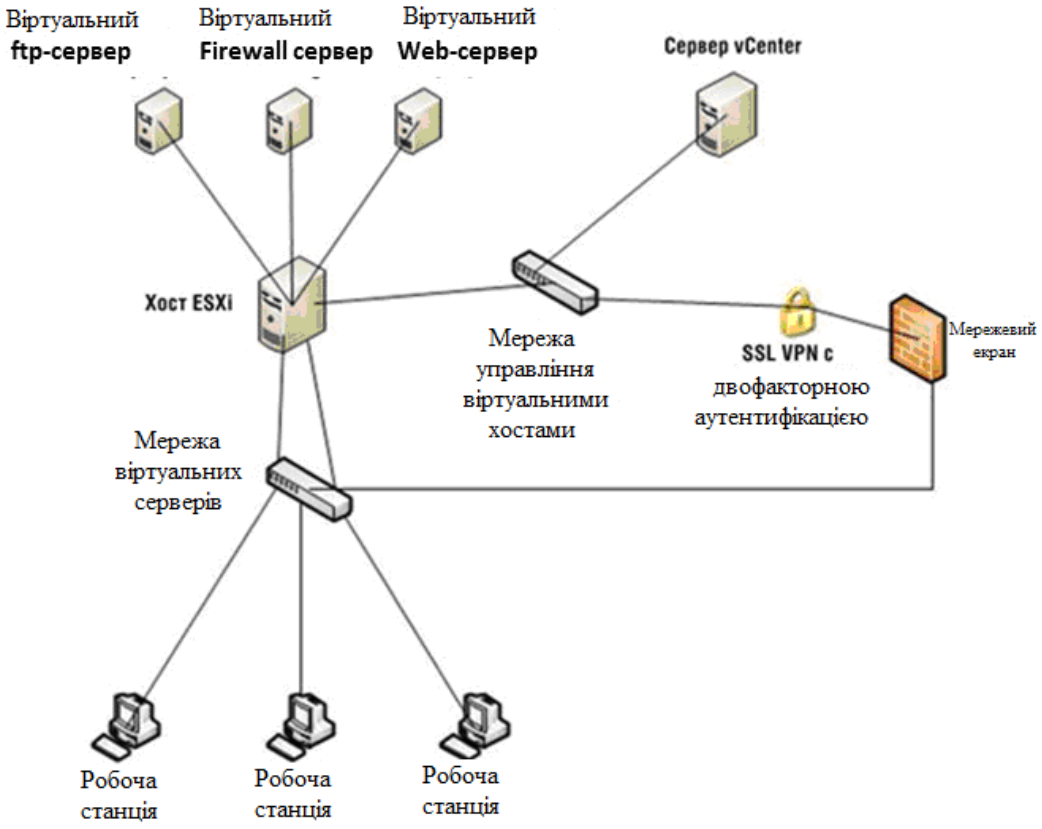

Рисунок 3.1 – Модель захищеності мережі налаштованої на одному ESXi хості.

VMware vSphere Storage Appliance 5.1 об’єднує в собі платформу віртуалізації і засоби управління. Програмний комплекс включає програмний гіпервізор корпоративного рівня VMware ESXi, призначений для віртуалізації серверів. Ним здійснюється поділ фізичних серверів на кілька віртуальних машин. Крім цього, до складу комплексу входить VMware vCenter, що є єдиною консоллю управління для всіх хостів ESXi і віртуальних машин.

Розглянемо принцип роботи компонентів програмного комплексу VMware vSphere 5.1.

Vsphere Storage Appliance (VSA) це програма, яка забезпечує можливості загального зберігання даних без збільшення вартості самого обладнання для зберігання (рис. 3.2–3.3).

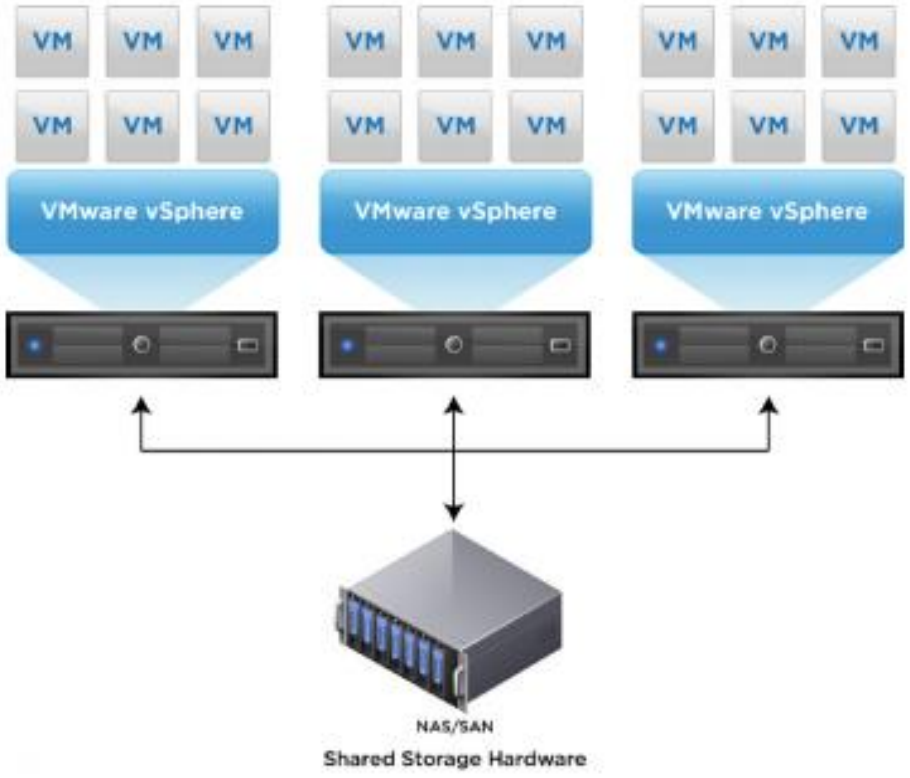

Рисунок 3.2 – Традиційна IT-інфраструктура підприємства

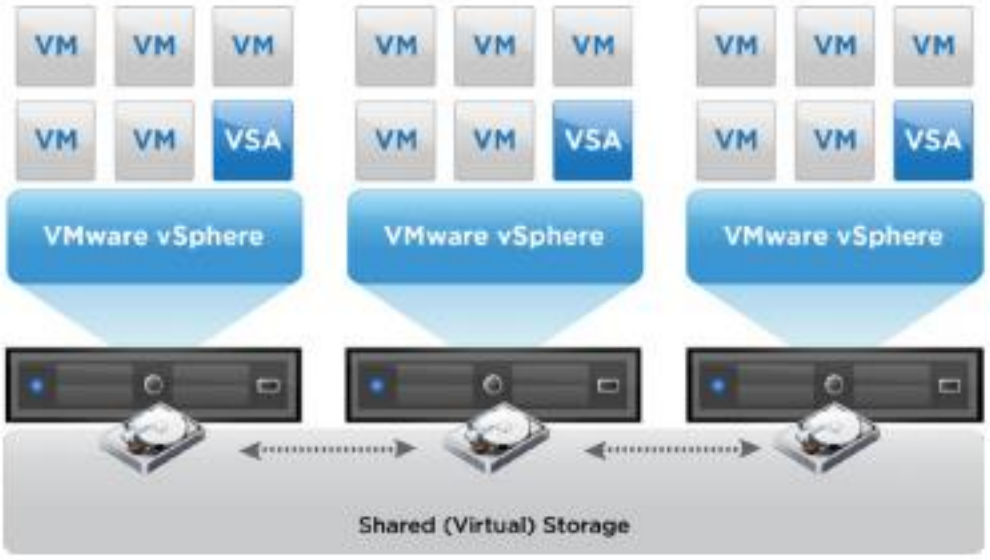

Рисунок 3.3 – IT-інфраструктура підприємства з VMware vSphere Storage Appliance

VSA кластер використовує обчислювальні ресурси і ресурси зберігання декількох ESXi хостів і надає набір сховищ даних, які доступні для всіх хостів в межах центру обробки даних.

Хост ESXi, що працює з Vsphere Storage Appliance і бере участь в кластері VSA є членом кластера VSA. З Vsphere Storage Appliance, можна створити кластер VSA з двома або трьома учасниками VSA кластеру.

VSA кластер дозволяє виконувати наступні функції:

– використання загальних сховищ даних для всіх хостів в центрі обробки даних;

– можливість створення загальної репліки для кожного сховища;

– використання Vsphere VMotion і Vsphere HA;

– підвищені апаратні і програмні можливості відмовостійкості і заміни елемента кластера VSA, що вийшов з ладу;

– відновлення існуючого VSA кластера.

Залежно від моделі ліцензування яка використовується можна мати кілька кластерів, керованих одним vCenter Server (рис. 3.4).

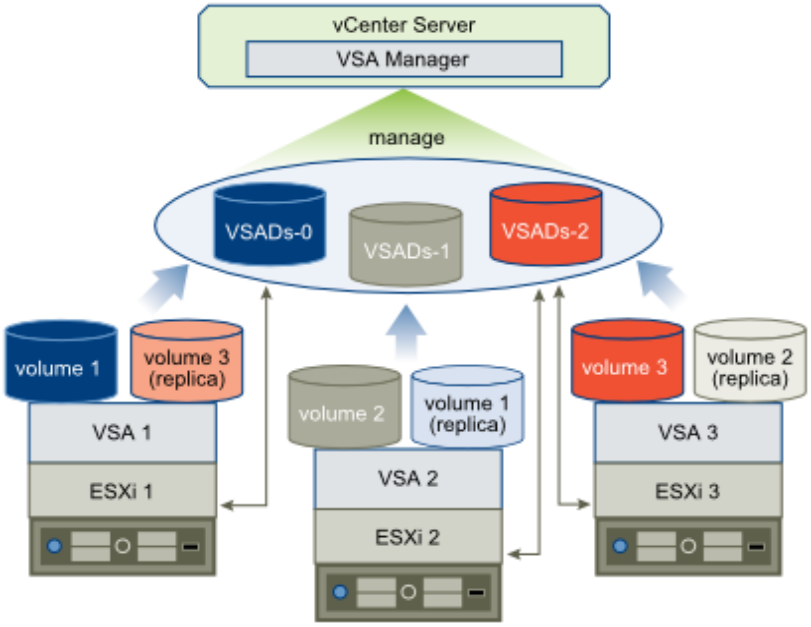

Рисунок 3.4 – vCenter Server архітектура

Для розгортання VSA кластера звернемо увагу на такі компоненти Vsphere і Vsphere Storage Appliance:

ESXi Hosts 2 або ESXi хост. Всі хости в кластері повинні мати ту ж версію ESXi. Також можна використовувати існуючі вузли, які мають віртуальні машини, запущені на локальних сховищах даних.

vCenter Server – це сервер фізичної або віртуальної машини, який керує всіма ESXi хостами, які беруть участь в кластері VSA. vCenter Server може працювати локально на одному або декількох ESXi хостах в кластері VSA. vCenter Server також може дистанційно керувати кількома кластерами VSA.

vSphere Web Client – це веб-додаток, який встановлюється на машини з мережевим доступом до vCenter Server. Клієнт дозволяє управляти кластером VSA з диспетчера VSA.

vSphere Storage Appliance – це VMware віртуальні пристрої, які запускають SUSE Linux Enterprise Server 11 SP2 забезпечує наступні завдання:

1) Управління ємністю, продуктивністю і даними для жорстких дисків, встановлених на ESXi хостах.

2) Управління апаратними й програмними збоями всередині кластеру VSA.

3) Управління зв’язками між усіма примірниками vSsphere Storage Appliance, і між vSphere Storage Appliance і менеджером VSA.

Тільки один vSphere Storage Appliance може працювати на хості ESXi.

VSA Manager розширення сервера, яке встановлюється на сервері в vCenter Server в режимі віртуальної машини.

VSA Cluster Member. ESXi, який запускає vSphere Storage Appliance в якості віртуальної машини. Це особливий тип віртуальної машини, що є функціональним членом VSA кластера, який виставляє сховище даних і підтримує сховища даних репліки.

VSA Cluster Service, служба яка встановлюється разом з VSA менеджером на vCenter Server, або окремо на різних платформах, в тому числі Windows Server 2003, Windows Server 2008, Windows 7, Linux RH, і SLES.

VSA Cluster Leader Vsphere Storage Appliance який повідомляє статус кластера VSA Менеджеру.

Ethernet Switches Gigabit Ethernet або 10 Gigabit Ethernet комутатори, які забезпечують високу швидкість магістральної мережі кластера VSA.

Архітектура кластера VSA включає в себе фізичні сервери, локальні жорсткі диски, ESXi в якості операційної системи фізичних серверів і віртуальних машин Vsphere Storage Appliance, на яких працюють служби кластеризації для створення томів, які експортуються як сховищ даних VSA.

Vsphere Storage Appliance підтримує створення кластера VSA з двома або трьома членами. Vsphere Storage Appliance використовує жорсткі диски хостів ESXi, щоб створити два томи того ж розміру. Vsphere Storage Appliance експортує один з томів як сховище. Інший том є точною копією тому, що експортується іншим Vsphere Storage Appliance з іншого хоста в кластері VSA.

VSA Кластер з двома ESXi хостами (рис. 3.5).

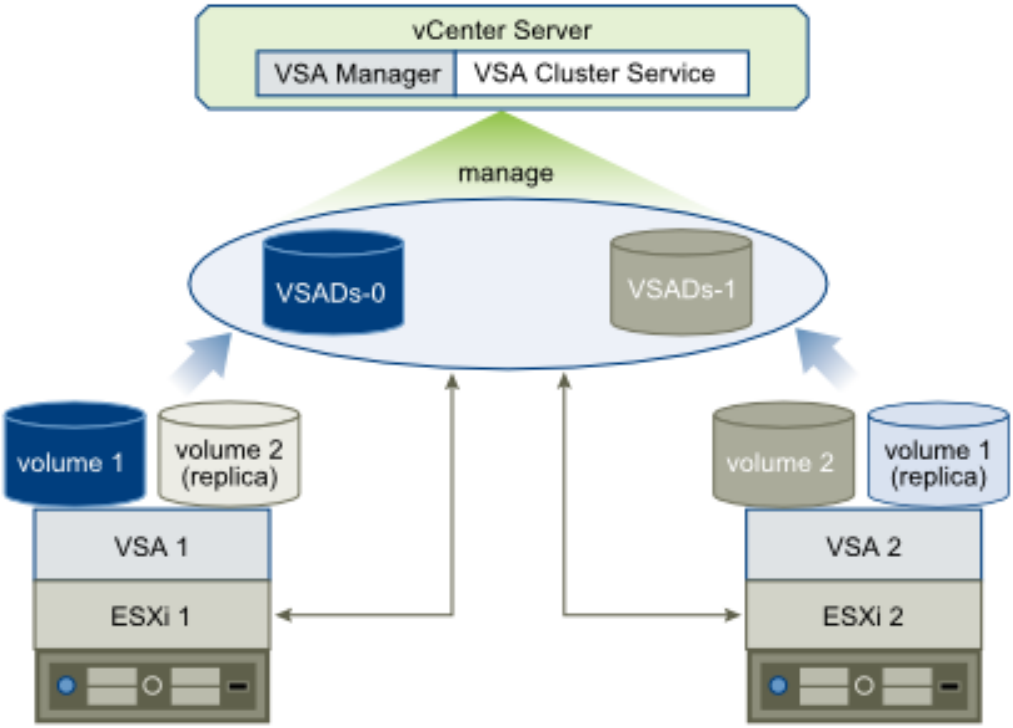

Рисунок 3.5. – VSA Кластер з двома ESXi хостами

У кластері VSA з двома членами VSA кластера, додатковий сервіс називається VSA cluster service і працює на машині з vCenter Server. Служба бере участь в якості члена в кластері VSA, але він не забезпечує зберігання. Щоб залишатися онлайн, кластер VSA вимагає, щоб більше половини членів також були онлайн. Якщо один екземпляр Vsphere Storage Appliance не закривається, кластер може залишатися в онлайні, тільки якщо інші VSA члени кластера і VSA cluster service залишаються в режимі онлайн.

VSA кластера з 2 членами має 2 VSA сховища даних і підтримує копію кожного сховища.

VSA кластера з 3 членами має 3 VSA сховища даних (рис. 3.6) і підтримує копію кожного сховища. Ця конфігурація не вимагає VSA cluster service і працює на системі vCenter Server.

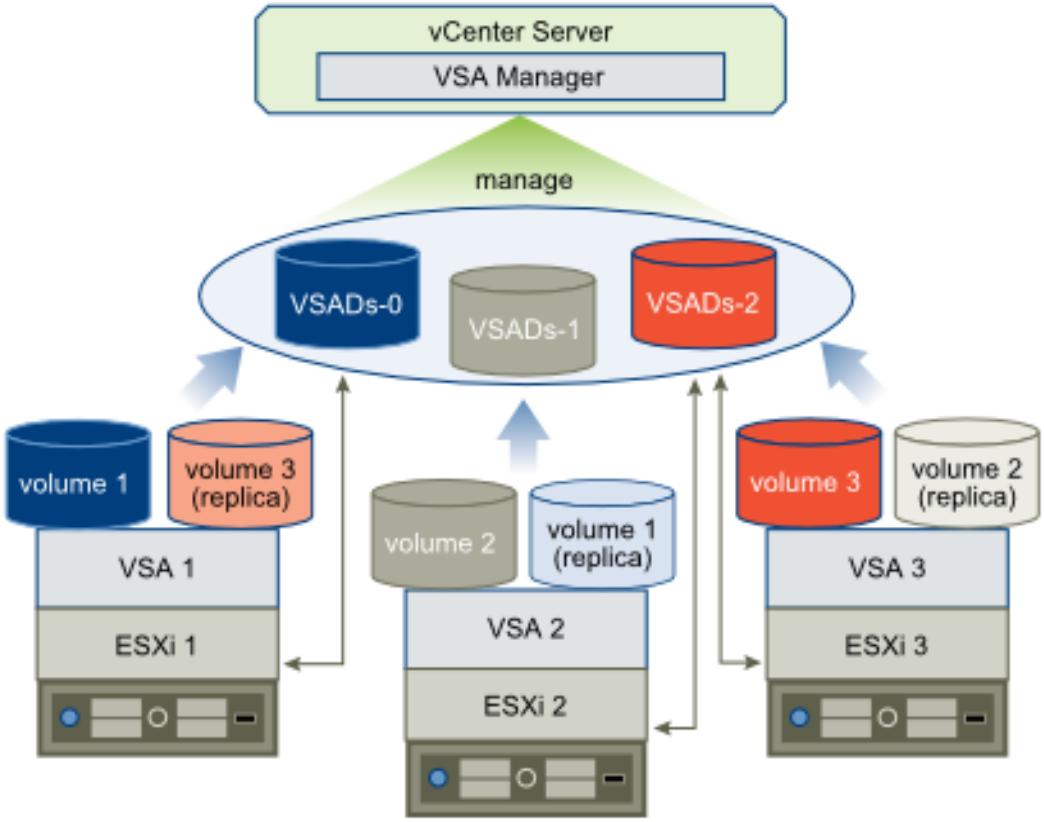

Рисунок 3.6 – VSA Кластер з трьома ESXi хостами

Мережева архітектура VSA кластера.

Фізична мережа кластеру VSA складається з комутаторів Gigabit Ethernet і мережевих карт (NIC), які встановлені на кожному комп'ютері.

Фізична мережева архітектура. Всі хости в кластері VSA повинні мати два подвійних порту або чотири одинарних порту мережевих інтерфейсних плат. Можна використовувати один перемикач Gigabit Ethernet для мережі кластера VSA. Для забезпечення надмірності мережі, можна використовувати два перемикача Gigabit Ethernet.

На рисунках 3.7–3.8 зображено резервування мережі в кластері VSA з 2 і 3 членів.

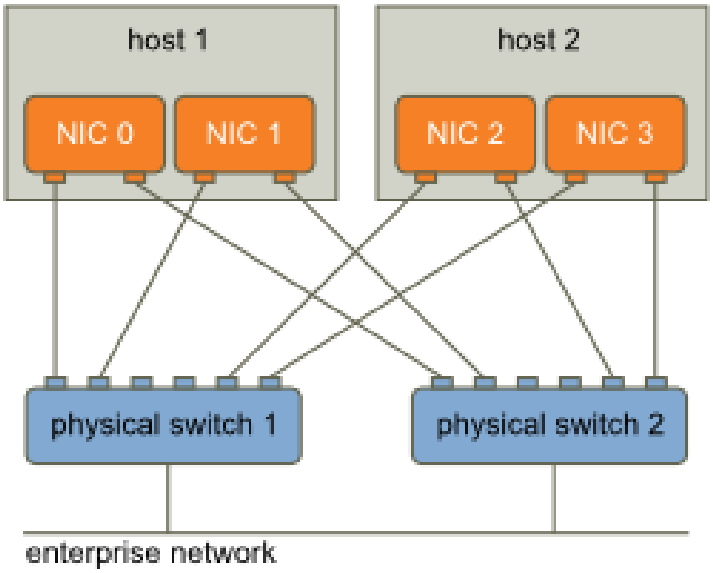

Рисунок 3.7 – Резервування мережі в кластері VSA з 2 членами

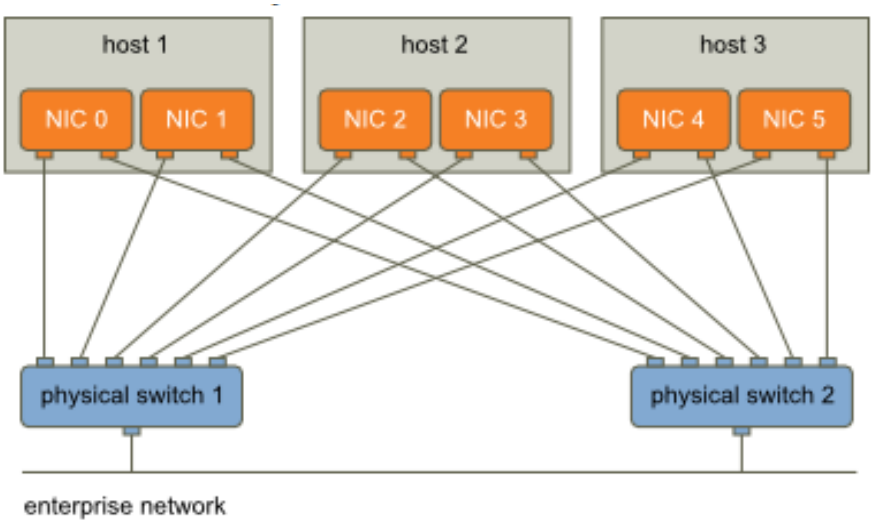

Рисунок 3.8 – Резервування мержі в кластері VSA з 3 членами

У кластері VSA, мережевий трафік ділиться на front-end і back-end.

Front-end трафік забезпечує:

– Зв’язок між кожним членом кластера VSA і VSA Manager.

– Зв’язок між ESXi і томами сховищ даних (СД) VSA.

– Зв’язок між членами кожної групи VSA і VSA cluster service.

– VMotion трафік між вузлами.

Back-end мережевий трафік забезпечує:

– Реплікація між томом СД і його копією, яка знаходиться на іншому хості.

– Кластеризація зв’язку між усіма членами кластеру VSA.

– Логічна мережева архітектура.

Кожен Vsphere Storage Appliance має два віртуальних мережевих адаптера: один обробляє інтерфейсний трафік (front-end), а інший обробляє фоновий трафік (back-end). Фонових віртуальний NIC має IP-адрес з приватної підмережі. Віртуальна front-end NIC може мати до 3 призначених IP-адреси:

1) IP-адреса для мережі управління VSA.

2) IP-адреса томи експортованої NFS.

3) IP-адрес кластера VSA (присвоюється тільки тоді, коли член кластера VSA обраний лідером кластера).

IP-адрес кластера VSA може переміщатися між членами VSA кластера. Він присвоюється front-end віртуальному NIC члену VSA кластера тільки тоді, коли цей член VSA кластера обрано лідером кластеру. Якщо лідер кластера стає недоступний, IP-адреса VSA присвоюється іншому члену VSA кластера, який стає лідером.

Інсталяція VSA кластера створює два стандартних Vsphere перемикача на кожному хості ESXi, щоб ізолювати front і back-end трафіки. Фізичні мережеві адаптери можуть виступати в якості висхідній лінії зв’язку для кожного стандартного перемикача Vsphere так, щоб кожен мережевий адаптер обробляв або front-end або back-end трафік. Стандартні комутатори використовують ESXi NIC teaming, щоб забезпечити відмовостійкість.

На рисунку 3.9 зображено логічна мережа VSA кластера, з лідером в кластері VSA.

VSA кластер забезпечує автоматичне перемикання для захисту від апаратних і програмних збоїв.

Кожне VSA сховище складається з двох томів. Член кластера VSA експортує основний тому як сховище даних VSA. Інший член кластера VSA підтримує другий том як репліку. Якщо відбувається збій в обладнанні, мережевому обладнанні, або член VSA кластера основного томи, стає недоступним, то тому репліки займає своє місце без переривання обслуговування. Після виправлення помилки і переходу елемента кластера VSA назад в онлайн, він синхронізує основний том з реплікою, щоб забезпечити відмовостійкість у разі подальших невдач.

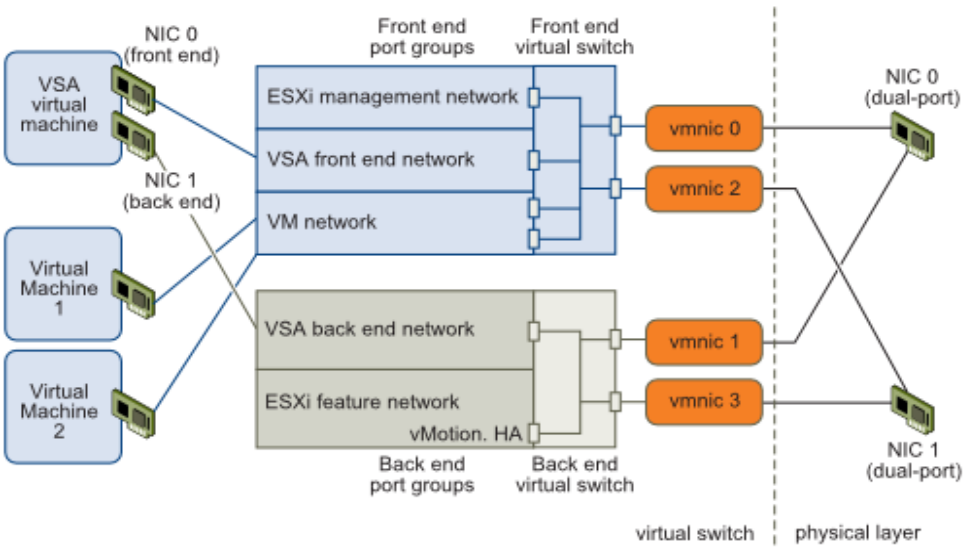

Рисунок 3.9 – Логічна мережі архітектури VSA кластера

VSA кластер забезпечує автоматичне перемикання від наступних збоїв:

– фізичний збій NIC;

– відмова одного фізичного перемикач;

– фізичний збій хоста;

– відмова члена кластеру VSA.

На рисунках 3.10–3.11 зображено автоматичний перехід в кластері VSA з 2 та 3 членами. Том репліки замінює відмови основного тому. У цьому випадку, щоб переконатися, що більше половини членів в режимі он-лайн, служба кластера VSA імітує члени VSA кластера.

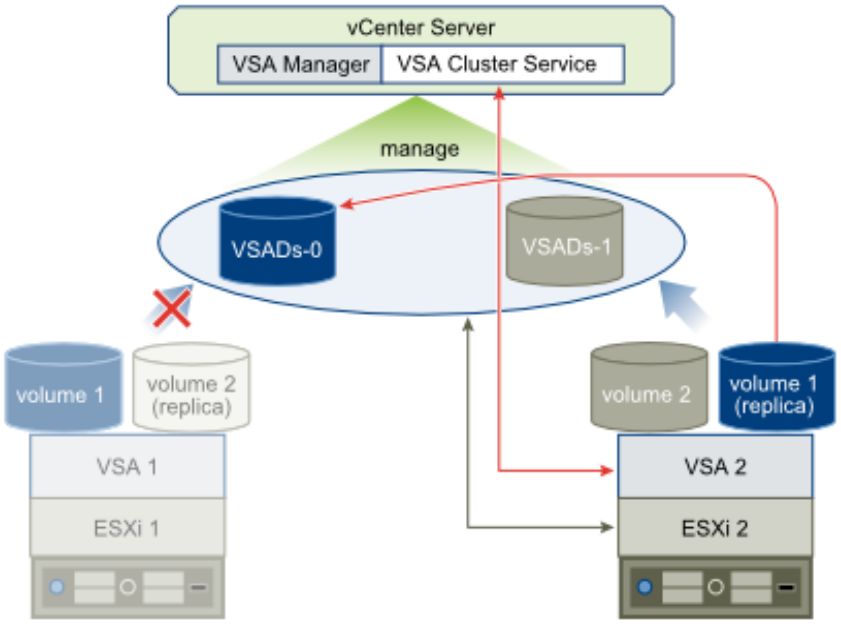

Рисунок 3.10 – Відмовостійкість у кластері VSA з 2 членами

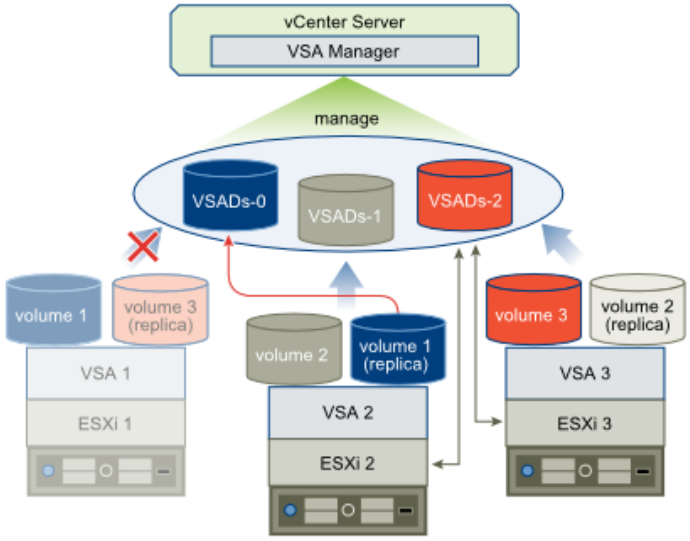

Рисунок 3.11 – Відмовостійкість у кластері VSA з 3 членами

VSA кластер є віртуальною альтернативою для дорогих систем SAN (Storage Area network). У той час як системи SAN надають централізовані масиви зберігання даних в високошвидкісній мережі, кластер VSA забезпечує розподілений масив, який працює на декількох фізичних серверах і використовує локальне сховище, яке додається до кожного хосту ESXi.

Системи SAN надають централізовані масиви зберігання, які управляються кількома процесорами зберігання. Vsphere Storage Appliance надає розподілений підхід до зберігання, де масив зберігання, розкиданий за декількома ESXi хостам і доступний через мережу (рис. 3.12).

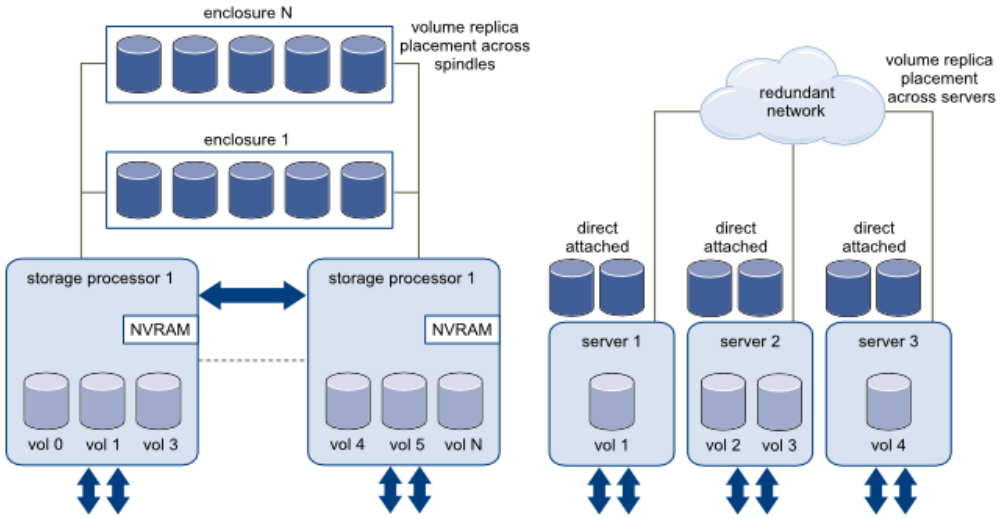

Рисунок 3.12 – Централізоване зберігання масивів у порівнянні з розподіленими Shared Storage

Сервери можуть отримати доступ до пам’яті через локальні жорсткі диски або через жорсткі диски, підключені до NAS або SAN систем. VSA кластер використовує жорсткі диски, які є локальними для кожного хоста ESXi.

Локальне зберігання даних. Локальне зберігання даних складається з внутрішніх жорстких дисків, розташованих усередині хоста ESXi.

Мережеве сховище. Мережеве сховище складається з зовнішніх систем зберігання даних, які хост ESXi використовує для зберігання файлів віртуальних машин віддалено. Як правило, господар отримує доступ до цих систем в мережі зберігання даних з високою швидкістю.

Для інсталяції та розгортання віртуалізованого середовища необхідно визначитися з масштабом і потужністю кластера VSA, а також розглянути деякі обмеження установки.

1. Установка vCenter Server на фізичному хості або в якості віртуальної машини на хості ESXi, який не є членом кластера VSA.

– ESXi хости не можуть запускати віртуальні машини до створення кластера.

– vCenter Server повинен бути встановлений і запущений до створення кластера VSA.

– Під час запуску vCenter Server на машині де встановлено сховище VSA і сховище даних переходить в автономний режим, то стає неможливо управляти кластером VSA через втрату доступу до vCenter Server і VSA Manager.

2. Визначитися з моделлю VSA кластера (2 або 3 члени). Після розгортання можна додати нові елементи до працюючого VSA кластеру.

3. Визначити здатність кластера VSA перед установкою.

– Vsphere Storage Appliance 1.0 не підтримує додавання нових томів і їх реплік для сховищ даних VSA після установки кластера VSA.

– VSA кластера вимагає томи RAID, створені з фізичних дисків. VMware рекомендує використовувати RAID5, RAID6 або RAID10. Vsphere Storage Appliance використовує RAID1 для підтримки копії сховища даних VSA. Ємність сховищ даних VSA залежить від кількості фізичних жорстких дисків, і

конфігурації RAID, який використовується. Фактичні реалізовані потужності розраховуються окремо для RAID5, RAID6 і RAID10.

4. Визначити кількість віртуальних машин, які будуть працювати в кластері VSA.

– Обмеження доступу Vsphere HA при визначенні кількості віртуальних машин і обсяг ресурсів, які підтримує кластер. Vsphere HA резервує 33% від усіх запасів процесора і ресурсів пам'яті в 3-членів кластера VSA і 50% всіх ресурсів процесора і ресурсів пам'яті в кластері з 2-членами.

– VSA СД не підтримує VMX заміну.

Мінімальні апаратні вимоги для vCenter Server представлені в таблиці 3.1.

Таблиця 3.1 – Мінімальні апаратні вимоги

vCenter Server Hardware	Вимоги
CPU	Два 64-розрядних процесора або один 62-розрядний двоядерний
Процесор	Intel или AMD 64 2.0 GHz
Пам'ять	4Gb
Сховище даних	4Gb
Microsoft SQL Server 2008 R2 Express	2GB
Мережа	Gigabit Ethernet

Вимоги до обладнання для ESXi хостів в кластері VSA. Можна розгорнути два або три хоста ESXi в кластері VSA. Кожен хост повинен відповідати вимогам апаратної конфігурації, щоб приєднатися до кластеру VSA (табл. 3.2).

Таблиця 3.2 – Вимоги до ESXi хосту в VSA Cluster

Hardware	Вимоги VSA Cluster
Конфігурація	Всі хости повинні мати однакову конфігурацію
CPU	64-bit x86 2 GHz и вище
Пам'ять	6 GB, мінімум 24 GB, рекомендується

	72 GB, максимальний підтримуючий с Vsphere Storage Appliance 1.0 1TB, максимальна підтримка ESXi 5.0
NIC	4 порту NIC повинен бути доступні на кожному хості ESXi. Для досягнення надмірності NIC, необхідно мати принаймні два Gigabit Ethernet адаптера на хості ESXi. Установка більше двох мережевих адаптерів, залежить від наявності вбудованих мережевих адаптерів і додаткових слотів PCI Express на материнській платі. Підтримуються наступні комбінації NIC: 4 однопортових мережевих адаптера 2 Двопортовий мережевих адаптера 2 однопортових мережевих адаптера і 1 двухпортовий мережевий адаптер 1 квад-порту NIC (не забезпечує надмірності NIC) Можна мати більше, ніж 4 NIC порту на хості ESXi, але не менше 4.
Жорсткий диск	Підтримувані конфігурації: жорсткі диски тієї ж моделі і того ж обсягу. Кількість дисків залежить від конфігурації RAID. 2TB максимальна ємність для кожного жорсткого диска 180GB Мінімальні вимоги за обсягом жорсткого диска на хості ESXi Всі диски SATA або все диски SAS Чи не підтримувані конфігурації: Поєднання SATA і SAS дисків не підтримується JBOD не підтримує
RAID	RAID controller

Мережа кластера VSA вимагає ряд статичних IP-адресів в підмережі vCenter Server. В залежності від кількості хостів у кластері кількість необхідних статичних IP-адресів змінюється. У таблиці 3.3 наведені приклади і загальна кількість статичних IP-адресів, які потрібні в підмережі vCenter Server для різних конфігурацій кластера VSA.

Таблиця 3.3 – Приклади статичних IP-адресів для різних VSA кластерних конфігурацій

Компоненти VSA Cluster	2-Member Cluster без DHCP	2-Member Cluster с DHCP	3-Member Cluster без DHCP	3-Member Cluster с DHCP
Кількість статичних IP-адрес в підмережі сервера	11	9	14	11
Кількість IP-адрес в приватній підмережі для серверної мережі	2	2	3	3
vCenter Server	10.15.20.100	10.15.20.100	10.15.20.100	10.15.20.100
ESXi host 1	10.15.20.101	10.15.20.101	10.15.20.101	10.15.20.101
ESXi host 2	10.15.20.102	10.15.20.102	10.15.20.102	10.15.20.102
ESXi host 3	НД	НД	10.15.20.103	10.15.20.103
VSA Cluster	10.15.20.103	10.15.20.103	10.15.20.104	10.15.20.104
VSA Cluster	10.15.20.104	10.15.20.104	НД	НД
VSA1 Manager	10.15.20.105	10.15.20.105	10.15.20.105	10.15.20.105
ХД VSA 1	10.15.20.106	10.15.20.106	10.15.20.106	10.15.20.106
Back-end VSA 1	192.168.0.1	192.168.0.1	192.168.0.1	192.168.0.1
VSA2 Manager	10.15.20.108	10.15.20.107	10.15.20.108	10.15.20.107
ХД VSA 2	10.15.20.109	10.15.20.108	10.15.20.109	10.15.20.108
Back-end VSA 2	192.168.0.2	192.168.0.2	192.168.0.2	192.168.0.2
VSA3 Manager	НД	НД	10.15.20.111	10.15.20.109
ХД VSA 3	НД	НД	10.15.20.112	10.15.20.110
Back-end VSA 3	НД	НД	192.168.0.103	192.168.0.103

Розглянемо функціональні можливості програмного комплексу, які дозволяють мінімізувати ризики загроз активу ІС інтернет-магазину.

Компоненти і загальна архітектура ESXi призначені для забезпечення безпеки системи ESXi в цілому.

З точки зору безпеки, ESXi складається з трьох основних компонентів: шару віртуалізації, віртуальної машини та мережі віртуального шару (рис. 3.13).

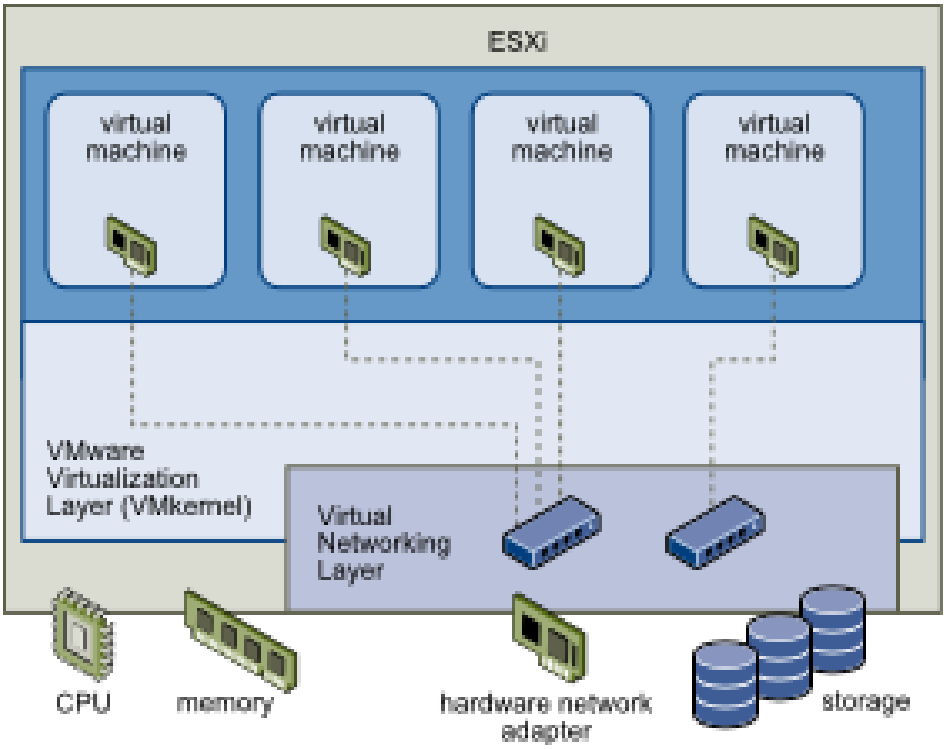

Рисунок 3.13 – ESXi архітектура

VMware використовує шар віртуалізації, або VMkernel, для запуску віртуальних машин. Він контролює апаратні засоби, які хости використовують і графіки розподілу апаратних ресурсів між віртуальними машинами. Так як VMkernel повністю присвячений підтримки віртуальних машин і не використовується для інших цілей, інтерфейс для VMkernel має строго обмежений набір API, необхідних для управління віртуальними машинами.

ESXi забезпечує додатковий захист VMkernel з наступними характеристиками:

Memory Hardening. Ядро ESXi, компоненти user-mode і виконувані компоненти, такі як драйвери і бібліотеки знаходяться в різних, не прогнозованих адресах пам’яті. У поєднанні із захистом доступної пам’яті мікропроцесора, це забезпечує захист, від шкідливого коду, який використовує експлоїти для пам’яті.

Модульна цілісність ядра. Цифровий підпис забезпечує цілісність і автентичність відбитку модулів, драйверів і додатків, коли вони завантажуються в VMkernel. Модуль дозволяє ESXi ідентифікувати постачальників модулів, драйверів і додатків, і перевіряти сертифікат справжності VMware.

Trusted Platform Module (TPM). Кожен раз при завантаженні ESXi, перевіряється VMkernel і підмножина завантажених модулів (VIBs), зміни зберігаються Platform Configuration Register (PCR).

Безпека віртуальних машин. Віртуальні машини є контейнерами, в яких працюють програми та гостьові ОС. Всі віртуальні машини VMware ізольовані один від одного, що дозволяє декільком віртуальним машинам надійно розділяти обладнання і забезпечувати доступ до апаратних ресурсів.

В результаті ізоляції віртуальної машини, якщо гостьова операційна система віртуальної машини відмовить, інші віртуальні машини на тому ж хості продовжать працювати. Відмова гостьової операційної системи не має ніякого впливу на:

– Здатність користувачів отримувати доступ до інших віртуальних машин.

– Можливість оперативної віртуальної машини отримувати доступ до необхідних ресурсів.

– Можливості інших віртуальних машин.

Кожна віртуальна машина ізольована від інших віртуальних машин, запущених на тому ж обладнанні. Хоча віртуальні машини використовують фізичні ресурси, такі як процесор, пам’ять і пристрої введення / виводу, гостьова операційна система на індивідуальній віртуальній машині не може виявити будь-який інший пристрій, крім тих віртуальних пристроїв, які є в її розпорядженні (рис. 3.14).

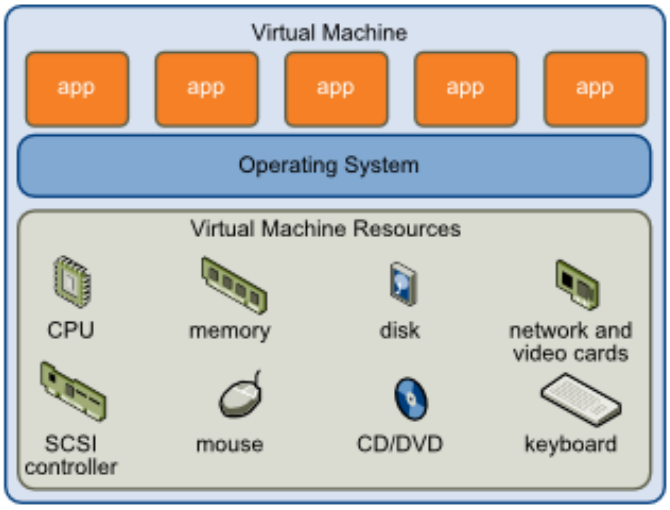

Рисунок 3.14. – Ізоляція віртуальної машини

Так як VMkernel є посередником для доступу до фізичних ресурсів і весь доступ до обладнання здійснюється через VMkernel, то віртуальні машини не можуть обійти цей рівень ізоляції.

Так само, як фізична машина взаємодіє з іншими машинами в мережі через мережеву карту, віртуальна машина взаємодіє з іншими віртуальними машинами, які працюють в тому ж хості через віртуальний комутатор. Крім того, віртуальна машина спілкується з фізичної мережею, в тому числі віртуальних машин на інших ESXi хостах, через фізичний мережевий адаптер (рис. 3.15).

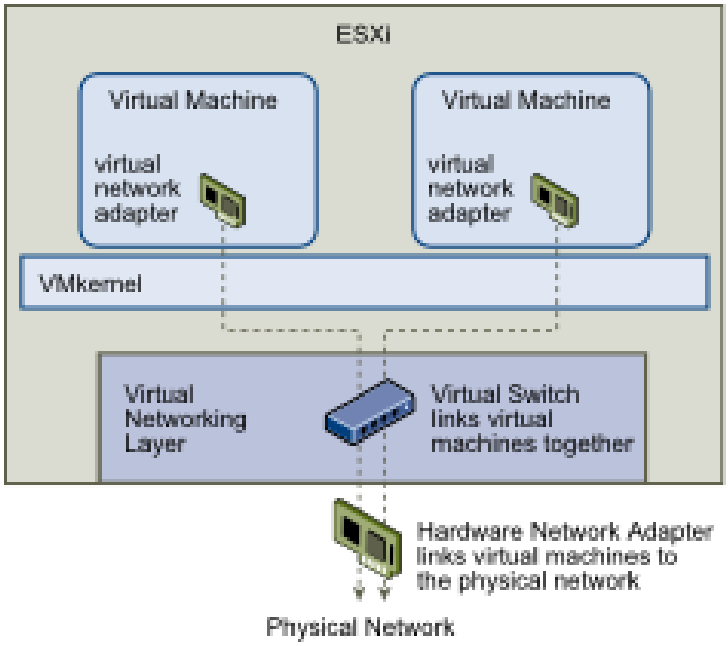

Рисунок 3.15 – Віртуальна мережа з використанням віртуальних комутаторів

Ці характеристики враховуються при визначенні ізоляції віртуальної машини в контексті мережі:

– якщо віртуальна машина не поділяє віртуальний комутатор з будь-якою іншою віртуальною машиною, він повністю ізольований від віртуальних мереж в межах хоста;

– якщо ніякої фізичний мережевий адаптер не налаштований для віртуальної машини, віртуальна машина повністю ізольована від будь-яких фізичних мереж;

– якщо використовуються одні і ті ж засоби захисту (брандмауери, антивірусне програмне забезпечення, і так далі), щоб захистити віртуальну машину від мережевих атак, на фізичній машині, віртуальна машина так само захищена, як і фізична машина.

Можна додатково захистити віртуальні машини, встановивши резервування ресурсів і лімітів на хості. Наприклад, через детальне управління ресурсами, доступними в ESXi, можна налаштувати віртуальну машину так, що вона завжди отримує принаймні 10 відсотків ресурсів процесора господаря, але не більше ніж 20 відсотків.

Бронювання ресурсів і межі захисту віртуальних машин від деградації продуктивності, дозволять захистити від надмірного споживання ресурсів іншою віртуальною машиною. Наприклад, якщо одна з віртуальних машин на хості недієздатна через атаки відмови в обслуговуванні (DoS), установка меж ресурсів на цій машині запобігає збій системи в цілому. Аналогічним чином, резервування ресурсів з кожною з віртуальних машин гарантує, що в разі високих вимог до ресурсів з боку віртуальної машини, яка стала мішенню для DoS атаки, це не вплине на всі інші віртуальні машини у яких залишиться достатньо ресурсів для роботи.

За замовчуванням, ESXi встановлює форму резервування ресурсів шляхом застосування алгоритму розподілу, який ділить наявні ресурси хоста порівну між віртуальними машинами, зберігаючи певний відсоток ресурсів для використання іншими компонентами системи. Це поведінка за умовчанням забезпечує ступінь

природного захисту від DoS атаки і розподіленої атаки відмови в обслуговуванні (DDoS). Можна встановити конкретні застереження і обмеження в ресурсах на індивідуальній основі, для налаштування поведінки за замовчуванням, так щоб розподіл не був однаковим для різних за конфігурацією машин.

Інформаційний захист шару віртуальної мережі. Віртуальна мережа включає в себе шар віртуальних мережевих адаптерів і віртуальних комутаторів. ESXi спирається на віртуальній мережевий шар для підтримки зв'язку між віртуальними машинами і їх користувачами. Крім того, хости використовують віртуальний мережевий шар для обміну даними з iSCSI SAN, NAS, ХД, і т. д.

Методи, які використовуються для захисту мережі віртуальної машини залежать, від операційної системи хоста, на якій працюють віртуальні машини в довіреному середовищі, а також ряду інших факторів. Віртуальні комутатори забезпечують значний ступінь захисту при використанні спільно з іншими практиками загальної безпеки, такими, наприклад, як установка міжмережевих екранів.

ESXi підтримує стандарт IEEE 802.1q VLAN, який можна використовувати для додаткового захисту віртуальної мережі клієнтів або сховищ даних. Мережі VLAN дозволяють сегментувати фізичну мережу так, щоб дві машини з однією і тією ж фізичною мережі не могли посилати пакети або отримувати пакети один від одного, якщо вони не знаходяться в одній і тій же VLAN.

Створення мережі DMZ (демілітаризованої зони) на одному ESXi хості. Одним із прикладів того, як використовувати ізоляцію ESXi і особливості віртуальних мереж для налаштування безпечного середовища є створення демілітаризованої зони (DMZ) на одному хості (рис. 3.16).

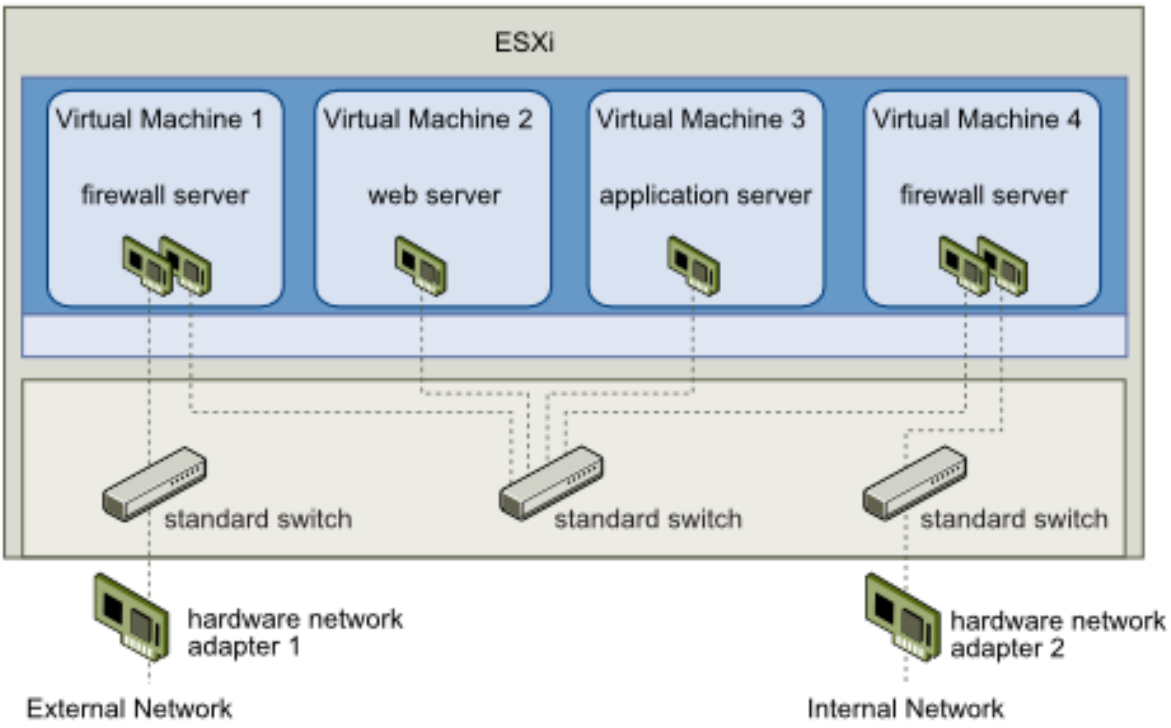

Рисунок 3.16 – DMZ налаштовано на одному ESXi хості

При створенні DMZ на одному хості, ви можете використовувати досить легкі брандмауери. Хоча віртуальна машина в цій конфігурації не може напряму впливати на іншу віртуальну машину або отримати доступ до її пам'яті, усі віртуальні машини як і раніше підключені через віртуальну мережу. Безпека віртуальних машин в DMZ еквівалентна окремим фізичним машинам, підключеним до тієї ж мережі.

Принципи ліцензування vSphere і варіанти поставки. Для отримання прав на використання програмного забезпечення VMware vSphere необхідно придбати окрему ліцензію Ліцензій. Кількість Ліцензій повинна відповідати кількості процесорів на віртуальних серверах. Обмеження, які накладаються на кількість процесорних ядер і об'єм оперативної пам'яті в серверах відсутні.

Для придбання ліцензії можна вибрати один з типів комплектації програмного забезпечення: Standard, Enterprise і Enterprise Plus. Кожен з комплектів відрізняється набором функціональних можливостей.

Придбаючи Ліцензій необхідно також придбати сервер управління VMware vCenter Server Standard. Сервер може обслуговувати до 1000 вузлів.

Програмне забезпечення VMware vSphere можна придбати також у вигляді готового Набору Ліцензій. Такий варіант є найкращим для компанії IT-послуг.

При покупці Ліцензій і Наборів Ліцензій необхідно також придбати відповідний пакет Підтримки та Підписка. Даний пакет дає право на звернення до служби підтримки компанії VMware в разі виникнення проблем в процесі експлуатації ПЗ віртуалізації, а також забезпечує можливість отримання оновлень придбаної версії ПЗ.

Існує також можливість Upgrade використовуваного ПЗ: наприклад, заміна Essentials Kit на Acceleration Kit, або перехід на іншу версію Ліцензій, наприклад, з версії Standard на Enterprise.

Згідно списку довірених осіб доступ до мережі управління віртуальною мережею закріплений за адміністратором безпеки і штатним адміністратор мережі.

Для доступу до мережі управління адміністратор безпеки або мережевий адміністратор повинен пройти перевірку справжності в SSL VPN, яка налаштована на двухфакторную авторизацію. Після аутентифікацію в Active Directory (AD) адміністратору видається одноразовий сесійний пароль one-time password (OTP), який надсилається в текстовому повідомленні на мобільний телефон. Це дає можливість захистити мережу управління від спроби входу в мережу за ім’ям і паролем, які були вкрадені. Система не пропустить користувача, якщо не пройдена авторизація через пристрій SSL VPN. Якщо перевірка в пристрої SSL VPN пройдена успішно, то адміністратор отримує посилання, яка дозволяє використовувати RDP для доступу до сервера vCenter.

Для забезпечення проходження трафіку SSL (TCP-порт 443) з мережі віртуального сервера в спеціалізовану мережу управління на брандмауері формується спеціальне правило. Для підвищення безпеки можна посилити правило брандмауера відкривши доступ до пристрою SSL VPN в захищеній мережі тільки з певних IP-адресів. У разі атаки ця спеціалізована мережа дозволяє забезпечити додатковий час, який знадобиться для того, щоб ізолювати мережу. Цей підхід дозволить організувати захист сервера управління віртуальною мережею за всяку ціну.

Така концепція виділеної мережі управління використовує сучасну модель безпеки під назвою «створення бункерів» (siloing). Використання даної концепції дає можливість розділити мережу на логічні підмережі, в яких користувачі отримують доступ тільки до тих комп'ютерів, які їм необхідні. При організації виділеної мережі управління необхідно враховувати такі фактори.

Плати HP Integrated Lights-Out (iLO) / Dell Remote Access Controller (DRAC). Ці плати дають можливість адміністратору отримати віддалений доступ до консолі на сервер ESX навіть коли він відключений.

Управління комутатором. Доступ до комутатора повинен бути організований лише з мережі управління.

Управління брандмауером здійснюється тільки з виділеної мережі управління.

Управління безперебійним джерелом живлення. Для захисту від атаки з відмовою в обслуговуванні (DoS) проти всіх віртуальних машин, коли імітується відмову в електропостачанні від джерела безперебійного живлення необхідно щоб мережева плата безперебійного джерела живлення з мережевою платою управління була підключена до мережі управління.

Для ESXi необхідно управління через особливу мережеву плату на сервері ESXi.

Для роботи з віртуальної мережею адміністратори повинні пройти навчальні курси, які розглядають питання, пов'язані з інсталяцією, конфігуруванням й управлінням рішеннями на базі vSphere, з використанням сервера ESXi 5.1 і vCenter Server 5.1.

Курс повинен включати наступні модулі

– Віртуалізувати дата-центр

– Створення віртуальних машин

– VMware vCenter Server

– Налагодження та управління віртуальними мережами

– Налагодження та управління віртуальним сховищем

– Управління віртуальними машинами

– Аутентифікація і контроль доступу

– Управління ресурсами та моніторинг

– Міцна та висока доступність

– Масштабованість

– Управління патчами

– Установка компонентів VMware

3.2 Контрольний приклад реалізації проекту і його опис

Так як компанія «ГІГАБАЙТ+» є невеликою компанією і в ній немає спеціально виділених структурних підрозділів для організації захисту даних, то всі обов'язки по організації захисних заходів покладено на адміністратора безпеки і штатного адміністратора мережі.

Згідно з постановкою задачі в компанії «ГІГАБАЙТ+» планується реалізація проекту з віртуалізації IT-інфраструктури з метою підвищення захищеності активів.

На рисунку 3.17 представлено проект розгортання корпоративної мережі інтернет-магазину IT-послуг «ГІГАБАЙТ+». У проекті виділено один хост для трьох типів різних віртуальних машин: FTP-сервера, внутрішні віртуальні машини і DMZ. Кожна зона виконує унікальну функцію.

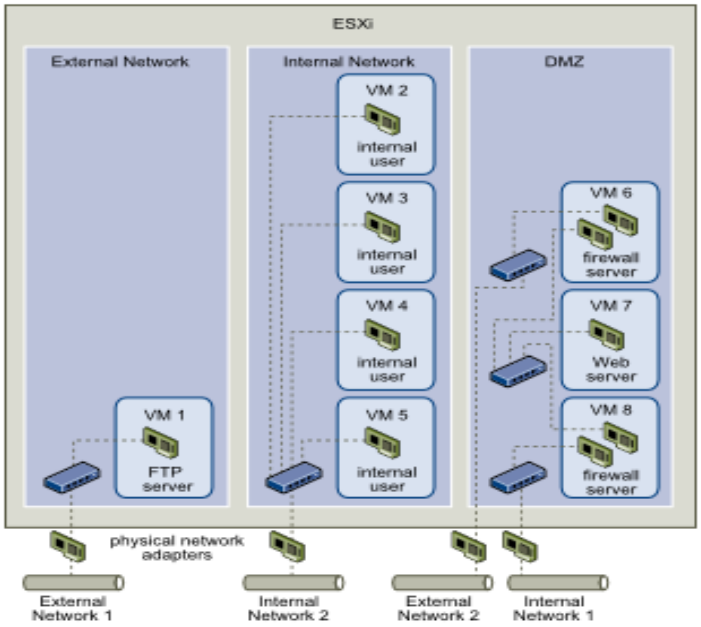

Рисунок 3.17 – Зовнішні мережі, внутрішні мережі та DMZ, налаштовані на одному ESXi хості

FTP-сервер. Віртуальна машина 1 налаштована з програмним забезпеченням FTP і виступає в якості холдингової області для даних, переданих в/із зовнішніх ресурсів. Ця віртуальна машина пов'язана тільки із зовнішньою мережею. Він має свій власний віртуальний комутатор і фізичний мережевий адаптер, який підключає її до зовнішньої мережі 1. Ця мережа призначена для серверів, які компанія використовує для отримання даних із зовнішніх джерел. Наприклад, компанія використовує зовнішню мережу 1 для отримання FTP трафіку від постачальників і надати їм доступ до даних, які зберігаються на зовнішніх доступних серверах, через FTP. Так як віртуальна машина 1 не поділяє віртуальний комутатор або фізичний мережевий адаптер з віртуальними машинами в хості, інші віртуальні машини резиденти не можуть передавати пакети або отримувати пакети з мережі віртуальної машини 1. Це обмеження запобігає розвідувальні атаки, які вимагають відправки мережевого трафіку жертві. Що ще більш важливо, зловмисник не може використовувати природні уразливості FTP для доступу до будь-якої з інших віртуальних машин хоста.

Внутрішні віртуальні машини. Віртуальні машини з 2 по 5 зарезервовані для внутрішнього використання. В результаті, системні адміністратори повинні забезпечити високий рівень захисту для цих віртуальних машин. Ці віртуальні машини підключення до внутрішньої мережі 2 через власний віртуальний комутатор і мережевий адаптер. Внутрішня мережа 2 зарезервована для внутрішнього використання персоналом. Віртуальні машини з 2 по 5 можуть спілкуватися один з одним через віртуальний комутатор або через фізичний мережевий адаптер. Вони не можуть спілкуватися з мережею зовнішніх машин. Як і FTP-сервер, ці віртуальні машини не можуть посилати пакети або отримати пакети від мережі інших віртуальних машин. Аналогічним чином, інші віртуальні машини хосту не можуть посилати пакети або отримати пакети від віртуальних машин від 2 до 5. Ці машини призначені для зберігання конфіденційної персональної інформації компанії.

DMZ. Віртуальні машини з 6 по 8 налаштовуються як DMZ. Ця група віртуальних машин пов'язана із зовнішньою мережею 2 і внутрішньою мережею 1. Компанія використовує зовнішню мережу 2 для підтримки веб-серверів.

Внутрішня мережа 1 є каналом, між відділами компанії і використовується для публікації контенту на корпоративному сайті, поштових розсилок, і підтримки таких послуг, як, наприклад, призначені для користувача форуми. Оскільки ці мережі відокремлені від зовнішньої мережі 1 і внутрішньої мережі 2, а віртуальні машини не мають спільні точки дотику, немає ніякого ризику атаки або від FTP-сервера або від внутрішньої групи машин.

Використовуючи правильні налаштування віртуальних комутаторів і підтримку поділу мережі, можна розмістити всі три віртуальні зони в тому ж хості ESXi і бути впевненим, що не буде ніяких втрат даних або порушення цілісності ресурсів.

Використання віртуальних комутаторів не дає можливості пропуску пакетів з однієї зони в іншу. Віртуальний комутатор, за конструкцією, не може пропускати пакети безпосередньо до іншого віртуального комутатора. Єдиний спосіб для пакетів перейти від одного віртуального комутатора до іншого можливий за таких обставин:

– Віртуальні комутатори з'єднані з однією фізичною мережею.

– Віртуальні комутатори підключені до загальної віртуальної машині, яка може бути використана для передачі пакетів.

Жодна з цих умов не виникає в разі використання представленої конфігурації.

Для захисту ресурсів на віртуальних машинах, системний адміністратор знижує ризик DoS і DDoS атак шляхом налаштування резервування ресурсів і установкою ліміту для кожної віртуальної машини. Системний адміністратор в подальшому захищає хост ESXi і віртуальні машини, встановлюючи програмні брандмауери на front-end і back-end зонах DMZ.

Технічна архітектура віртуальної мережі підприємства представлена на рисунку 3.18.

У таблиці 3.4 представлені технічні характеристики обладнання.

Таблиця 3.4 – Технічні характеристики технічної архітектури

Наименование	Характеристики
HP ProLiant DL380 Gen7 (EXSi хост)	Сервер Hewlett Packard Proliant DL380R07 E5645 Rack2U/Xeon6C 2.4Ghz (12Mb)/ 3x4Gb R1D /P410i wBBWC (512Mb/ RAID (5+0/5/1+0/1/0)/ HDD 2x300GB SAS (8/16up) SFF/ DVD RW/ iLO3 std/ 4xGigEth/ 1xRPS 460HE
HP ProLiant DL380 Gen7 (vCenter Servre)	Сервер Hewlett Packard Proliant DL380R07 E5620 Rack2U/ XeonQC 2.4Ghz (12Mb)/ 2x4Gb R1D/ P410i wBBWC (512Mb/ RAID (5+0/5/1+0/1/0)/ HDD 1x300GB SAS (8/16up) SFF/ DVD RW/ iLO3 std/ 4xGigEth/ 1xRPS 460 Plat, analog 470065-361

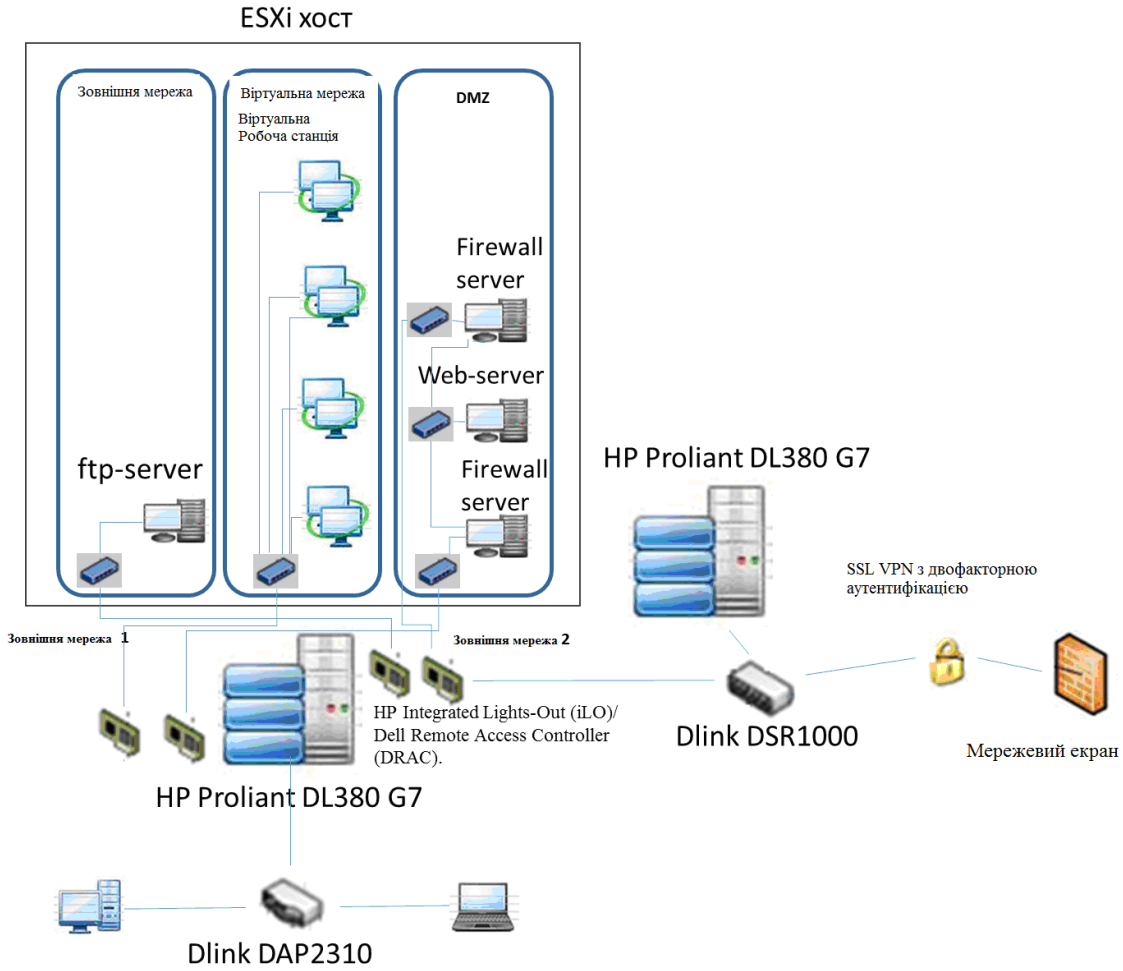

Рисунок 3.18 – Технічні архітектура підприємства

З урахуванням проекту віртуалізації програмна архітектура мережі компанії буде виглядати наступним чином (рис. 3.19)

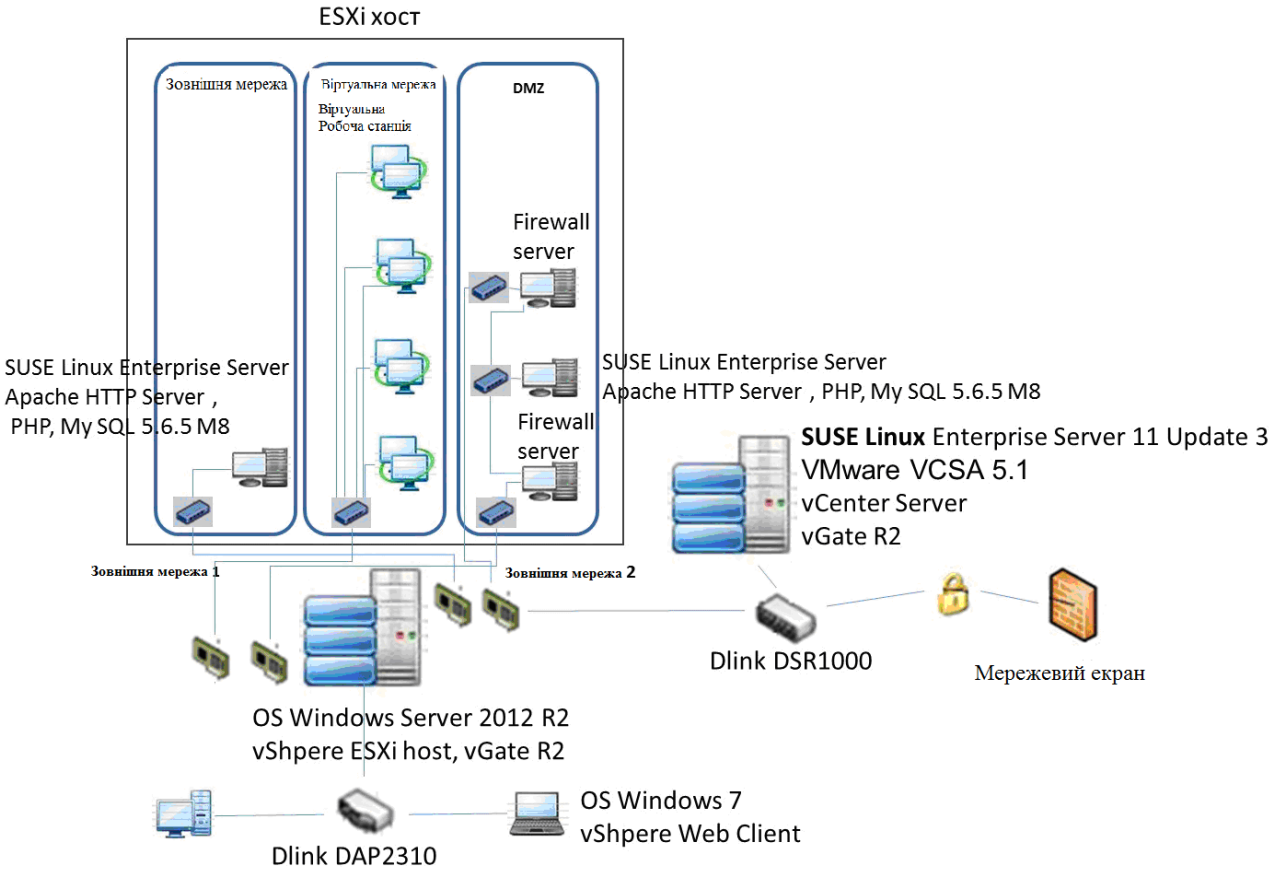

Рисунок 3.19 – Програмна архітектура мережі компанії

Технічні характеристики програмного забезпечення мережі компанії надано у таблиці 3.5.

Таблиця 3.5 – Технічні характеристики програмної архітектури

Наименование	Характеристики
vCenter Server	SUSE Linux Enterprise Server 11 Up 3 VMware VCSA 5.1, vCenter Server vGate R2
ESXi host	OS Windows Server 2012 R2 vShpere ESXi host, vGate R2
ftp-server	SUSE Linux Enterprise Server Apache HTTP Server , PHP, My SQL 5.6.5 M8
Web-server	SUSE Linux Enterprise Server Apache HTTP Server , PHP, My SQL 5.6.5 M8
Firewall-server	SUSE Linux Enterprise Server Apache HTTP Server with SuSEfirewall2 and YaST_Firewall module
Client computer	OS Windows 7, vShpere Web Client

Для забезпечення контролю доступу до серверної кімнаті і бухгалтерії пропонується установка СКУД RusGard з контролем доступу на 2 двері.

Для монтажу необхідні наступні комплектуючі:

– ML295K, електромагнітний замок

– Matrix 3EH, 2 шт, зчитувач СКУД

– ACS-102-CE-B, мережевий контролер

– ББП- 20 ісп. 01, джерело живлення безперебійний

– 12V, 7Ач, акумулятор

– StandProx, proxy-карта Em-marin, 5шт, магнітні картки

Схема установки представлена на рисунку 3.20.

Рисунок 3.20 – Схема установки СКУД

3.3 Висновки до розділу 3

Таким чином, в розділі 3 зпроектовано і створено систему безпеки в локальній мережі на прикладі інтернет-магазину «ГІГАБАЙТ+». Розроблено політику, що дозволить підвищити рівень захищеності персональних даних від несанкціонованого доступу, які зберігаються і обробляються в інформаційній системі підприємства.

4 БЕЗПЕКА ЖИТТЄДІЯЛЬНОСТІ, ОСНОВИ ХОРОНИ ПРАЦІ

4.1 Вимоги до профілактичних медичних оглядів для працівників ПК.

Працівники, які використовують у своїй роботі персональні комп'ютери, підлягають обов'язковим медичним оглядам. Але водночас згідно з роз'ясненням МОЗ від 20.01.2006 р. № 05.0101-18-58/21 проведення обов'язкових медоглядів поширюється на роботу з комп'ютерами на основі електронно-променевих трубок та не поширюється на роботу з рідкокристалічними терміналами.

У сучасних умовах важко знайти галузь економіки, де б не використовувалися комп'ютери. Бюджетні організації не є винятком, адже в них за комп'ютерами працюють бухгалтери, секретарі, економісти, юристи, оператори комп'ютерного набору тощо.

Обов'язковість проведення медичних оглядів для працівників, які працюють за електронно-обчислювальними машинами, передбачена розд. 6 Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин ДСанПіН 3.3.2.007-98, затверджених постановою Головного державного санітарного лікаря України від 10.12.98 р. № 7 (далі — ДСанПіН № 7).

Так, працюючі з візуальними дисплейними терміналами (ВДТ) електронно-обчислювальних машин (ЕОМ) колективного використання та персональних ЕОМ (ПЕОМ) підлягають обов'язковим медичним оглядам: попереднім — при влаштуванні на роботу і періодичним — протягом трудової діяльності (п. 6.1 розд. 6 ДСанПіН № 7).

Такі медичні огляди проводяться відповідно до вимог Порядку проведення медичних оглядів працівників певних категорій, затвердженого наказом МОЗ від 21.05.2007 р. № 246 (далі — Порядок № 246).

Періодичні медичні огляди мають проводитися раз на два роки комісією в складі терапевта, невропатолога та офтальмолога.

До речі, до складу комісії, що проводить попередні та періодичні медичні огляди, при необхідності (за наявності медичних показань) можуть залучати лікарів інших спеціальностей.

Основними критеріями оцінки придатності до роботи з ВДТ ЕОМ і ПЕОМ мають бути показники стану органів зору: гострота зору, показники рефракції, акомодації, стану бінокулярного апарату ока тощо. При цьому також враховується стан організму в цілому.

У розд. 6 ДСанПіН № 7 передбачено й протипоказання для роботи за комп'ютерами. До них відносять усі хронічні форми психічних захворювань, ендокринні захворювання, тяжкий ступінь бронхіальної системи, гіпертонічна хвороба III стадії та інші захворювання.

До відома зазначимо, що монітор або дисплей — це електронний пристрій для відображення інформації. Комп'ютерні монітори бувають кількох типів:

- на основі електронно-променевої трубки(CRT);
- рідкокристалічні(LCD, TFT як підвид LCD);
- плазмові;
- проекційні;
- OLED-монітори.

Плазмові і проекційні монітори використовують там, де потрібен великий розмір екрану (діагональ метр і більше).

І тут виникає запитання: чи необхідно проходити обов'язкові медогляди працівникам, які працюють за більш сучасними «тонкими» моніторами?

Дійсно, як зазначив наш читач у своєму запитанні, з цього приводу було надано роз'яснення заступника Головного державного санітарного лікаря України в листі від 20.01.2006 р. № 05.01.01-18-58/21. У цьому листі зазначено, що ДСанПіН № 7 поширюються на ВДТ усіх типів вітчизняного та зарубіжного виробництва на основі електронно-променевих трубок, тому вимога щодо проведення попередніх та періодичних медичних оглядів на працюючих з рідкокристалічними відеотерміналами ЕОМ машин у цьому випадку не діє.

Звичайно, якась логіка в цьому є, адже до шкідливих випромінювань комп'ютера належать низькочастотні електромагнітні поля та іонізуюче (рентгенівське) випромінювання моніторів на електронно-променевих трубках.

Але все ж таки, слід розуміти, що лист не є нормативним документом і носить лише рекомендаційний характер. Винятків щодо непроведення обов'язкових медичних оглядів для працівників, які працюють з рідкокристалічними та іншими сучасними «тонкими» моніторами, до ДСанПіН № 7 внесено не було. Тож із фахівцями санепідстанцій можуть виникнути непорозуміння з цього приводу.

Вирішувати, звичайно, вам, але ми б рекомендували все ж таки додержуватися правил, визначених ДСанПіН № 7, та проводити обов'язкові медогляди працівників, які працюють за будь-якими видами моніторів комп'ютерів, як того вимагають ці Правила.

Нагадаємо деякі правила проведення обов'язкових медоглядів.

Як уже було зазначено вище, працівники, які працюють за комп'ютерами, підлягають обов'язковим попередньому та періодичним медоглядам.

Попередній медичний огляд проводиться під час прийняття на роботу з метою:

– визначення стану здоров'я працівника і реєстрації вихідних об'єктивних показників здоров'я та можливості виконання без погіршення стану здоров'я професійних обов'язків в умовах дії конкретних шкідливих та небезпечних факторів виробничого середовища і трудового процесу;

– виявлення професійних захворювань (отруєнь), що виникли раніше при роботі на попередніх виробництвах, та попередження виробничо зумовлених і професійних захворювань (отруєнь).

Періодичні медичні огляди проводяться з метою:

– своєчасного виявлення ранніх ознак гострих і хронічних професійних захворювань (отруєнь), загальних та виробничо зумовлених захворювань у працівників;

– забезпечення динамічного спостереження за станом здоров’я працівників в умовах дії шкідливих та небезпечних виробничих факторів і трудового процесу;

– вирішення питання щодо можливості працівника продовжувати роботу в умовах дії конкретних шкідливих та небезпечних виробничих факторів і трудового процесу;

– розробки індивідуальних та групових лікувально-профілактичних та реабілітаційних заходів працівникам, що віднесені за результатами медичного огляду до групи ризику;

– проведення відповідних оздоровчих заходів.

Заклади державної санітарно-епідеміологічної служби щорічно за заявкою роботодавця (його представника), за участю представника первинної профспілкової організації або уповноваженої працівниками особи, визначають категорії працівників, які підлягають попередньому (періодичним) медичному огляду та до 1 грудня складають Акт визначення категорій працівників, які підлягають попередньому (періодичним) медичному огляду за формою, зазначеною у додатку 1 до Порядку № 246.

Потім на підставі зазначеного Акта роботодавець складає протягом місяця у чотирьох примірниках поіменні списки працівників, які підлягають періодичним медичним оглядам. Форма таких списків наведена у додатку 2 до Порядку № 246.

Ці списки на паперовому та електронному носіях узгоджують у санітарно-епідеміологічній станції. Один примірник списку залишається на підприємстві (у відповідальної за організацію медогляду посадової особи), другий надсилається до закладу охорони здоров’я, третій — до закладу державної санітарно-епідеміологічної служби, четвертий — до робочого органу виконавчої дирекції Фонду соціального страхування від нещасних випадків на виробництві та професійних захворювань.

Отже, як видно, списки працівників, які мають пройти медогляди, надаються та узгоджуються з санепідслужбою.

Для проведення попереднього (періодичних) медичного огляду працівників роботодавець повинен укласти або вчасно поновити договір із закладом охорони здоров'я та надати йому список працівників, які підлягають попередньому (періодичним) медичному огляду.

Питання придатності до роботи в кожному окремому випадку вирішується індивідуально з урахуванням особливостей функціонального стану організму (характеру, ступеня прояву патологічного процесу, наявності хронічних захворювань), умов праці та результатів додаткових методів обстеження.

При цьому кожен лікар, який бере участь в обстеженні пацієнта, дає висновок щодо стану здоров'я працівника, підтверджує його особистим підписом та особистою печаткою, бере участь в остаточному обговоренні придатності обстежуваної особи до роботи в обраній професії та в разі необхідності визначає лікувально-оздоровчі заходи.

За результатами періодичних медичних оглядів (протягом місяця після їх закінчення) комісія з проведення медичних оглядів закладів охорони здоров'я оформляє Заключний акт за результатами періодичного медичного огляду працівників. Форма цього акта наведена у додатку 9 до Порядку № 246 (ср. 025069200). Такий акт складається у шести примірниках — один примірник залишається в закладі охорони здоров'я, що проводив медогляд, інші надаються роботодавцю, представнику профспілкової організації або вповноваженій працівниками особі, профпатологу, закладу державної санітарно-епідеміологічної служби, робочому органу виконавчої дирекції Фонду соціального страхування від нещасних випадків на виробництві та професійних захворювань.

Також зазначимо, що роботодавець зберігає за працівником на період проходження медогляду місце роботи (посаду) і середній заробіток та за результатами медичного огляду інформує працівника про можливість (неможливість) продовжувати роботу за професією (п. 2.21 Порядку № 246).

Наприкінці також звернемо вашу увагу на те, що право на додаткову відпустку за роботу на комп'ютері мають усі працівники, незалежно від того, за якими моніторами вони працюють.

4.2 Психофізіологічне розвантаження для працівників

При проведенні сеансів психофізіологічного розвантаження рекомендується використовувати деякі елементи методу аутогенного тренування, який ґрунтується на свідомому застосуванні комплексу взаємопов'язаних прийомів психічної саморегуляції й виконанні нескладних фізичних вправ із словесним самонавіюванням. Головна увага при цьому приділяється набуванню й закріпленню навичок м'язового розслаблення (релаксації).

У рекомендованому сеансі, який має проводитися в кімнаті психофізіологічного розвантаження з відповідним інтер'єром та кольоровим оформленням, виділяються три періоди, що відповідають фазам відновлювального процесу.

Перший період – абстрагування працівників від виробничої обстановки – відповідає фазі залишкового збудження. Лунають повільна мелодійна музика, пташиний спів. Обравши зручну позу, працівники адаптуються і психологічно готуються до наступних періодів.

Другий – заспокоєння – відповідає фазі відновлювального гальмування. Пропонується показ фотослайдів із зображеннями квітучого лугу, березового гаю, гладенької поверхні ставка тощо. Через навушники транслюється спокійна музика, а на її фоні негучно, повільно висловлюються заспокійливі формули аутогенного тренування.

Як функціональне освітлення застосовують зелене світло. Яскравість світла має поступово знижуватись протягом періоду, а наприкінці його світло вимикається зовсім на 1-2 хвилини. Екран теж гасне.

Третій період – активізація – відповідає фазі підвищеної збудженості.

На початку періоду світло вимкнене, через певний час на екрані з'являється червона пляма, розміри і яскравість якої поступово збільшуються. Наприкінці періоду лунає бадьора музика. Тричі вимовляються мобілізуючі формули аутогенного тренування, яким мають передувати глибоке вдихання та довге глибоке видихання

Сеанси психологічного розвантаження можуть проводитись за єдиною програмою через індивідуальні навушники і складатись із двох періодів по 5 хвилин кожний:

– повне розслаблення;

– активізація працездатності.

У разі потреби, на фоні музичних програм можуть вимовлятися окремі фрази навіювання відпочинку, гарного самопочуття і, на заключному етапі, бадьорості.

Після сеансів психофізіологічного розвантаження у працівників зменшується відчуття втоми, з’являються бадьорість, гарний настрій. Загальний стан відчутно поліпшується.

ВИСНОВКИ

Компанії все більше залежать від комп’ютерної / мережевий технологій, які вони застосовують для підвищення ефективності і продуктивності свого бізнесу, щоб вижити і процвітати в сучасному конкурентному світі. Це бізнес-потреба, а іноді це є юридичною вимогою, необхідність захистити свою конфіденційну інформацію від загроз несанкціоноване доступу, зміни і руйнування, від комп’ютерного шахрайства або порушення в процесі роботи системи. Компанії можуть понести величезні втрати в фінансових активах або в продуктивності, а також втратити репутацію через великої внутрішньої і / або зовнішню загрозу безпеки. Правильно реалізований контроль доступу забезпечує захист активів від загроз, гарантує безперервність бізнесу, мінімізує потенційний збиток, а також забезпечує максимальну віддачу від інвестицій. Сильний контроль доступу включає в себе розумну політику безпеки, чітко визначені моделі безпеки, добре продуману архітектуру системи, належну реалізація механізмів захисту, таких як паролі, шифрування, списки управління доступом, а також міжмережеві екрани. Доступ до інформації повинен регулюватися за принципом службової необхідності. Тільки з правильно розробленої і реалізованої системою контролю доступу, компанії зможуть реалізувати всі переваги і потенціал використання комп’ютерних технологій.

В дипломній роботі розглянута актуальна тема, пов’язана з необхідністю проектування і створення системи безпеки в локальній мережі на прикладі інтернет-магазину «ГІГАБАЙТ+». Розроблена політика дозволить підвищити рівень захищеності персональних даних від несанкціонованого доступу, які зберігаються і обробляються в інформаційній системі підприємства.

.

СПИСОК ЛІТЕРАТУРНИХ ДЖЕРЕЛ

1. Инструментальный контроль и защита информации: учебное пособие. Воронеж: Воронежский государственный университет инженерных технологий, 2013. – 192 с.

2. Киреенко А. Е. Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения [Текст] / А. Е. Киреенко // Молодой ученый. — 2012. — №3. — С. 40-46.

3. ЗАКОН УКРАЇНИ від 20.03.2020, підстава - 524-IXПро захист персональних даних [Електроний ресурс]: https://zakon.rada.gov.ua/laws/main/2297-17#Text.

4. ЗАКОН УКРАЇНИ від 25.01 .2021 р. Про загальнообов’язкове державне пенсійне страхування. [Электронный ресурс]: https://www.profiwins.com.ua/uk/legislation/laws/74.html

5. Пістун І. П та ін. Охорона праці (Законодавство. Організація роботи): навчальний посібник / Пістун І. П., Березовецька О. Г., Трунова І. О. — Львів: Тріада плюс, 2010. — 648 с.

6. Охорона праці в галузі комп'ютингу: підручник / Л. А. Катренко, А. В. Катренко ; [за наук. ред. В. В. Пасічника] ; М-во освіти і науки, молоді та спорту України. — Л. : Магнолія 2006, 2012. — 544 с