Хмельницький національний університет
Факультет інформаційних технологій
Кафедра кібербезпеки

КВАЛІФІКАЦІЙНА РОБОТА

бакалавр
Освітній рівень

Архітектура системи захисту інформації діяльності ПП «МайстерКомп»
Назва теми

КРКБ. 101173.18.01.05 ПЗ
Шифр

Галузь знань 12 – Інформаційні технології
Шифр, назва

Спеціальність 125 – Кібербезпека
Шифр, назва

Освітня програма Кібербезпека
Шифр, назва

Виконав студент 4 курсу, група КБ-18-01 6.06.22 О. Г. Костовський
Підпис, дата Ініціали, прізвище

Керівник 6.06.22 В. М. Чешун
Підпис, дата Ініціали, прізвище

Нормоконтролер 16.06.22 С. В. Мостовий
Підпис, дата Ініціали, прізвище

До захисту допускаю:
Зав. кафедри кібербезпеки Ю. П. Кльоц
Підпис, дата Ініціали, прізвище

16 06 2022 р.

Хмельницький, 2022

№ ряд ка	Фо рма т	Позначення	Найменування	К-сть листк ів	№ екз.	При мітк а
1	А4		Завдання на кваліфікаційну	1		
			роботу			
2	А4		Анотація	2		
3	А4	КРКБ.101173.18.01.05 ПЗ	Архітектура системи захисту	64		
			Інформації діяльності ПП			
			«МайстерКомп»			
			Пояснювальна записка			
4	А2	КРКБ.101173.18.01.05 Е8	Ситуаційний план	1		
			ПП «МайстерКомп»			
			Схема структурна			
5	А2	КРКБ.101173.18.01.05 Е8	Генеральний план	2		
			ПП «МайстеКомп»			
			Схема структурна			
6	А2	КРКБ.101173.18.01.05 Е8	Схема заходів системи захисту	1		
			інформації			
			ПП «МайстерКомп»			
			Схема структурна			

Зм.	Аркуш	№ докум.	Підпис	Дата	КРКБ.101173.18.01.05 ВП			
Розробив		Костовський О.		6.06	*Архітектура системи захисту інформації діяльності ПП «Майстеркомп» Відомість проекту*	Літ	Аркуш	Аркушів
Перевірив		Чешун В. М.		6.06		Н	1	1
Н.контр.		Мостовий С. В.		16.06.2		ХНУ КБ-18-1		
Затвер.		Кльоц Ю. П.		16.06.2				

ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій
Кафедра кібербезпеки
Освітній рівень *бакалавр*
Галузь знань 12 «Інформаційні технології»
Спеціальність 125 «Кібербезпека»
Освітня програма освітньо-професійна програма підготовки бакалавра

ЗАТВЕРДЖУЮ:
Завідувач кафедри Ю.П.Кльоц
_____
1. 03 . 2022

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ

Костовському Олесю Геннадійовичу
Прізвище, ім'я, по батькові студента

1 Тема роботи Архітектура системи захисту інформації діяльності ПП «МайстерКомп»
Керівник роботи Чешун Віктор Миколайович
кандидат технічних наук, доцент кафедри комп'ютерних систем та мереж ХНУ
Прізвище, ім'я, по батькові, науковий ступінь, вчене звання

Затверджено наказом ректора університету від 1 03 2022 р. № 18
2 Строк подання студентом роботи на кафедру: _____
3 Вихідні дані до роботи розробка ефективної моделі архітектури систем захисту інформації з обмеженим доступом для приватного підприємства
4 Зміст пояснювальної записки (перелік питань, які потрібно розробити) аналіз об'єкту захисту, обгронтування вибору системи заходів, що гарантує побудову ефективної архітектури захисту інформації, її проєктування та реалізація на ПП «МайстерКомп»
5 Перелік графічного матеріалу (із зазначенням обов'язкових креслень): «Ситуаційний план підприємства»; «Генеральний план підприємства»;

6 Консультанти розділів кваліфікаційної роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Нормоконтроль	Мостовий С.В., ст. викладач	-	
Антиплагіат	Мостовий С.В., ст. викладач	-	

7 Дата видачі завдання «30» січня 2022 р.

КАЛЕНДАРНИЙ ПЛАН

Назва етапу (розділу) кваліфікаційної роботи	Строк виконання етапу роботи	Примітка
1. Вибір та затвердження теми кваліфікаційної роботи, отримання завдання	Січень	Виконано
2. Аналіз об'єкта захисту	Лютий- березень	Виконано
3. Аналіз літературних джерел	Лютий- березень	Виконано
4. Проєктування та розробка моделі архітектури системи захисту інформації на об'єкті захисту.	Березень- квітень	Виконано
5. Впровадження та тестування запропонованої моделі архітектури захисту інформації.	Квітень	Виконано
6. Написання та оформлення тексту пояснювальної записки	Квітень- травень	Виконано
7. Оформлення графічних матеріалів та оформлення презентації	Травень	Виконано
8. Нормоконтроль. Отримання супровідних документів.	Червень	
9. Підготовка до захисту та захист роботи	Червень	

Студент _____ О.Г. Костовський
Підпис Ініціали, прізвище

Керівник роботи _____ В.М. Чешун
Підпис Ініціали, прізвище

АНОТАЦІЯ

Тема кваліфікаційної роботи: Архітектура системи захисту інформації діяльності ПП «Майстеркомп».

Автор роботи: Костовський Олесь Геннадійович.

Керівник роботи: Чешун Віктор Миколайович.

Пояснювальна записка: 64 с., 23 рис., 16 табл., 6 дод., 18 джерел.

Графічна частина: 22 презентаційних слайдів.

АРХІТЕКТУРА СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ, МОДЕЛЬ АРХІТЕКТУРИ, КОНФІДЕЦІЙНА ІНФОРМАЦІЯ, ОБ'ЄКТ ЗАХИСТУ, НЕСАНКЦІОНОВАНИЙ ДОСТУП.

Метою роботи є розробка моделі архітектури системи захисту інформації для ПП «МайстерКомп». Об'єктом розробки моделі архітектури є інформаційно-телекомунікаційна система приватного підприємства «МайстерКомп».

У першому розділі роботи зроблений детальний аналіз законодавчих актів та нормативних документів України та визначена актуальність цієї проблеми для приватних підприємств. Також розглянуті питання принципів та етапів побудови архітектури системи захисту інформації, представлена їх детальна класифікація. Проаналізовані переваги та недоліки існуючих моделей архітектур систем.

У спеціальні частині роботи розглянуті питання, пов'язані з розробкою архітектури системи інформаційного захисту на ПП «МайстерКомп». Під час виконання роботи було проведено аудит інформаційної безпеки підприємства, зроблене категорування інформації, яка обробляється, виявлено можливі канали витоку інформації, наведено характеристику компонентів системи. Також сформовані основні положення політики безпеки для створення моделі архітектури системи захисту інформації.

6.06

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

ПП – приватне підприємство;

ЗУ – Закон України;

АС - автоматизована система;

ЕОТ - електронно-обчислювальна техніка;

ІБ - інформаційна безпека;

ІТС - інформаційно-телекомунікаційна система;

КСЗІ - комплексна система захисту інформації;

НСД – несанкціонований доступ;

ОІД – об'єкт інформаційної діяльності;

ОС – операційна система;

ПБ – політика безпеки;

ПЗ – програмне забезпечення;

ТЗІ – технічні засоби інформації;

ПЕОМ – персональна електронно-обчислювальна машина;

СУІБ – система управління інформаційною безпекою;

МКД – магнітно-контактний датчик;

КВІ – канали витоку інформації.

ВСТУП

З кожним роком у світі швидкими темпами збільшується кількість інформації, яка містить державну, комерційну та особисту інформацію, або таємницю. Отже, щорічно збільшується попит на заволодіння цінною інформацією, а також збільшується її цінність та постійно зростає попит на неї. У зв'язку з цими, збільшується необхідність постійного надійного захисту будь-якої інформації з боку держави, організацій, підприємців.

Також в сучасному суспільстві швидкими темпами розробляються нові і вдосконалюються існуючі комп'ютерні технології. Завдяки постійному оновленню та вдосконаленню цих сучасних комп'ютерних технологій виникають нові і нові загрози для витоку секретної та конфіденційної інформації. Отже, зростає необхідність її захисту. Для того, щоб захист був повноцінним, постійним та достатньо надійним, необхідно розробляти та удосконалювати архітектуру систем захисту інформації комплексно.

Витік будь-якої інформації може суттєво вплинути на діяльність організації, або підприємства. Особливо гостро стоїть питання збереження конфіденційної інформації, втрата якої може викликати великі зміни в самої організації та вплинути на її матеріальні ресурси. Тому питання архітектури систем захисту інформаційної безпеки в наш час дуже актуальні та важливі.

Можливості малого бізнесу та приватних підприємців часто не дозволяють організувати кваліфіковану роботу спеціальних служб, які б надійно забезпечили інформаційну безпеку організації, здійснювали виявлення, попередження та усунення загроз, що виникають у ній, і можуть стати причиною пошкодження, викрадення, спотворення важливої інформації.

Актуальність теми данної роботи визначається ще тим, що малий бізнес є одним із найменш захищених і досить вразливим від загроз інформаційної безпеки через цілу низку причин:

- непомірно висока вартість технічних засобів захисту інформації;
- потреба у регулярному залученні сторонніх кваліфікованих фахівців;

- галузі побудови та обслуговування архітектури систем захисту інформації;

- недостатнє методичне забезпечення діяльності з розробки надійних архітектур систем захисту інформації.

Слід зазначити, що актуальність даної роботи полягає ще у тому, що нині дедалі більше організацій та приватних підприємців приділяють належну увагу питанням інформаційної безпеки. Особливо це стосується компаній та фізичних осіб, що займаються роздрібною торгівлею, наданням різноманітних послуг населенню, оскільки конфіденційність, достовірність, цілісність та доступність інформації є надзвичайно важливими ознаками безупинності та успішності ведення бізнесу. Комплекс заходів, спрямований на забезпечення надійної інформаційної безпеки та кваліфіковано розроблена архітектура систем захисту інформації може суттєво вплинути на конкурентоспроможність підприємницької діяльності, відповідність законодавству, прибутковість приватного бізнесу, або організації.

Мета роботи створити модель архітектурою системи захисту інформації для ПП «МайстерКомп» в місті Хмельницькому. Під час виконання роботи було проведено ретельний аналіз інформаційної бази ПП та наявних засобів захисту інформації, внаслідок якого виявлено кілька джерел та носіїв інформації, проведено категорування існуючої інформації, виявлені можливі канали витоку та втрати важливої інформації. Були розреблені заходи для усунення недоліків системи захисту, які представлені у роботі.

В результаті виконання кваліфікаційної роботи було розроблено модель архітектури системи захисту інформації, був проведений підбір технічних та програмно-апаратних засобів.

РОЗДІЛ 1. ПОБУДОВА ЕФЕКТИВНОЇ АРХІТЕКТУРИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

1.1 Аналіз нормативно-правової бази

Адміністрація організації, або приватний підприємець для визначення необхідності створення архітектури системи інформаційного захисту повинен керуватися нормативними актами та вимогами діючого законодавства. Саме вони встановлюють необхідність та обов'язковість обмеження доступу до певних видів інформації. Має проводитися аналіз нормативно-правових актів, на основі яких повинні здійснюватися обмеження доступу до окремих видів інформації чи заборона для такого обмеження, чи визначення необхідності забезпечення захисту інформації у відповідності до інших критеріїв, визначення наявності у складі інформації, яка належить автоматизованій обробці, таких її видів, які вимагають щоб до неї був обмежений доступу чи забезпечення цілісності та доступності у відповідності з вимогами. На основі проведеного такого аналізу приймається рішення про необхідність створення архітектури системи інформаційної безпеки на підприємстві чи в організації.

Головною метою архітектури системи ІБ є забезпечення захисту конфіденційної інформації від розголошення, витоку, несанкціонованого доступу та фальсифікації даних в системі, охорону продукції, яка пропонується та реалізується, а також персоналу, який працює на підприємстві чи в організації.

Перелік інформації, що існує на підприємстві: інформація про постачальників та партнерів, клієнтів, податки, укладені договори та підписані контракти, банківські рахунки, внутрішні накази адміністрації подається та описана в нормативних документах України.

За порушення передбачається відповідальність. Порушення можуть призвести до позбавлення ліцензії комерційної організації, конфіскація майна, або штрафи тощо.

Найважливішою складовою правового забезпечення у сфері захисту інформації є стандартизація, що має на меті:

- створення основних стандартів організаційно-методичного і термінологічного забезпечення системи захисту інформації;

- сталість вимог по захисту інформації в технічних засобах захисту, в інформаційно-телекомунікаційних системах.

Необхідність впровадження на конкретному підприємстві чи в установі архітектури системи захисту інформації продиктована вимогами стандартів України з управління інформаційною безпекою.

Інформація – будь-які відомості та дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Під інформацією розуміють сукупність задокументованих або публічно озвучених даних про різні події або явища, які трапляються у суспільстві, державі, в довкіллі.

Також роз'яснюється, що інформація це є сукупність усіх даних , які використовуються та обробляються в автоматизованих системах, незалежно від способу їхнього надання.

Згідно законодавства в залежності від надання доступу, інформація можна поділити на такі два види: відкриту інформацію та інформацію з обмеженим доступом.

Інформацію з обмеженим доступом називають таку інформацію, право і можливість доступу до якої обмежено керівником установи, який при цьому керується лише нормами законодавства. Інформація з обмеженим доступом, яка потребує відповідного захисту, може оброблятися, передаватися та зберігатися за допомогою різних ресурсів, а саме: серверів, робочих станцій, запам'ятовуючих пристроїв, периферійних пристроїв, мережевого обладнання, системного програмного забезпечення, засобів, що забезпечують взаємодію всіх компонентів та об'єктів ІТС.

Під таємною інформацією як правило розуміють інформацію з обмеженим доступом, яка містить державну або іншу, передбачену законом, таємницю.

Конфіденційна інформація – це також інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи і які самостійно визначають порядок доступу до відповідних відомостей.

Відповідно до законодавства захисту підлягає: відкрита інформація, яка є власністю держави і визначенні в законі Вона належить до статистичної, правової, соціологічної інформації, має довідковий характер та використовується для забезпечення діяльності державних та місцевих органів влади, а також інформація про діяльність вище зазначених органів, яка стає загальновідомою в Інтернеті, інших інформаційних мережах і передається телекомунікаційними мережами (відкрита інформація). Будь-яка інформація вважається відкритою, окрім тієї, яа відноситься законом до інформації з обмеженим доступом.

Інформаційний ресурс установи, організації, чи компанії це загальна сукупність усіх документів у інформаційних системах.

Документ розуміють як матеріальну форму одержання, зберігання, поширення та використання інформації шляхом її фіксації та зберігання на різноманітних носіях.

Поняття «документа» надзвичайно важливо, оскільки документи є невід’ємною частиною інформаційних ресурсів.

1.2 Поняття архітектури системи захисту інформації

Архітектура системи безпеки представляє собою стандартний дизайн безпеки, який враховує потреби захисту інформації та потенційні ризики, які пов'язані з конкретним сценарієм чи середовищем. Архітектура системи захисту інформації також вказує, коли та де застосовувати заходи безпеки. Процес проектування, як правило, відтворюєється.

В архітектурі системи захисту інформації принципи проектування викладено і повідомляються чітко, а докладні інструкції щодо управління та контролю безпекою як правило документуються в незалежних документах.

Системна архітектура може розглядатися як проект або конструкція, які включають структуру і відображають зв'язк між усіма структурними компонентами системи захисту.

Головними атрибутами архітектури системи захисту інформації є:

- взаємозв'язок між різними компонентами всередині IT-архітектури та те, як вони взаємодіють один одним;

- основною перевагою архітектури захисту інформації визнають її стандартизацію, що є дуже важливим тому, що робить її доступною. Архітектура системи безпеки переважно є економічно ефективною завдяки тому, що можливе повторне використання елементів управління, які описані в архітектурі.

Усі засоби безпеки інформації, можна індентифікувати на основі чотирьох факторів:

- управління різноманітними ризиками;

- вивчення чужого досвіду а також хороша практика;

- фінансові фактори;

- законодавчі та нормативні.

Фахівці виділяють основними фази процесу побудови архітектури систем захисту інформації :

- оцінка ризиків архітектури системи захисту інформації оцінює можливий вплив бізнесу на усі активи, а також можливості та наслідки для загрози безпеки;

- архітектура та дизайн безпеки має на увазі служби безпеки, які в повній мірі можуть сприяти досягненню різних цілей, які тісно пов'язані із ризиком для приватного бізнесу;

- впровадження архітектури захисту інформації має на увазі усі процеси, які використовуються та контролюються. Служби захисту розроблені таким чином, що вони здатні забезпечити виконання стандартів безпеки, рішень архітектури системи захисту інформації та управління ризиками в будь якій реальній ситуації;

- операції та моніторинг. Це повсякденні процеси управління загрозами та вразливістю. Тут вживаються заходи щодо забезпечення контролю та управління робочим станом системи безпеки.

1.3 Принципи архітектури системи захисту інформації

Якими б потужними та надійними не були би різноманітні сервіси безпеки, вони самі по собі не можуть гарантувати організаціям та приватним підприємцям 100 відсоткової надійності програмно-технічного захисту. Тільки перевірена архітектура системи може забезпечити та гарантувати ефективне об'єднання усіх сервісів, а також надати можливість керування, її здатністю розвиватися і протистояти новим загрозам, а також зберігати такі властивості, як висока продуктивність, простота і зручність використання.

Зазвичай виділяють такі три основні принципи для вирішення проблеми архітектурної безпеки мережевих конфігурацій та систем:

- необхідність створення та впровадження єдиної політики захисту інформації, яка б забезпечувала її безпеку;

- забезпечення конфіденційності та цілісності інформації при мережевих обробках та інших взаємодіях;

- формування складених сервісів потрібно здійснювати таким чином, щоб кожен з компонентів мав повний набір надійних захисних засобів і, одночасно, був єдиним цілим цілої системи.

З огляду на практичне застосування слід вказати на такі важливі принципи архітектурної безпеки:

- здатність здійснювати безперервний захисту будь де і будь коли, а також забезпечити неможливість оминути захисні засоби. Якщо у зловмисника з'явиться можливість оминути захисні засоби, він безперечно скористається такою нагодою;

- дотримання перевірених та визнаних у світі стандартів, використання

рішень, які вже пройшли апробацію. Все вище згадане підвищує надійність ІС та зменшує можливість потрапити в ситуацію, коли для забезпечення безпеки інформації буде потрібно робити занадто великі витрати і здійснювати певні модифікації архітектури системи захисту інформації;

- організація архітектури системи має містити невелику кількістю об’єктів на кожному рівні, що є просто необхідним з технологічних міркувань. При порушенні даного принципу система може стане некерованою і забезпечити її безпеку буде вкрай складно, а інколи і неможливо;

- визначення та посилення найслабкішої ланки в системі захисту. Найчастіше зловмисник не буде намагатися зруйнувати сильні сторони захисту, він навпаки, спробує знайти слабку ділянку. Практика показує, що дуже часто найслабкішою ланкою захисту стає людина, а не комп'ютер або програма. В результаті цього проблема забезпечення ІБ має нетехнічний характер;

- засіб захисту не може переходити в небезпечний стан, а має повністю виконувати свої безпосередні завдання та функції, або повністю блокувати доступ до мережі;

- потреба в зменшенні до мінімуму переваг для будь кого. Слід надавати користувачам або адміністраторам тільки ті права доступу, які будуть необхідні їм для виконання своїх безпосередніх обов’язків. Цей принцип архітектури захисту гарантує зменшення втрат від випадкових, або навмисних некоректних дій з боку користувачів чи адміністраторів;

- необхідність розділення обов’язків між працівниками. Важливо, щоб одна людина не могла порушити критично важливий для організації процес, або здійснити прогалину у захисті за замовленням зловмисників. Зокрема, дотримання даного принципу унеможливить здійснення протиправних дій з боку системних адміністраторів;

- не потрібно покладатися на всі 100% на один захисний засіб, яким би надійним він не був. Має здійснюватися багатоетапний та багаторівневий захист. Ешелонована оборона дасть можливість затримати зловмисника і його дії не залишаться таємними;

- використання різноманітність засобів захисту інформації в архітектурі системи дає можливість створення різних оборонних кордонів. В такому випадку зловмиснику буде потрібно мати дуже високу кваліфікацію;

- простота використання та керування засобами захисту. Тільки при використанні простого захисного засобу можна перевірити коректність його роботи узгодженість взаємодії різних компонентів архітектурисистеми захисту і одночасно здійснювати всебічне адміністрування та контроль.

Для забезпечення високої доступності та результативності роботи необхідно дотримуватися таких принципів архітектурної безпеки:

- застосування додаткового резервного устаткування та використання додаткових каналів зв'язку;

- використання сучасних засобів для термінового виявлення різноманітних неординарних ситуацій;

- використання засобів реконфігурації, які дали би можливість відновлювати, блокувати, заміняти складові компоненти архітектури системи, які дали збій в роботі або зазнали атак з боку зловмисників;

- розділення управління мережею, має бути відсутня єдина точка відмови;

- створення допоміжних мереж та здійснення блокування та ізоляції різних груп користувачів один від одного. Цей принцип є узагальненням принципу розділення процесів на рівні операційної системи, і в наслідок цього, дає змогу обмежити зону ураження в випадку порушень інформаційної безпеки.

Також слід відмітити ще один важливий принцип архітектури системи захисту інформації – зведення до мінімуму обсягу засобів захисту, які будуть використовуватися в системі. До мінімальної кількості слід зменшити використання сервісів безпеки на різних рівнях (мережевому і транспортному) і підтримку засобів для проведення автентифікації, які були би стійкими до різних мережевих загроз.

1.4 Основні компоненти архітектури систем захисту інформації

Архітектуру системи інформаційної безпеки слід розглядати як сукупність технічних засобів захисту та організаційних заходів, які використовуються для протидії актуальним загрозам інформаційної безпеки та здатність знизити ризики для захисту активів організації або компанії.

Оптимальна архітектура систем захисту інформації має відповідати декільком базовим принципам:

- втілювати у собі концепцію багаторівневого захисту (Defense in depth). Неможливо обмежитись використанням лише міжмережевого екрану. Це не дасть можливості вирішити усі проблеми інформаційної безпеки;

- необхідно надати можливість для розширення та зростання, горизонтального та вертикального масштабування. Побудована система повинна відповідати зростаючим потребам бізнесу на момент створення;

- архітектура систем інформаційної беспеки має бути простою у використанні та діагностиці;

- архітектура систем інформаційної беспеки має мати змогу інтеграції з усіма необхідними інфраструктурними системами компанії. Якщо ви використовуєте службу каталогів AD (Active Directory) під час аутентифікації адміністраторів у всіх системах, засіб захисту також повинен інтегруватися з AD;

- реально підвищувати рівень безпеки. Можна встановити всі можливі засоби захисту, але якщо архітектура буде побудована невірно то це не принесе очікуваних результатів, а інформаційна безпека все одно залишиться на попередньому рівні.

Можна виділити основні компоненти архітектури систем ІБ:

- засоби захисту периметра , а саме міжмережові екрани, системи захисту від витоків даних, системи захисту пошти, системи виявлення та запобігання вторгненням, мережеві екрани, мережеві «пісочниці», засоби організації захищеного віддаленого доступу до мережі , системи захисту від атак;

- засоби для криптографічного захисту інформації;

- засоби захисту внутрішньої мережевої інфраструктури (тут необхідно використовувати міжмережеві екрани, засоби контролю доступу до мережі NAC, мережеві IDS/IPS);

- засоби захисту серверної інфраструктури а також робочих місць (антивіруси, засоби захисту баз даних, хостові «пісочниці», хостові IDS/IPS, засоби контролю доступу);

- засоби для проведення моніторингу про стан роботи засобів захисту, збору та кореляції подій ІБ, а також сканери вразливостей.

При створенні архітектури систем інформаційної безпеки, визначенні складу її компонентів потрібно врахувати актуальні загрози, цінність активів, що захищаються, як кількісних, так і якісних, а також ймовірність реалізації загроз.

Зазвичай кожен компонент, який задіяний в архітектурі систем інформаційного захисту має виконувати конкретні задачі, але зараз існують і широко застосовуються багатофункціональні компоненти: міжмережні екрани нового покоління, пристрої для комплексного захисту від мережевих загроз. Отже дуже часто фінансово вигідніше купувати багатофункціональні компоненти.

1.5 Класифікація архітектур систем захисту інформації

Архітектури систем захисту інформації можна поділити на моновендорні та мультивендорні, а також на централізовані та децентралізовані.

Проведемо аналіз кожного типу архітектури.

Для моновендорних архітектур слід виділити такі переваги та недоліки, (рисунок 1.1):

Рисунок 1.1 – Моновендорна архітектура систем захисту інформації

Що стосується мультивендорних архітектур систем захисту інформації, то слід відмітити такі переваги та недоліки (рисунок 1.2):

Рисунок 1.2 – Мультивендорна архітектура систем захисту інформації

У централізованій архітектурі систем захисту інформації можна виділити такі переваги та недоліки (рисунок 1.3):

Рисунок 1.3 – Централізована архітектура систем захисту інформації

Децентралізована архітектура також має свої переваги та недоліки (рисунок 1.4):

Рисунок 1.4 – Децентралізована архітектура систем захисту інформації

1.6 Вибір архітектури систем захисту інформації

При виборі цільової архітектури систем захисту інформації слід насамперед керуватися даними про існуючу інфраструктуру компанії, для якої розробляється ця система. Також потрібно враховувати цілі, яких необхідно досягти та про експлуатаційні можливості системи, яка пропонується.

З огляду на класифікацію архітектурних систем інформаційного захисту, яка наведена вище, слід зазначити, що централізована архітектура систем краще підійде тим компаніям, у яких:

- великий бізнес із чітко виділеними центром обробки даних, або ключовими майданчиками;

- велика розподілена регіональна структура; відсутність кваліфікованого персоналу для адміністративних функцій на віддалених майданчиках;

- часто відбуваються зміни політики безпеки щодо засобів захисту; великий обсяг засобів захисту, які постійно використовуються в роботі;

- потрібно забезпечити синхронізацію політик безпеки між різними майданчиками.

В свою чергу, децентралізована архітектура буде зручнішою та кориснішою для тих компаній, у яких:

- незалежні бізнес-напрямки, франшизи або великі філії зі своїми власними політиками безпеки;

- є кваліфікований персонал для виконання адміністративних функцій на кожному майданчику;

- зміни політики безпеки для засобів захисту відбуваються вкрай рідко; невеликий обсяг засобів захисту, які використовуються в роботі;

- не має потреби забезпечувати синхронізацію політик безпеки між різними майданчиками.

Якщо йдеться мова про застосування мультивендорної архітектури, то вона найкраще підійде для компаній з наступними характеристиками:

- потрібно забезпечити незалежність від конкретного постачальника засобів захисту (компанія має мати можливість вільного використання в архітектурі продукцію інших постачальників);

- компанія володіє достатнім бюджетом, який вона може використати на інформаційну безпеку;

- потрібний великий ІБ-функціонал, який не може надати один постачальник засобів захисту, або його продукти мають слабкі сторони в тому чи іншому напрямку і не можуть забезпечити потрібний рівень безпеки;

- є висококваліфікований персонал, який може працювати з різними засобами захисту від різних постачальників та з різним функціональними можливостями.

Моновендорна архітектура систем інформаційного захисту буде кращим рішенням для компаній, якщо:

- немає великих потреб по функціональним можливостям засобів захисту (один постачальник може закрити всі потреби);

- бюджет компаній, який може бути виділений на інформаційну безпеку, невеликий;

- немає обмежень щодо використання пропрієтарних технологій;

- є персонал, який здатен працювати та обслуговувати засоби захисту конкретного постачальника, або його легко навчити чи найняти;

- вже є засоби захисту від постачальника в інфраструктурі компанії, а персонал може побудувати архітектуру з урахуванням кращих світових практик.

При побудові архітектури систем інформаційного захисту і виборі модулів архітектури слід враховувати взаємодію цих модулів з об'єктом захисту, а також можливість взаємодії цих модулів між собою. Формально модулі архітектури систем захисту інформації існують у вигляді наступних класів, що реалізують відповідну функціональність:

- антивіруси;

- міжмережеві екрани (пакетна фільтрація, фільтрація на основі

перевірки вмісту, виконують захист у реальному часі, мають гнучкість при використанні);

- засоби для контролю та розмежування доступу, у тому числі засоби ідентифікації та аутентифікації (реалізація правил розмежування доступу суб'єктів та їх процесів, запобігають витоку даних, обмежують доступ до програмного середовища);

- VPN (швидкість, безпека, гнучкість, конфіденційність);

- системи виявлення та запобігання різноманітним вторгненням (використовуються для захисту у реальному часі, спрямовані на виявлення спроб порушення безпеки, мають можливість виявляти аномалій у діях користувача, та аномалії у зовнішньому мережевому оточенні, використовуються для усунення вразливостей);

- засоби захисту інформації від копіювання, зміни, видалення (забезпечують цілісність інформації, швидкодіючі,);

- системи аналізу захищеності (надають ефективний аналіз системи, регулярно оновлюються, виконують аналіз у реальному часі, мають здатність усунення вразливостей);

- засоби захисту середовища віртуалізації (здійснюють контроль доступу до віртуального середовища, , забезпечують цілісність).

1.7 Висновки

В першому розділі кваліфікаційної роботи зроблено оглядовий аналіз основної нормативно-правової бази, що безпосередньо стосується і пов’язана з захистом інформації, зазначено основні положення та проблематика захисту інформації в країні. В розділі дається визначення архітектури систем захисту інформації та детальний опис головних принципів створення архітектури систем захисту для компаній та організацій. В розділі наведена класифікація існуючих ефективних архітектур систем інформаційного захисту. Даються рекомендації по

вибору архітектури захисту для компаній і організацій в цілому. Також в розділі наведені головні засоби захисту існуючої інформації, та тієї яка обробляється, з яких складається надійна архітектура системи. В розділі можна ознайомитися з перевагами та недоліками застосування тієї, чи іншої існуючої моделі архітектури систем інформаційного захисту (моновендорної, чи мультівендерної; централізованої, чи децентралізованої, горизонтального чи вертикального масштабування тощо).

РОЗДІЛ 2. ОБГРОНТУВАННЯ ВИБОРУ МОДЕЛІ АРХІТЕКТУРИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ПП «МАЙСТЕРКОМП»

2.1 Етапи побудови архітектури системи захисту інформації

В наші дні багато різноманітних компаній вирішують завдання створення архітектури систем інформаційної безпеки, яка відповідала б найкращим світовим аналогам та стандартам в галузі інформаційної безпеки та відповідала б сучасним вимогам захисту інформації за такими параметрами: конфіденційність, цілісність та доступність.

Багато компаній мають проблемами в процесі створення архітектури систем інформаційної безпеки. Дуже часто створення архітектури системи здійснюється досить хаотично; небагато компаній спираються на продуману IT-стратегію чи плани розвитку ІС. Відсутня продумана архітектура системи ІБ, мало хто намагається визначити, наскільки система інформаційної безпеки повна, наскільки вона покриває ризики, надмірна вона або, навпаки, недостатня. Слід також наголосити, що архітектура систем ІБ рідко буває економічно обґрунтованою.

Побудова ефективної архітектури системи ІБ має спиратися на аналіз ризиків, обов’язково включаючи аналіз можливої шкоди, що є основою при виборі засобів захисту, їх економічному обґрунтуванні. Необхідно додати комплекс організаційних заходів та створення системи управління ІБ. І, нарешті, потрібно дотримуватися практично перевірених принципів побудови архітектури системи ІБ, наприклад, принципу багаторівневого захисту.

Таким чином, при побудові нової, або модернізації існуючої архітектури системи ІБ доцільно реалізовувати цілий ряд робіт, що включає обов'язковий етап діагностичного обстеження з оцінкою вразливостей інформаційної системи та загроз, на основі якого провадиться проектування архітектури системи інформаційного захисту та її впровадження (рисунок 2.1).

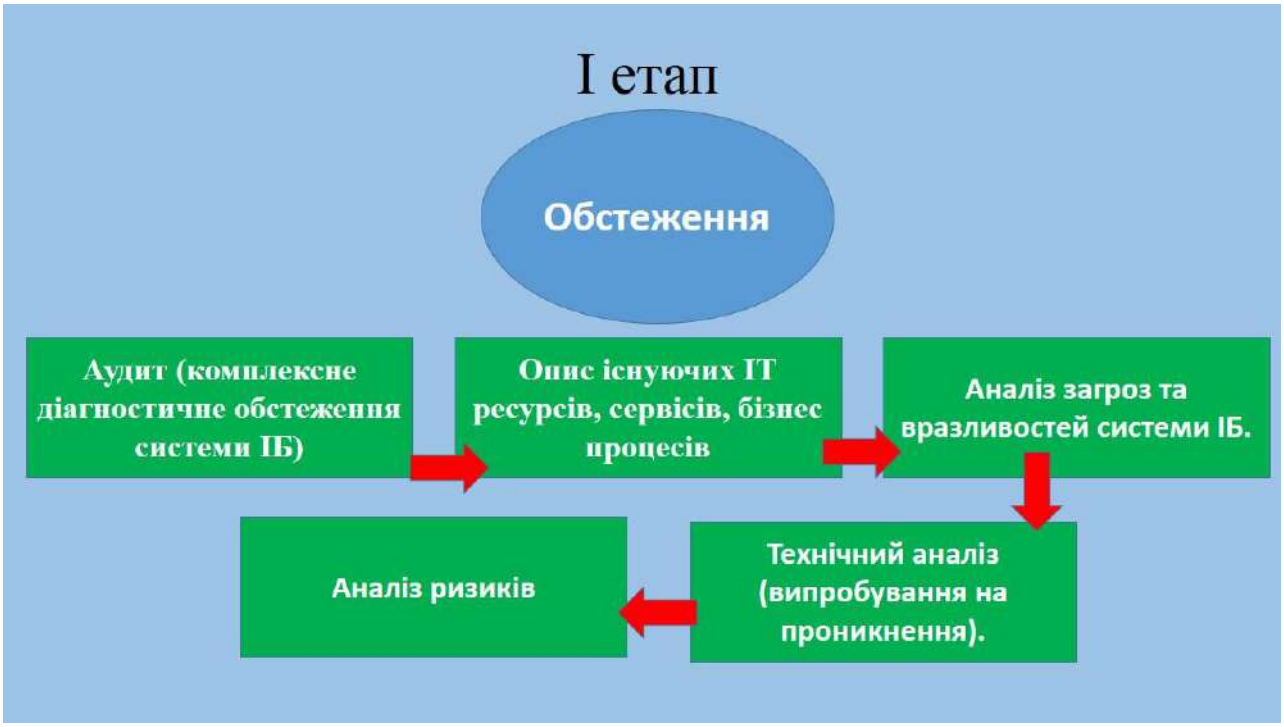


Рисунок 2.1 – І етап побудови архітектури системи ІБ

Для побудови ефективної архітектури системи захисту інформації, вибору та запровадження адекватних технічних засобів захисту має передувати аналіз загроз, вразливостей інформаційної системи та на цій основі робиться аналіз ризиків інформаційної безпеки. Вибір програмно-апаратного забезпечення захисту та проектування архітектури систем ІБ ґрунтується на результатах такого аналізу з урахуванням економічної обгрунтування співвідношення вартісті контрзаходів направлених на зниження ризиків та можливих втрат компанії від інцидентів інформаційної безпеки.

Таким чином, проектування архітектури системи ІБ компанії доцільно починати з повного комплексного діагностування основних бізнес-процесів та чинної інформаційної системи компанії, а також вже існуючих засобів контролю інформаційної безпеки. (рисунок 2.2).

Рисунок 2.2 – II етап побудови архітектури системи ІБ

Побудова архітектури системи ІБ, дотримання балансу між рівнем захисту та інвестиціями компанії в систему ІБ забезпечують цілу низку переваг: інтеграція підсистем дозволяє знизити сукупну вартість системи, підвищити можливість повернення інвестицій при впровадженні, покращує керованість системи ІБ, а отже, можливості відстеження подій, пов'язаних з ІБ.

Після проведення повного тестування спроектованої архітектури системи ІБ можна переходити до її використання (рисунок 2.3).

Рисунок 2.3 – III етап побудови архітектури системи ІБ

Роботи з впровадження архітектури системи містять в собі виконання таких завдань:

- постачання програмних та технічних засобів захисту інформації;
- інсталяцію компонентів програм;
- налаштування всіх компонентів та підсистем;
- проведення попередніх випробувань;
- використання системи управління ІБ;
- навчання користувачів та персоналу компанії;
- введення архітектури системи ІБ в експлуатацію.

Для ефективної подальшої експлуатації системи необхідно забезпечити її підтримку та супровід (це можна робити власними силами компанії або силами фахівців, які спеціально наймаються) (рисунок 2.4).

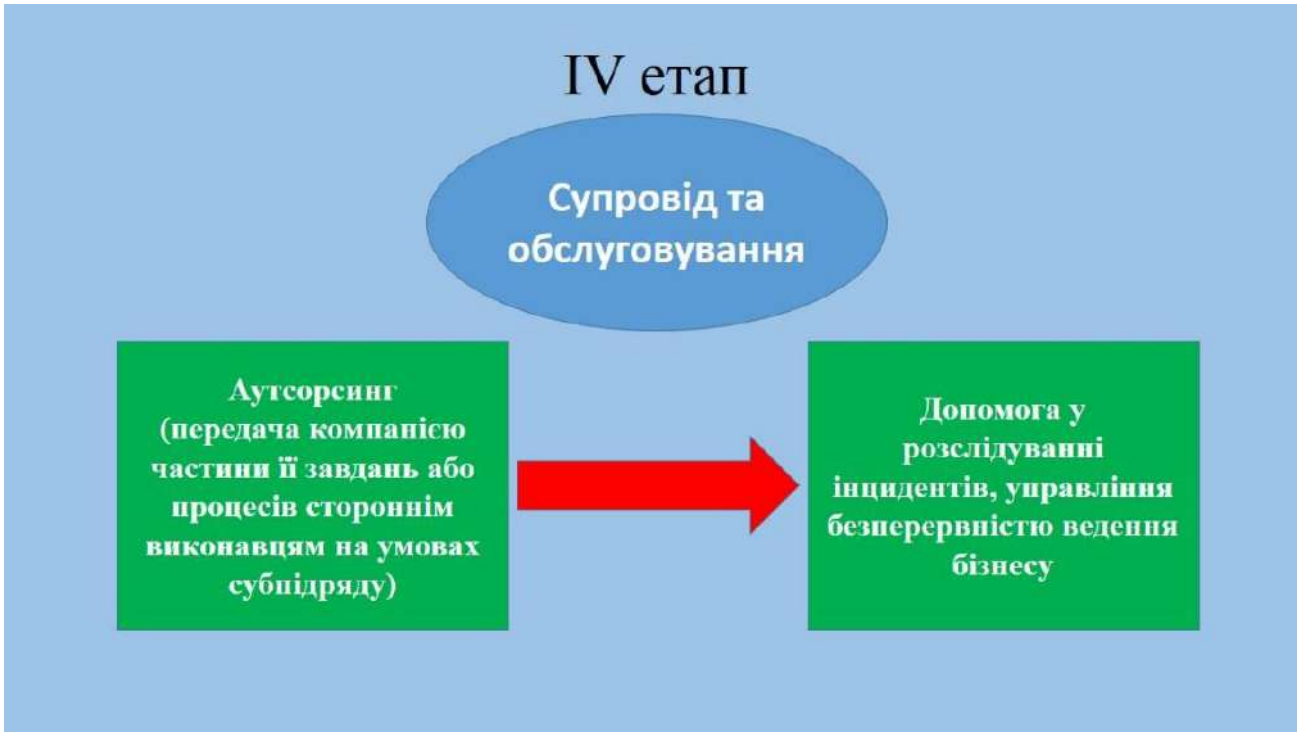


Рисунок 2.4 – IV етап побудови архітектури системи ІБ

2.2 Горизонтальне та вертикальне масштабування архітектури систем захисту інформації. Вибір масштабування для обэкту захисту

Постійне та стрімке зростання потреб бізнесу призводить до збільшення навантаження на засоби захисту. Ось чому виникає необхідність вирішувати питання щодо масштабування ІБ-рішень, які використовуються. Найчастіше застосовуються горизонтальний та вертикальний підходи.

Горизонтальне масштабування передбачає установку систем захисту інформації (наприклад, міжмережевих екранів) однакової продуктивності в один ряд (рисунок 2.5).

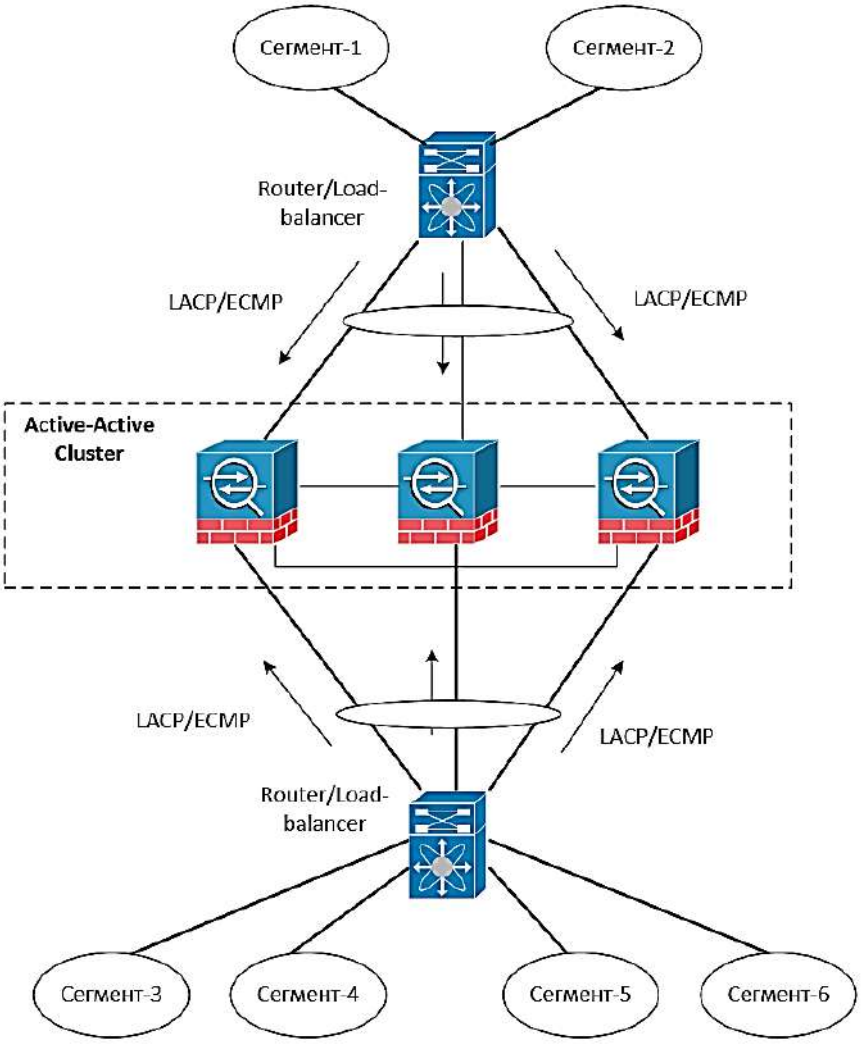


Рисунок 2.5 – Схема горизонтального масштабування СЗІ

Вертикальне масштабування передбачає встановлення СЗІ високої продуктивності (із запасом для збільшення) (рисунок 2.6).

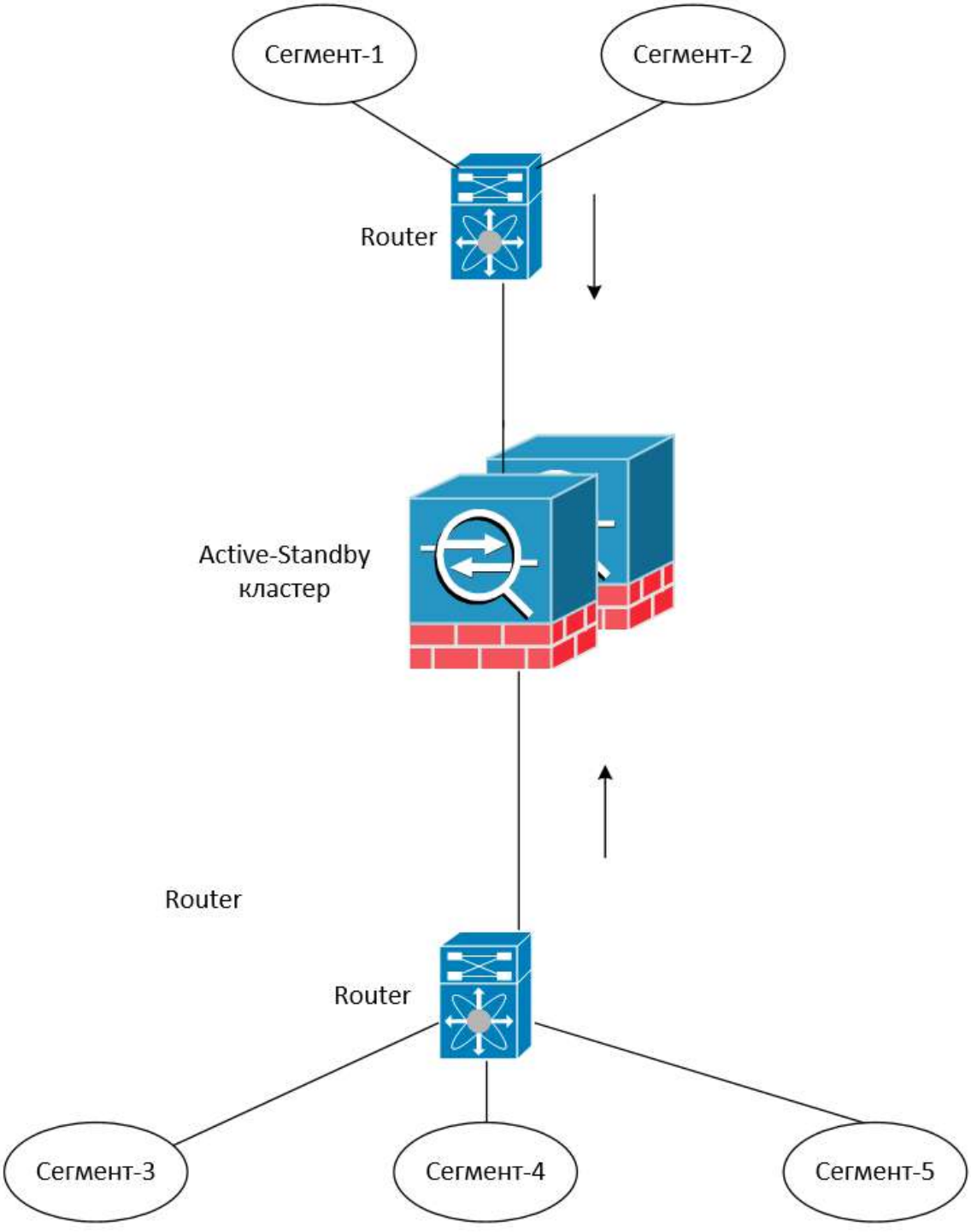


Рисунок 2.6 – Схема вертикального масштабування СЗІ

Обидва цих підходи мають як переваги, так і недоліки (рисунки 2.7 та 2.8).

Рисунок 2.7 – Переваги та недоліки горизонтального масштабування архітектури системи захисту інформації

Рисунок 2.8 – Переваги та недоліки вертикального масштабування архітектури системи захисту інформації

2.3 Методи побудови архітектури системи захисту інформації

Архітектура безпеки інформаційних систем спирається на дві складові: архітектуру ІБ загалом та організаційну структуру підприємства. Але вона має специфічні особливості, які пов'язані з розробленою для організації чи компанії моделлю загроз. У ній враховуються слідуючи ризики:

- ризик вірусних загроз та хакерських атак;
- ризик витоку персональних даних;
- ризик витоку конфіденційної інформації;
- ризик для безпеки національної таємниці;
- ризик порушення роботи всієї системи захисту, або її окремих елементів через технологічні або програмні збої в роботі.

Захисту підлягає інформація, яка зберігається в електронному вигляді та на паперових носіях. Важлива інформація міститься у відеоконференціях та голосових додатках, а також та IP-телефонії. Система повинна враховувати ці ризики та забезпечувати захист від:

- дій інсайдерів;
- ненавмисних помилок користувачів чи системних адміністраторів;
- зовнішніх ризиків.

Слід зазначити, що деякі фахівці вважають, що розробка системи захисту від ризиків інформаційної безпеки має відбуватися окремо від розробки спільної IT-архітектури бізнесу, що дасть можливість вирішувати важливі завдання окремо, роблячи акцент на досягненні конкретних цілей. Неузгодженність цілей безпеки та бізнесу виникає у випадках:

- зацікавленість бізнесу у використанні хмарних технологій, що в кілька разів збільшують ризики втрати або витоків важливої інформації;
- використання проектних та групових методів роботи над важливими рішеннями, що не дає змоги виявити відповідального користувача;
- застосування єдиних каналів комунікацій для кількох груп користувачів;

- активної взаємодії з клієнтами без урахування ІБ-ризиків.

Все вище зазначене виключає можливісті створення єдиного загального периметра безпеки, а рішення, які впроваджуються, суперечать загальному напрямку розвитку бізнесу компанії чи організації. Дуже часто служба інформаційної безпеки забуває, що вона працює для бізнесу, а не всупереч йому.

Недомовленості призводять до:

- перекривання протоколів на мережевому екрані;

- ускладненню доступу до інтернету для окремих співробітників;

- блокування доступу до край важливих для бізнесу сайтів.

Підсумком всього вище згаданого стає те, що підрозділи інформаційної безпеки починають називати business prevention department, тобто такими, чия робота перешкоджає бізнесу, а не сприяють йому. Інколи неможливо змінити організаційну структуру цілого підприємства або бізнес-процеси під систему інформаційного захисту, яку пробують впровадити, а навпаки, саме їм має відповідати ІБ-система.

2.4 Стратегія формування архітектури систем захисту інформації

Створення архітектури систем захисту інформації слід почати з розробки стратегії, яка представляє собою послідовність етапів досягнення цілей і ресурсів, що використовуються. Зараз розглядають три групи ресурсів: людські, фінансові та тимчасові. Всі вони мають бути скоординовані між собою. Тому розробку стратегії не можна доручати окремим департаментам чи відділам, вона має контролюватись на рівні керівництва компанії. Саме адміністрація визначає, що є найбільшим пріоритетом – короткий час створення системи захисту, або зведення до мінімуму кількість ресурсів, що витрачаються.

Головна мета стратегії формування архітектури систем захисту інформації визначає бажані елементи архітектури, які мають забезпечити її надійне та безперебійне функціонування:

- інформація. Вказуються інформаційні активи та види даних, які надаються. Серед них – текстові, відео а також аудіофайли, усна інформація, дані на паперових носіях. У цьому розділі, як правило, визначають ступінь важливості даних, рівень їх існуючого захисту;

- інфраструктура. Цей підрозділ документ має на меті визначити матеріальні об'єкти, які містять інформацію, яка підлягає захисту. Це комп'ютери, матеріальні носії, периферійні пристрої, місця знаходження та зберігання інформації на паперових носіях, наприклад реєстратура в шпиталі, де знаходяться медичні картки пацієнтів, що містять конфіденційну інформацію;

- інформаційні системи. Саме вони містять конфіденційні дані: різноманітні системи та програми, бізнес-додатки, програми, які використовуються для бухгалтерського обліку;

- інформаційна безпека. У розділі описується, які завдання безпеки мають бути вирішені та які засоби, програмні засоби, наприклад, будуть використані в архітектурі системи, планується інсталяція готового програмного засобу захисту, або планується розробка власного засобу;

- служба інформаційної безпеки. Тут детально описується структура підрозділу, який відповідає за підтримання елементів архітектури безпеки інформаційних систем, його завдання та функціональні обов'язки, методи оцінки головних показників ефективності.

Враховуючи все вище зазначене необхідно враховувати напрямки розвитку бізнесу та ринку програмного забезпечення в цілому, передбачати дії регуляторів. Потрібно постійно проводити моніторинг зміни загроз. З точки зору витрат потрібно враховувати той факт, що ринок програмного забезпечення постійно змінюється та оновлюється, і все більшої популярності набуває такий напрямок «програмне забеспечення в якості необхідної послуги». Також потрібно враховувати галузеву специфіку конкретної компанії, передбачуватиі зміни нормативних актів у межах державної доктрини інформаційної безпеки. Вирішення всіх цих питань дасть можливість побудувати саме оптимальну архітектуру захисту ІС та мати можливість знизити загальні витрати.

2.5 Висновки

В розділі представлений детальний аналіз етапів побудови ефективної моделі архітектури системи захисту інформації на ПП «МайстерКомп». Слід зазначити, що при побудові ефективної архітектури системи потрібно обов’язково враховувати результати аналізу ймовірних ризиків, проаналізувати результати можливої шкоди. Все перераховане стало основою при виборі засобів захисту та економічному обґрунтуванні їх вибору та застосування. Таким чином, при побудові нової, або модернізації існуючої архітектури системи ІБ доцільно реалізовувати цілий ряд робіт, поєтапність яких детально описана та проаналізована в розділі.Також детально розписана стратегія вибору архітектури систем інформаційного захисту для ПП «МайстерКомп» та її поетапна побудова. Головна мета цієї стратегії формування архітектури систем захисту інформації щоб усі елементи архітектури забезпечували її надійне та безперебійне функціонування та експлуатацію.

РОЗДІЛ 3. РОЗРОБКА АРХІТЕКТУРИ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ПП «МАЙСТЕРКОМП»

3.1 Загальні відомості про ПП «МайстерКомп»

Об’єктом інформаційної діяльності (ОІД) є інформаційно-комунікаційних система приватного підприємства «МайстерКомп» в місті Хмельницькому. Приватне підприємство знаходиться на вулиці Народної Волі, 1а мікрорайон Ракове. Об’єкт розташований на першому поверсі шестиповерхового будинку. Огородження по периметру відсутнє. Біля об’єкту є майданчик для паркування автомобілів. Ситуаційний план підприємства наведено у додатку Б.

Фізико-технічні характеристики приміщень мають такі властивості:

Приміщення займає площу 65 м^2;

Стіни зовнішні:

- матеріал: залізобетонні; товщина 0,8 м;
- екранування та штукатурка: присутні;
- інші матеріали: з внутрішньої сторони стіни оздоблені під "Євростандарт";

Вікна:

- розмір отвору: 2,0 * 1,5 м;
- тип вікна: склопакет із подвійним потовщеним склом.

Двері:

- розмір отвору: 2,2*1,8м
- тип: одностулкові, металеві двері, замок механічний.

Система вентиляції припливно-витяжна.

Система опалення центральне водяне.

Система електроживлення (освітлення):

- мережа: 220 В/50 Гц;

Система заземлення: присутня.

Предметом діяльності ПП «МайстерКомп» є:

- створення власного комерційно-торгівельного підприємства;
- надання платних послуг населенню по ремонту комп’ютерного обладнання;
- оптова та роздрібна торгівля комп’ютерною технікою та комплектуючими товарами.

Асортимент магазину «МайстерКомп» достатньо різноманітний та має широку номенклатуру, а саме:

- планшети (планшетні комп'ютери);
- монітори;
- моноблоки;
- ноутбуки;
- аксесуари для ноутбуків, планшетів, телефонів тощо;
- процесори;
- відеокарти;
- карти пам'яті;
- жорсткі диски;
- принтери та комплектуючі;
- різноманітні блоки та стабілізатори живлення;
- звукові прилади та акустичні системи;
- інша периферія для комп'ютера;
- канцелярські товари для друку.

3.2 Обґрунтування необхідності створення архітектури системи захисту інформації.

Згідно українського законодавства умови обробки та збереження інформації в системі визначаються власником компанії чи організації. Порядок надання доступу до конфіденційної інформації, перелік користувачів, їх права та

обов’язки стосовно цієї інформації можуть визначатися лише власником інформації. Згідно законодавства уся відповідальність за забезпечення захисту та збереження інформації в системі покладається на власника системи.

Згідно українсого законодавства об’єкти, на яких відбувається обробка інформації технічними засобами, або оприлюднюється інформація з обмеженим доступом, що не становить державної таємниці, обов’язково підлягають категоріюванню.

В залежності від строків проведення категоріювання, його можна поділити на такі категорії:

- первинне (здійснюється вперше);

- чергове (здійснюється згідно попереднього плану (раз на 5 років);

- позачергове (проводиться раніше запланованого часу).

Категоріювання проводиться на підприємстві з метою визначення необхідного рівня захисту інформації, яка обробляється технічними засобами, або озвучується на об’єкті. Відповідальність за своєчасність, об’єктивність проведення категоріювання та правильність встановлення категорії об’єкта, покладається на керівника установи-власника об’єкта. Об’єктами категоріювання на приватному підприємстві є всі об’єкти інформаційної діяльності.

Категоріювання завжди здійснюється за такими ознаками:

- ступінь обмеження доступу до інформації, що обробляється технічними засобами, або оголошується на об’єкті інформаційної діяльності;

- об’єктам охорони, на яких обробляється інформація за допомогою технічних засобів, або оголошується інформація з обмеженим доступом, що не містить державної таємниці, має обов’язково бути встановлена IV категорія. Потрібно зазначити, що за рішенням користувача інформації, або власника, об’єкту може бути встановлена III категорія.

Інформаційна система об’єкту захисту має бути простотою і керованою тому, що лише в такій системі можна об’єктивно перевірити рівень взаємодії різних компонентів і провести централізоване адміністрування об’єкту.

Забезпечення загальної підтримки заходів безпеки носить нетехнічний

характер. Рекомендується запланувати комплекс заходів, який був би спрямований на стимулювання персоналу до постійного теоретичного та практичного навчання.

На підставі проведеного аудиту власником об’єкту захисту було прийняте рішення про побудову архітектури системи захисту інформації на ПП «МайстерКомп» та був виданий відповідний наказ.

3.3 Обстеження об’єкту захисту.

Під час проведеного обстеження була перевірена обчислювана система, фізичне середовище, середовище користувачів та проаналізована інформація, яка обробляється на об’єкті.

3.3.1 Обстеження обчислювальної системи

Обчислювальна система є локальною та має з’єднання з інтернетом. Пристрої, що розташовані в межах ОІД, з’єднані між собою Локальна мережа була створена з метою забезпечення внутрішніх потреб підприємства.

Інформаційно-телекомунікаційна система об’єкту захисту представляє собою мережу з окремо підключеним сервером та використовується лише один комутатор. Структурна схема мережі показана на рисунку 3.1.

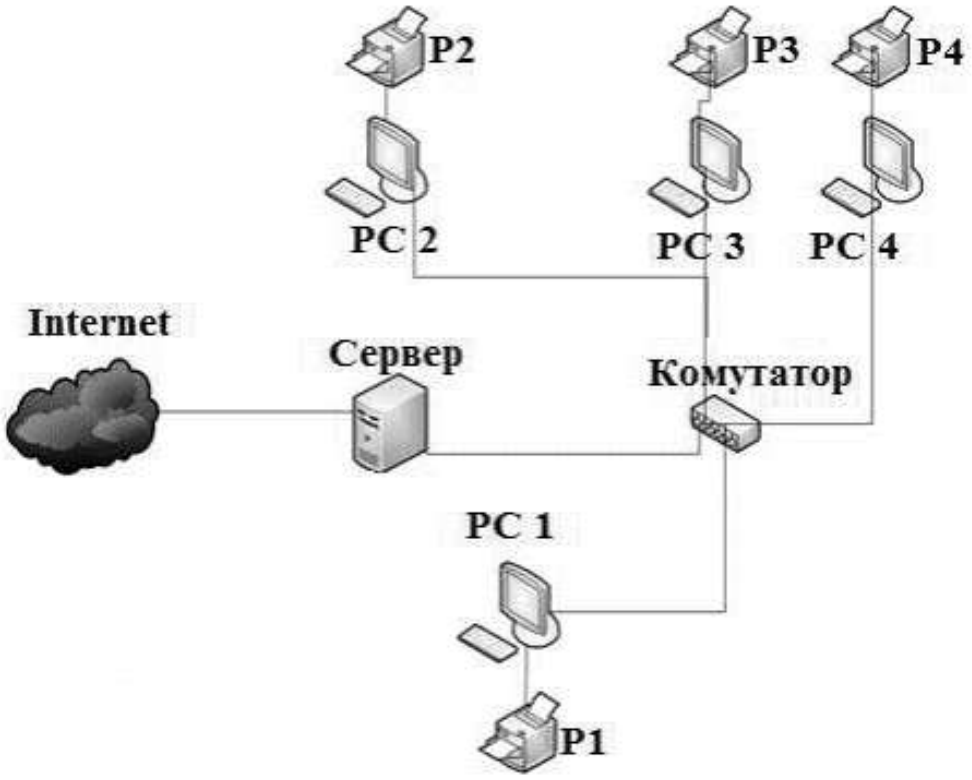


Рисунок 3.1 – Структурна схема мережі ПП «МайстерКомп»

Інвентаризаційні данні елементів системи а також додаткових технічних засобів представлені в таблиці 3.1 та таблиці 3.2

Таблиця 3.1 – Інвентаризаційна відомість додаткових технічних засобів ПП «МайстерКомп»

№	Назва	Модель	Серійний номер	Кількість	Відповідальний
1	Пасивні ІЧ датчики руху	DSC LC-100PI	YT85E90 OI74UY1 IU967R0 EDR9FG RFVD6G SKIUY75	6	Системний адміністратор
2	Датчики на розбиття скла	PATROL-USR	7S5F8T0 9H5J4Q6 7K6G0F1 Q9W8E71	4	Системний адміністратор
3	Знищувач документів	Шредер Agent 007 S	AS4W5Y7	1	Системний адміністратор

Таблиця 3.2 – Інвентаризаційна відомість апаратного забезпечення ІТС ПП «МайстерКомп»

№ Відповідно до плану	Назва	Характеристика	Ім'я в ІТС	Серійний номер	Кіл-сть	Відповідальна особа
1	Системний блок ASUS PN40-BB013M	Процесор Intel Celeron N4000/ ОЗУ 8GB/ Відеокарта Intel HD Graphics 600/ Материнська плата ASUS Mini PC PN40	PC 1	KS105UB	4	Системний адміністратор
			PC 2	VCX888		
			PC 3	DE74L98		
			PC 4	YTR759E		
2	Wi-Fi роутер (комутатор) D-Link DSR-250N	Інтерфейс : 1 x WAN Мбит/с 8 x LAN Мбит/с 1 порт USB 2.0 Консоль RJ-45/ Частота роботи: 2.4 ГГц / Скорость WiFi: 150 Мбіт/с	R 1	PI0D89S	1	Системний адміністратор
3	Сервер	Dell PowerEdge R720XD/ 2 x XEON	S 1	IF7E2Q1	1	Системний адміністратор
4	Монітор	21,5" LG 22M38A-B	PC 1-4	OL473PD PIH976 FUOT54 OLPT96	4	Системний адміністратор
5	Клавіатура	Sven Comfort 3535	PC 1-4	OL473PD PIH976 FUOT54 OLPT96	4	Системний адміністратор
6	Миша	ASUS ROG Sica USB Black	PC 1-4	BI4588C GTR74L WER987 KOTGE5	4	Системний адміністратор
7	Принтер	Canon PIXMA G1411	PC 1-4	AW963K XQ96L5 ERT012	3	Системний адміністратор
8	Камери відеоспостереження	Green Vision GV-047-GHDG-COA20-20 1080P	Cam 1	P8MH43Z	2	Системний адміністратор
			Cam 2			

На робочих комп'ютерах персоналу об'єкту встановлені автоматизовані робочі місця (АРМ) з різним набором програмного забезпечення в залежності від посадових обов'язків.

Інформація з обмеженим доступом в ІТС обробляється за допомогою наступних програм:

- АРМ «Керівник» (встановлене на РС 2 директора);

- АРМ «Адміністратор» (встановлене на РС 1 системного адміністратора);

- АРМ «Консультант» (встановлене на РС 3 та РС 4 консультантів спеціалістів).

Більш детальна інформація про програмне забезпечення, що встановлене в системі, наведена в таблиці 3.3.

Таблиця 3.3 – Інвентаризаційна відомість програмного забезпечення ПП «МайстерКомп»

№	Найменування	Комп'ютер на якому встановлено	Тип ліцензії
1	ОС Windows 10 Максимальна x64 (64-біт)	PC 1, PC 2, PC 3, PC 4	Відсутня
2	Microsoft Office 2013 14.0.6023.1000		Відсутня
3	Google Chrome 96.0.4664.110	PC 1, PC 2, PC 3, PC 4	Відкрита
4	Total Commander 8.01		Відкрита
5	Avast Pro 19.5.4444		Відкрита
6	WinRAR 4.20		Відкрита
7	Adobe Reader 2021.007.20099		Відкрита
8	1С підприємство 8.3	PC 2, PC 3, PC 4	Комерційна
9	CCleaner 5.31.6105	PC 1, PC 2	Відкрита
10	Winamp 2.0	PC 1, PC 2, PC 3, PC 4	Відкрита
11	Adobe Photoshop Elements 132.0.9	PC 2	Відкрита

3.3.2 Інформаційне середовище ОІД

Також було виконано аналіз інформаційного середовища ПП «МайстерКомп» та проведено детальний аналіз та класифікацію існуючої інформації відповідно до загальних вимог.

Вся інформація приватного підприємства, яка циркулює на об’єкті захисту, вказана нижче в таблиці Г.1 (Додаток Г)

Рівні конфіденційності інформації представлені в таблиці 3.4

Таблиця 3.4 – Рівні конфіденційності

Рівні конфіденційності інформації	
К1	рівень конфіденційності інформації, при якому можна знехтувати збитками у разі розкриття інформації особам, що не мають допуску до неї, або при якому інформація не є конфіденційною;
К2	рівень конфіденційності інформації, при якому компанія зазнає незначних збитків у разі розкриття інформації особам, що не мають допуску до неї;
К3	рівень конфіденційності інформації, при якому організація зазнає відчутних збитків у разі розкриття інформації особам, що не мають допуску до неї;
К4	рівень конфіденційності інформації, що може призвести до значних матеріальних втрат у разі розкриття інформації особам, що не мають допуску до неї
К5	критичний рівень конфіденційності інформації, що може призвести до краху компанії у разі втрати конфіденційності інформації.

Рівні цілісності інформації представлені в таблиці 3.5:

Таблиця 3.5 – Рівні цілісності

Рівні цілісності інформації	
Ц1	рівень цілісності інформації, при якому можна знехтувати втратою цілісності інформації;
Ц2	рівень цілісності інформації, при якому компанія зазнає незначних збитків у разі втрати цілісності інформації;
Ц3	рівень цілісності інформації, при якому організація зазнає відчутних збитків у разі втрати цілісності інформації;
Ц4	рівень цілісності інформації, що може призвести до значних матеріальних
Ц5	втрат у разі втрати цілісності інформації;

Рівні доступності інформації представлені в таблиці 3.6:

Таблиця 3.6 – Рівні доступності

Рівні доступності інформації	
Д1	рівень доступності інформації, при якому можна знехтувати втратою доступності інформації;
Д2	рівень доступності інформації, при якому компанія зазнає незначних збитків у разі втрати доступності інформації;
Д3	рівень доступності інформації, при якому організація зазнає відчутних збитків у разі втрати доступності інформації;
Д4	рівень доступності інформації, що може призвести до значних матеріальних втрат у разі втрати доступності інформації;
Д5	критичний рівень доступності інформації, що може призвести до краху компанії у разі втрати доступності інформації.

Були встановлені сновні інформаційні потоки на ПП «МайстерКомп»:

1) облік внутрішніх та статутних документів компанії – облік внутрішніх документів завжди завантажується на сервер, де кожен працівник в будь який час може ознайомитись з ними, та одночасно ці документи друкується директором, щоб додатково зберігати необхідну інформацію на паперових носіях в спеціально відведеній для них папці;

2) облік інформації про надання послуг, тарифи, контактна інформація магазину та сервісного центру – інформація, про надання послуг населенню з ремонту техніки, тарифи на послуги та ціни на товари, контактна інформація співробітників магазину та майстрів використовується, як правило споживачами та консультантами, щоб надати інформація клієнтам в будь який час, оскільки інформація знаходиться у вільному доступі;

3) облік інформації про робітників приватного підприємства – інформація про штат персоналу використовується винятково директором в разі зміни працівників, або у випадку виникнення надзвичайних ситуацій;

4) облік і реєстрація вхідних та вихідних документів організації – статутні документи підприємства (правила діяльності організації) можуть використовується клієнтами, працівниками, особами, що можуть здійснювати перевірку; облік і реєстрація вхідних та вихідних документів організації (дані про наявність продукції, дані про продаж та закупівлі продукції) – використовується консультантами, в разі потреби інформації для клієнтів, а також директором з метою контролю рівня витрат та суми прибутку;

5) облік усіх трудових договорів робітників – трудові договори робітників використовується виключно директором, в них вносяться зміни в разі звільнення або прийняття нового працівника, переведення працівника на іншу посаду;

6) облік відомостей про фінанси підприємства та відомостей про постачальників – відомості про фінанси підприємства – використовується бухгалтером при складанні фінансової звітності та директором з метою контролю фінансових операцій; відомості про постачальників – використовується консультантом для замовлення продукції; бухгалтером для оформлення

кошторису та директором для контролю та аналізу постачальників продукції;

7) облік відомостей про реалізацію продукції – відомості про реалізовану продукцію – використовується бухгалтером при складанні звітних документів та директором для контролю та аналізу рівня продажів;

8) облік договорів, контрактів, однією із сторін яких виступає приватне підприємство – зміст та характер договорів, контрактів, однією із сторін яких виступає ПП – використовується консультантом для надання споживачам додаткової інформації про товар та використовується директором при складанні та підписанні цих договорів з партнерами;

9) облік відомостей щодо обладнання приміщення підприємства охоронної сигналізації і місце її встановлення – відомості які стосуються охоронного обладнання приміщення використовується переважно системним адміністратором для постійного контролю за його станом, а також використовується директором в випадках закупівлі нового, або оновленні існуючого обладнання;

10) облік відомості щодо наданої гарантії – відомості щодо гарантії на продукцію та послуги – використовуються системним адміністратором для контролю за станом обладнання (обміном, поверненням, ремонтом за гарантією тощо), та використовується директором облік копій товарних чеків.

11) копії товарних чеків – використовується консультантом для відновлення вже наданого товарного чеку клієнтом та використовується директором з метою систематичного контролю.

Усі встановлені основні інформаційні потоки на ПП «МайстерКомп» були систематизовані в єдину схему, яка міститься в Додатку А та на рисунку 3.2

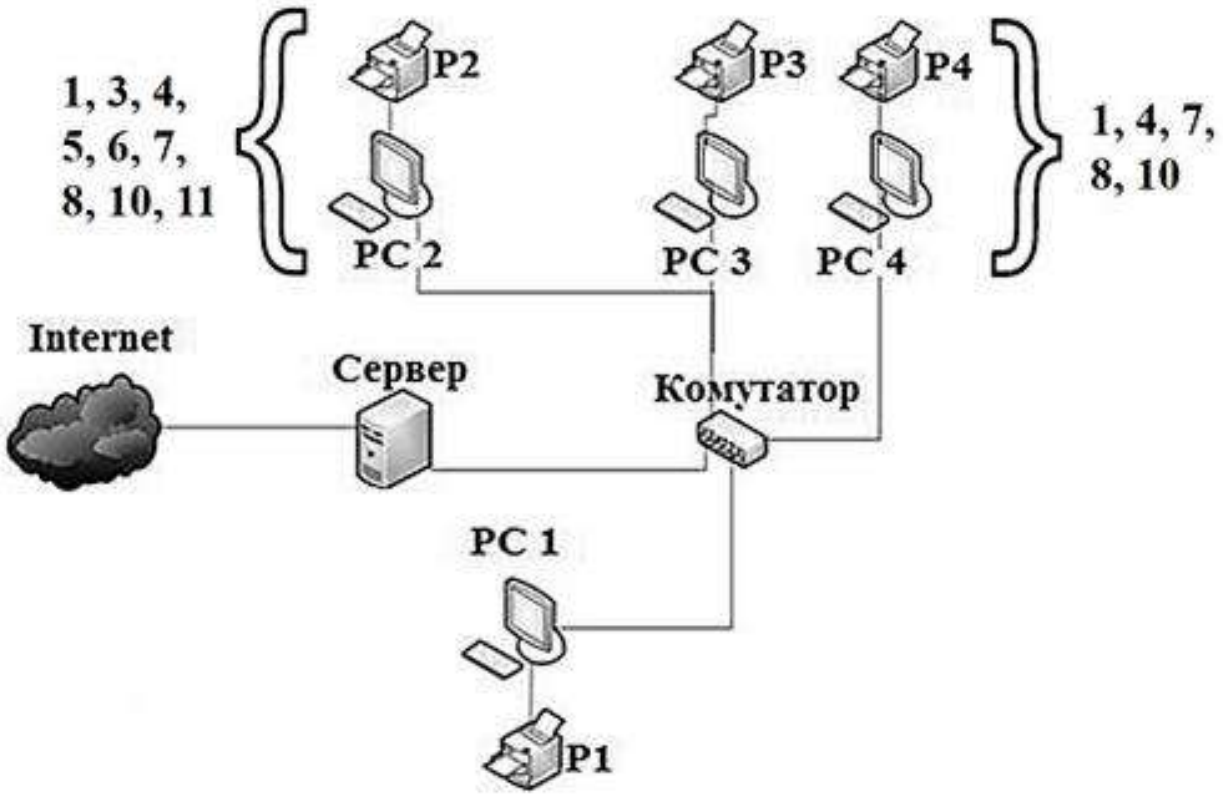


Рисунок 3.2 – Схема інформаційних потоків на ПП «МайстерКомп»

Дії стосовно інформації на ПП наведені в матриці доступу в табл.3.7

- С – створення;
- Ч – читання;
- З – зберігання;
- К – копіювання;
- М – модифікація;
- Д – друк;
- В – видалення, або знищення.

Таблиця 3.7 – Матриця доступу до інформації

Користувачі	Інформація
Системний адміністратор	1, 4, 6- Ч, З, М, Д 2- Ч 11-Ч, Л, М, Д, В
Консультанти	1, 2, 4, 8, 10- Ч, С, З, В
Бухгалтер	1-Ч 2-Ч, С, З,К, Д, В 3- Ч, С, З, Д, В 6- Ч,С, З, К, М, Д, В 9,10- Ч, С, Д, М,З

Доступ до ресурсів ПП «МайстерКомп» надається згідно з посадовими обов'язками та наказами директора, але явних заборон на використання інформаційних ресурсів не виявлено.

3.3.3 Обстеження середовища користувачів

Штат працівників ПП «МайстерКомп»:

1. Директор;
2. Системний адміністратор (1 чол.);
3. Консультант-спеціаліст (2 чол.);
4. Прибиральниця (1 чол.);
5. Бухгалтер (1 чол.).

Серед персоналу основними користувачами мережі є – директор, системний адміністратор, та консультанти-спеціалісти. Бухгалтер працює на одному комп'ютері з директором. Нижче в таблиці 3.8 наведений список суб'єкти доступу до інформації на ПП «МайстерКомп».

Таблиця 3.8 – Суб'єкти доступу до інформації ПП «МайстерКомп»

№	Прізвище, ім'я, по батькові	Умовне позначення пристрою	Посада	Виконуюча роль в системі
1	Коваль Віктор Іванович	PC 1	Системний адміністратор	адміністратор
2	Дорош Дмитро Павлович	PC 2	Директор	Користувач
3	Бойко Олена Павлівна	PC 2	Бухгалтер	Користувач
4	Мариняк Віталій Сергійович	PC 3	Консультант-спеціаліст	Користувач

3.4 Аналіз та оцінка інформаційних ризиків

Аналіз ризиків інформаційної безпеки розроблений на основі нормативного документу з урахуванням усіх встановлених особливостей діяльності приватного підприємства «МайстерКомп».

Наданий аналіз включає в себе:

- модель порушника;
- модель загроз;
- ідентифікація наслідків реалізації загроз;
- оцінку ризиків та ймовірності їх появи.

3.4.1 Модель порушника

Важливою складовою частиною успішного аналізу ризиків та визначення вимог складу засобів захисту і характеристик архітектури системи захисту інформації є підготовка моделі ймовірного порушника.

Модель порушника використовується з метою оцінювання рівня ймовірних загроз, виявлення слабких місць в архітектурі системи інформаційного захисту, прогнозування можливих атак, а також дій по відновленню архітектури системи після проведеної атаки.

При розробці моделі порушника необхідно:

- визначити, до якої категорії осіб він може належати;

- виявити цілі і мотиви дій порушника;

- врахувати можливі обмеження на дії порушника;

- визначити рівень кваліфікації та обізнаності щодо роботи з комп'ютерними системами;

- визначити можливості дій за часом;

- проаналізувати можливості дій за місцем.

Категорії осіб, до якої може належати порушник:

- внутрішні порушники (ним може бути особа з числа авторизованих користувачів інформаційної системи ПП, які мають право доступу до інформації з обмеженим доступом);

- технічний персонал, що обслуговує приміщення та особи, яким не передбачено доступ до кондиційної інформації, але які мають доступ до приміщень, де розміщено ІТС і потенційно можуть отримати доступ до інформації;

- зовнішні порушники (особи, які знаходяться за межами ІТС, але мають можливість фізичного підключення до каналів зв'язку ними можуть бути відвідувачі, конкуренти, найманці тощо.

Визначення категорій ймовірних порушників узагальнено та наведено в таблицях 3.9 – 3.15 за різними специфікаціями. У колонці «Рівень загроз» наведених таблиць вказано рейтингову оцінку загроз порушника. Рівень загрози характеризується наступними рівнями:

1. незначний (низький);

2. нижчий за середній;

3. середній;

4. вищий за середній;

5. високий (неприпустимо високий).

Таблиця 3.9 – Категорії порушників

Умовне позначення	Категорія	Рівень загрози
П1	Внутрішні порушники (персонал)	5
П2	Технічний персонал, що обслуговує будівлю та приміщення	2
П3	Зовнішні порушники	4

Таблиця 3.10 – Специфікація моделі за мотивами дій порушника

Умовне позначення	Мотив порушення	Рівень загрози
М1	Ненавмисне порушення (безвідповідальність)	3
М2	Навмисне порушення (наявність умислу)	5

Таблиця 3.11 – Специфікація моделі порушника за можливостю використання засобів інформаційної системи

Умовне позначення	Характеристика можливостей дій порушника	Рівень загрози
З1	Має фізичний доступ до компонентів системи, але не є авторизованим користувачем	1
З2	Має можливість запуску програм, що реалізують функції обробки інформації	3
З3	Має можливість керувати функціями інформаційної системи конфігурує програмне забезпечення.	5

Таблиця 3.12 – Специфікація моделі порушника за рівнем знань щодо КС та систем захисту

Умовне позначення	Рівень знань та обізнаності щодо КС та систем захисту	Рівень загрози
К1	Не володіє знаннями про роботу КС, не має навичок користування засобами системи	1
К2	Має навички роботи на ПК на рівні користувача	2
К3	Володіє базовими знаннями щодо роботи програмного забеспечення та операційної системи і практичними навичками роботи	4
К4	Володіє знаннями щодо функціонування засобів захисту і знає недоліки їх роботи	5

Таблиця 3.13 – Специфікація моделі порушника за часом дії

Умовне позначення	Характеристика можливостей дій порушника за часом	Рівень загрози
Ч1	Під час бездіяльності засобів системи (під час планових перерв у роботі, неробочий час).	4
Ч2	Під час функціонування інформаційної системи.	5
Ч3	Під час перерв у роботі з метою обслуговування та ремонту.	3

Таблиця 3.14 – Специфікація моделі порушника за місцем дії

Умовне позначення	Характеристика місця дії порушника	Рівень загрози
Д1	Усередині приміщення ПП, але без доступу до технічних засобів інформаційної системи	1
Д2	З робочих місць користувачів та персоналу, а також змісця розміщення обладнання для обробки інформація, яка підлягає захисту.	5
Д3	Без доступу до приміщень, в тому числі з зовнішніх каналів зв'язку, з можливістю застосування	2

Таблиця 3.15 – Профілі можливостей порушників на ПП «МайстерКомп»

Позначення	Категорія	Характер дій порушника					Рівень загроз
		Мотив	Можливості	Знання	Місце	Час	
П1	Внутрішні порушники	М1, М2	З2, З3	К3, К4	Д2	Ч1, Ч2, Ч3	4
П2	Технічний персонал, що обслуговує будівлю	М2	З1	К1, К2	Д1, Д2	Ч3	2
П3	Зовнішні порушники	М2	З1	К1, К2	Д3	Ч2	3

3.4.2 Модель загроз

Загроза інформації є ключовим поняттям інформаційної безпеки. Існую багато різноманітних класифікації загроз. Для аналізу інформаційної системи та

побудови моделі загроз на ПП «МайстерКомп» найкраще підійде класифікація за результатами їх впливу на інформацію. Оскільки, основними властивостями інформації, яка потребує захисту, є: конфіденційність, цілісність, доступність і спостереженість, то з цієї точки зору при проектуванні архітектури системи інформаційного захисту розрізняються наступні види загроз для інформації:

1) порушення конфіденційності:

- загрози при керуванні потоками інформації;
- загрози існування прихованих потоків інформації;
- порушення конфіденційності при обміні інформацією через незахищене середовище;

2) порушення цілісності (логічної чи фізичної):

- загрози при керуванні потоками інформації;
- неможливість повернення захищеного об'єкта у початковий стан;
- порушення цілісності інформації при обміні через незахищене середовище;

3) порушення доступності або відмовлення в обслуговуванні:

- порушення при керуванні послугами користувача;
- порушення стійкості до відмов;
- порушення при терміновій заміні;
- порушення при відновленні роботи після атак;

4) порушення спостереженості чи керованості:

- порушення при реєстрації небажаних дій;
- порушення при ідентифікації та автентифікації;

5) несанкціоноване використання інформаційних ресурсів.

Оскільки досить складно отримати об’єктивні дані про вирогідність вищезгаданих загроз, їх ймовірність було визначено за методом, який аналізує статистичні данні.

Шкала оцінки загроз:

К1 – визначає ступінь доступності до об’єкту (таблиця 3.16):

Таблиця 3.16 – Ступень доступності до обєкту

1	в іншій країні (для технічних засобів);
	немає доступу до об’єкта (для суб'єктів загроз).
2	в тій самій країні (для технічних засобів);
	віддалений доступ до об’єкта (для суб'єктів загроз).
3	поблизу будівлі, де знаходиться об’єкт захисту, або в тій самій будівлі (для технічниз засобів);
	фізичний несанкціонований доступ до об’єкта інформації, або несанкціоноване проникнення в приміщення (для суб'єктів загроз).
4	в тому ж приміщенні (для технічних засобів);
	доступ у приміщення, де знаходиться об’єкт (для суб'єктів загроз).
5	сам об’єкт (для технічних засобів)
	фізичний дозволенний доступ до об’єкта (для суб'єктів загроз).

К2 – наявність необхідних умов для здійснення загрози, включає в себе ступінь кваліфікації та ступінь його бажання виконавця загрози:

1. Виконавець постраждає при реалізації загрози; він не має відповідних можливостей, оскільки технічні засоби та програмне забезпечення постійно оновлюється, кваліфіковано обслуговуються та постачається надійним виробником;

2. Виконавець загрози особисто сам не постраждає не постраждає, але її виконання не принесе йому користі; у нього недостатня кваліфікація для здійснення загрози; програмне забезпечення та технічні засоби на об’єкті оновлюється не регулярно;

3. Виконавцю буде вигідна реалізація загрози; віна принесе йому необхідні навички та уміння; програмне забезпечення та технічні засоби можуть бути вразливі для деяких атак;

4. Виконавцю буде дуже вигідна реалізація запланованої загрози; він в достатньо кваліфікований для здійснення загрози; на об’єкті охорони спостерігається відсутність оновлень програмного забезпечення або використовуються застарілі технічні засоби, використовується техніка сумнівної якості;

5. Реалізація загрози є метою суб'єкта; виконавець має високу кваліфікацію для здійснення загрози (наприклад, він за фахом є спеціалістом); на об’єкті охорони використовується стара або зламані технічні засоби; встановлене піратське програмне забезпечення, тощо.

К3 – критичність наслідків:

1. Об’єкт охорони нічого не втратить після реалізації загрози, або наслідки навпаки принесуть позитивний результат;
2. Наслідки загрози можна ігнорувати;
3. Наслідки будуть відчутні, але результати не будуть критичними;
4. Наслідки можуть призвести до відчутних проблем, усунення наслідків буде вимагати значних матеріальних коштів та потрібно буде багато часу;
5. Наслідки будуть критині, що стане причиною банкрутства, закриття компанії, втрати бізнес партнерів та клієнтів.

Загальне значення К для загроз можна розрахувати за формулою:

$$\text{К загальне} = \frac{\text{К1}*\text{К2}*\text{К3}}{125},$$

Результати зведені в таблиці Д.1 (Додаток Д) та на рисунку 3.3

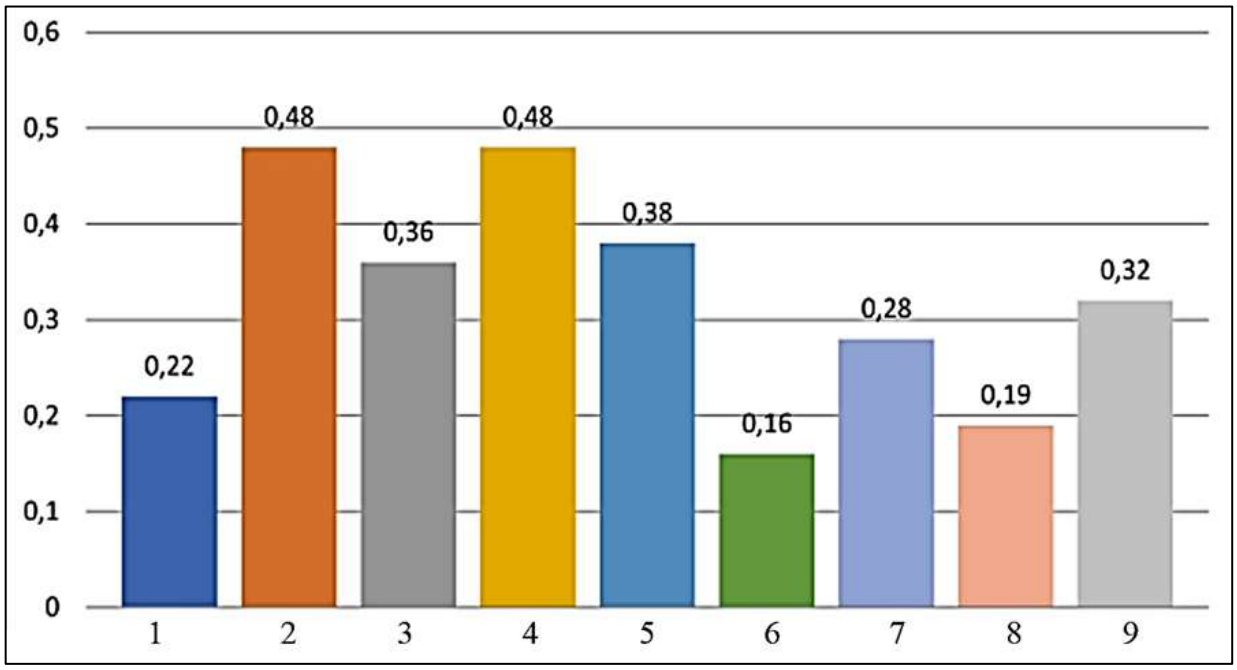


Рисунок 3.3 – Результати аналізу загроз та вразливостей інформації в системі захисту ПП «МайстерКомп»

Таким чином, найбільш вірогідними загрозами для інформаційної системи можна вважати:

- несанкціонований доступ сторонніх осіб до інформації через бездротову мережу (злам WiFi);

- несанкціонований перехват інформації, яка зберігається на паперових або електронних носіях;

- несанкціоноване проникнення в приміщення;

- планування та реалізація атак на ОС;

- соціальна інженерія (шантаж, підкуп тощо з метою наживи);

- несанкціоноване копіювання конфіденційної інформації;

- ненавмисне пошкодження носіїв інформації чи інформації в цілому, яка зберігається на цих носіях.

Якщо всі вищевказані загрози будуть використовувати відповідні вразливі місця архітектури системи інформаційної безпеки і призведуть до небезпечної ситуації для інформаційної безпеки, то як наслідок, підприємство може повністю або частково втратити необхідну інформації, або вона буде пошкодження, або

сфальсифікована. Ці інциденти можуть вплинути на ресурси ПП і призвести до сутєвих фінансових втрат.

3.5 Вибір моделі архітектури для ПП «МайстерКомп»

З огляду на все вище зазначене та враховуючи усі результати обстежень та характеристики існуючої інформаційної системи та вимог до властивостей інформації, було обрано для впровадження і тестування стандартний функціональний профіль архітектури системи захисту інформації для ПП «МАйстерКомп», а саме такий профіль:

3.КЦ.1 = {КД-2 , КВ-1, ЦД-1, ЦВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НВ-1}

Перелік послуг та заходів, що входять в обраний профіль архітектури системи інформаційної безпеки зроблений відповідно до чиного законодавства та відповідних вимог:

- КД-2 Базова довірча конфіденційність, відноситься до критеріїв такогозахисту конфіденційності інформації;
- КВ-1 Мінімальна конфіденційність при обміні інформацією потрібно відности до такого критерію, як конфіденційность;
- ЦД-1 Мінімальна довірча цілісність, яка відноситься до критерія цілісності;
- ЦВ-1 Мінімальна цілісність інформації, при будь якому обміні, необхідно відности до критерії цілісності;
- НР-2 Захищений журнал, який є надзвичайно необхідним і важливим, потрібно відности до критерії спостереженості такого пункту, як реєстрація;
- НИ-2 Персональна ідентифікація і автентифікація користувачів;
- НК-1 Однонаправлений достовірний канал передачі інформації, відноситься до критерії спостереженості ;
- НЦ-1 це комплекс усіх засобів захисту інформації за контролем її цілісності, потрібно відности до критерія спостереженності;

- НВ-1 і останне це автентифікація вузла, що має бути віднесенно до спостереженості.

3.6 Висновки

У розділі було виконано обстеження інформаційної діяльності об’єкту захисту відповідно до етапів побудови моделі архітектури системи хахисту. А саме було ретельно розглянуто обчислювальну систему ПП «Майстер Комп», а також фізичне середовище, інформаційне середовище, та середовище постійних користувачів. Детально проаналізовано та оцінено усі можливі ризики для існуючої інформації на ПП «МайстерКомп» і виділено найбільш значущі та ймовірні загрози. Згідно з проведеним аудитом, запропоновані до впровадження та тестування на ПП моделі архітектури системи захисту інформації та політики інформаційної безпеки від можливого несанкціонованого доступу, а також для забезпечення ефективної роботи всіх складових частин інформаційної системи. Також були запропонованінові підходи, які стосуються управління персоналом на підприємстві, були надані конкретні рекомендації по поступовому вдосконаленню організаційної структури підприємства.

РОЗДІЛ 4. ТЕСТУВАННЯ ТА ДОСЛІДЖЕННЯ НАДІЙНОСТІ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ ПП «МАЙСТЕРКОМП»

4.1 Розробка політики безпеки інформації на ПП «МайстерКомп»

З огляду на наявність на підприємстві інформації з обмеженою відповідальністю, яка обробляється та зберігається в операційні системі, а також фінансових на матеріальних ресурсів, прийняте рішення про обрання принципу розробки політики безпеки, при якому необхідне впровадження архітектури системи інформаційного захисту, досягнення необхідного рівня захищеності конфіденційної інформації з використанням мінімальних матеріальних.

Усі заходи, які представлені в політиці безпеки, мають на меті зниження можливих ризиків реалізації потенційних загрози через вразливості інформаційної системи, спираючись на зроблений детальний аналіз ризиків представлених в таблиці Б.1 (додаток Б).

Першочерговим завданням є необхідність проведення заходів для зниження ризиків по парі загроза вразливість, які, згідно аналізу, мають критичний рівень ризику для системи 0,48. До цієї категорії потрібно віднести несанкціонований перехоплення інформації, які знаходяться на паперових або електронних носіях та здійснення атак на ОС.

Для зниження рівня ризику несанкціонованого перехвату інформації яка зберігаються на паперових або електронних носіях розробляється політика антивірусного захисту та обмеження використання мережі Інтернет користувачами.

Для здійснення політики антивірусного захисту необхідно:

- обрати серед доступних найефективніше антивірусне програмне забеспечення. Пропонується ESET NOD32 Platinum Edition. Це програмне забеспечення розроблене словацькою компанією ESET. Остання версія випущена

в жовтні минулого року. Програма представляє собою комплексну систему для захисту ПК від будь-яких видів вірусів. Також продукт добре зарекомендував себе в боротьбі з рекламним ПЗ, спам-софтом, фішинговими сайтами. У програмі використовується інноваційна технологія для виявлення комп'ютерних вірусів. Пакет Platinum Edition містить ліцензію на використання ESET NOD32 протягом двох років. ПЗ сумісне з операційними системами – Windows, OS X, Linux, Android. Дозволяє одночасно захистити 4 пристрої; має інтуїтивно зрозуміле налаштування та цілодобову технічну підтримку;

- антивірусне ПЗ необхідно негайно встановити на всіх робочих станціях ПП «МайстерКомп» та постійно оновлюватись;

- слідкувати за терміном дії ліцензії антивірусного програмного забеспечення та продовжувати її вчасно.

Розроблені слідуючі рекомендації для уникнення проблем з зараженням вірусів, які єобов'язковими до виконання всіма працівниками ПП «МайстерКомп»:

- всім працівникам перед початком роботи з системою захисту, необхідно перевірити, що антивірусне програмне забеспечення увімкнено;

- заборонено відкривайте сайти соціальних мереж на робочому місці або інші невідомі сайти, які не пов'язані з виконанням посадових обов'язків;

- завжди перевіряти електронну пошту та ніколи не відкривайте файли з прикріпленнями до електронного листа від невідомого або сумнівного відправника. Слід видаляйте такі листі;

- завжди при підключенні невідомого носія інформації на робочому місці необхідно проводити сканування його на наявність вірусів;

- заборонити встановлюйте додаткове програмне забеспечення з невідомого або підозрілого носія інформації шляхом відключення антивіруса.

Для здійснення політики контролю за використання мережі Інтернет користувачами системи захисту приватного підприємства необхідно:

- встановити постійний контроль за використанням мережі Інтернет користувачами системи з метою зменшення випадків зараження системи

вірусами;

- забов’язати системного адміністратора здійснювати постійний контроль за використанням мережі Інтернет всіма працівниками на всіх робочих місцях, які є складовою частиною системи захисту;

- запровадити ведення журналу фіксації данних: IP-адреси джерел, дату, час та місце. Фіксувати ідентифікатор користувача. Зроблені записи про використання Інтернету зберігати протягом 180 діб;

- проводити блокування доступу до Інтернет-сайтів, які вважаються ненадійними, які містять азартні ігри, сайти соціальних мереж, та чатів, сайти, що містять порнографію та насильство. Зробити відповідний перелік цих сайтів, який має регулярно переглядатися, змінюватися та доповнюватися;

- внести необхідні зміни в діючі посадові інструкції певні зміни, відповідно до яких працівники виконували би заходи,щодо захисту інфрормації;

- необхідно запровадити використання цифрового підпису для прийому та передачі інформації;

- необхідно запровадити шифрування конфіденційної інформації інформаційній базі ПП «МайстерКомп»;

- застосувати індивідуальний електронний ключ для кожного співробітника, який має доступ до системи захисту;

- для запобігання несанкціонованого проникнення в приміщення слід встановити більш функціональну систему відеоспостереження.

Схема заходів системи безпеки представлена в додатоку А.

4.2 Аналіз інформаційних ризиків після впровадження політики безпеки

Повторний аналіз розробляється відповідно до методик та шкал, зазначених в таблицях розділу 2.4 – Аналіз та оцінка інформаційних ризиків.

Метою повторного аналізу є перевірка ефективності впровадження нової архітектури системи інформаційної безпеки.

На діаграмі зазначені пари загроза, які піддавалися повторному аналізу. (рисунок 4.1)

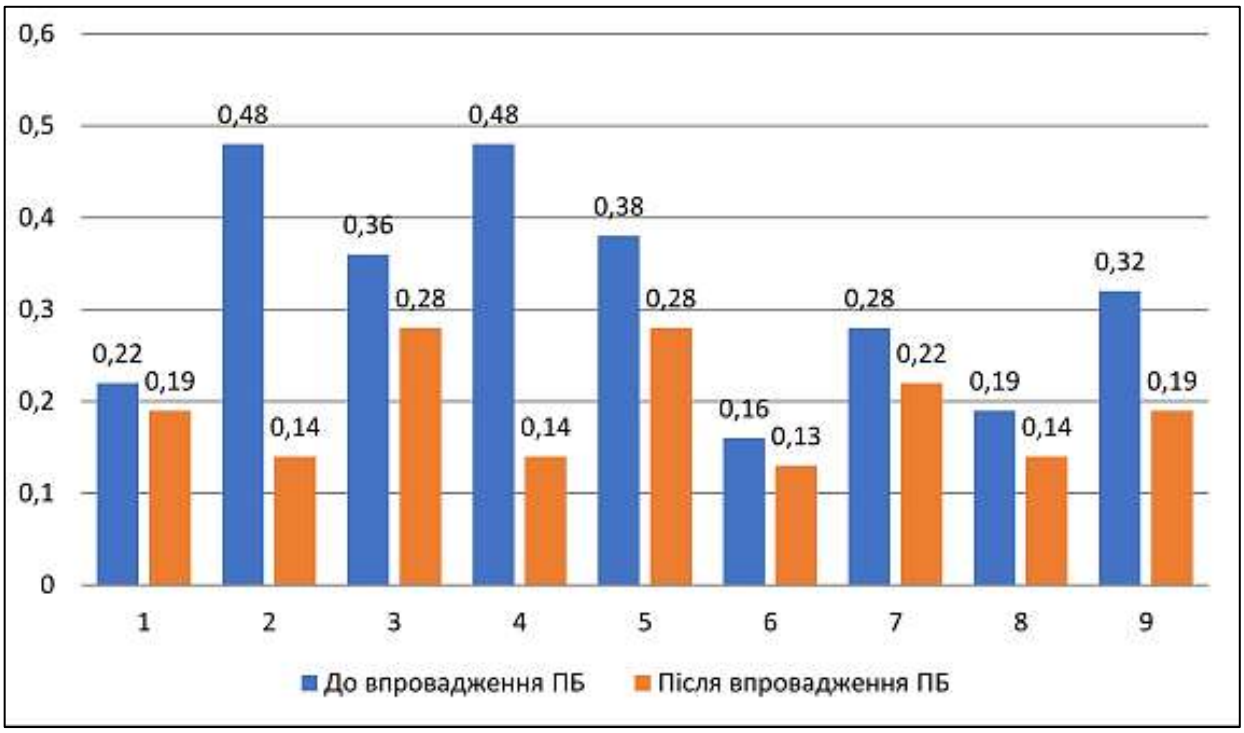


Рис 4.1 – Рівень ризику після впровадження архітектури системи інформаційного захисту на ПП «МайстерКомп»

В таблиці Г.1 (Додаток Г) – Рівень ризику після впровадження архітектури безпеки.

Аналіз ризиків після впровадження розробленої архітектури системи захисту інформації вказує на їх ефективність. Адже, рівень ризику, що розрахований за кожною парою загроза, став меншим

4.3 Висновки

У розділі було виконано повтерне обстеження інформаційної діяльності ПП «МайстерКомп», з метою перевірити та переконатися в коректному функціонувані запропонованої моделі архітектури системи захисту інформації,

яка знаходиться і оперується на об’єкті. Повторно були оцінені ризики інформації у відповідності до виділених раніше найбільш ймовірних загроз. Згідно з проведеним повторним аудитом, усі запропоновані рішення дають непоганий результат. Запропонована адміністрації до впровадження політика інформаційної безпеки від несанкціонованого доступу, показала гарні результати по забезпеченню ефективної роботи всіх складових частин системи, впровадженні заходи по управлінню персоналом дали свої результати. А саме, повторний аналіз ймовірних ризиків, після впровадження запропонованих заходів безпеки показав на зниження рівня ризиків на систему в цілому. Отже можна зробити висновок, що розроблена, впровадженна і протестована модель архітектури системи захисту інформації на конкретному об’єкті показала свою ефективність і надійність.

ВИСНОВКИ

Об’єктом розробки моделі архітектури системи захисту інформації в данній роботі є інформаційно-телекомунікаційна система приватного підприємства «МайстерКомп».

У першому розділі роботи був зроблений детальний аналіз законодавчих актів та нормативних документів України, які стосуються захисту інформації та визначена актуальність цієї проблеми для приватних підприємств. Також розглянуті питання принципів та етапів побудови архітектури системи захисту інформації, представлена їх детальна класифікація. Проаналізовані переваги та недоліки існуючих моделей архітектур систем захисту інформації.

У спеціальні частині роботи розглянуті питання, пов'язані з розробкою архітектури системи інформаційного захисту на ПП «МайстерКомп». Під час виконання роботи було проведено аудит інформаційної безпеки підприємства, зроблене категорування інформації, яка обробляється у інформаційно-телекомунікаційній системі ПП, виявлено можливі канали витоку інформації, наведено характеристику компонентів системи. Також в розділі розроблені моделі загроз та ймовірного порушника безпеки інформації. Також сформовані основні положення політики безпеки інформації для створення моделі архітектури системи захисту інформації. Зроблений аналіз моделі архітектури інформаційної безпеки вказує на зниження рівня ризиків в системі через виявлені канали, що свідчить про ефективність та надіність запропонованого рішення. Усі складові системи захисту ефекктивно взаємодіять та функціонують між собою.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАНЬ

1. Г.Ф. Конахович, Захист інформації в телекомунікаційних системах: Навчальний посібник.(лист МОНУ №1.4/18 – Г – 183 від 02.06.2009р.). – К.: НАУ,2009. – 380с.

2. Етапи створення комплексної системи захисту інформації [Електронний ресурс]: Режим доступу: https://infopedia.su/1xa505.html: (дата звернення: 19.04.2022) – Назва з екрана.

3. Що таке комплексна система захисту інформації (КСЗІ) [Електронний ресурс]: Режим доступу: https://zahyst-ua.com/korisna-informaciya/shho-take-kompleksna-sistema-zahistu-informacii-kszi/: (дата звернення: 19.04. 2022) – Назва з екрана.

4. Етапи побудови СУІБ) [Електронний ресурс]: Режим доступу: https://zahyst-ua.com/etapi-pobudovi-suib/: (дата звернення: 30.04.2022). – Назва з екрана.

5. Лужецький В. А. Основи інформаційної безпеки. Навчальний посібник [рекомендований МОН] / Лужецький В. А., Войтович О. П., Кожухівський В. Д. – Вінниця ВНТУ, 2013. – 246 с.

6. Гребенніков В. В. Комплексні системи захисту інформації: проектування, впровадження, супровід /В. В. Гребенніков/ Litres, 2019. – 613 с.

7. Хорошко В. О. Проєктування комплексних систем захисту інформації: підручник / В. О. Хорошко, І. М. Павлов, Ю. Я. Бобало, В. Б. Дудикевич, І. Р. Опірський, Л. Т. Пархуць/ Львів : Видавництво Львівської політехніки, 2020. – 320 с.

8. Богуш В.М. Основи кіберпростору, кібербезпеки та кіберзахисту: Навч.посіб. /В.М. Богуш, В.В. Богуш, В.Д. Бровко, В.П. Настрадін – К. : Ліра – К, 2020. – 554 с.

9. Конспект лекцій з дисципліни «Архітектура та проектування програмного забезпечення/ Укл. В. В. Завгородній, К. М. Ялова. – Кам’янське: Д2019. – 144с.

10. Архітектура систем захисту інформації [Електронний ресурс]: Режим доступу:https://wiki.donntu.edu.ua/view/Архітектура_систем_захисту_інформації дата звернення: 30.04.2022). – Назва з екрана.

11. Задірака В.К. Сучасні методи розв'язання задач інформаційної безпеки. Вісник НАН України. 2014. № 5. С. 65–69

12. Захист інформації в комп'ютерних системах та мережах : навч. посіб. / С.Г.Семенов, А.О.Подорожняк, О.І.Баленко, С.Ю.Гавриленко – Х.: НТУ «ХПІ», 2014. – 251 с.

13. Архітектура системи безпеки інформації [Електронний ресурс]: Режим доступу: https://helpiks.org/7-19544.html (дата звернення: 02.05.2022). – Назва з екрана.

14. Гордейчик С.В. Политика информационной безопасности предприятия // Экономический лабиринт [Электронный ресурс]. – 2001. - №09(38). – Режим доступа: http://www.economer.khv.ru/content/n038/45it: (дата звернення: 08.05.2022). – Назва з екрана.

15. Інформаційна безпека: організаційно-правові основи: Навчальний посібник/ Борис Кормич. – К.: Кондор, 2005. – 382 с.

16. Інформаційні системи і технології у фінансових установах А.В.Олійник, В.М.Шацька – Навчальний посібник – Львів: "Новий Світ – 2000", 2006 – 436 с.

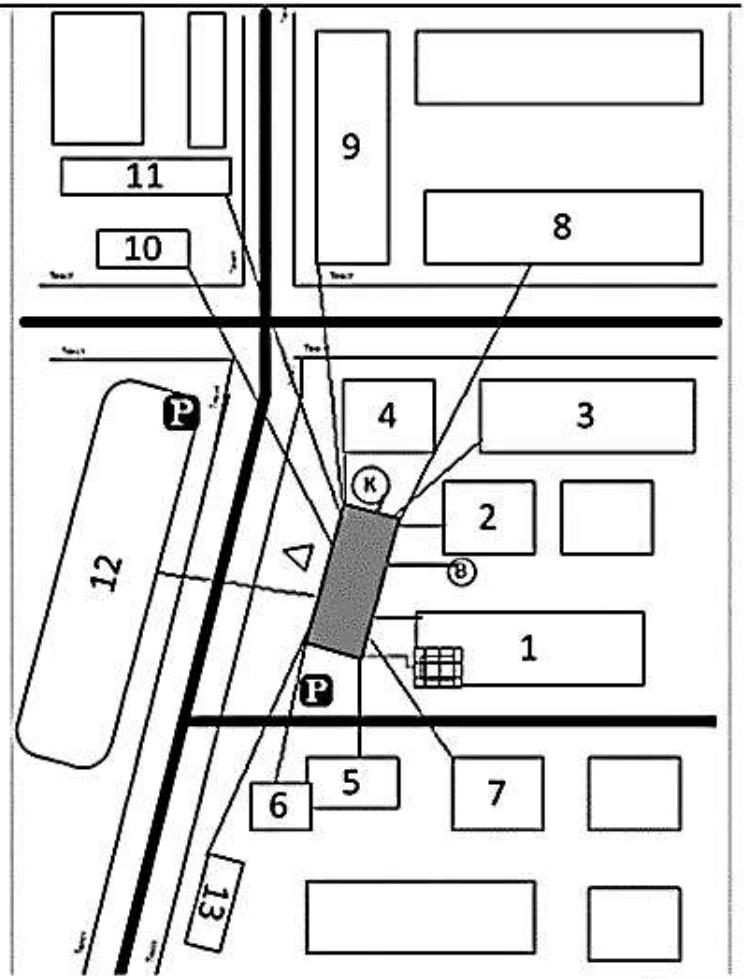
17. Алена Ярутич. Захист інформації від витоку технічними каналами//Наука онлайн: Міжнародний електронний науковий журнал – 2019. - №1. - https://nauka-online.com/ua/publications/natsionalnaya-bezopasnost/2019/1/zahist-informatsiyi-vid-vitoku-tehnichnimi-kanalami/: (дата звернення: 12.05.2022). – Назва з екрана.

18. Технічні канали витоку інформації. Порядок створення комплексів технічного захисту інформації. Навчальний посібник / Іванченко С.О., Гавриленко О.В., Липський О.А., Шевцов А.С. – К.: ІСЗЗІ НТУУ «КПІ», 2016. – 104 с.

ДОДАТОК А

(обов’язковий)

Копія графічної частини



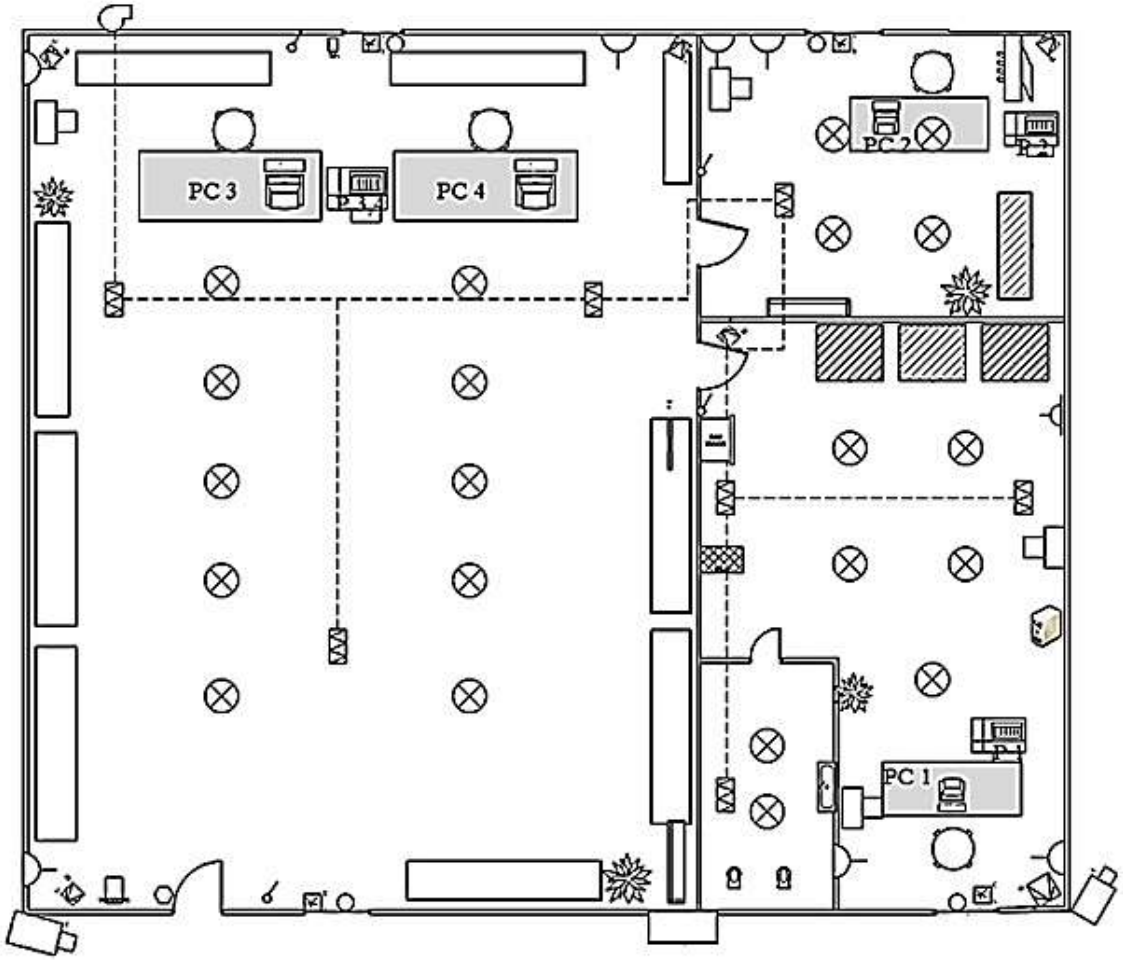
Умовні позначки

	Пішохідна дорога
	Дорога
P	Місце для паркування
	Вхід у будівлю
К	Люк міської системи каналізації

В	Люк міської системи водопостачання
	Трансформаторна підстанція

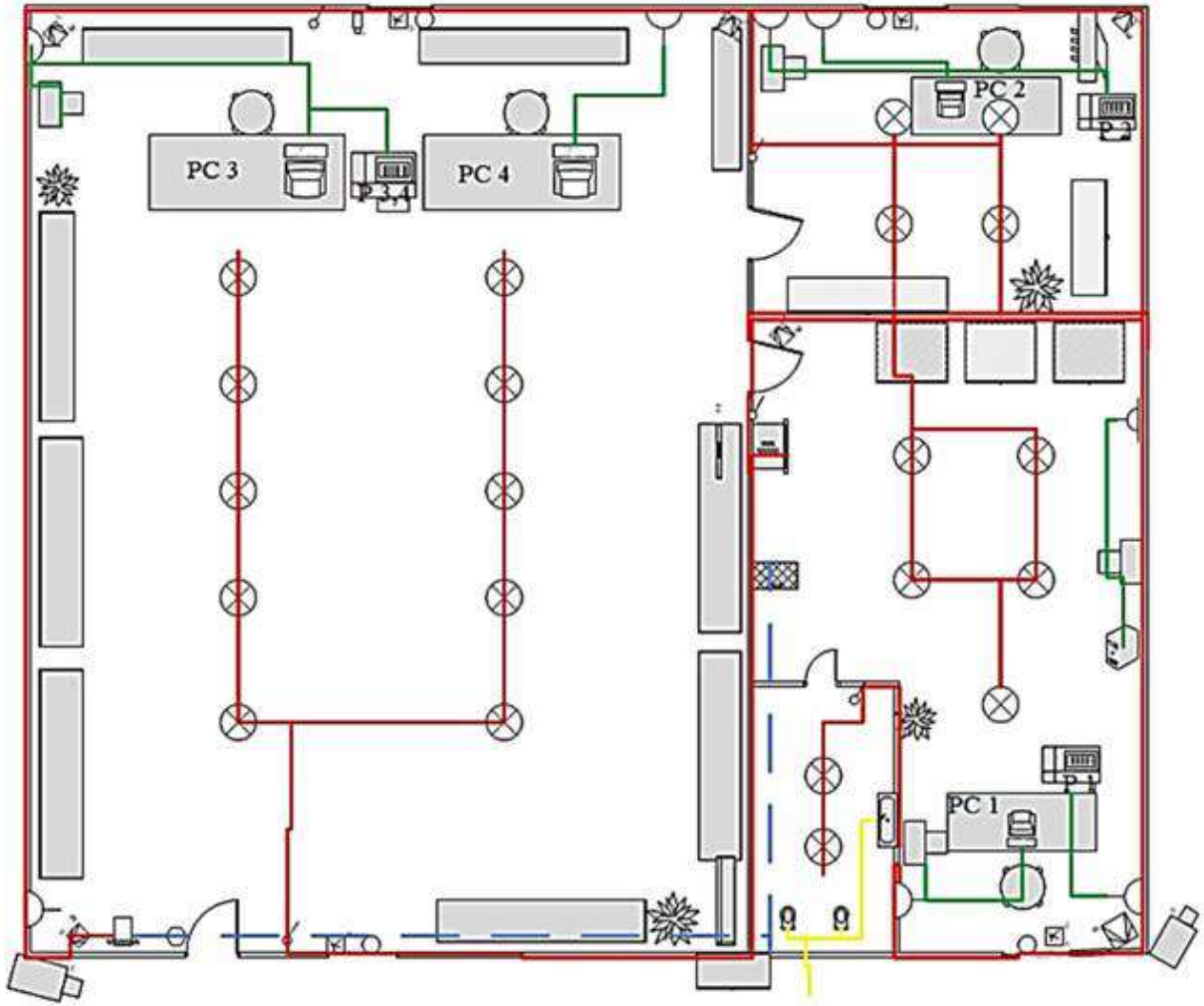
Зм.	Аркуш	№ докум.	Підпис	Дата	КРКБ.101173.18.01.05 Е8		
Розробив		Костовський О.			Генеральний план приватного підприємства «МайстерКомп»	Літ	Аркуш	Аркушів
Перевірив		Чешун В. М.				Н	1	3
Н.контр.		Мостовий С. В.				КБ-18-1		
Затверд.		Кльоц Ю. П.						

КРКБ.101173.18.01.05 Е8

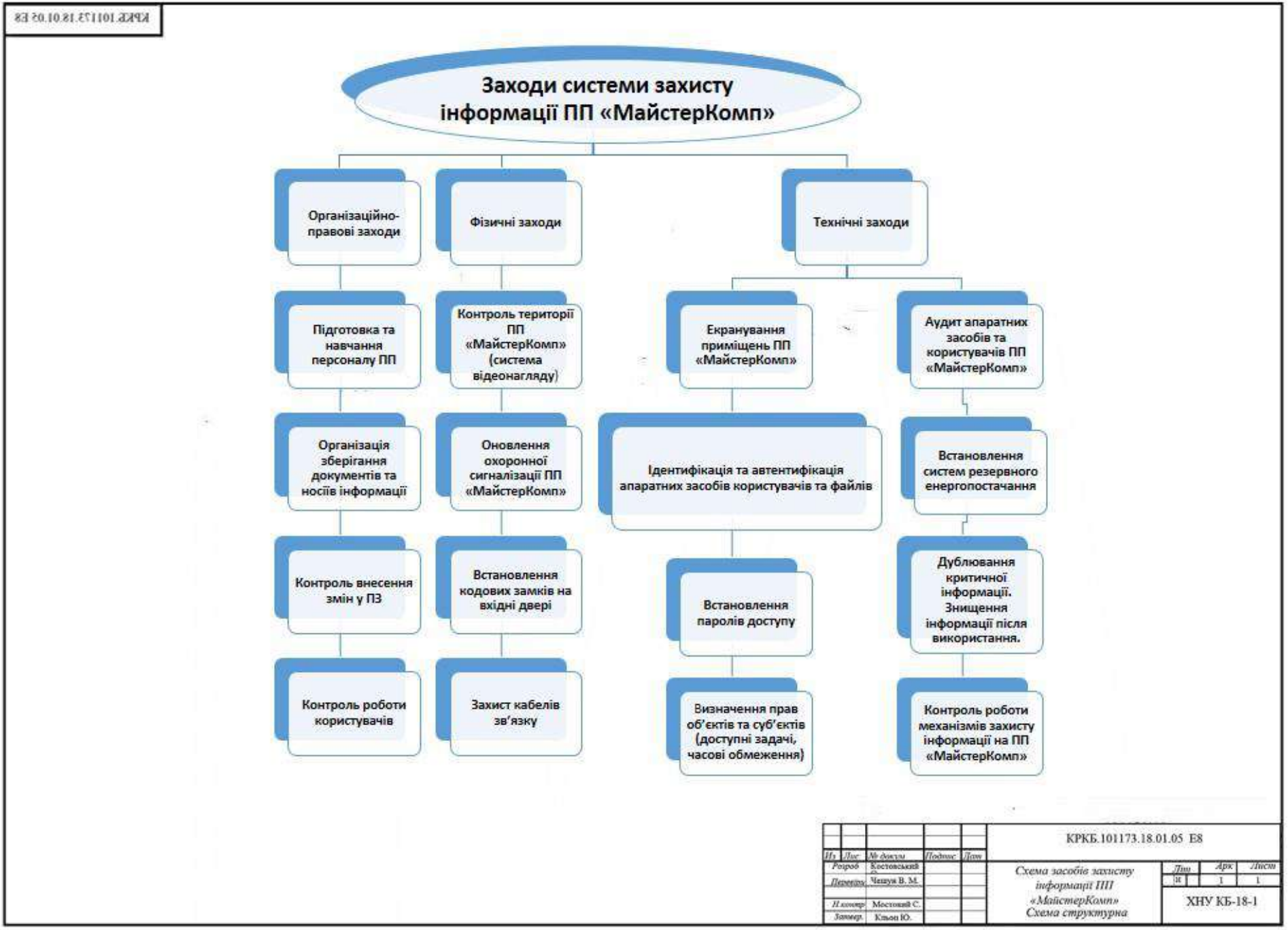


Зм.	Аркуш	№ докум.	Підпис	Дата	КРКБ.101173.18.01.05 Е8		
Розробив		Костовський О.			Генеральний план приватного підприємства «МайстерКомп»	Літ	Аркуш	Аркушів
Перевірив		Чешун В. М.				Н	2	3
Н.контр.		Мостовий С. В.				КБ-18-1		
Затверд.		Кльоц Ю. П.						

КРКБ.101173.18.01.05 Е8



Зм.	Аркуш	№ докум.	Підпис	Дата	КРКБ.101173.18.01.05 Е8		
Розробив		Костовський О.			Генеральний план приватного підприємства «МайстерКомп»	Літ.	Аркуш. 3 / Аркушів 3
Перевірив		Чешун В. М.				Н	
Н.контр.		Мостовий С. В.			КБ-18-1		
Затверд.		Кльоц Ю. П.					


Заходи системи захисту інформації ПП «МайстерКомп»
Організаційно-правові заходи
Фізичні заходи
Технічні заходи
Підготовка та навчання персоналу ПП
Організація зберігання документів та носіїв інформації
Контроль внесення змін у ПЗ
Контроль роботи користувачів
Контроль території ПП «МайстерКомп» (система відеонагляду)
Оновлення охоронної сигналізації ПП «МайстерКомп»
Встановлення кодових замків на вхідні двері
Захист кабелів зв'язку
Екранування приміщень ПП «МайстерКомп»
Ідентифікація та автентифікація апаратних засобів користувачів та файлів
Встановлення паролів доступу
Визначення прав об'єктів та суб'єктів (доступні задачі, часові обмеження)
Аудит апаратних засобів та користувачів ПП «МайстерКомп»
Встановлення систем резервного енергопостачання
Дублювання критичної інформації. Знищення інформації після використання.
Контроль роботи механізмів захисту інформації на ПП «МайстерКомп»
КРКБ.101173.18.01.05 Е8
Схема засобів захисту інформації ПП «МайстерКомп» Схема структурна
ХНУ КБ-18-1

ДОДАТОК Б

Таблиця Б.1- Інформація на ПП «МайстерКомп» та її рівні конфіденційності, цілісності та доступності.

Інформація	Режим доступу	Правовий режим	Особи які мають доступ	Рівень конфіденційності	Рівень цілісності	Рівень доступності
1	2	3	4	5	6	7
Облік внутрішніх документів (накази,службові записи, інструкції ітощо)	З обмеженим доступом	Конфіденційна	Директор	К2	Ц4	Д4
Інформація про надання послуг,тарифи,контактна інформація магазину	Відкрита як для працівників,так і для клієнтів		Директор, консультанти та спеціалісти	К1	Ц4	Д3
Інформація про робітників (зберігається на сервері та в кабінеті у директора на паперовому носії)	З обмеженим доступом	Конфіденційна	Директор, бухгалтер	К4	Ц3	Д3
Статутні документи підприємства (зберігається на сервері та в кабінеті у директора на паперовому носії)	Відкрита для працівників, клієнтів та перебуваючих		Всі працівники	К1	Ц4	Д3
Облік і реєстрація вхідних та вихідних документів організації (зберігається на сервері та в кабінеті у директора на паперовому носії)	З обмеженим доступом	Конфіденційна	Директор	К4	Ц3	Д5

Продовження таблиці Б.1

1	2	3	4	5	6	7
Трудові договори робітників (зберігається на сервері та в кабінеті у директора на паперовому носії)	Відкрита для працівників		Всі працівники	К4	Ц4	Д4
Відомості про фінанси підприємства (зберігається на сервері та в кабінеті у директора на паперовому носії)	З обмеженим доступом	Комерційна	Директор, бухгалтер	К4	Ц4	Д5
Відомості про постачальників (зберігається а сервері та в кабінеті у директора на паперовому носії)	З обмеженим доступом	Комерційна	Директор, Консультант-спеціаліст, бухгалтер	К4	Ц3	Д4
Відомості про реалізацію продукції (зберігається на сервері та в кабінеті у директора на паперовому носії)	З обмеженим доступом	Комерційна	Директор, бухгалтер	К3	Ц3	Д3
Зміст та характер договорів, контрактів, однією із сторін яких виступає підприємство (зберігається на сервері та в кабінеті у директора на паперовому носії)	З обмеженим доступом	Комерційна	Директор, Консультант-спеціаліст	К2	Ц4	Д5

Кінець таблиці Б.1

1	2	3	4	5	6	7
Відомості щодо наданої гарантії (зберігається на сервері та в кабінеті у директора на паперовому носії)	З обмеженим доступом	Комерційна	Системний адміністратор, директор, консультант-спеціаліст	К3	Ц3	Д4
Копії товарних чеків (зберігається в кабінеті у директора паперовому носії)	З обмеженим доступом	Комерційна	Директор, Консультант-спеціаліст	К2	Ц3	Д3

ДОДАТОК В

Таблиця В.1 Результати аналізу загроз та вразливостей інформації в інформаційні системі ПП «МайстерКомп».

№	Загрози	Вразливості системи, що призведуть до реалізації загроз	Джерело	К1	К2	К3	$К_{загальне}$
1	2	3	4	5	6	7	8
1	Несанкціонований доступ до інформації через Wi-Fi	- нерегулярна зміна паролів на Wi-Fi.	Зовнішнє	3	3	3	0,22
2	Несанкціонований заволодіння інформації на паперових або електронних носіях	- неналежне зберігання документів та пристроїв з інформацією підприємства.	Внутрішнє	3	5	4	0,48
3	Проникнення зловмисника в приміщення	- неефективна система охорони; - недостатній контроль за приміщенням	Зовнішнє	3	3	5	0,36
4	Здійснення атак на ОС	- відсутність або неефективність антивірусного ПЗ; - наявність незахищеного з'єднання.	Внутрішнє, зовнішнє	5	4	3	0,48
5	Соціальна інженерія (шантаж, підкуп інші протизаконні дії) з корисливою метою	- неправильний підбір персоналу	Внутрішнє	4	4	3	0,38
6	Отримання та використання інформації про доступу до системи охорони сторонніми особами через необережне поводження користувачів	- передавання паролів у відкритому вигляді; - необізнаність персоналу з питань інформаційної безпеки.	Зовнішнє	4	5	1	0,16

Кінець таблиці В.1

1	2	3	4	5	6	7	8
7	Несанкціоноване копіювання інформації	відсутність журналу подій.	Внутрішнє	4	3	3	0,28
8	Ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цех носіях	- недосвідченість персоналу.	Внутрішнє	4	2	3	0,19
9	Випадкове зараження програмних засобів комп'ютерними вірусами	- недосвідченість персоналу; - вільний доступ до мережі Internet; - неякісне антивірусне ПЗ.	Внутрішнє	5	2	4	0,32

ДОДАТОК Г

Таблиця Г.1 – Рівень ризику після впровадження архітектури безпеки

№	Загрози	Вразливості системи, що призведуть до реалізації загроз	К1	К2	К3	$К_{загальне}$
1	Несанкціонований доступ до інформації через Wi-Fi	- нерегулярна зміна паролів на Wi-Fi.	4	3	2	0,19
2	Несанкціонований заволодіння інформації на паперових або електронних носіях	- неналежне зберігання документів та пристроїв з інформацією підприємства.	3	3	2	0,14
3	Проникнення зловмисника в приміщення	- неефективна система охорони; - недостатній контроль за приміщенням	3	3	4	0,28
4	Здійснення атак на ОС	- відсутність або неефективність антивірусного ПЗ; - наявність незахищеного з'єднання.	3	2	3	0,14
5	Соціальна інженерія (шантаж, підкуп інші протизаконні дії) з корисливою метою	- неправильний підбір персоналу	4	3	3	0,28
6	Отримання та використання інформації про доступу до системи охорони сторонніми особами через необережне поводження користувачів	- передавання паролів у відкритому вигляді; - необізнаність персоналу з питань інформаційної безпеки.	4	4	1	0,13
7	Несанкціоноване копіювання інформації	відсутність журналу подій.	3	3	3	0,22
8	Ненавмисне пошкодження носіїв інформації чи інформації, яка зберігається на цех носіях	- недосвідченість персоналу.	3	2	3	0,14
9	Випадкове зараження програмних засобів	- недосвідченість персоналу; - вільний доступ до мережі	4	2	3	0,19

Завідувачу кафедри кібербезпеки
к.т.н., доц. Кльоцу Ю.П.
Костовського Олеся Геннадійовича
ПІБ здобувача вищої освіти

студента ФІТ, 4 курсу, групи КБ-18-1

ЗАЯВА

З правилами чинного Положення «Про дотримання академічної доброчесності в Хмельницькому національному університеті» від 26.09.2020 (зі змінами від 26.11.2020), згідно з яким виявлення плагіату є підставою для відмови в допуску кваліфікаційної роботи до захисту та застосування заходів дисциплінарної та академічної відповідальності, ознайомлений (а). Про використання програмно-технічних засобів для перевірки кваліфікаційних робіт здобувачів вищої освіти на плагіат оповіщений (а) та надаю свою згоду на обробку та збереження університетом моєї роботи в інституційному репозитарії університету.

Також надаю університету право на передачу моєї роботи для обробки та збереження в базах даних програмно-технічних засобів (Unicheck та Anti-Plagiarism) та використання роботи для виявлення плагіату в інших роботах, які перевіряються програмно-технічними засобами та користувачами, що мають доступ до цих програмно-технічних засобів, виключно в обмежених цілях для виявлення плагіату в текстах робіт.

Робота для перевірки університетом надається в друкованому та електронному варіанті. Електронна версія моєї роботи збігається (ідентична) з друкованою.

6.06.2022
дата

підпис

Thu Jun 16 16:38:42 EEST 2022, Мостовий Сергій Володимирович, Хмельницький національний університет, ХНУ

Anti-Plagiarism v-15.257

Максимальное совпадение с одним документом 0.0%

Словари проверки: en_US, ru_RU, ua_UA. **Ошибок в документах: 7%**

	Документ		Суммарное совпадение по Базе Данных	
ID: 105738 Название: Архітектура системи захисту інформації діяльності фізичної особи-підприємця Добавлено в БД: 2022-06-16 Авторы: Костовський Олесь Геннадійович Руководители: Чешун В.М. Консультанты: Опоненты:	Символы	Лексемы	Символы	Лексемы
	64776	994	1086 (2%)	21 (2%)

Источник плагиата

ID	Описание	Наличие плагиата в документе	
		Символы	Лексемы

UNICHECK

Ім'я користувача:
Кафедра кібербезпеки

ID перевірки:
1011597496

Дата перевірки:
16.06.2022 17:34:13 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
16.06.2022 17:34:50 EEST

ID користувача:
100008300

Назва документа: **костовський олесь робота кб-18-1**

Кількість сторінок: **64** Кількість слів: **10992** Кількість символів: **89450** Розмір файлу: **2.13 MB** ID файлу: **1011466175**

14.7%
Схожість

Найбільша схожість: **10.7%** з Інтернет-джерелом (http://ir.nmu.org.ua/bitstream/handle/123456789/154453/%D0%A2%D..

13.4% Джерела з Інтернету 163 ..... Сторінка 66

1.49% Джерела з Бібліотеки 56 ..... Сторінка 66

0% Цитат

Включення цитат вимкнене

Включення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи 3

РІШЕННЯ ЕКСПЕРНОЇ КОМІСІЇ

КАФЕДРИ КІБЕРБЕЗПЕКИ

ПРО ДОПУСК КВАЛІФІКАЦІЙНОЇ РОБОТИ ДО ЗАХИСТУ

Підтверджуємо ознайомлення з результатом звіту подібності щодо роботи, генерованого системою виявлення текстових збігів/ідентичності/схожості:
Назва: Архітектура системи захисту інформації діяльності ІПІ «МайстерКомп»

Автор: Костовський Олесь Геннадійович
Спеціальність: 125 – Кібербезпека
Освітня програма: освітньо-професійна
Науковий керівник: Чешун Віктор Миколайович, к.т.н, доцент

Після аналізу звіту подібності зроблено такий висновок:

№	Висновок	Позначка про відповідність
1	Запозичення, виявлені в роботі, є законними і не є плагіатом. Робота приймається до захисту.	відповідає
2	Виявлені запозичення не є плагіатом, розміщені в розділах, які не описують безпосередньо авторське дослідження, але кількість цитат перевищує обсяг, виправданий поставленою метою роботи Робота приймається до захисту, але має бути відкоригована. Відкоригований варіант має бути поданий на кафедру за 2 дні до захисту, разом із заявою щодо самостійності виконання письмової роботи та ідентичності друкованої та електронної версії роботи	
3	Виявлені запозичення не є плагіатом, але частково розміщені в розділах, які описують безпосередньо авторське дослідження, а кількість цитат перевищує обсяг, виправданий поставленою метою роботи. В зв'язку з цим мета роботи та поставлені завдання не були досягнені. Робота може бути допущена до захисту (наступного року) після того як буде відкоригована та допрацьована і успішно пройде повторну перевірку на академічний плагіат.	
4	Робота містить навмисні текстові спотворення, передбачувані спроби укриття запозичень або інші прояви академічного плагіату. Робота містить фабрикацію або фальсифікацію даних. Робота не допускається до захисту.	

Підтвердження:

Оригінальність тексту роботи за результатами перевірки системою Unichek складає 85,3%, оригінальність тексту роботи за результатами перевірки системою Anti-Plagiarism v-15.257 складає 100%.

Згідно з Положенням про систему забезпечення академічної доброчесності в Хмельницькому національному університеті (https://www.khnu.km.ua/root/files/01/10/03/0101.pdf), така авторська робота визнається роботою з достатньою унікальністю тексту.

Запозичення, виявлені в роботі, є законними і не є плагіатом, оскільки:

1. В якості запозичень системою Unichek розпізнано типові елементи стандартного бланку титульної сторінки та рамок пояснювальної записки.
2. В файлі пояснювальної записки наявний розділ «Перелік умовних скорочень», який містить набір широко вживаних фахових термінів та їх скорочень, що також визнано системою перевірки як запозичення.
3. Запозиченнями системою Unichek визнано збіги в назвах використаних друкованих видань, розміщених в переліку джерел посилань, які оформлені за вимогами стандартів і не можуть не співпадати з описами аналогічних джерел в інших роботах.
4. Запозиченнями системою Unichek визнано зміст стандартних таблиць з нормативними даними, на використанні яких базується робота, але на авторство яких здобувач не претендує.
5. Інші збіги є загальновживаними фразами.

Керівник роботи Віктор Чешун

Гарант ОП Віктор Чешун

Завідувач кафедри Кб Юрій Кльоц

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ХМЕЛЬНИЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

РЕЦЕНЗІЯ НА КВАЛІФІКАЦІЙНУ РОБОТУ

освітнього ступеня «бакалавр»

Студент Костовський Олесь

Тема Архітектура системи захисту інформації діяльності ПП «Майстеркомп»

Спеціальність 125 – Кібербезпека

Обсяг кваліфікаційної роботи освітньо-кваліфікаційного рівня «бакалавр»:

кількість листів креслень 6 ; кількість сторінок записки 69 .

1. Короткий зміст роботи та прийнятих рішень У кваліфікаційній роботі розроблено систему контролю доступу та захисту інформації для підприємства, в ході проєктування якої також була розроблена модель порушника, модель загроз, система відеоспостереження та захисту корпоративної мережі, надано рекомендації для персоналу у роботі з конфеденційними данними а також з апаратними системами .

2. Висновок про відповідність кваліфікаційної роботи завданню Кваліфікаційна робота у повній мірі відповідає поставленому завданню як в теоретичній, так і в практичній частині

3. Характеристика виконання кожного розділу роботи, ступінь використання останніх досягнень науки і техніки і передових методів роботи: У першому розділі роботи був зроблений детальний аналіз законодавчих актів та нормативних документів України, які стосуються захисту інформації та визначена актуальність цієї проблеми для приватних підприємств. Також розглянуті питання принципів та етапів побудови архітектури системи захисту інформації, представлена їх детальна класифікація. Проаналізовані переваги та недоліки існуючих моделей архітектур систем. В наступних розділах розглянуті питання, пов'язані з розробкою архітектури системи інформаційного захисту на ПП «МайстерКомп». Під час виконання роботи було проведено аудит інформаційної безпеки підприємства, зроблене категорування інформації, яка обробляється у інформаційно-телекомунікаційній системі ПП, виявлено можливі канали витоку інформації, наведено характеристику компонентів системи, розроблені моделі загроз та ймовірного порушника безпеки інформації; сформовані основні положення політики безпеки інформації для створення моделі архітектури системи захисту інформації.

4. Позитивні сторони роботи Проведений в роботі аналіз пропонованої моделі архітектури інформаційної безпеки вказує на зниження рівня ризиків в системі через виявлені канали, що свідчить про ефективність запропонованого

5. Негативні сторони роботи роботи В роботі недостатньо деталізовано положення політики безпеки, яка є основою запропонованої архітектури системи захисту інформації діяльності

6. Оцінка графічного оформлення та пояснювальної записки роботи Графічне оформлення виконане відповідно до теми кваліфікаційної роботи з дотриманням стандартів. В загальному графічне оформлення виконане якісно, пояснювальна записка відповідає нормам щодо її оформлення.

7. Відгук про роботу в цілому В загальному кваліфікаційна робота заслуговує позитивної оцінки. Весь матеріал кваліфікаційної роботи структурований, чіткий та послідовний. Усі розділи роботи послідовні та логічні, що дозволяє чітко розуміти викладений матеріал в рамках тематики кваліфікаційної роботи. Графічний матеріал дозволяє наочно побачити доцільність та ефективність рішень, які були прийняті за основу для досягнення поставленої мети.

8. Інші зауваження В пояснювальній записці багато великих таблиць, які доцільно виносити в додатки до роботи.

9. Оцінка кваліфікаційної роботи Враховуючи всі позитивні та негативні сторони представленої кваліфікаційної роботи, можна зробити висновок, що вона заслуговує оцінку «добре».

РЕЦЕНЗЕНТ (прізвище, ім'я, по батькові, посада, місце роботи) Нічепорук Андрій Олександрович, к.т.н., доцент кафедри комп'ютерної інженерії та інформаційних систем

«8» 06 2022. (підпис)