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: *" Аналіз та вибір програмного та технічного забезпечення для створення системи захисту на основі NGFW "*

Виконав: студент

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

Грищук Д.В.
підпис (прізвище та ініціали)

Керівник *Карпінський М.П.*
підпис (прізвище та ініціали)

Нормоконтроль
підпис (прізвище та ініціали)

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

Рецензент
підпис (прізвище та ініціали)

м. Тернопіль – 2022

АНОТАЦІЯ

Аналіз та вибір програмного та технічного забезпечення для створення системи захисту на основі NGFW // Кваліфікаційна робота ОР «Бакалавр» // Грищук Дмитро Володимирович // Тернопільський національний технічний університет імені Івана Пулюя, факультет комп'ютерно-інформаційних систем і програмної інженерії, кафедра кібербезпеки, група СБс-42 // Тернопіль, 2022 // С. , рис. – , табл. – , кресл. – , додат. – .

Ключові слова: КІБЕРБЕЗПЕКА, РИЗИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, ПОЛІТИКА БЕЗПЕКИ.

Метою дипломного проєкту є розробка та реалізація політики інформаційної безпеки у мережі інтернет-магазину компанії ТОВ "ОКЕЙ".

Для досягнення поставленої мети потрібно вирішити такі завдання:

– навести короткий опис компанії та таблицю показників її діяльності, малюнок організаційної структури та його опис.

– провести аналіз ризиків інформаційної безпеки;

– специфікувати комплекс завдань, що підлягають подальшому вирішенню;

– провести аналіз та обґрунтування вибору системи безпеки;

– провести вибір нормативних актів вітчизняного та міжнародного права, які будуть використовуватися як основа для розробки внутрішніх нормативних документів, а також розробити зразки документів безпекової політики;

– описати програмно-апаратні засоби інформаційної безпеки, що впроваджуються (розробляються), а також описати контрольний приклад застосування обраних засобів інформаційної безпеки.

Об'єктом дослідження є процес проєктування та розробки системи безпеки.

Предметом дослідження є інтернет-магазин компанії ТОВ "ОКЕЙ" та забезпечення його інформаційної безпеки

Практична вагомість. Впровадження запропонованих у роботі заходів дозволить підвищити захищеність інформаційних активів, знизить ризики їх безпеки та підвищить ефективність їх захисту.

ANNOTATION

Software-hardware Analysis and Choice to Create NGFW-based Security System // Qualification thesis of educational level "Bachelor" // Hryshchuk Dmytro Volodymyrovych // Ternopil National Technical University named after Ivan Pulyuy, Faculty of Computer Information Systems and software engineering, Department of Cybersecurity, СБс-42 group // Ternopil, 2022 // P. , fig. - , table. - , chair. - , added. - .

Keywords: CYBERSECURITY, RISKS OF INFORMATION SECURITY, SECURITY POLICY.

The purpose of the graduation project is the development and implementation of an information security policy in the network of the online store of the company “OKEY”.

To achieve this goal, it is necessary to solve the following tasks:

– provide a brief description of the company and a table of indicators of its activities, a drawing of the organizational structure and its description.

– conduct an analysis of information security risks;

– specify a set of tasks to be further solved;

– analyze and justify the choice of a security system;

– conduct a selection of normative acts of domestic and international law, which will be used as the basis for the development of internal normative documents, as well as develop samples of security policy documents;

– describe the implemented (developed) software and hardware information security tools, as well as describe a control example of the application of the selected information security tools.

The object of the study is the process of designing and developing a security system.

The subject of the study is the online store of the company “OKEY” and ensuring its information security.

Practical significance. The implementation of the measures proposed in the work will improve the security of information assets, reduce the risks of their security and increase the effectiveness of their protection.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

LAN – Local Area Network (локальна обчислювальна мережа).

SLE – Single Loss Exposure (оцінка очікуваного можливого збитку від одиничної реалізації певної загрози).

ALE – Annual Loss Exposure (Підсумкові очікувані втрати від конкретної загрози за певний період).

ЛОМ –локальна обчислювальна мережа.

ІБ – інформаційна безпека.

ІС –інформаційна система.

ПЗ – програмний застосунок.

ІАУ (Ідентифікація та Аутентифікація суб'єктів доступу та об'єктів доступу) – забезпечуються програмними засобами ОС: Windows 8, Windows 10, Ubuntu 14.04, Windows 2016 Server.

УДС – Управління доступом суб'єктів доступу до об'єктів доступу.

ОПС – Обмеження програмного середовища.

ЗМНІ – Захист машинних носіїв персональних даних.

РПБ – Реєстрація подій безпеки.

АЗ – Антивірусний захист.

СВВ –Система Виявлення вторгнень.

КЗД – Контроль (аналіз) захищеності персональних даних.

ЗЦІ –Забезпечення цілісності інформаційної системи та персональних даних.

ЗДІ – Забезпечення доступності персональних даних.

ЗСВ – Захист середовища віртуалізації.

ЗІС – Захист інформаційної системи, її засобів, систем зв'язку та передачі даних.

ЗТЗ – Захист технічних засобів.

ВІР – Виявлення інцидентів та реагування на них.

УКФ – Управління конфігурацією інформаційної системи та системи захисту персональних даних.

ЗЗІ – Засоби захисту інформації.

СЗІ – система захисту інформації.

ПЕМВН – побічні електромагнітні випромінювання та наведення.

ВСТУП

Новітня технологія комп'ютерних мереж дає змогу зберігати, обробляти, передавати інформацію і, головне, давати людям можливість вести бізнес у будь-якій точці африканського континенту. Інтернет-технології включають корпоративні програми, програми управління знаннями, системи підтримки прийняття рішень, зберігання даних і пошукові запити, а також частини зовнішніх систем, наприклад ті, що працюють з постачальниками, клієнтами (електронна комерція) і бізнес-партнерами. Завдяки всій потужності комп'ютерних, мережевих та Інтернет-технологій організації можуть скористатися багатьма перевагами, зокрема швидшим доступом до інформації, більшою функціональністю для користувачів, покращеним обслуговуванням клієнтів, нижчими витратами та покращеною видимістю в Інтернеті. Ці переваги також спонукають компанії впроваджувати Інтернет-технології незалежно від загроз безпеці, які вони представляють.

ІТ продовжує ставати більш централізованою. У той час як десять років тому кожен бізнес мав свою власну програмну систему заробітної плати, складування і продажів, сьогодні такі функції все частіше передаються на зовнішній поспіль зовнішнім постачальникам. Іноді може бути просто зберігання чи обчислювальні функції, але й саме програмне забезпечення також здається у найми, тобто. програмне забезпечення надається як послуга. Основою для таких рішень є бажання знизити постійні витрати - набагато дешевше обходиться один центр зберігання та обробки даних для кількох компаній, ніж якби кожна з них мала свій власний.

Критично важливим бізнес-активом для повсякденної діяльності будь-якої компанії та її виживання є конфіденційна інформація про продукти, процеси, клієнтів та постачальників. Найбільш поширеною загрозою в мережній системі є несанкціонований доступ до інформаційних та обчислювальних ресурсів компанії. Це може призвести до втрати

конфіденційності, цілісності та доступності інформації, яка є технологічним активом.

Несанкціонований доступ до даних через компрометування комп'ютерної безпеки також відомий як злом. В ідеалі будь-яка організація повинна мати якийсь план реагування на інциденти для боротьби зі зломами локальної мережі, але дослідження показують, що цьому моменту приділяється мало уваги.

Для того, щоб забезпечити безперервність бізнесу та звести до мінімуму потенційні збитки, компаніям необхідно встановити контроль доступу, щоб захистити свою особисту інформацію від навмисного або випадкового розкриття, модифікації, знищення або копіювання, а також свої IT-ресурси від неправомірного використання. Такий контроль забезпечить організацію можливістю обмежувати, контролювати та захищати конфіденційність, цілісність та доступність своїх інформаційних ресурсів.

Тільки технічних рішень (апаратних чи програмних) у тому, щоб процес роботи у компанії з допомогою складних локальних мереж був надійним і безпечним явно недостатньо. Потрібний єдиний комплексний план, що включає як список щоденних заходів щодо забезпечення безпеки та резервного копіювання даних при збоях системи, так і спеціальні плани дій у позаштатних ситуаціях (пожежа, відключення електроживлення, стихійні лиха).

Високий рівень системи інформаційної безпеки підвищує довіру клієнтів і партнерів і часто є однією з основ успіху компанії.

Слід також зазначити, що окремі сфери діяльності (банки та фінансові установи, інформаційні мережі, системи державного управління, оборонні та спеціальні структури) вимагають особливих заходів безпеки даних і, залежно від їх характеру та важливості, висувають підвищені вимоги до достовірності інформації. системи їх завдання.

Відповідні технічні та організаційні заходи повинні бути вжиті проти несанкціонованої або незаконної обробки даних, а також від випадкової втрати або знищення або пошкодження. На практиці це означає, що компанії повинні

мати відповідний захист, щоб запобігти втраті інформації. Зокрема, необхідно розробити та організувати безпеку компанії таким чином, щоб відповідати природі інформації, яка в ній зберігається та використовується, а також передбачати шкоду, яка може виникнути внаслідок порушення безпеки. Особливо важливим є чітке знання та розуміння, хто в компанії відповідає за забезпечення інформаційної безпеки. Необхідно переконатися, що у компанії існує право фізичної та технічної безпеки, підкріплене надійною політикою та процедурами проведення інформаційної безпеки. Не мало важливим є наявність добре навченого персоналу, готового швидко та ефективно реагувати на будь-яке порушення безпеки.

Актуальність цієї роботи залежить від необхідності проектування та розробки систем безпеки, таких як інтернет-магазини відеоігор та консолей. Розроблена система дозволить підвищити рівень захисту персональних даних, що зберігаються та обробляються в корпоративних інформаційних системах.

РОЗДІЛ 1
АНАЛІЗ ПРЕДМЕТНОЇ ОБЛАСТІ

1.1. Техніко-економічна характеристика предметної галузі

1.1.1. Загальна характеристика предметної галузі.

Інтернет-магазин компанії ТОВ “Окей” забезпечує клієнтам зручний інструмент для вибору та замовлення продуктів та напівфабрикатів. Також що існує інтернет-магазин допомагає в оформленні замовлень та їх оплату клієнтами безпосередньо з сайту, та забезпечує зворотний зв’язок між клієнтом та менеджером за допомогою дзвінка, замовлення (без онлайн оплати) або навіть просто питання із сайту.

Також Інтернет-магазин забезпечує можливість реалізації маркетингових інструментів та стратегії (акцій, знижок, персоналізованих пропозицій тощо) з метою підвищення середнього чека, відсотка повторних замовлень та рекомендацій.

Захист інформації – це сукупність заходів, спрямованих на забезпечення захисту та збереження даних, що зберігаються та обробляються в інформаційній системі підприємства.

Щодо інтернет-магазину, то він працює з великою кількістю персональних данних, які потребують захисту, таких як:

- особисті дані покупців;
- банківські та інші реквізити;
- особисті дані постачальників;
- облік наявного майна;
- внутрішній документообіг.

Ці дані потребують пристальної уваги щодо захисту. Тому система захисту інформації інтернет-магазину розроблена для вирішення таких завданнь:

– створення контролю доступу до хостингу, доступи до панелі керування хостингом (шлях/ір, логін, пароль), FTP-доступи (шлях/хост, логін, пароль),

– доступи до БД (шлях до бази даних, ім'я баз даних, ім'я адміністратора та користувачів бази даних, паролі);

– призначити відповідальних осіб, які мають доступ до адміністративної панелі Інтернет-магазину;

– створити та налаштувати корпоративну пошту для комунікації клієнтів та співробітників компанії;

– здійснення контролю та фільтрування вхідної та вихідної пошти, використання у робочих процесах особистих акаунтів;

– розмежування доступом до поштових аккаунтів та адміністративної панелі керування Інтернет-магазину;

– здійснення контролю наявного та нового контенту Інтернет-магазину;

– резервне копіювання всіх файлів, які мають інформаційну цінність (бази даних, листів, клієнтської бази, бази товарів, контенту).

При реалізації бізнес-процесу, який пов’язаний із захистом даних Інтернет-магазину, необхідно сформувати такі документи:

– перелік даних, що потребують захисту;

– перелік назначених відповідальних осіб;

– перелік заходів та засобів, що забезпечують захист даних;

– політика безпеки компанії.

Діяльність компанії ТОВ “Окей” спрямована на продаж харчові продукти та напівфабрикатів гуртом та в роздріб за допомогою однойменного інтернет-магазину.

Компанія має ряд філій в яких працює від 20 і більше фахівців, співробітники мають високу кваліфікацію та великий досвід. Робота співробітників пов’язана із консультуванням клієнтів, а також оформленням замовлень.

Для зберігання товарів використовується склад загальною площею 1000 м^2, що знаходиться в Тернопільської області. Для безплатного доставлення по Тернонілю використовується кур'єрське доставлення, що здійснюється за допомогою власного автопарку.

Основні види діяльності компанії «Окей», пов'язані зі зберіганням та обробкою даних, включають:

- обробка замовлень клієнтів;
- зберігати контактні дані покупця;
- обробка реквізитів платежів;
- обробка даних постачальника;
- складський облік;
- внутрішній документообіг;
- забезпечити безперервну роботу порталу;
- внутрішній аудит інформаційних систем компанії;
- регулювання діяльності з обробки інформації;
- доступ до інформаційних ресурсів;
- контроль корпоративного трафіку.

Основні показники ефективної діяльності наведена у табл. 1.1

Таблица 1.1 – Основні характеристики (показники ефективності) видів діяльності

№ з\п	Найменування характеристики (показника)	Значення показника місяць
1	Робота із замовленнями клієнті	200 замовлень на день
2	Зберігання контактних даних клієнтів	200 транзакцій на день
3	Робота з реквізитами	300 транзакцій на день
4	Робота з відомостями постачальників	250 транзакцій на день
5	Складський облік	400 транзакцій на день
6	Документообіг (внутрішній)	300 повідомлень на день
7	Забезпечення безперервної роботи Web-порталу	24/7
8	Аудит внутрішньої корпоративної інформаційної системи	Щотижнево
9	Регламентація обробки інформації з регламентуванням	Щотижнево
10	Доступ до інформаційних ресурсів	24/7
11	Контроль корпоративного трафіку	Щоденно

1.1.2. Організаційно-функціональна структура підприємства.

Структура компанії ТОВ “Окей” включає та наведена на рис.1.1:

– відділ по роботі з клієнтами;

– відділ доставлення;

– складський облік;

– відділ кадрів;

– бухгалтерія;

– ІТ-відділ.

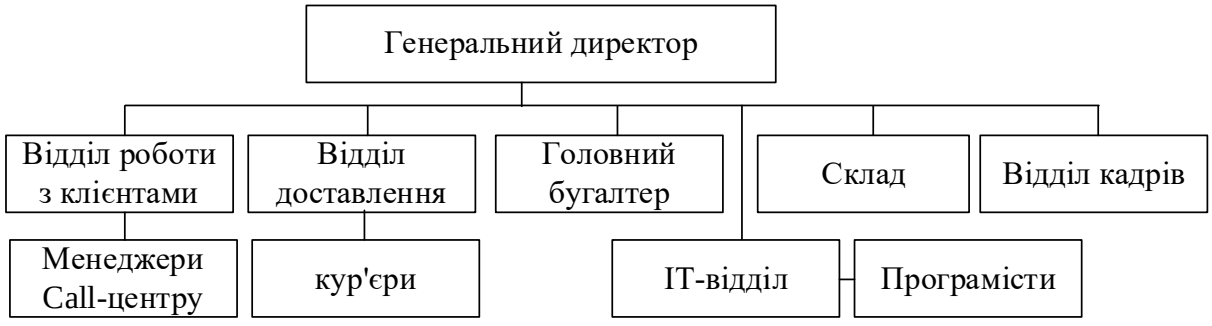

Рисунок 1.1 – Організаційно-функціональна структура підприємства

Відділ обслуговування клієнтів координує діяльність усіх відділів компанії, які займаються продажем ігрових приставок.

Основними функціями цього відділу є:

- Обробка персональних даних клієнтів.
- Координувати роботу різних відділів обслуговування клієнтів компанії.
- Консультувати клієнтів з усіх аспектів закупівлі.
- Виконувати замовлення клієнтів, формувати платіжні документи та доставляти замовлення;
- Ознайомлення клієнтів про процес виконання та доставлення їх замовлень.

– Організація та підтримка документообігу між клієнтами та відділами компанії.

1.2. Аналіз ризиків інформаційної безпеки

1.2.1. Ідентифікація та оцінка інформаційних активів.

Розробка правил політики безпеки покликане забезпечити завдання, які пов’язані з наступною діяльністю:

– забезпечення захисту персоналу та конфіденційної інформації, що збирається, зберігається та обробляється в компанії;

– набір правил, яких повинні дотримуватись користувачі, системні адміністратори та інші співробітники фірми, які працюють з конфіденційною інформацією;

- забезпечення доступу співробітників компанії до конфіденційних даних через проходження авторизації, логування всіх подій;
- визначати ризики від зовнішніх загроз та мінімізувати їх наслідки;
- визначити основну концепцію безпеки компанії;
- розробкити заходи, спрямовані на зниження ризиків від виявлених загроз та вразливостей;
- гарантія контролю для дотримання політики безпеки.

Аналіз бізнес-процесів інтернет-магазинів дозволяє ідентифікувати такі дані, які обробляються та зберігаються в інформаційних системах підприємства.

1. Персональні дані замовника. Містить особисту інформацію клієнта. Необхідно забезпечити цілісність, доступність і конфіденційність даних.

2. Інформація про постачальників компанії. Містить інформацію про постачальника товару. Необхідно забезпечити високий ступінь конфіденційності даних. Бо витік цих даних принесе підприємству економічні збитки.

3. Потік внутрішніх файлів компанії включає документи компанії, такі як офіційні документи співробітників компанії, накази та накази. Захист даних повинен забезпечувати цілісність і конфіденційність таких даних.

4. Облік складу – це інформація, яка вказує на кількість товару на складі, а також його рух. При захисті цього активу зберігається цілісність та доступність даних.

У табл. 1.2 представлено оцінку вразливості інформаційних активів підприємства.

Таблиця 1.2 – Оцінка вразливості інформаційних активів підприємства

Вид діяльності	Найменування активу	Форма уявлення	Власник активу	Критерії вартості	Розмірність оцінки	
					кількісна	якісна
Інформаційні активи						
Робота із замовленнями клієнтів	Персональні дані клієнта	Електронний ресурс	Адміністратор системи, менеджери	Втрата конфіденційності	100000 грн.	Висока
Зберігання контактних даних покупців						
Робота з платіжними реквізитами	Внутрішній документообіг	Електронний ресурс, Паперові носії		Втрата конфіденційності Порушення цілісності	250000 грн.	
Робота з даними постачальників	Дані про постачальників	Електронний ресурс		Втрата конфіденційності	70000 грн.	Середня
Складський облік	Складський облік			Вартість активу	70000 грн.	Середня
Активи програмного забезпечення						
безперервна робота Web-порталу	ПЗ Web-сервер, ПЗ інтернет магазину	Електронний ресурс	Адміністратор системи	Втрата конфіденційності Порушення	50000 грн.	Висока

Вид діяльності	Найменування активу	Форма уявлення	Власник активу	Критерії вартості	Розмірність оцінки	
					кількісна	якісна
				цілісності Втрата доступності Вартість відтворення		
Доступ до інформаційних ресурсів	ПЗ Web-сервер, ПЗ інтернет магазину	Електронний ресурс	Адміністратор системи	Втрата конфіденційності Порушення цілісності Втрата доступності Вартість відтворення	50000 грн.	Висока
Фізичні активи						
Забезпечення безперервної роботи Web-порталу	Web-сервер	сервер	Адміністратор системи	Вартість оновлення чи ремонту обладнання	50000 грн.	Висока

Перелік інформаційних активів, обов’язкове обмеження доступу, яких регламентується чинним законодавством, зведено у таблицю 1.3.

Таблиця 1.3 – Перелік відомостей конфіденційного характеру

№ з/п	Найменування відомостей	Гриф конфіденційності
1	Відомості, що розкривають характеристики засобів захисту інформації ЛОМ підприємства від несанкціонованого доступу.	конфіденційно
2	Вимоги щодо забезпечення збереження службової таємниці працівниками підприємств	
3	Персональні дані працівників	для службового користування
4	Дані постачальників	
5	Дані про складський облік	
6	Внутрішній документообіг	

Результат ранжування подається у вигляді інтегрованої оцінки ступеня важливості активу для підприємства, які оцінені за п'ятибальною шкалою та внесені до табл. 1.4.

Таблиця 1.4 – Результати ранжування активів

Найменування активу	Цінність активу (ранг)
Інформаційні активи	

Дані співробітників компанії	3
Внутрішній документообіг	4
Дані клієнтів компанії	4
Дані складського обліку	5
Фінансова звітність	5
Фізичні активи	
Мережеве обладнання	3
Сервер баз даних	4
Web-сервер	5
Активи програмного забезпечення	
ПЗ “Master:Бухгалтерія”	3
ПЗ Сервера Ubuntu Server	4
ПЗ Сервера Windows Server 2019	5
ПЗ Інтернет-магазину	5
СУБД Mysql 5.6.5 M8	5

Активи, що мають найбільшу цінність:

1. Дані складського обліку;
2. Дані клієнтів компанії;
3. Фінансова звітність;
4. Web-сервер;
5. ПЗ сервера;
6. ПЗ інтернет-магазину;
7. СУБД My SQL 5.6.5 M8.

1.2.2. Оцінка вразливостей активів.

Ризик інформаційної безпеки або IT-ризик, пов'язаний з будь-яким ризиком інформаційної безпеки. Хоча інформація довгий час вважалася цінним активом, розвиток економіки знань призвів до того, що організації стають все більш залежними від інформації та результатів її обробки. Різні загрози або події, які компрометують інформацію, можуть призвести до несприятливих наслідків в організації, починаючи від незначних проблем і закінчуючи катастрофічними.

Для оцінки та вимірювання IT-ризику використовуються імовірнісні оцінки різних типів загроз та/або подій та їх очікуваних впливів чи наслідків. Альтернативні підходи до вимірювання IT-ризику часто включають оцінку

інших сприятливих факторів, таких як загрози, вразливості, ризики та вартість активів.

Вразливості в мережевій безпеці з кожним днем з’являються нові, і також вони присутні в кожній мережі. Вразливості можуть бути присутніми як в мережі так і в окремих мережевих пристроях.

Існує три основні типи вразливостей [3]:

- недоліки мережевих технологій;
- недоліки конфігурації;
- недоліки політики безпеки.

Недоліки технологій виражаються недоліками протоколу TCP/IP, вразливостями операційної системи, слабкими сторонами і вразливостями мережевого обладнання. У табл.1.5 представлені описи цих вразливостей.

Таблиця 1.5 – Опис недоліків технологій

Ідентифікатор	Недоліки	Опис
У1.1	Вразливість протоколу TCP/IP	Протоколи TCP/IP, HTTP, FTP, ICMP є по суті незахищеними
У1.2	Вразливості ОС	Операційні системи UNIX, Linux, Macintosh, Windows мають внутрішні проблеми безпеки, які ще остаточно вирішені
У1.3	Вразливості мережного обладнання	Різні типи мережного обладнання, як-от маршрутизатори, міжмережеві екрани тощо. мають такі недоліки: відсутність захисту паролем; відсутність авторизації та верифікації; протоколи маршрутизації; недоліки захисту на рівні портів.

Недоліки та вразливості мережевої конфігурації представлені у табл. 1.6 та 1.7.

Таблиця 1.6 – Вразливості конфігурації

Ідентифікатор	Недоліки	Опис
У2.1	Незахищені дані користувачів	Передачі через мережу незахищеного даних користувача (логін, пароль тощо)
У2.2	Помилки у конфігурації інтернет-сервісів	Надання дозволу на використання JavaScript у браузерах дозволяє здійснювати атаки з підозрілих сайтів. Використання IIS, Apache, FTP та консольних програм також створюють ризик для інформаційної безпеки.
У2.3	Використання слабких паролів у облікових записах користувача	Використання простих та слабких паролів
У2.4	Використання стандартних налаштувань безпеки в ПЗ	Багато програмних продуктів мають налаштування безпеки які встановлені по замовчуванню, які часто не відповідають необхідному рівню безпеки.
У2.5	Використання стандартних установок мережного обладнання	Неправильна конфігурація програмного та апаратного забезпечення може призвести до значних проблем безпеки. Наприклад, помилки конфігурації списків доступу, помилки настроювання протоколів маршрутизації. Відсутність шифрування та керування віддаленим доступом може також завдати значної шкоди безпеці

Таблиця 1.7 – Вразливості у політиці безпеці

Ідентифікатор	Недоліки	Опис
У3.1	Незахищені дані користувачів	Передачі через мережу незахищеного даних користувача (логін, пароль тощо)
У3.2	Використання слабких паролів у облікових записах користувача	Використання слабких або легко згадуваних паролів
У3.3	Використання встановлених налаштувань безпеки у програмних продуктах/застосунках	Багато програмних продуктів мають встановлені за промовчанням налаштування безпеки, які часто не відповідають необхідному рівню безпеки.
У3.4	Використання стандартних установок мережного обладнання	Неправильна конфігурація обладнання може призвести до значних проблем безпеки. Наприклад, помилки конфігурації списків доступу, помилки настроювання протоколів маршрутизації. Відсутність шифрування та керування віддаленим доступом може також завдати значної шкоди безпеці

Недоліки безпеки можуть спричинити непередбачені загрози безпеці. Загрози мережної безпеки можуть виникнути, також якщо користувачі не дотримуються політики безпеки. Табл. 1.8 містить деякі загальні недоліки ПБ.

Таблиця 1.8 – Уразливості політики безпеки

Ідентифікатор	Недоліки	Опис
У4.1	Недоліки в існуючій безпеці	Відсутність стандартної політики безпеки чи наявність у ній помилок
У4.2	Відсутність наступності	Слабкі паролі та паролі, які мають просту структуру або закоротку довжину або ж стандартні паролі, відкривають можливість до несанкціонованого доступу до мережі
У4.3	Відсутність логічного контролю доступу	Недостатній контроль та неналежне здійснення аудит мережі дають можливість зловмисникам проводити атаку на мережеві ресурси
У4.4	Використання апаратного забезпечення та ПЗ без урахування політики безпеки	Встановлення несанкціонованого програмного або апаратного забезпечення без використання політик безпеки може призвести до порушення інформаційної безпеки компанії

У табл. 1.9 представлені результати оцінки вразливості інформаційних активів підприємства

Група вразливостей Зміст вразливості	Дані складського обліку	Дані клієнтів компанії	Фінансова звітність	Web-сервер	ПЗ сервера	ПЗ інтернет-магазину	СУБД
1. Середовище та інфраструктура							
Помилки конфігурації				висока			
Використання стандартних налаштувань				середня			
2. Апаратне забезпечення							
Вразливість веб-сервера	середня			висока			
Вразливість ОС				середня			
Використання встановлених настройок ПЗ				середня	висока		
Установка ПЗ без урахування				середня			

політики безпеки							
4. Комунікації							
Вразливість засобів комунікації	високa						
Вразливість протоколу TCP/IP	високa						
5. Документи (документообіг)							
Недоліки існуючої політики безпеки.	високa						
Передача незахищених даних	середня						
6.Персонал							
Використання слабких паролів	низька				низька		
Відсутність контролю над дією персоналу	низька				низька		
7. Загальні вразливі місця							
Фізичний доступ зловмисників до апаратного забезпечення				середня			

1.2.3. Оцінка загроз активам.

В основному враховують такі фактори, які порушують нормальну роботу інформаційної системи компанії:

- Природна катастрофа. Порушення ІБ спричинені стихійними лихами (наприклад, повені, сильний вітер, блискавки, зсуви тощо), які не контролюються людиною.

- Соціальний хаос. Порушення ІБ через соціальну нестабільність (наприклад, акти саботажу, акти терору, війни тощо).

- Тілесні ушкодження. Інформація, отримана в результаті навмисного або випадкового фізичного впливу на IP компанії або її компоненти (наприклад, пожежа, вода, електростанції, вплив на навколишнє середовище (забруднення,

пил, корозія, замерзання), вандалізм, крадіжка, втрата, неправильне поводження з обладнанням/інформацією про медіа Уступити) .

- Порушення ІБ через вихід з ладу IP компанії та основних компонентів сервісів, які підтримують роботу ІБ (наприклад, вихід з ладу електромережі, системи кондиціонування повітря, системи водопостачання).

- Порушення ІБ через електромагнітне випромінювання, коливання напруги, електронні перешкоди тощо.

- Технічний збій. Або порушення інформаційної безпеки через збій IP-адреси компанії або пов'язані нетехнічні можливості. Такі ризики включають збої апаратного або програмного забезпечення, перевантаження тощо..

– Технічні атаки. Недотримання ІБ, обумовлено атаками на ІС компанії та використанням її вразливостей у конфігуруванні, протоколах, програмах. Наприклад, мережеве сканування, експлуатація вразливості/бекдору, спроба входу, втручання, відмова в обслуговуванні (DOS/DDoS).

За останні роки в країні було прийнято кілька стандартів, які відповідають за регламентацію дій у рамках інформаційної безпеки. До цих стандартів відносяться стандарти сімейства міжнародних стандартів на системи управління інформаційною безпекою ISO/IEC 27 000.

Відповідно до цих стандартів визначено вимоги до систем управління інформаційною безпекою, управління ризиками, метрики та вимірювання, а також посібник із впровадження. Це говорить про актуальність забезпечення інформаційної безпеки та розроблення методик оцінки інформаційної безпеки. Це зумовлюється тим, що розвиток сучасних інформаційних технологій значно випереджає темпи розробки даних методик.

Для оцінки ризику ІБ компанії можна використовувати метод розрахунку. Ця методика призначена для оцінки ризиків інформаційної безпеки під час функціонування або вдосконалення систем інформаційної безпеки.

Цей метод дозволяє визначити числові показники ризиків інформаційної

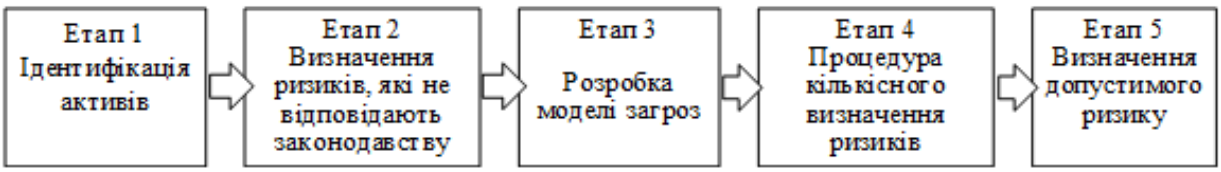

Рисунок 1.2 – Алгоритм проведення оцінки ІБ

безпеки з метою застосування ефективних заходів захисту інформації. Узагальнений алгоритм оцінки ризиків інформаційної безпеки ілюструє рис. 1.2.

Процедури оцінки ризиків інформаційної безпеки як комплексний підхід можуть бути реалізовані співробітниками підприємства спільно з керівництвом. Результати оцінки загроз активам наведені у табл. 1.10.

Таблиця 1.10 – Результати оцінки загроз активам

Група загроз Зміст погроз	Дані складського обліку	Дані клієнтів компанії	Фінансова звітність	Web-сервер	ПЗ сервера	ПЗ інтернет-магазину	СУБД
1. Загрози, зумовлені навмисними діями							
Викрадення бази даних	середня						
Шахрайство з ел. платіжками	низька	висока	низька				
Втручання у процес роботи магазину					висока		
Використання шкідливого коду					середня		
DDoS атаки					середня		
“Сайт-паразит”						середня	
2. Загрози, зумовлені випадковими діями							
Помилки введення інформації	середня						
3. Загрози, зумовлені природними причинами (природні, техногенні фактори)							
Пожежа				середня			
Землетрус				низька			
Повінь				низька			

1.2.4. Оцінка наявних та запланованих засобів захисту.

Інтернет-магазини відеоігор і консолей використовують усі види інформаційних технологій, обладнання, програмного забезпечення та організації.

Компанія представила апаратні технології:

- серверне обладнання для зберігання та обробки даних;

- термінальне обладнання, тобто персональні комп'ютери для отримання інформації;

- мережне обладнання, тобто. Мережевий зв'язок, комп'ютерне та телефонне мережеве обладнання (комутатори, маршрутизатори, АТС тощо);

Програмне забезпечення демонструється в компанії через велику кількість програм. Використовуйте операційні системи Windows та Linux. Використовуйте базу даних MySQL 8.0. Майстер: Для управління компаніями використовуються бухгалтерські платформи. Також існує безліч утиліт та утиліт, таких як: MS Office, антивірусні програми, програми резервного копіювання, електронна пошта тощо. По-перше, організаційна підтримка включає планування, розробку та впровадження нових рішень, призначених для підвищення ефективності бізнесу. Сюди також входить заповнення та обробки баз даних співробітниками компанії, підтримка актуального статусу веб-сайту компанії.

Тому сьогодні неможливо уявити жодну сферу діяльності, яка б не використовувала інформаційні технології.

В епоху швидкого розвитку інформаційних технологій, швидкості апаратного забезпечення збільшується, з’являються нові оновлення програмного забезпечення та вдосконалення методів взаємодії з ними, потрібно постійно бути в курсі подій. «Хороші» компанії постійно збирають та аналізують інформаційні технології, тим самим впроваджуючи необхідні інновації в робочий процес. Так само нові технології використовуються в міру зростання компаній і появи нових сфер діяльності.

Однією з найважливіших ролей компанії є обладнання. Його основні складові: робочі станції, сервери, мережеве обладнання та телефонія (АТС, телеком, телефонія).

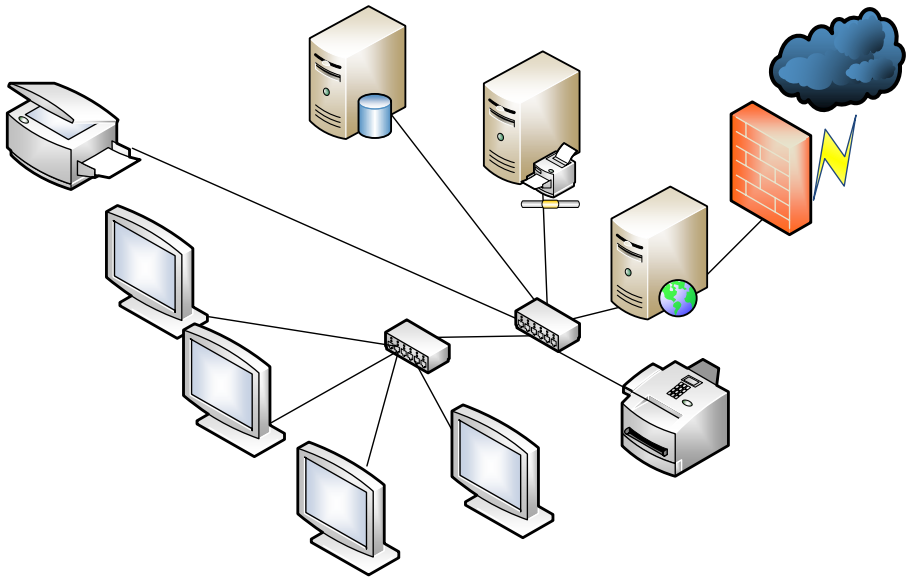

Рис.1.3. – Структурна схема мережі філії

Компанія працює зі своїми співробітниками за допомогою офісних ПК під керуванням сімейства операційних систем Windows 10. Ці робочі станції мають доступ до локальної мережі компанії, глобальної мережі, Інтернету. Вони також використовуються для обробки документів, доступу до баз даних, обробки веб-сайтів компаній, обробки електронних листів тощо. На операційних системах Windows і Linux є два сервера, які використовуються для різних цілей компанії. Вони використовуються як веб-сервери, сервери баз даних, сервери зберігання даних, поштові сервери, термінальні сервери. В якості мережевих пристроїв використовуються комутатори Cisco. Так само, локальна мережа компанії підключена до Інтернету через маршрутизатор брандмауера Cisco (рис. 1.3).

Компанія має 2 клас захищеності даних, оскільки масштаб інформаційної системи є регіональним.

На основі обраного класу захищеності в компанії ТОВ “Окей” реалізується такі набори захисних заходів:

– IAU (Identification and Authentication of Access Entities and Access Objects) - забезпечується програмним забезпеченням операційної системи: Windows 8, Windows 10, Ubuntu 14.04, Windows 2016 Server.

– УДС (Управління доступом суб’єктів доступу до об’єктів доступу) для програмного забезпечення операційної системи: Windows 10, Ubuntu 14.04, Windows 2019 Server..

– ОПС (Обмеження програмного середовища) – Виконується системним адміністратором співробітника організації.

– ЗМНІ (Захист машинних носіїв персональних даних) – надаються особою, відповідальною за організацію обробки даних.

– РПБ (Реєстрація подій безпеки) – забезпечуються міжмережевими екранами (МЕ) не нижче 3 класу.

– СОВ (Виявлення вторгнень) – забезпечується вибраним антивірусним програмним забезпеченням і IU рівня 3 або вище (Антивірус Касперського).

– ЗЦІ (Забезпечення цілісності інформаційної системи та персональних даних) – Надається адміністратором персоналу організації.

– ЗДІ (Забезпечення доступності персональних даних) – Надається адміністратором персоналу організації.

– ЗСВ (Захист середовища віртуалізації) – Надається програмним забезпеченням операційної системи: Windows 10, Ubuntu 14.04 та адміністратором співробітника організації.

– ЗІС (Захист інформаційної системи, її засобів, систем зв’язку та передачі даних) – забезпечується безпечними каналами зв'язку та шифруванням інформації, що передається через них.

– ЗТЗ (Захист технічних засобів) – надається особою, відповідальною за організацію обробки даних.

– ВІР (Виявлення інцидентів та реагування на них) – забезпечується відповідальним за організацію обробки даних.

– УКФ (Управління конфігурацією інформаційної системи та системи захисту персональних даних) – забезпечуються відповідальним за організацію обробки даних.

Численні публікації останніх років показали, що інформація, що розповсюджується в корпоративних IP або через канали зв'язку,

використовується не зловживано, оскільки вдосконалюються запобіжні заходи. На даний момент захист інформації вимагає не лише створення механізмів приватного захисту, а й впровадження системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних програмно-технічних засобів, організаційних заходів, нормативних актів, морально-етичних контрзаходів тощо). Складність захисту пов'язана зі складною поведінкою зловмисників, які намагаються отримати доступ до всього, що для них важливо. Сьогодні можна сказати, що народжується нова сучасна технологія – технологія захисту інформації в комп'ютерних інформаційних системах і мережах даних.

Потужність і засоби різних підприємств відрізняються за структурою, характером і порядком використання. Оскільки компанія має справу лише з конфіденційною інформацією на постійній основі, а захист інформації не є основним видом діяльності компанії, у компанії немає відділу, а є деякі спеціалісти із захисту інформації. Відповідальні особи підприємства представлені у табл. 1.11.

Таблиця 1.11 – Перелік довірених осіб

Довірені користувачі	Обґрунтування
Штатний програміст організації	Рекомендації з попередніх місць роботи Його звільнили не за втрату впевненості достатньо досвіду Підписати договір про нерозголошення
Штатний адміністратор організації	Рекомендації з попередніх місць роботи Його не звільнили за невпевненість достатньо досвіду Підписати договір про нерозголошення
Адміністратор безпеки	Рекомендації з попередніх місць роботи Його звільнили не за втрату впевненості достатньо досвіду Підписати договір про нерозголошення конфіденційної інформації
Оператор, який діє у межах повноважень	Отримувати доступ до деяких даних на основі посадових обов'язків Підписати договір про нерозголошення
Спецслужби	Спецслужби можуть отримати доступ до даних за допомогою законних механізмів.

Технічними засобами, поданими у табл.1.12, гарантується діяльність підприємств.

Таблиця 1.12 – Технічні характеристики апаратних засобів

Назва	Характеристика	Вартість
Сервер для баз даних	Server 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 2.66ГГц Модуль пам'яті 4 GB (2x2GB) PC2-5300 667 MHz ECC Chipkill DDR2 FBDIMM Вінчестер SAS 146GB HS 2.5" 10K RPM HDD	179088
Веб-сервер	Server IBM x3650 1x Quad-Core Xeon E5430 2.66 GHz/1333 MHz 12MB L2 2x2GB PC2-5300 DDR2 Chipkill SDRAM, 0 GB HD 2,5", SR 8k, CD-RW/DVD-ROM Combo, ATI RN50 video (16 MB), 2x Broadcom Гігабіт Езернет, 1x 835 W power supply Модуль пам'яті 4 GB (2x2GB) PC2-5300 667 МГц ECC Chipkill DDR2 FBDIMM Жорсткий диск 146GB Hot-Swap 2.5" 10K RPM Ultra320 SAS HDD	123291
Клієнтські компютери	POWERMAN ES722BK, Intel Celeron J1800 2400MGs DDR3 4 Gb Hynix 60 Гб SSD SB60, Відео-карта: Вбудований блок живлення FSP 400W	10660
Маршрутизатор	TPlink DSR-1000 2 порти WAN 10/100/1000Base-T 4 порта LAN 10/100/1000Base-T 2 порта USB3.0	14028
Точка доступу	Точка доступу TP-Link < DAP-2310 > AirPremier N Точка доступу (1UTP 10 / 100Mbps, 802.11b / g / n, 300Mbps) Характеристики: 2.4 Ggs N300 Мбіт/с Безпровідний 2 антени WDS-Bridge, Adapter, AP Фільтрація по MAC-адресам WPA2-Розширений, WPA-Розширений, WPA2-Персональний, WPA-Персональний, WEP-кодування з 64- або 128-бітним ключом	1455
МФУ	Лазерне МФУ Panasonic KX-MB2000RUB Лазерне МФУ Brother DCP-1510R	8890 9940
Джерело безперебійного живлення	Блок живлення Redundant power supply HS 835W Блок живлення Express Redundant Power and Cooling Option (39Y5836) x3400/x3500	4964 4692

Наглядним прикладом технічної архітектури компанії можна ознайомитись на рис.1.4. Технічні характеристики ПЗ підприємства представлено у табл. 1.13.

Таблиця 1.13 – Технічні характеристики ПЗ

Назва	Опис ПЗ	Вартість
Сервер баз даних	MY SQL 8.0. Enterprise Edition Windows Server 2016	2000 USD
Веб-сервер	Ubuntu Server 14.04, Apache 2.4, PHP 8.0, Perl, phpMyAdmin 5.1,	1400 USD
Клієнтські комп'ютери	Windows 10, БП FSP 400W	240 USD
Антивірус	Avast для Windows Workstations (20 комп'ютерів + 2 сервера)	320 USD на рік
MASTER: Бухгалтерія	MASTER: Бухгалтерія Клієнтська ліцензія на 5 робочих місць	2500

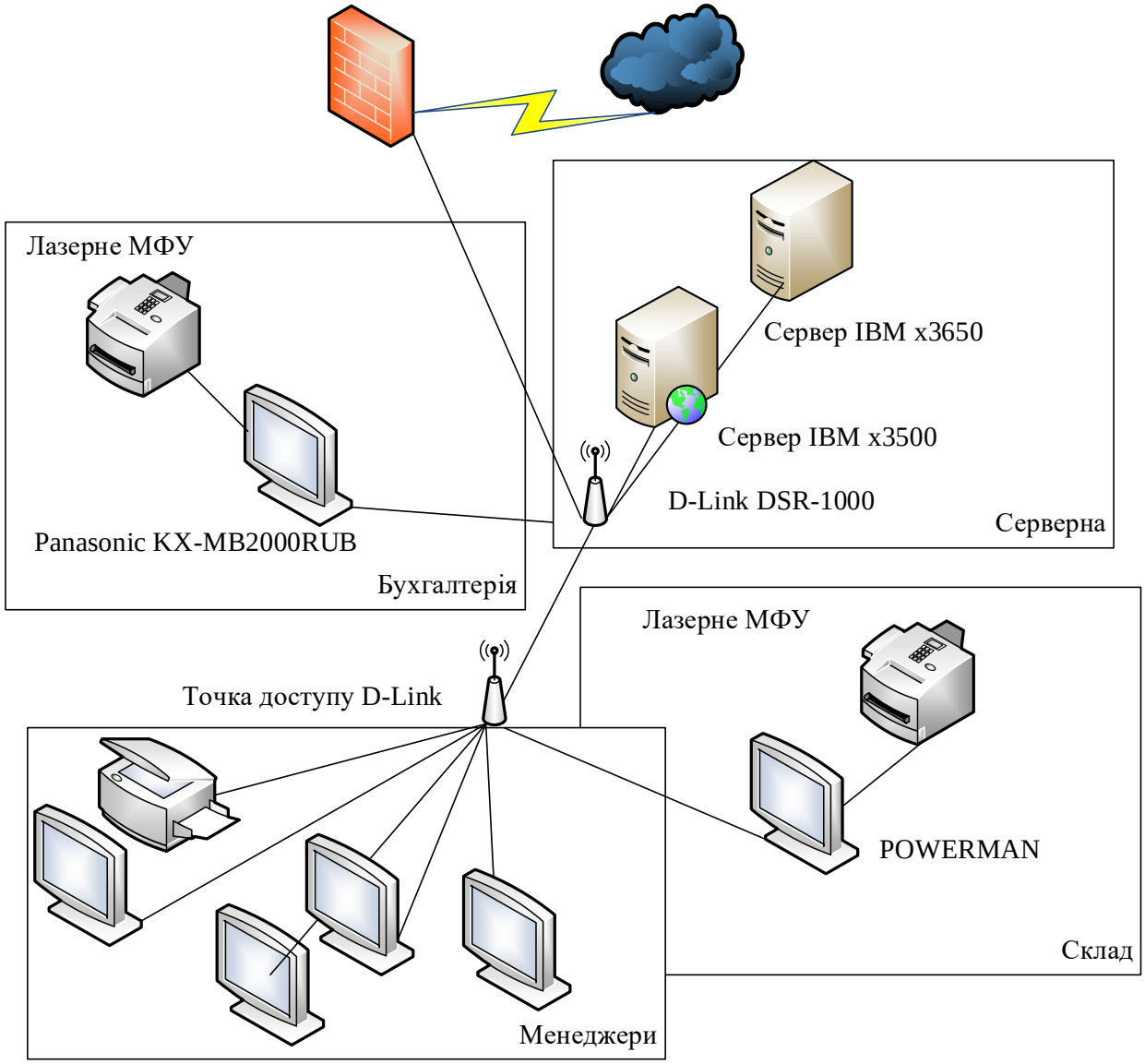

Рисунок 1.4 – Приклад технічної архітектури компанії

В організації реалізовано інженерно-технічне забезпечення у вигляді системи відеоспостереження. Офіс компанії розташований на 1 поверсі офісної будівлі. Офіс фірми складається з коридору, одного технічного приміщення (серверна) та 4 кабінетів. Перед входом до офісу розташувався пост охорони та зона ресепшн. Камери відеоспостереження розміщені так (рис. 1.5).

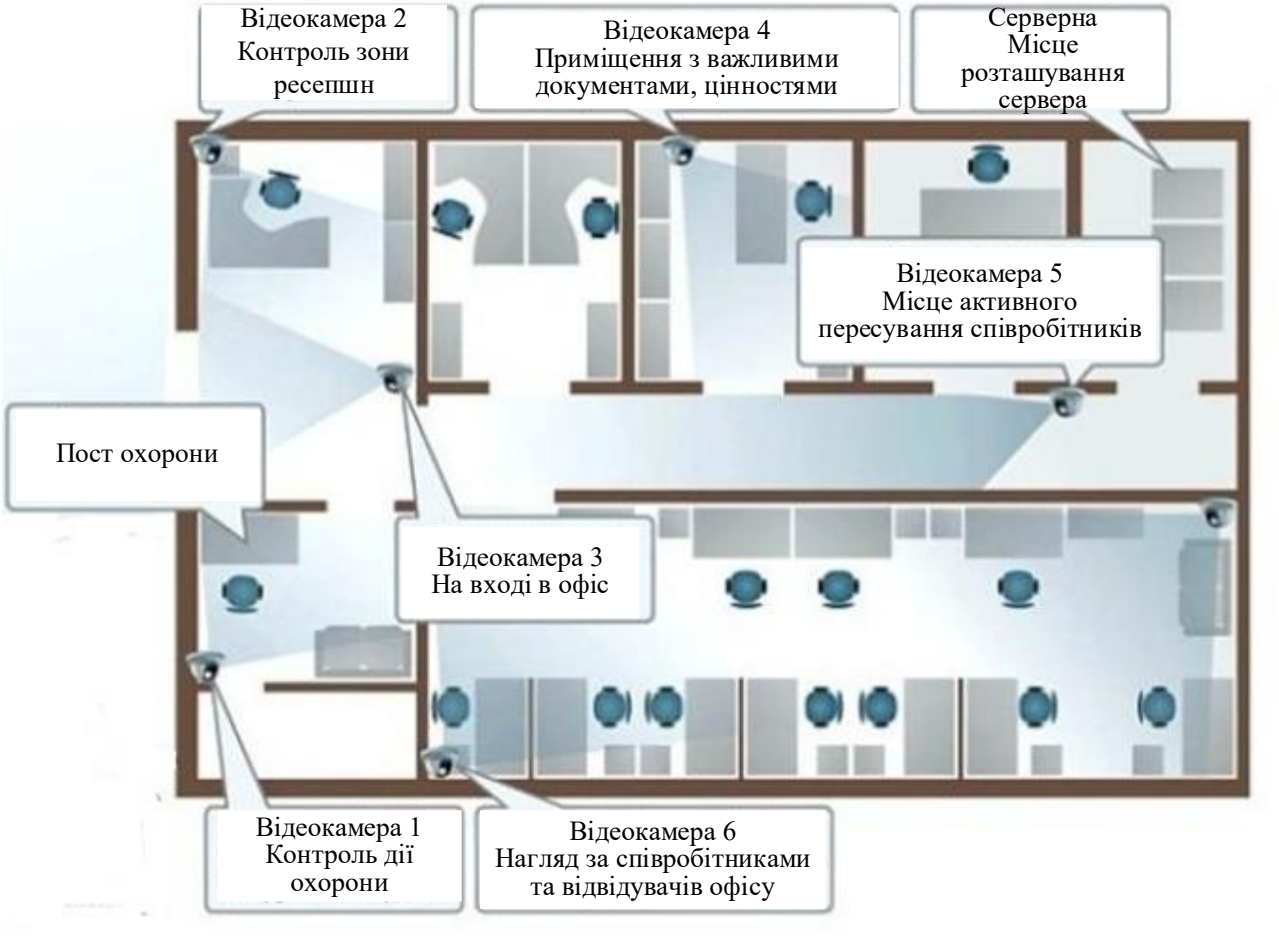

Рисунок 1.5 – План розташування відеокамер в офісі фірми

Система відеоспостереження повинна реалізована на базі IP-відеореєстратора та шести кольорових IP-відеокамер високої роздільної здатності, що працюють у режимі день/ніч. У кожному робочому кабінеті та коридорі встановлено по одній відеокамері, що дозволяє контролювати весь периметр офісного приміщення. Місткість відеоархіву становить приблизно 3-4 тижні. Також організований доступ до системи через Інтернет із веббраузера комп'ютера або з мобільного пристрою на базі Android та iOS.

Система відеоспостереження реалізована на основі програмного забезпечення Лінія.

Результати оцінки, що діє системи безпеки інформації, що показує, наскільки повно виконуються однотипні об’єктивні функції під час вирішення завдань по гарантії захисту важливої інформації, представлені в табл. 1.14.

Таблиця 1.14 – Аналіз виконання основних завдань із забезпечення інформаційної безпеки

Основні завдання щодо забезпечення інформаційної безпеки	Ступінь виконання
забезпечення безпеки торгової діяльності, захист інформації та відомостей, що є комерційною таємницею;	Середня
організація роботи з правового, організаційного та інженерно-технічного (фізичного, апаратного, програмного та математичного) захисту комерційної таємниці;	Середня
організація спеціального діловодства, що унеможливлює несанкціоноване отримання відомостей, що є комерційною таємницею;	Низка
Не допускати необгрунтованого доступу та публічного доступу до інформації та творів, що становлять комерційну таємницю;	Висока
виявляти та знаходити канали, через які конфіденційна інформація може витікати під час щоденної виробничої діяльності та в екстремальних (аварії, пожежі тощо) ситуаціях;	Середня
забезпечення режиму безпеки під час здійснення таких видів діяльності, як різноманітні зустрічі, переговори, наради, засідання та інші заходи, пов'язані з діловим співробітництвом на національному та міжнародному рівні;	Низка
забезпечення охорони території, будівель приміщень, з інформацією, що захищається.	Середня

Проведений аналіз показав, що в організації недостатньо приділяється уваги питанням гарантії інформаційного захисту даним, які зберігаються та обробляються компанією. Для збільшення ступеня захищеності в роботі пропонується використання брандмауерів наступного покоління (Next-Generation Firewall NGFW) для захисту внутрішньої структури локальної мережі підприємства та додавання нових засобів контролю доступу. Також розглядаються питання уточнення та зміни політики безпеки компанії.

1.2.5 Оцінка ризиків.

У більшості випадків для розрахунку ризику використовується формула з наступними параметрами:

– вартість ресурсу (Asset Value, AV). Ці відділи та посади є органами захисту інформації. Це значення представляє вартість ресурсу. У якісних оцінках ризику вартість ресурсу зазвичай становить від 1 до 3, де 1 — найнижча вартість ресурсу, 2 — середня вартість ресурсу, а 3 — найвища вартість ресурсу. У нашому прикладі сервер баз даних і веб-сервер мають значення AV = 3, а інформаційна система інтернет-магазину клієнтського комп'ютера має AV = 1;

– Вимірює вразливість ресурсу до загроз (коефіцієнт впливу, EF). Цей параметр показує, наскільки вразливий ресурс до аналітичних загроз. У нашому випадку найбільш доступним виявився ресурс інтернет-магазину. Тому атаки відмови в обслуговуванні (DoS) становлять для нього найбільшу загрозу. При якісній оцінці ризику це значення також ранжується за шкалою від 1 до 3, де 1 - найменш уразливі (слабкі дії), 2 - середні (ресурси, які необхідно відновити), 3 - найбільші (ресурси, які необхідно відновити). замінити після повної загрози);

– Річний коефіцієнт виникнення (ARO) показує, наскільки добре можна досягти певної загрози за певний період часу (зазвичай рік), а також оцінюється за шкалою від 1 до 3 (низький, середній, високий).

На основі отриманих даних виводиться оцінка очікуваного збитку (рівень ризику):

Оцінка очікуваного можливого збитку від одноразової реалізації певної загрози (Single Loss Exposure, SLE) розраховується за наступною формулою:

$$SLE = AV \times EF.$$

Річний ризик збитків (ALE) характеризує величину ризику і розраховується за такою формулою:

$$ALE = SLE \times ARO.$$

Кінцевий результат є добуток:

$$ALE = ((AV \times EF = SLE) \times ARO).$$

Результат розрахунків ризиків представлені у табл. 1.15.

Таблиця 1.15 – Результати оцінки ризиків інформаційним активам організації

Ризик	Актив					Ранг ризику
	База даних	Фінансова звітність	Веб-сервер (апаратна частина)	ПЗ сервера	ПЗ Інтернет-магазина	
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

Аналіз показав, що найбільш уразливими виявилися бази даних і програмне забезпечення інтернет-магазинів, а також сервери баз даних і веб-сервери.

1.3.2. Визначити місце розташування планового комплексу завдань, деталізуючи завдання з інформаційної безпеки та захисту інформації

Дослідження показують, що темпи розвитку сучасних інформаційних технологій значно випереджають темпи розробки рекомендацій керівних документів та нормативної бази. При проектуванні та розробці систем захисту в компанії дуже часто виникають проблеми, пов’язані з проблемою вибору критеріїв та показників захищеності. Крім того, виникають питання щодо

оцінки ефективності корпоративних систем інформаційної безпеки. Тому, крім нормативних вимог та рекомендацій стандартів, виникає необхідність у використанні міжнародних стандартів та рекомендацій. При цьому виникає необхідність адаптації міжнародних стандартів таких, як ISO 17799, 9001, 15408, BSI [36–38] та інших до вітчизняних умов.

Використання сучасних методів оцінки інформаційної безпеки при проектуванні та супроводі систем інформаційної безпеки компанії має забезпечити відповідність діяльності компанії захисту конфіденційної інформації [42].

Сучасний метод дозволяє:

– Кількісна оцінка поточного рівня інформаційної безпеки компанії. Для цього необхідно визначити ризики на правовому, організаційному, управлінському, технічному та технічному рівнях;

– Розробити та впровадити комплексний план модернізації систем інформаційної безпеки підприємства. Удосконалення ГІС може забезпечити належний захист інформаційних активів компанії.

При розробці плану модернізації ГІС підприємства необхідно вирішити наступні завдання:

– Визначте необхідні фінансові вкладення для забезпечення безпеки. Вартість повинна враховувати можливі втрати та ймовірність виникнення потенційної загрози;

– Перевірте існуючий рівень безпеки компанії, щоб заблокувати наявні вразливості;

– Розробити необхідні організаційні документи для визначення сфер відповідальності підрозділів та керівників;

– Розробляти та узгоджувати з усіма зацікавленими службами та наглядовими органами створення та розгортання проектів ГІС з урахуванням сучасного стану інформаційних технологій;

– Забезпечує підтримку функціональності ГІС з урахуванням змін у бізнес-процесах організації, змін і виправлень в організації та управлінні документами.

Розробка та впровадження комплексу заходів із захисту інформації дає змогу керівництву компанії:

– Оцінити поточний рівень інформаційної безпеки компанії;

– Формування комплексу правил і положень, що описують єдину концепцію безпеки;

– Оцінити необхідні витрати на проектування, розробку та впровадження корпоративного захисту.

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

Міжнародні стандарти ISO та вимоги замовників щодо оцінки та дослідження інформаційної безпеки компаній. Для дослідження інформаційної безпеки проводиться аналіз ризиків на основі вивчення корпоративної мережевої інфраструктури, виявлення можливих загроз та ризиків для корпоративної ІС. Крім цього, необхідно проводити аналіз документообігу компанії, який можна розглядати як самостійний розділ дослідження безпеки.

При цьому розробляються рекомендації щодо забезпечення безпеки інформації, які включають розробку концепції інформаційної безпеки, розробку корпоративної політики захисту інформації на організаційно-управлінському, правовому, технологічному та технічному рівнях.

За виконання організаційно-технологічного аналізу ІБ підприємства виконується порівняння чинних СЗІ підприємства з вимогами керівних документів. Також виконується аналіз документообігу компанії з грифом “конфіденційно”, при цьому оцінюється забезпечення інформаційної безпеки вимогам нормативних документів.

Аналіз документообігу та упорядкування та управління наборами документів, як правило, здійснюється у двох напрямках:

– Аналіз процесу оформлення документів компаній з позначкою «конфіденційно»;

– Розробити та надати типовий комплект організаційно-розпорядчих документів з урахуванням вимог та рекомендацій політики інформаційної безпеки компанії.

Для реальної реалізації заходів щодо реалізації політики інформаційної безпеки необхідно виконати наступні кроки:

– розроблено проект модернізації засобів захисту інформаційних систем на основі досліджень мереж підприємства;

– підготовка компанії до атестації (до атестації об’єктів інформатизації замовника на відповідність вимогам керівних документів, а також на відповідність вимогам безпеки міжнародних стандартів ISO 15408, ISO 17799, стандарту ISO 9001 у разі забезпечення вимог інформаційної безпеки;

– оцінити документи компанії та розширити перелік захищених документів;

– розробити комплекс нормативних документів, які відповідають рекомендаціям корпоративної політики інформаційної безпеки компанії.

Це має великий вплив на рівень інформаційної безпеки компанії, а кваліфікація співробітників, відповідальних за політику безпеки компанії, значною мірою залежить від кваліфікації експертів. Для підвищення кваліфікації співробітників необхідне регулярне навчання з використання ГІС компанії, передового досвіду та вивчення прийомів захисту даних.

З метою підвищення інформаційної безпеки компанії необхідно проводити регулярні дослідження поточної безпекової ситуації.

Основними цілями захисту є:

– Запобігайте витоку інформації, крадіжці, втраті, спотворення, фальсифікації;

– запобігання несанкціонованим діям, спрямованим на знищення, модифікацію, спотворення, копіювання, блокування інформації;

– запобігання іншим формам втручання зловмисників у інформаційні системи та їх ресурси.

Основною метою розробленої та розробленої компанією ГІС є забезпечення стабільної роботи об’єкта:

– запобігати загрозам їх безпеці;

– захищати законні інтереси власника інформації від протиправних посягань, у тому числі злочинних дій у сфері відносин, передбачених Кримінальним кодексом. [15];

– забезпечення нормальної промислової діяльності всіх підрозділів об’єкта.

Щоб ефективно вирішити поставлені завдачі необхідно:

– поширювати інформацію, яка використовується в корпоративних бізнес-процесах, відповідно до відповідних категорій обмежень доступу;

– визначати поточні загрози та прогнозувати можливі загрози безпеці інформаційних ресурсів компанії, виявляючи передумови та умови, що призводять до фінансової, матеріальної та моральної шкоди та порушення інтелектуальної власності компанії;

– забезпечити необхідні умови для функціонування об'єктів інтелектуальної власності, мінімізувати можливість загроз та зменшити всі види збитків;

– розробити механізми та умови швидкого реагування на можливі загрози інформаційній безпеці;

– створити умови для максимально можливої компенсації та локалізації збитків.

Під час роботи ви можете побудувати систему інформаційної безпеки підприємства (рисунок 1.10) за такою моделлю, яка базується на адаптації Загальних критеріїв (ISO 15408) та аналізу ризиків (ISO 17799). Модель

відповідає спеціальним нормам інформаційної безпеки, міжнародному стандарту ISO/IEC 15408 «Інформаційні технології – методи захисту – критерії оцінки інформаційної безпеки», стандарту ISO/IEC 17799 «Управління інформаційною безпекою», а також враховує розвиток тенденція внутрішніх правил безпеки. інформації.

Структурна схема моделі побудови корпоративної системи захисту інформації наведена на рис.1.6.

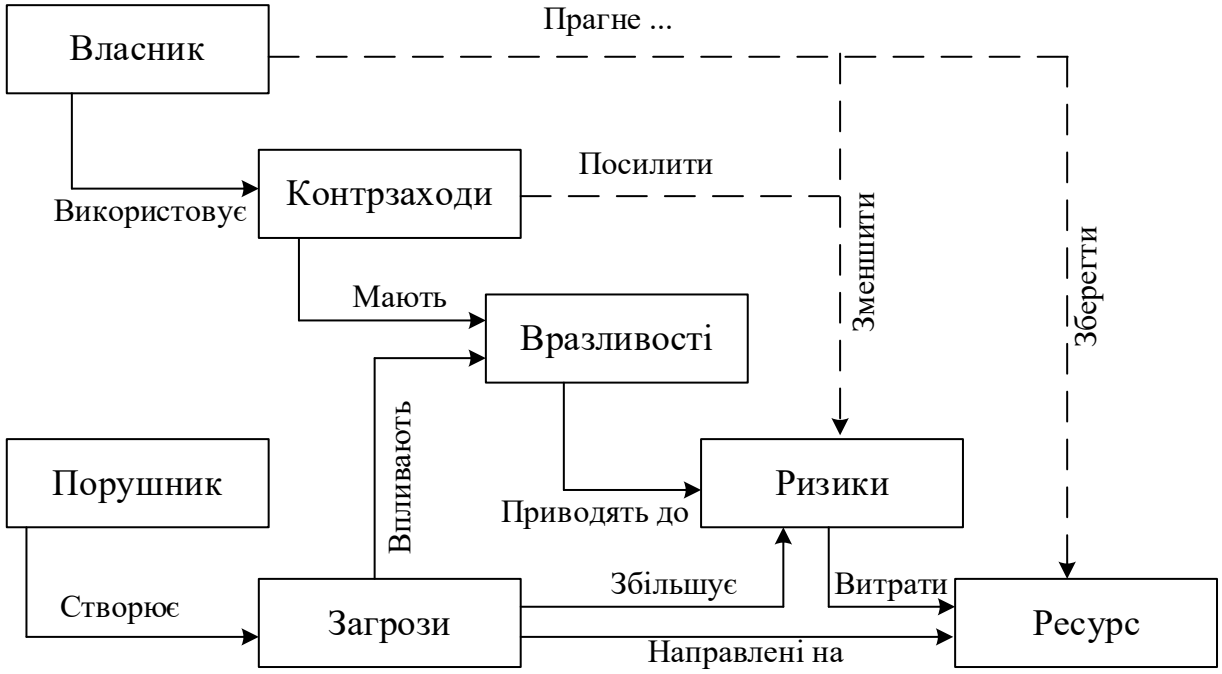

Рисунок 1.6 – Структурна схема моделі побудови корпоративної системи захисту інформації

1.4. Вибір захисних заходів

1.4.1. Вибір організаційних заходів.

Закони та підзаконні акти можуть бути реалізовані лише за умови їх підтримки організаційною діяльністю відповідних структур, створених у державі, секторі, відомстві та організації. При розгляді питань інформаційної безпеки така діяльність підпадає під організаційний підхід до захисту інформації.

Організаційний підхід до захисту інформації включає заходи та дії, які вживають посадові особи при створенні та експлуатації інформаційних систем для забезпечення заданого рівня інформаційної безпеки.

Відповідно до законів і нормативно-правових актів різних міністерств, відомств, підприємств (незалежно від форм власності) для захисту інформації створені спеціальні служби безпеки (які на практиці можуть називатися по-різному). Ці служби, як правило, підпорядковані керівництву установи. Довіритель сервісу організовує створення та функціонування системи інформаційної безпеки. За стан інформаційної безпеки відповідає виключно керівництво організації.

На організаційному рівні в системі вирішуються такі завдання інформаційної безпеки:

- організація розробки систем інформаційної безпеки;
- обмежувати доступ до об'єктів і системних ресурсів;
- розділити права доступу до системних ресурсів;
- планування заходів;
- підготовка документів;
- навчання та навчання обслуговуючого персоналу та користувачів;
- відповідна сертифікація засобів захисту інформації;
- ліцензування діяльності із захисту інформації;
- підтвердження об'єкта охорони;
- удосконалити систему захисту інформації;
- оцінка ефективності систем захисту інформації;
- контролювати виконання встановлених правил роботи в системі.

Метод організації є основою системи комплексної системи гарантій. Тільки за допомогою цих методів можна буде на правовій основі об’єднати технології, програмне забезпечення та засоби захисту паролем в єдину цілісну систему. При розгляді загроз інформаційної безпеки будуть передбачені конкретні методи організаційного захисту. Вирішуючи питання щодо побудови

та організації інтегрованої системи інформаційної безпеки, найбільше занепокоєння викликають організаційні заходи.

До методів і засобів організаційного захисту інформації належать організаційно-технічні, організаційно-правові заходи, що вживаються для забезпечення захисту інформації в процесі створення та функціонування системи. Ці заходи мають бути вжиті під час будівництва або реконструкції майданчика, де розташована система; проектування, встановлення та налаштування апаратного та програмного забезпечення; тестування та перевірка продуктивності системи.

Фундаментальний характер методів і засобів захисту тканин:
обмеження фізичного доступу до об'єктів охорони та здійснення інституційних заходів;

– обмежити можливість перехоплення PEMVN;

– поділ прав доступу до інформаційних ресурсів і процесів (встановлення правил розподілу прав доступу, шифрування інформації під час зберігання та передачі, виявлення та знищення закладок апаратного та програмного забезпечення);

– резервне копіювання найважливіших з погляду втрати масивів документів;

– перед проведенням наради необхідно проводити візуальний огляд приміщення щодо виявлення заставних пристроїв;

– кількість осіб, які беруть участь у конфіденційних переговорах, повинна бути обмежена до мінімуму;

– вхід сторонніх осіб під час проведення наради має бути заборонено;

– має бути чітко розроблено охорону виділеного приміщення під час наради, а також спостереження за обставини на поверсі;

– будь-які роботи, що проводяться в приміщенні поза конфіденційним часом зустрічі, такі як: прибирання, ремонт побутової техніки, дрібне гоління, повинні виконуватися в присутності працівників охорони;

– після засідання слід ретельно оглянути приміщення, закрити та опечатати;

– кімнати між засіданнями повинні бути закриті та опечатані відповідальною особою;

– запобігання комп'ютерним вірусам.

Основою організаційної діяльності є використання та формулювання законодавчих та нормативно-правових актів у сфері інформаційної безпеки, а доступ користувачів до інформації має регулюватися на правовому рівні.

1.4.2. Вибір інженерно-технічних заходів.

Технічні підходи до захисту інформації в поєднанні з організаційними відіграють важливу роль у забезпеченні захисту інформації під час зберігання, накопичення та обробки за допомогою автоматизованих засобів. Для ефективного використання доступних для компаній засобів захисту на основі нових інформаційних технологій необхідні технічні підходи.

Безпека мережі включає в себе політики контролю авторизованого доступу та запобігання несанкціонованому використанню, зміні або блокуванню ресурсів комп’ютерної мережі. Безпека мережі включає доступ до мережевих даних, які контролюються адміністраторами мережі. [9] Користувачі вибирають або призначають ідентифікатор і пароль, які дають їм змогу отримати доступ до інформації та програм у межах своїх повноважень. Кібербезпека охоплює всі види комп’ютерних мереж, державних і приватних; політика кібербезпеки забезпечує комунікації та надання послуг підприємствам, державним установам та приватним особам. Мережі можуть бути приватними, наприклад, всередині компанії, або загальнодоступними, відкритими для всіх. Кібербезпека використовується організаціями, підприємствами та іншими установами. Найпоширеніший і найпростіший спосіб захисту мережевих ресурсів – це надання їм унікальних імен і паролів.

Кібербезпека починається з аутентифікації. Зазвичай для цього використовуються ім’я користувача та пароль. Якщо все, що вам потрібно, це

ім’я користувача та пароль, то такий тип аутентифікації називається однофакторною. За допомогою двофакторної автентифікації користувачі повинні підтвердити свою автентичність за допомогою токена безпеки або «ключа», картки банкомату, коду, надісланого на їхній телефон). Трифакторна автентифікація використовує біометричні параметри користувача, такі як відбиток пальця або сканування сітківки, для автентифікації користувача.

Після аутентифікації брандмауер забезпечує відповідність політикам доступу до мережевих служб і ресурсів. Хоча брандмауери ефективні для запобігання несанкціонованому доступу, цей компонент може не перевіряти потенційно небезпечний вміст, наприклад комп’ютерних хробаків або троянських коней, які передаються по мережі. Антивірусне програмне забезпечення або системи запобігання вторгненням (IPS) можуть допомогти виявити та придушити наслідки цього типу зловмисного програмного забезпечення. Такі програми, як аналізатор трафіку Wireshark, можуть допомогти виявити аномалії мережевого трафіку. Програму можна використовувати для аудиту та подальшого аналізу трафіку.

Зашифровану інформацію можна використовувати для збереження конфіденційності.

Щоб запобігти потенційним зловмисникам, ви можете створити спеціальні приманки (honeypots), які імітують доступні мережеві ресурси та служать інструментом для моніторингу та запобігання ранніх вторгнень. При цьому своєчасно та після атаки проводити дослідження методів, які використовуються зловмисниками для запобігання подібним загрозам у майбутньому. Цей аналіз можна використовувати для подальшого підвищення безпеки мережі. Приманка може приховати робочий сервер зловмисника. Приманки дозволяють зловмисникам витрачати час і зусилля на неправильному сервері, коли дані на реальному сервері залишаються непоміченими.

Управління безпекою мережі відрізняється для всіх типів ситуацій. У домашній або невеликих офісних мережах достатньо лише базової безпеки, тоді як великим підприємствам може знадобитися високотехнологічне та розширене

програмне та апаратне забезпечення, щоб запобігти зловмисному злому та спам-атакам.

РОЗДІЛ 2
ПРОЕКТНА ЧАСТИНА

2.1 Комплекс організаційних заходів забезпечення інформаційної безпеки та захисту інформації підприємства

2.2.1. Нормативно-правова основа створення системи забезпечення інформаційної безпеки та захисту інформації підприємства.

Розглянемо представлені на ринку засоби захисту для віртуалізованих інфраструктур. У переліку наведено 10 технічних заходів:

1. Ідентифікація та аутентифікація суб’єктів доступу та об’єктів доступу у віртуалізованої інфраструктурі.

2. Керування доступом принципів доступу до об’єктів доступу у віртуалізованій інфраструктурі, особливо всередині віртуальних машин.

3. Реєстрація подій безпеки у віртуалізованої інфраструктурі.

4. Управління (фільтрація, маршрутизація, контроль з'єднання, односпрямована передача) інформаційними потоками, які створюються між інформаційними потоками та частинами віртуалізованої інфраструктури, а також периметром віртуалізованої інфраструктури.

5. Довірене завантаження серверів віртуалізації, віртуальної машини (контейнера), серверів керування віртуалізацією.

6. Управління переміщенням віртуальних машин (контейнерів) та даних, що обробляються на них.

7. Контроль цілісності віртуалізованої інфраструктури та її конфігурацій.

8. Резервне копіювання даних, резервування технічних засобів, програмного забезпечення віртуалізованої інфраструктури та каналів зв’язку всередині віртуалізованої інфраструктури.

9. Реалізація та управління антивірусним захистом у віртуалізованої інфраструктури.

10. Розбиття віртуалізованої інфраструктури на сегменти (сегментування віртуалізованої інфраструктури) для обробки персональних даних окремим користувачем та (або) групою користувачів.

2.1.2. Організаційно-адміністративна основа створення системи забезпечення інформаційної безпеки та захисту інформації підприємства.

На додаток до описаних вище цілей, політика безпеки також визначає відповідність нормативним та законодавчим документам. У сучасному корпоративному світі важливо, щоб внутрішні бізнес-процеси компанії відповідали чинному законодавству та готові до можливих змін законодавства.

Таким чином, політика безпеки містить вказівки на те, що базові елементи управління безпекою в компанії відповідають чинним правилам, нормам та законодавству.

Приклад політики безпеки для інтернет-магазину наведено у дод. А.

2.2. Комплекс проектованих програмно-апаратних засобів забезпечення інформаційної безпеки та захисту інформації підприємства.

2.2.1. Структура програмно-апаратного комплексу інформаційної безпеки та захисту інформації підприємства.

У роботі пропонується побудова захищеної інформаційної системи підприємства на основі використання програмно-апаратного комплексу Palo alto PA7080 та Palo Alto PA5000.

Даний програмно-апаратний комплекс дозволяє проводити аналіз трафіку, як вхідного та вихідного, включаючи елемент подій брандмауера в PAN-OS. Ця операційна система надає кілька нових можливостей адміністраторам брандмауера. ОС дає адміністратору аналізувати тренд потоку даних (мережевого трафіку), віддаленого, зовнішнього, внутрішнього чи

забороненого. Наприклад, ОС дозволяє адміністраторам отримувати графічний аналіз, як брандмауер Next Generation обробляє вихідний трафік, що спрямовується до Інтернету.

Якщо у вищезгаданому тренді стався аномальний сплеск або падіння, адміністратори можуть проаналізувати цю подію, щоб дізнатися, які машини були залучені, які програми використовувалися на той час. Ці дані також можуть бути об'єднані разом з кількома брандмауерами, щоб отримати узагальнене уявлення про корпоративну поведінку в Інтернеті.

Адміністратори можуть використовувати цей звіт для встановлення порогових значень для неприпустимих "заборонених" подій. Якщо хост викликає з'єднання якимось чином, що порушує поріг, то дані відхилені порушення можуть ініціювати події, які призводять до повідомлень про можливі атаки.

Структурна схема оновленої локальної мережі підприємства наведена рис. 2.1.

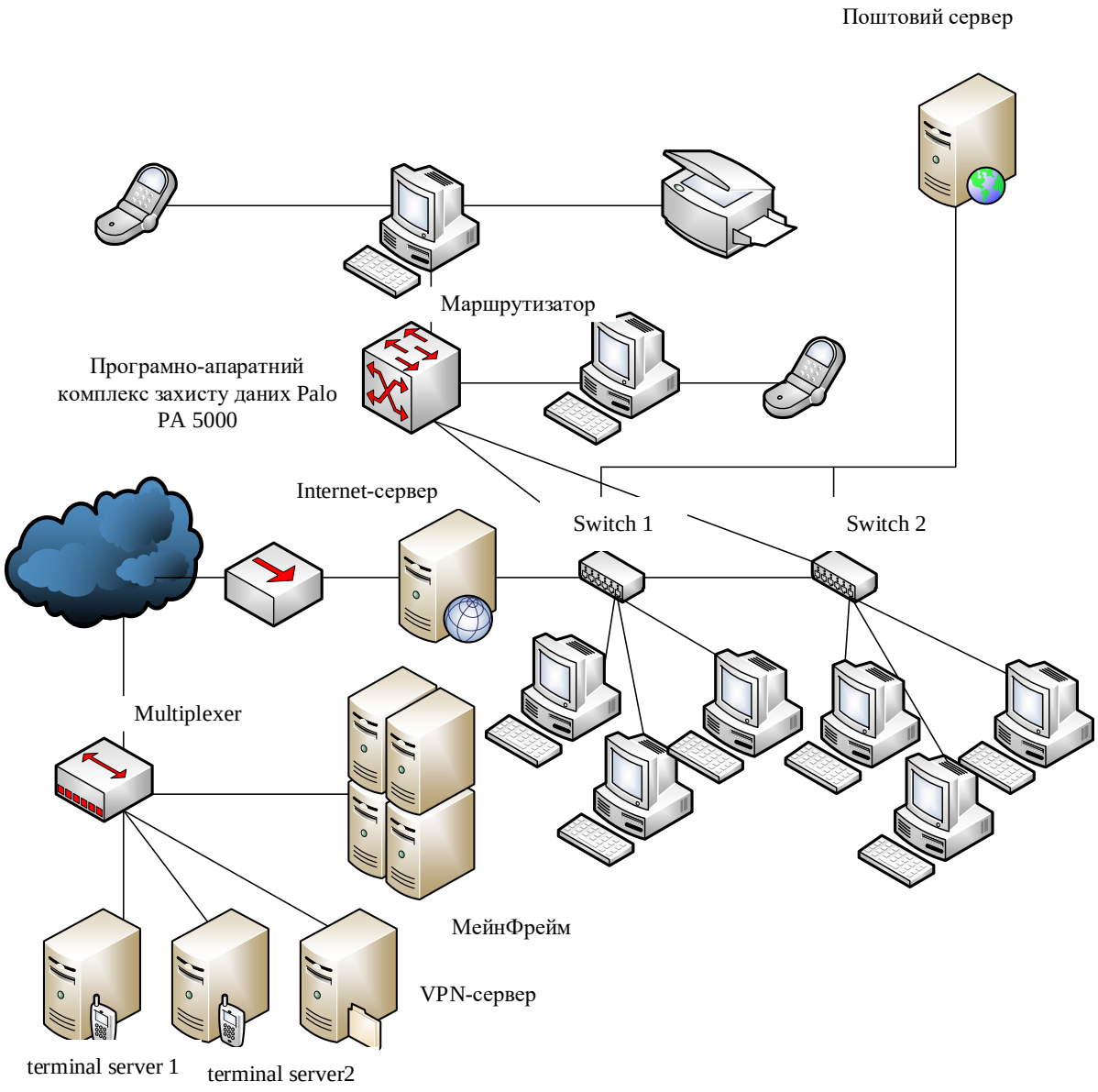

Рисунок 2.1 – Структурна схема локальної мережі

На підставі проведеного аналізу було обрано програмно-апаратний комплекс Palo Alto PA-7080 (рис.2.2).

Великі підприємства та постачальники телекомунікаційних послуг є постійними цілями кібератак. Кіберзлочинці прагнуть вкрасти інформацію про клієнтів з центрів обробки даних, порушити доступ до сервісів та використовувати мережі постачальників послуг як вектори для атак на підприємства та споживачів. У міру зростання пропускної здатності, швидкості та складності центрів обробки даних та мереж необхідно забезпечити пропозицію безпеки, що запобігає кібератакам у масштабі.

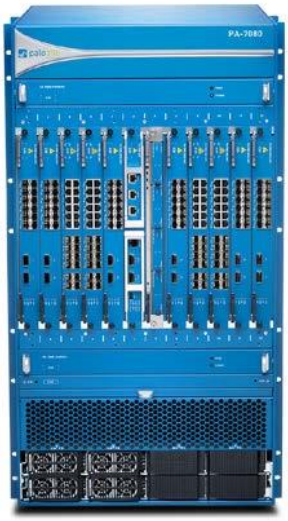

Рисунок 2.2 – Palo Alto PA-7080

Palo Alto Networks дозволяє розв’язувати цю проблему на основі платформи безпеки Palo Alto Networks, яка складається з брандмауера Next-Generation Palo Alto Networks, хмари Intelligence Cloud та розширеного захисту кінцевих точок. Ця платформа усуває недоліки безпеки, продуктивності та експлуатації застарілих продуктів та захищених архітектур безпеки. Вона призначена для запобігання кібератакам, забезпечуючи при цьому масштабовану продуктивність, автоматизацію політики.

Новий брандмауер наступного покоління PA-7080 забезпечує потужну, інтелектуальну масштабованість та просту в управлінні систему безпеки, яка ідеально підходить для реалізації у великих корпоративних мережах та середовищах постачальників послуг для захисту своїх активів та сервісів.

PA-7080 забезпечує обчислювальну потужність та архітектуру програмного забезпечення, необхідні для запобігання кібератакам у всіх додатках навіть у найбільших мережах та центрах обробки даних. Заснований на перевіреній архітектурі, яка поєднує в собі ультра ефективне програмне забезпечення з майже 700 функціональними процесорами, призначеними для роботи в мережі, безпеці, контролю контенту та управління, PA-7080 може забезпечити пропускну здатність до 200 Гбіт/с та 100 Гбіт/с із включеними усіма можливостями безпеки.

Через поєднання потужності, інтелекту та простоти PA-7080 ідеально підходить для забезпечення захисту:

– Центрів обробки даних, в яких постачальники послуг та підприємства реалізують свою бізнес-інфраструктуру;

– Інфраструктури надання послуг, де швидкість та масштаб мають першорядне значення, а загроза має вирішальне значення;

– Інтернет-шлюзи, де безпечне включення всіх програм та захист від відомих та невідомих загроз мають вирішальне значення.

PA-7080 призначений для безперебійної інтеграції у великі мережі та за мінімальних поточних експлуатаційних витрат. Він підтримує віртуальні мережі, L2 та L3, режими високої доступності у поєднанні зі спрощеним управлінням, спрощеним ліцензуванням та інтелектуальним управлінням трафіком. PA-7080 сумісний з NEBS, має джерела живлення змінного/постійного струму як стандартні функції.

Продуктивність та ємність пристрою серії PA-7000 можна масштабувати шляхом додавання нових обчислювальних ресурсів при додаванні нових плат обробки. Щоб спростити адміністрування системи та витрати, пристрої керуються та ліцензуються як єдині уніфіковані системи.

Основні технічні характеристики програмно-апаратного комплексу PA-7080:

– Міжмережевий екран із вбудованим розпізнаванням програм (App-ID);

– Розпізнавання облікових записів користувачів (User-ID);

– IPS – захист від вторгнень;

– Антивірус – ЗАХИСТ від відомих вірусів;

– Технологія динамічного аналізу WildFire – захист від невідомих та нових вірусів, 0-day та APT;

– Фільтрування URL-адрес;

– Розпізнавання контенту та форматів даних (Content-ID);

– User VPN та Site-to-Site VPN (SSL, IPsec);

– Дешифрування та контроль SSL-трафіку;

– Якість обслуговування (QOS);

– Віртуальні маршрутизатори та зони безпеки;

– Інтегрований вебінтерфейс, інтерфейс командного рядка або централізоване управління (Panorama);

– Повністю настроюванні звіти, графічне подання зведених даних.

Характеристики PA-7080:

– Пропускна здатність міжмережевого екрана (при включеному App-ID) – 200 Гбіт/с;

– Пропускна здатність при запобіганні загрозам (при включеному DSRI, Disable Server Response Inspection) – 160 Гбіт/с;

– Пропускна здатність при запобіганні загрозам – 100 Гбіт/с;

– Пропускна здатність IPSec VPN – 80 Гбіт/с;

– Макс. у сеансів – 40000000;

– Кількість нових сеансів на секунду – 1200000;

– Кількість віртуальних систем (базовий варіант/макс.) – 25/225;

– Інтерфейси – 120*GE, 80*1 Gigabit SFP, 40*1– Gigabit SFP+.

2.2.2 Контрольний приклад реалізації проекту та його опис.

Розглянемо приклад налаштування та конфігурації високошвидкісної мережі на програмно-апаратному комплексі PA-7080.

Під час конфігурації використовується PAN-OS.

Для початку роботи потрібно відкрити вкладку Network-Interface (рис. 2.3).

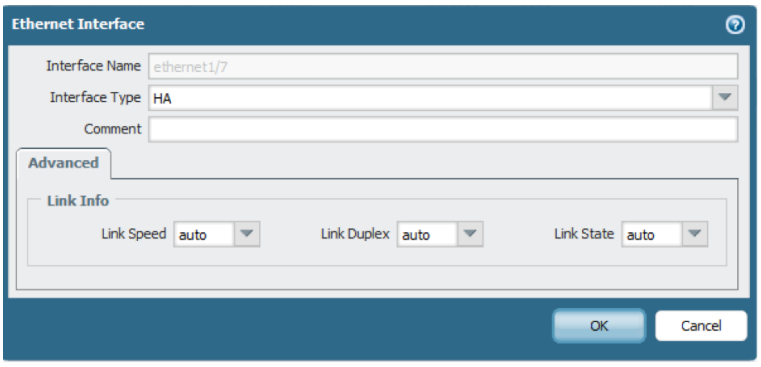

Рисунок 2.3 – Вкладка Network-Interface

Далі потрібно перейти на вкладку Device tab > HIgh Availability > General (рис. 2.4).

Далі необхідно увійти до розділу налаштування.

1. Увімкнути HA.

2. Введіть ідентифікатор групи.

3. Введіть IP-адресу для керуючого пристрою.

4. Увімкнути Config Sync.

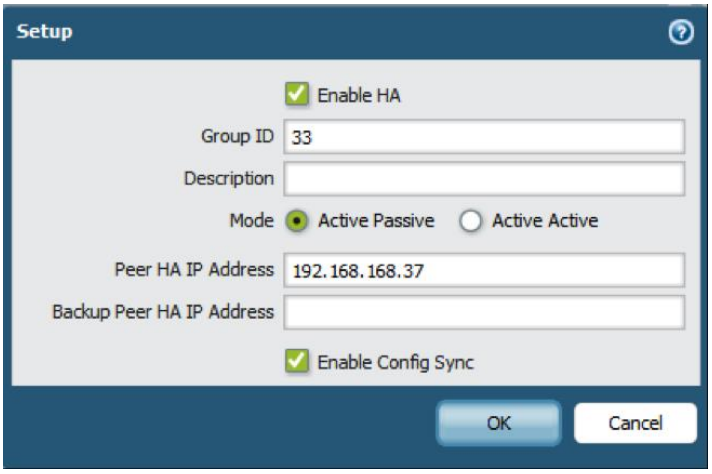

Рисунок 2.4 – Вкладка General

Ідентифікатор кластера використовується для створення віртуального MAC для екземплярів L3. Якщо кілька кластерів знаходяться в одній мережі L2, ідентифікатор має бути різним для кожного кластера.

IP-адреса Peer HA (Control Link) може бути будь-якою IP-адресою, яка не використовується в цей час в мережі.

Рекомендується додати IP-адресу Backup Peer HA, якщо є достатньо вільних портів.

На вкладці General відкрийте секцію Control Link і натисніть Primary (рис. 2.5).

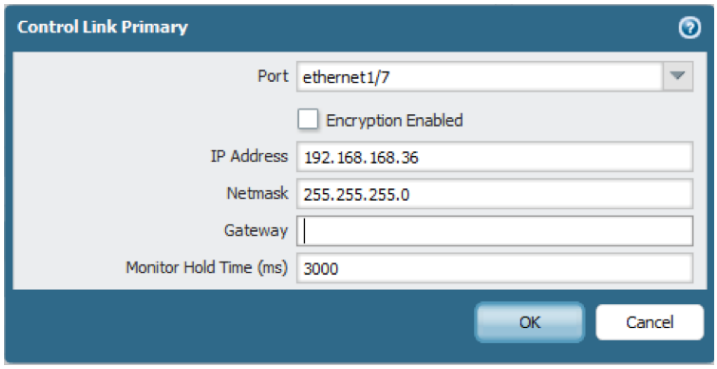

Рисунок 2.5 – Секція Control Link

Виберіть перший інтерфейс HA, який використується для Control Link першого пристрою.

Увімкніть IP-адресу, яка знаходиться в тій же підмережі, що й IP-адреса Peer HA, налаштована на кроці 2.

Якщо контрольне посилання не підключене безпосередньо до іншого брандмауера, можна ввімкнути шифрування (AES-256).

Якщо IP-адреси Control Link знаходяться в окремих широкомовних доменах, необхідно налаштувати лише шлюз.

На вкладці General відкрийте розділ Data Link (рис. 2.6) і натисніть Primary.

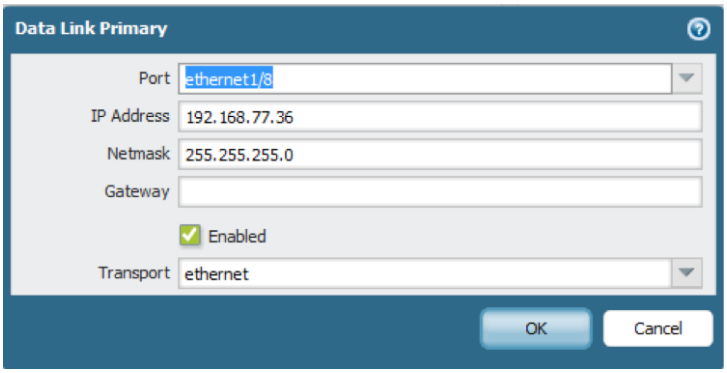

Рисунок 2.6 – Секція Data Link

Виберіть інтерфейс HA, який буде використовуватися для передачі даних.

Налаштуйте IP-інформацію для передачі даних.

Перевірте, чи встановлено прапорець Увімкнене.

Ethernet: використовуйте, коли брандмауери підключаються назад або через комутатор (Ethertype 0x7261).

IP: використовуйте, коли потрібний транспорт третього рівня (IP-протокол № 99).

UDP: Використовуйте, щоб скористатися тим фактом, що контрольна сума розраховується по всьому пакету, а не лише за заголовком, як в опції IP (UDP-порт 29281).

На вкладці General, відкрийте секцію Election Settings (рис. 3.7) та натисніть кнопку налаштування.

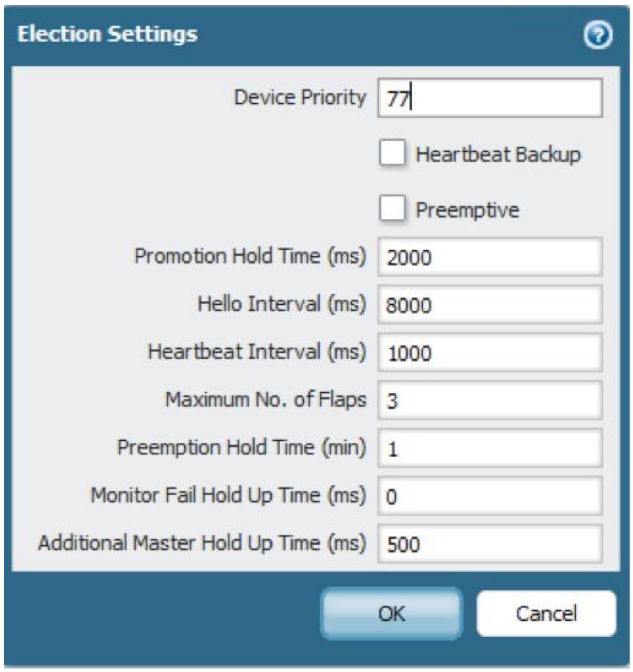

Рисунок 2.7 – Секція Election Settings

Щоб вказати один із брандмауерів як активний, увімкніть Preemptive на обох брандмауерах та встановіть пріоритет пристрою. Пристрій із найменшим пріоритетом пристрою є активним пристроєм.

Коли увімкнене синхронізацію стану; таблиця сеансу, таблиця переадресації, таблиця ARP та асоціації безпеки VPN (SA) копіюються з активного пристрою на пасивний пристрій через HA2.

Якщо пристрої мають IP-з’єднання між IP-адресами керування, рекомендується увімкнути резервне копіювання Heartbeat, яке надсилає пінги через інтерфейс керування.

Статус брандмауера повинен бути активним, а інші значення мають бути невідомими, як показано на рис 2.8.

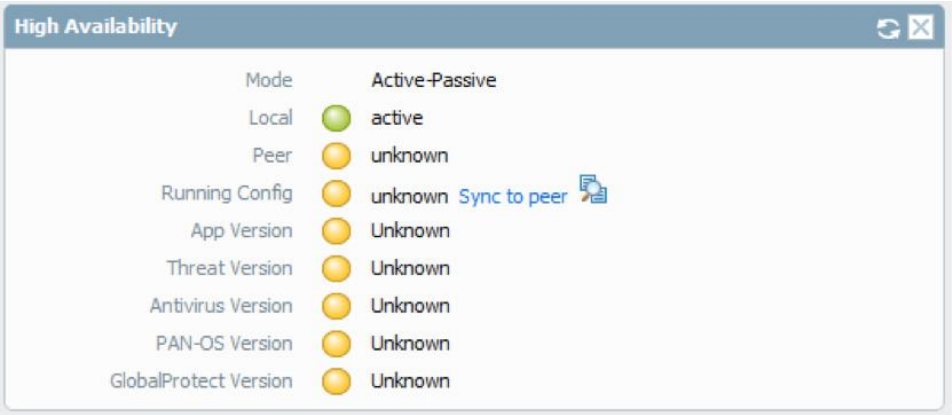

Рисунок 2.8 – Статус брандмауера

Перейдіть на вкладку Dashboard.

Додайте віджет високої доступності. Widgets > System > High Availability. Для налаштування однорангового пристрою необхідно переконатись, що одноранговий пристрій має два канали HA, налаштовані для зв'язку з HA-каналами першого пристрою (рис. 2.9).

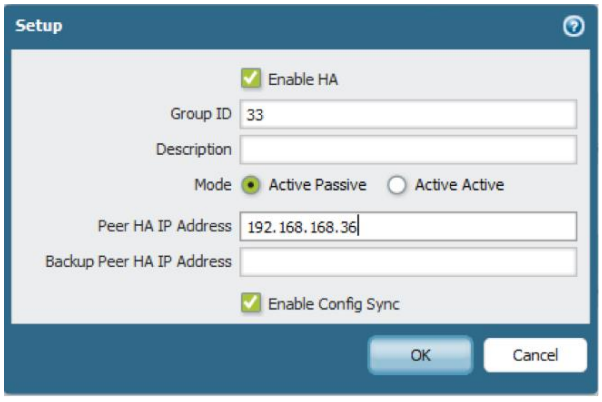

Рисунок 2.9 – Налаштування однорангового пристрою

Перейдіть до розділу налаштування однорангового пристрою та увімкніть HA. Призначте той самий ідентифікатор кластера, що й на брандмауері. Введіть

IP-адресу, яка призначена для контрольного посилання брандмауера. Увімкнути Config Sync.

На вкладці “General” знайдіть розділ “Control Link” (рис. 2.10) і натисніть “Primary”.

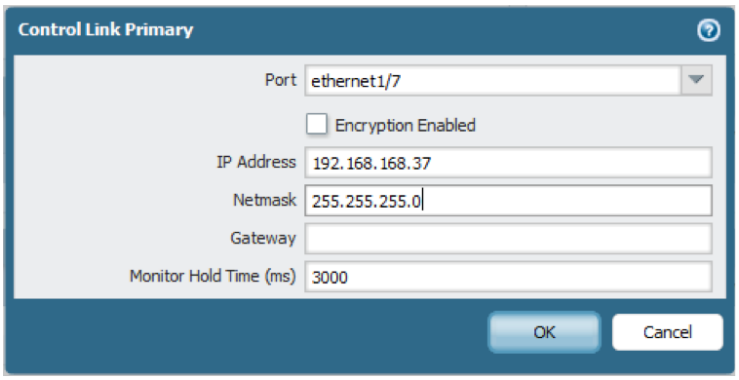

Рисунок 2.10 – Секція Control Link

Якщо на першому пристрої увімкнене шифрування, увімкніть його.

Виберіть перший інтерфейс HA, який використовуватиметься для Link Control другого пристрою.

Введіть IP-адресу, яка знаходиться в тій же підмережі, що й IP-адреса Peer HA.

На вкладці “General” знайдіть розділ “Data Link” (рис.2. 11) і натисніть “Primary”.

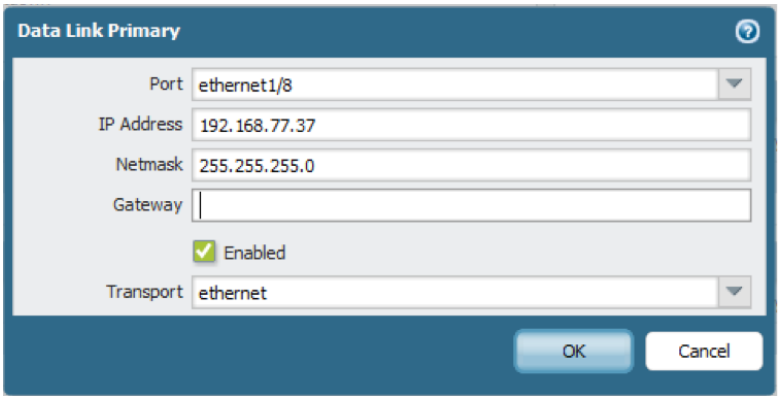

Рисунок 2.11 – Секція Data Link

Виберіть інший інтерфейс HA, який буде використовуватися для передачі даних. Налаштуйте IP-інформацію для передачі даних. Перевірте, чи встановлено прапорець Увімкнене. Переконайтеся, що список транспорту

відповідає конфігурації першого пристрою. Реплікуйте налаштування на першому пристрої (рис. 2.12).

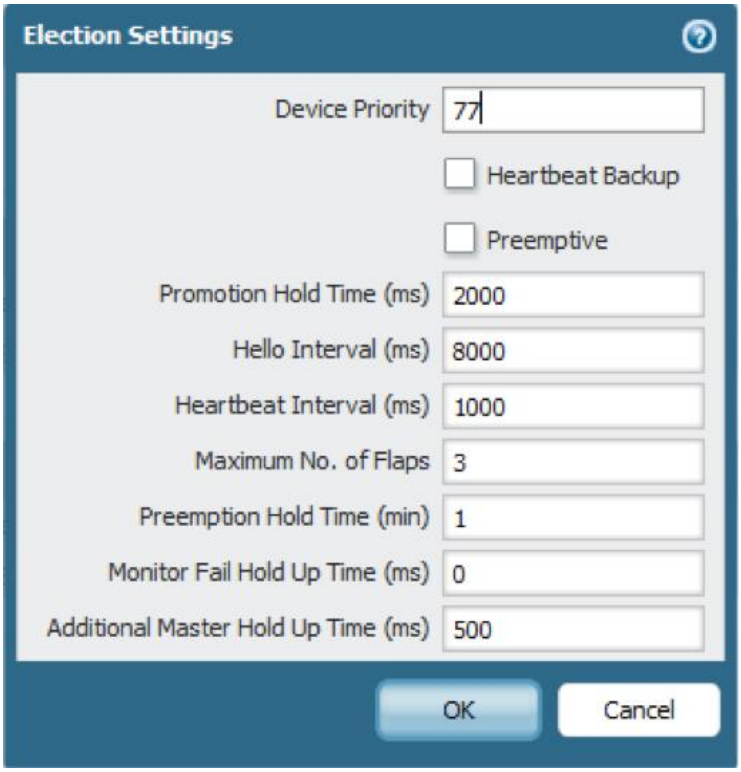

Рисунок 2.12 – Налаштування реплікації

Увімкнути Preemptive. Налаштуйте поле пріоритету. Більше значення означає нижчий пріоритет. Зафіксуйте зміни на другому пристрої: Перейдіть до першого пристрою (рис. 2.13).

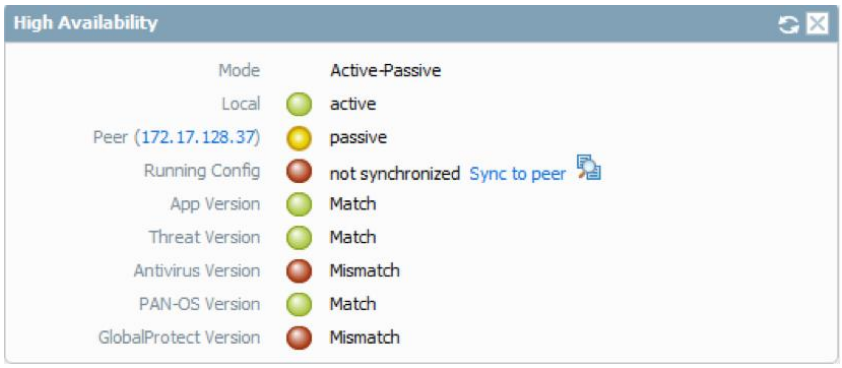

Рисунок 2.13 – Статус брандмауера

Переконайтеся, що він як і раніше зображаться як активний, і він сприймає одноранговий пристрій як пасивний. Переконайтеся, що всі динамічні оновлення синхронізовані. У цьому прикладі Antivirus та GlobalProtect не синхронізуються.

Обновляйте при необхідності, щоб все відповідало, як показано на рис. 2.14.

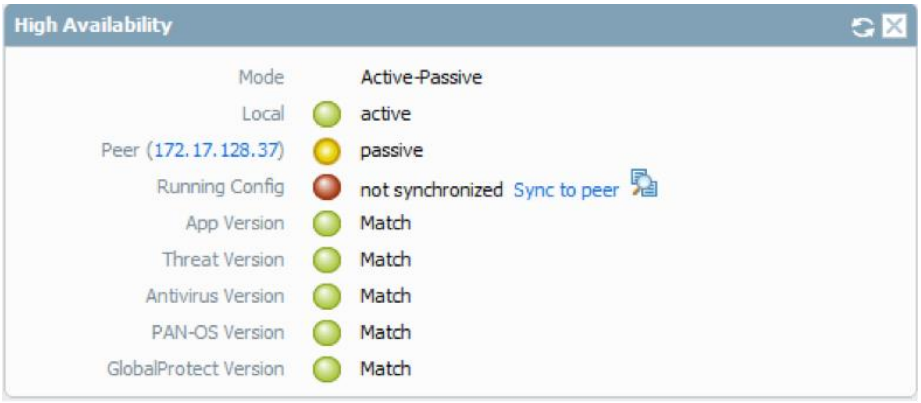

Рисунок 2.14 – Оновлений статус брандмауера

Налаштуйте моніторинг каналів та моніторинг шляхів (рис.2.15).

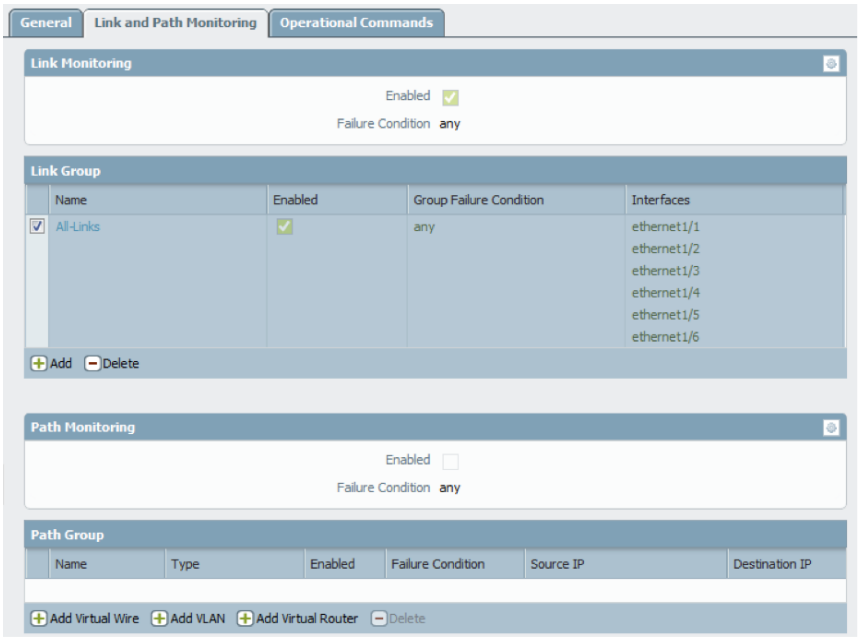

Рисунок 2.15 – Налаштування моніторингу каналів

РОЗДІЛ 3
ОБҐРУНТУВАННЯ ЕКОНОМІЧНОЇ ЕФЕКТИВНОСТІ ПРОЕКТУ

3.1 Вибір та обґрунтування методики розрахунку економічної ефективності

Вихідною посилкою при економічної ефективності є майже очевидне припущення: з одного боку, при порушенні захищеності інформації завдається певних збитків, з іншого – забезпечення захисту інформації пов'язане з витрачанням коштів. Повна очікувана вартість захисту може бути виражена сумою видатків на захист та втрат від її порушення.

Очевидно, що оптимальним рішенням було виділення на захист інформації коштів, що мінімізують загальну вартість робіт із захисту інформації.

Також очевидно, що економічна ефективність заходів щодо захисту інформації може бути визначена через обсяг запобіжних збитків або величину зниження ризику для інформаційних активів організації.

Для того, щоб скористатися даним підходом до розв’язання проблеми, необхідно знати (або вміти визначати), по-перше, очікувані втрати у разі порушення захищеності інформації; по-друге, залежність між рівнем захищеності та засобами, що витрачаються на захист інформації.

Для визначення рівня витрат R_i, що забезпечують необхідний рівень захищеності інформації, необхідно принаймні знати:

–повний перелік загроз інформації;

–потенційну небезпеку для інформації для кожної загрози;

–розміри витрат, необхідних для нейтралізації кожної загрози.

Оскільки оптимальне розв’язання питання про доцільний рівень витрат на захист полягає в тому, що цей рівень повинен дорівнювати рівню очікуваних втрат при порушенні захищеності, достатньо визначити лише рівень втрат. Як

одна з методик визначення рівня витрат можливе використання наступної емпіричної залежності очікуваних втрат (ризиків) від *i*-ї загрози інформації:

$$R_i = 10^{(Si + Vi - 4)},$$

де S_i – коефіцієнт, що характеризує можливу частоту виникнення відповідної загрози; V_i – коефіцієнт, що характеризує значення можливої шкоди у разі її виникнення.

3.2. Розрахунок показників економічної ефективності проект

При розрахунку сумарного показника рекомендується прийняти, що загрози конфіденційності, цілісності та доступності реалізуються порушником незалежно. Тобто, якщо в результаті дій порушника було порушено цілісність інформації, передбачається, що її зміст, як і раніше, залишається йому невідомим (конфіденційність не порушена), а авторизовані користувачі, як і раніше, мають доступ до активів, нехай і спотворених. У табл. 3.1 наведені величини втрат (ризиків) для критичних інформаційних ресурсів до впровадження/модернізації системи захисту інформації

Таблиця 3.1 – Величини втрат (ризиків) для критичних інформаційних ресурсів до впровадження/модернізації системи захисту інформації

Активи	Загроза	Величина втрат (тис. у.е.)
База даних	Викрадення БД	100
Фінансова звітність	Шахрайство з платежами	100
Апаратна частина сервера	Фізичне проникнення	75
ПЗ сервера	Шкідливий код	5,5
ПЗ веб-порталу	DDos атака	5
Сумарна величина втрат		285,5

Ризик власника інформації залежить від рівня інженерно-технічного захисту інформації, який, своєю чергою, визначається ресурсами системи.

Ресурс може бути визначений у вигляді кількості людей, що залучаються до захисту інформації, у вигляді інженерних конструкцій та технічних засобів, що застосовуються для захисту, грошових сум для оплати праці людей, будівництва, розробки та купівлі технічних засобів, їх експлуатації та інших витрат.

Для реалізації запланованих заходів забезпечення захисту даних компанії виконати такі дії:

– розробка сценаріїв захисту для програмно-апаратного комплексу РА-7080 (трудовитрати 56 людино-годин, а фінансові вкладення становитимуть 50 тис. у.е.);

– придбання 2 пристроїв РА-7080 та РА-5000. Вартість становитиме 85 тис. у.е.

– вартість придбання ліцензії – 61,5 тис. у.е.

– вартість доставлення та встановлення програмно-апаратного комплексу 6,1 тис. у.е.

Дані про зміст та обсяг разового ресурсу, що виділяється на захист інформації представлені в табл. 3.2;

Дані про зміст та обсяг постійного ресурсу, що виділяється на захист інформації представлені в табл. 3.3.

Таблиця 3.2 – Зміст та обсяг разового ресурсу, що виділяється на захист інформації

Організаційні заходи				
№ з\п	Дії	Середньогодинна зарплата спеціаліста (у.е.)	Трудомісткість операції (чол.час)	Вартість, всього (тис. у.е.)
1	Розробка сценаріїв для ПА комплексу	15	56	0,89
2	Встановлення брандмауерів	10	61	0,61
3	Налаштування брандмауерів	10	81	0,81
4	Реалізація сценаріїв захисту	20	125	2,5
5	Установка СКУД Сфінкс	10	17	0,17
Вартість проведення організаційних заходів, всього				4,98
Заходи інженерно-технічного захисту інформації				

№ з\п	Номенклатура, витратні матеріали	Вартість, одиниці (тис. у.е.)	кількість	Вартість, всього (тис. у.е.)
1	PA-7080, PA – 5000	2,8	2	5,6
2	ПО PAN-OS	0,17	2	0,34
Вартість проведення заходів інженерно-технічного захисту інформації				5, 94
Обсяг разового ресурсу, що виділяється на захист інформації				10,92

Таблиця 3.3 – Зміст та обсяг постійного ресурсу, що виділяється на захист інформації

Організаційні заходи				
№ з\п	Дії	Середньогодинна зарплата спеціаліста (у.е.)	Трудомісткість операції (чол.час)	Вартість, всього (тис. у.е.)
1	Контроль цілісності БД	15	120	1,8
2	Навчання персоналу	20	200	4,0
3	Контроль цілісності IT-інфраструктури	10	130	1,3
4	Аналіз безпеки веб-порталу компанії	15	142	2,1
5	Забезпечення безпеки конфіденційної інформації	10	120	1,2
Вартість проведення організаційних заходів, всього				10,4
Заходи інженерно-технічного захисту інформації				
№ з\п	Номенклатура, витратні матеріали	Вартість, одиниці (тис. у.е.)	кількість	Вартість, всього (тис. у.е.)
1	Кабель, роз'єм підключення, кабельні канали, гофротруба, кріпильні матеріали	0,05	–	0,05
2	Кабель, роз'єм підключення, кабельні канали, гофротруба, кріпильні матеріали для локальної мережі	0,001	–	0,001
Вартість проведення заходів інженерно-технічного захисту інформації				0,051
Обсяг разового ресурсу, що виділяється на захист інформації				10,5

Оскільки витрати на модернізацію системи захисту та підтримання її працездатності можна порівняти з можливим збитком від реалізації ризиків інформаційної системи, то модернізація системи захисту інформації є доцільною.

Для проведення розрахунку окупності системи захисту інформації, що модернізується, необхідно отримати прогнозовані дані про величину втрат

(ризиків) для критичних інформаційних ресурсів після модернізації системи захисту інформації. Результати оцінки ризиків представлені у табл. 3.4.

Таблиця 3.4 – Величини втрат (ризиків) для критичних інформаційних ресурсів після впровадження/модернізації системи захисту інформації

Активи	Загроза	Величина втрат (тис. у.е.)
База даних	Викрадення БД	50
Фінансова звітність	Шахрайство з платежами	50
Апаратна частина сервера	Фізичне проникнення	35
ПЗ сервера	Шкідливий код	5,5
ПЗ веб-порталу	DDos атака	5
Сумарна величина втрат		140,5

Динаміка величини втрат за період не менше 1 року та внести дані до таблиці 3.5.

а) сумарне значення ресурсу, ($R_{\sum}$) виділеного на захист інформації, становило 21,42 тис. у.е;

б) обсяг середньорічних втрат компанії ($R_{сер}$) через інциденти інформаційної безпеки становив 285,5 тис. у.е;

в) прогнозований щорічний обсяг втрат ($R_{прогн}$) становитиме 140,5 тис. у.е;

г) динаміка втрат представлена таблиці.

Таблиця 3.5 – Оцінка динаміки величин втрат

	1 кв.	2 кв.	3 кв.	1 год	1 кв.	2 кв.	3 кв.	2 год
До впровадження СЗІ	285	1648	1933	2472	2757	3042	3327	3612
Після впровадження СЗІ	140	280	420	560	700	840	980	1120
Зниження втрат	145	1368	1513	1912	2057	2202	2347	2492

Після прийняття обов’язкових припущень про незмінність частоти появи загроз, а також про незмінний рівень надійності створеної системи захисту інформації можна визначити термін окупності системи ($C_{ок}$). Це виконується аналітичним способом, з використанням наведеної нижче формули:

$$T_{ок} = R_{\sum} / (R_{ср} – R_{прогн})$$

$$T_{ок} = 10 \text{ місяців та } 24 \text{ дні.}$$

ВИСНОВКИ

У роботі розглянуто актуальну тему, пов’язану з розробкою моделі захисту від несанкціонованого доступу мережі підприємства з використанням технологій NGFW. Розроблена модель дозволяє забезпечити рівень захисту персональних даних, що зберігаються та обробляються в інформаційних системах підприємства.

Метою роботи була розробка моделі захисту від несанкціонованого доступу до локальної мережі підприємства з використанням технологій NGFW.

Визначено основні проблеми та особливості захисту інформації у комп’ютерних мережах. Проведено аналіз загроз та атак на локальну комп’ютерну мережу, а також визначено канали витоку інформації. Проведено класифікацію методів та засобів забезпечення безпеки.

Подано проєкт побудови захищеної інформаційної системи підприємства на основі використання програмно-апаратного комплексу Palo alto PA7080 та Palo Alto PA5000.

Даний програмно-апаратний комплекс дозволяє проводити аналіз трафіку, як вхідного та вихідного, включаючи елемент подій брандмауера в PAN-OS.

Описано основні характеристики Palo Alto PA7080. Наведено приклад налаштування високошвидкісної мережі на програмно-апаратному комплексі PA-7080.

Виконано оцінку ефективності впровадження програмно-апаратного комплексу. Розраховані величини втрат (ризиків) для критичних інформаційних ресурсів до впровадження/модернізації системи захисту. Ця сума складе 140,5 тис. у.е. Для реалізації запланованих заходів щодо забезпечення захисту даних компанії визначено основні витрати, що включають:

– розробку сценаріїв захисту для програмно-апаратного комплексу PA-7080 (трудовитрати 56 людино-годин, а фінансові вкладення становитимуть 50 тис. у.е.);

– придбання 2 пристроїв РА-7080 та РА-5000. Вартість становитиме 85 тис.у.е.

– вартість придбання ліцензії – 61,5 тис. у.е;

– вартість доставлення та встановлення програмно-апаратного комплексу 6,1тис.у.е.

Термін окупності програмно-апаратного комплексу складе 10 міс. та 24 дні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу. НД СТЗІ 1.1-003-99. – Чинний від 28.04.1999. – К.: Держстандарт України, 1999. – 24 с..

2. C. P. Pfleeger and S. L. Pfleeger, Security in Computing, 5th ed. Englewood Cliffs, NJ: Prentice-Hall, 2015 – 944 p.

3. Knuth D. The Art of Computer Programming, Volume3: Sortingand Searching, Third Edition.Addison-Wesley,1997..

4. Edited by Serhii Yevseiev, Volodymir Ponomarenko, Oleksandr Laptiev, Oleksandr Milov. Synergy of building cybersecurity systems: monograph / S. Yevseiev, V. Ponomarenko, O. Laptiev, O. Milov and others. – Kharkiv: PC TECHNOLOGY CENTER, 2021. – 188 p.

5. Томашевский Б.П. Анализ моделей атак злоумышленника на подсистему криптографической защиты в компьютерных системах и сетях / Б.П.Томашевский // Системи обробки інформації. – 2010. – №1(82). – С. 144 – 146.

6. Грищук Р. В., та Даник Ю. Г., "Синергія інформаційних та кібернетичних дій", Труди університету. НУОУ, № 6 (127), с. 132–143. 2014.

7. Бурячок В. Л., Грищук Р. В., та Хорошко В. О., під заг. ред. проф. В. О. Хорошка, "Політика інформаційної безпеки", ПВП «Задруга». 2014.

8. Information Technology–Security Technique–Evaluation Criteria for IT Security, IEC 15408, 2005.

9. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. H.R. 3162.

10. Леоненко Г. П., и Юдин А. Ю., "Проблемы обеспечения информационной безопасности систем критически важной информационной инфраструктуры Украины", Information Technology and Security, № 1(3), с. 44 – 48. 2013.

11. ISO/IEC 27031:2011 Information Technology – Security Techniques – Guidelines for Information and Communication Technology Readiness for Business Continuity. [Online]. Available: http://www.iso.org/iso/ru/home/store/catalogue_tc/catalogue_detail.htm?csnumber=44374.

12. ISO/IEC 27001:2013. Information technology – Security techniques – Information security management systems – Requirements. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

13. Доктрина інформаційної безпеки України, затверджено Указом Президента України від 25 лютого 2017 року № 47/2017. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/47/2017/paran2#n2.

14. Закон України "Про захист персональних даних".[Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/main/2297-17#Text.

15. Указ Президента України від 15 березня 2016 року № 96 "Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року "Про Стратегію кібербезпеки України". [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/96/2016/paran11#n11.

16. Закон України "Про ліцензування видів господарської діяльності". [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/222-19#Text.

17. Закон України "Про бухгалтерський облік та фінансову звітність в Україні" [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/996-14#Text.

18. Модельний закон щодо соціального захисту інвалідів. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/997_k81#Text.

19. Положення щодо обробки та захисту персональних даних користувачів. . [Електронний ресурс]. Доступно: https://ibis.shop/aux_pages/?aux_page_id=3

20. ДСТУ ISO/IEC 9594-8:2006 Інформаційні технології. Взаємозв'язок відкритих систем. Каталог. Частина 8. Основні положення щодо сертифікації відкритих ключів та атрибутів, [Електронний ресурс]. Доступно: http://document.ua/informaciini-tehnologiyi_-vzaemozvE28099jazok-vidkritih-sist-std10750.html

21. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів національного банку України/ [Електронний ресурс]. Доступно: zakon.rada.gov.ua/laws/show/v0365500-11.

22. С. В. Ленков, Д. А. Перегудов, и В. А. Хорошко, Методы и средства защиты информации : монография [в 2-х т.] Т. 2. Информационная безопасность. К., 2008.

23. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Методи захисту в банківській діяльності система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD). К: НБУ., 2010.

24. Ю. Г. Даник та ін., “Основи захисту інформації” навч. пос., Житомир : ЖВІ ДУТ, 2015.

25. І. С. Іванченко, В. О. Хорошко, Ю. Е.Хохлачова, та Д. В. Чирков під заг. ред. проф. В. О. Хорошка, “Забезпечення інформаційної безпеки держави”, К: ПВП “Задруга”, 2013.

26. Корченко А. О., Скачек Л. М., та Хорошко В. О., під заг. ред. проф. В. О. Хорошка, “Банківська безпека” підручник, К: ПВП “Задруга”, 2014.

27. Корченко О. Г., Архипов О. Є., та Дрейс Ю. О., “Оцінювання шкоди національній безпеці України у разі витоку державної таємниці”, монографія, К: наук.-вид.центр НА СБУ України, 2014.

28. Евсеев С., “Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины”, Науково-технічний журнал “Захист інформації”, том. 22, № 2, с. 297 – 309, 2016.

29. Грищук, та С. Євсеєв, “Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах”, Науково-технічний журнал “Безпека інформації”, том 23, № 3, с. 204 – 214, 2017.

30. Грищук Р. В, Теоретичні основи моделювання процесів нападу на інформацію методами теорій диференціальних ігор та диференціальних перетворень, Житомир : Рута, 2010.

31. Потій О., Лєншин А., “Методика оцінки відповідності поточної зрілості цільовим орієнтирам”, Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник, Вип. 1(12), с. 31 – 43, 2006.

32. ISO/IEC 27032:2012 Information technology – Security techniques – Guidelines for cybersecurity [Online]. Available: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375

33. ISO/IEC 18045:2014 Information technology – Security techniques – Guidelines for cybersecurity [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46412

34. Цивільний кодекс України від 16.01.2003 № 435-IV. [Електронний ресурс]. Доступно: https://kodeksy.com.ua/tsivil_nij_kodeks_ukraini.htm.

35. Кримінальний кодекс України. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

36. Закон України “Про інформацію”. [Електронний ресурс]. Доступно: https://zakon.rada.gov.ua/laws/show/2657-12#Text

37. ISO/IEC 17799:2005. Information technology – Security techniques – Code of practice for information security management – Technical Corrigendum 1: [Електронний ресурс]. Доступно:: https://www.iso.org/ru/standard/46381.html

38. ISO/IEC 27035-3:2020 Information Technology — Information Security Incident Management. [Електронний ресурс]. Доступно: https://www.iso.org/ru/search.html?q=27035.

39. ISO/IEC 15408-2:2008 Information Technology – Security Techniques – Evaluation Criteria For It Security – Part 2: Security Functional Components: [Електронний ресурс]. Доступно: https://www.iso.org/ru/search.html?q=ISO%2015408%20&hPP=10&idx=all_ru&p=0

40. Kleidermacher “Securing embedded systems. Embedded Systems Security, 1st Edition Practical Methods for Safe and Secure Software and Systems Development” Newness, Apr. 2012.

41. Michael Vai, David J. Whelihan, Benjamin R. Nahill, Daniil M. Utin, Sean R. O’Melia, and Roger I. Khazan, “Security in embedded systems” [Електронний ресурс]. Доступно: https://www.ll.mit.edu/publications/journal/pdf/vol22_no1/22_1_9_Vai.pdf

42. Грищук Р. В., та Даник Ю. Г. Основи кібернетичної безпеки: Монографія /; за заг. ред. Ю. Г. Данника. Житомир: ЖНАЕУ, 2016..

43. Грищук Р. В., “Атаки на інформацію в інформаційно-комунікаційних системах”, Сучасна спеціальна техніка, №1(24), с.61 – 66. 2011.

ДОДАТКИ

Додаток А

Політика безпеки інтернет-магазину компанії ТОВ “Окей”.

1. Загальні положення

1.1 Ця Політика обробки персональних даних (далі – Політика) складена відповідно до Закону України “Про захист персональних даних”. та діє щодо персональних даних, які можуть бути отримані від суб’єктів персональних даних.

1.2 Метою Політики є опис вимог до безпечних способів обробки персональних даних, а також розробка на базі даної Політики процедур, які покликані запобігти або вчинити реакцію на спроби порушення безпеки персональних даних.

2. Оброблювані персональні дані

2.1 Основні поняття, що використовуються у Політиці:

• персональні дані – це будь-яка інформація, яка має відношення до певної чи визначеної на підставі такої інформації фізичної особи (суб’єкта персональних даних). До персональних даних можуть належати його прізвище, ім’я, по батькові, рік, місяць, дата та місце народження, адреса, сімейний, соціальний, майновий стан, освіта, професія, доходи, інша інформація;

• обробка персональних даних – це набір дій (операцій), що виконуються із персональними даними. До таких операцій належать збирання, систематизація, накопичення, зберігання, уточнення (оновлення, зміна), використання, розповсюдження (у тому числі передачу), знеособлення, блокування, знищення персональних даних;

2.2 Обробка персональних даних виходить з принципами:

• сумлінності та законності цілей та способів, що використовуються при обробці персональних даних;

• відповідності цілей обробки персональних даних повноваженнями, якими володіє компанія ТОВ “Окей”;

• відповідності обсягу та змісту персональних даних, що обробляються та способів обробки персональних даних цілям обробки;

• вірогідність персональних даних, їх актуальності та достатності для цілей обробки, неприпустимості обробки персональних даних, надлишкових стосовно цілей, заявлених під час збору персональних даних;

• неприпустимість об’єднання баз даних, які містять персональні дані, несумісні між собою;

• обмеження обробки персональних даних при досягненні конкретних та законних цілей, заборони обробки персональних даних, несумісних з метою збору персональних даних.

• здійснення зберігання персональних даних у формі, що дозволяє визначити суб’єкта персональних даних, не довше, ніж цього вимагають мети їхньої обробки, якщо термін зберігання персональних даних не встановлений чинним законодавством. Персональні дані підлягають знищенню або знеособленню після досягнення цілей обробки або у разі втрати необхідності досягнення цих цілей, якщо інше не передбачено чинним законодавством.

2.3 В рамках цієї Політики під персональними даними, що обробляються, розуміються:

• персональні дані, що надаються громадянами при та зверненні до компанії ТОВ “Окей”;

• персональні дані працівників компанії ТОВ “Окей” чи кандидатів на заміщення вакантних посад;

• громадян, які є однією зі сторін цивільно-правових договорів із компанією ТОВ “Окей”.

3. Цілі збору та обробки персональних даних

3.1 Компанія ТОВ “Окей” збирає, зберігає та обробляє персональні дані суб’єктів персональних даних у таких цілях:

• для виконання умов трудового договору та виконання всіх прав та обов’язків, які виникають відповідно до трудового законодавства України;

• для ухвалення рішення про працевлаштування;

• для ведення персоніфікованого обліку відповідно до чинного законодавства;

• для оформлення документів, встановлених чинним законодавством та іншими нормативними правовими актами;

• для прийняття рішень щодо звернень громадян України відповідно до чинного законодавства.

3.2 Термін зберігання персональних даних суб'єкта персональних даних повинен визначатися відповідно до чинного законодавства та інших нормативно-правових документів.

4. Особливості обробки персональних даних та їх передача третім особам.

4.1 Доступ до персональних даних, що обробляються, мають особи, які мають відповідні повноваження визначені у наказі керівника компанія "Назва фірми", а також особи, дані яких обробляються.

4.2 Доступ працівників компанії ТОВ "Окей" до персональних даних, що обробляються, здійснюється відповідно до чинних посадових інструкцій, затверджених наказом керівника компанії ТОВ "Окей".

4.3 Передача оброблюваних персональних даних третім особам можливе лише за прямим письмовим розпорядженням керівника компанії ТОВ "Окей" за наявності письмової згоди суб'єкта персональних даних, якщо інше не передбачено федеральним законодавством.

5. Заходи, що застосовуються для захисту персональних даних, що обробляються

5.1 Компанія ТОВ "Окей" вживає необхідних та достатніх організаційно-технічних заходів, спрямованих на забезпечення захисту оброблюваних персональних даних від неправомірного або випадкового доступу, від знищення, зміни, блокування, копіювання, розповсюдження, а також від інших неправомірних дій з ними з боку третіх осіб. До таких заходів, зокрема, відносяться:

призначення відповідального співробітника, який забезпечує організацію обробки персональних даних;

• здійснення внутрішнього контролю відповідності обробки персональних даних;

• ознайомлення працівників, які безпосередньо виконують обробку персональних даних, з положеннями чинного законодавства про персональні дані, вимогами до захисту персональних даних та іншими нормативно-правовими документами, пов’язаними з питаннями обробки персональних даних;

• виявлення можливих загроз безпеці персональних даних, що виникають під час роботи з персональними даними в інформаційних системах обробки та зберігання персональних даних;

• використання засобів захисту інформації, які пройшли в установленому порядку процедуру оцінювання відповідності державним стандартам безпеки;

• здійснення обліку носіїв персональних даних;

• визначення та встановлення правил доступу до персональних даних, що обробляються в інформаційних системах обробки та зберігання персональних даних;

• безперервний контроль за заходами, що вживаються з метою забезпечення безпеки персональних даних, а також контроль та оцінка рівня захищеності інформаційних систем з обробки та зберігання персональних даних;

• розробка локальних актів, пов’язаних із питаннями обробки персональних даних

6. Зміна політики. Застосовне законодавство

6.1 Компанія ТОВ “Окей” має право вносити зміни до цієї Політики.

6.2 При внесенні змін до заголовка Політики необхідно вказувати дату останнього оновлення редакції.

6.3 Нова редакція Політики набирає чинності з її затвердження керівником компанії ТОВ “Окей” розміщення на сайті компанії, якщо інше не передбачено новою редакцією Політики.