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

Інститут електроенергетики
Факультет інформаційних технологій
Кафедра безпеки інформації та телекомунікацій

ПОЯСНЮВАЛЬНА ЗАПИСКА
кваліфікаційної роботи ступеню магістр

студента *Данильченка Олексія Ігоровича*

академічної групи *125м-21-1*

спеціальності *125 Кібербезпека*

спеціалізації[1]

за освітньо-професійною програмою *Кібербезпека*

на тему *Розробка системи управління інформаційною безпекою торгівельного підприємства «Автохімія»*

Керівники	**Прізвище, ініціали**	**Оцінка за шкалою**		**Підпис**
		рейтинговою	**інституційною**	
кваліфікаційної роботи	д.т.н., проф. Корченко А.О.			
розділів:				
спеціальний	ст. викл. Начовний І.І.			
економічний	к.е.н., доц. Пілова Д.П.			
Рецензент				
Нормоконтролер	ст. викл. Мєшков В.І.			

Дніпро
2022

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

«_____»_____20___року

ЗАВДАННЯ
на кваліфікаційну роботу
ступеня магістр

студенту *Данильченку Олексію Ігоровичу* **академічної групи** *125м-21-1*
(прізвище ім'я по-батькові) (шифр)

спеціальності *125 Кібербезпека*
(код і назва спеціальності)

на тему ***Розробка системи управління інформаційною безпекою торгівельного підприємства «Автохімія»***

затверджену наказом ректора НТУ «Дніпровська політехніка» від 31.10.22р. № 1200-с

Розділ	Зміст	Термін виконання
Розділ 1	Створення системи управління інформаційною безпекою торговельних підприємств	20.10.2022
Розділ 2	Розробити комплекс заходів та рекомендацій щодо створення системи управління інформаційною безпекою торговельних підприємств	16.11.2022
Розділ 3	Обґрунтувати економічну доцільність використання наведеної в роботі створеної та впровадженої СУІБ на підприємстві	05.12.2022

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

Дата видачі: 05.09.2022 р.

Дата подання до екзаменаційної комісії: 12.12.2022 р.

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

РЕФЕРАТ

Пояснювальна записка: 116 с., 5 рис., 10 табл., 4 додатка, 16 джерел.

Об'єкт дослідження: потоки інформації на типових торгівельних підприємствах.

Предмет дослідження: захист інформації торгівельних підприємств.

Мета роботи: створення системи управління інформаційною безпекою торговельних підприємств.

У спеціальній частині розроблені комплекс заходів та рекомендацій щодо створення системи управління інформаційною безпекою торговельних підприємств. Розглянуто як об'єкт дослідження торгівельне підприємство «Автохімія». Дана СУІБ була впроваджена на підприємстві. Були розроблені рекомендації з інформаційної безпеки торгового підприємства.

В економічному розділі обґрунтована економічна доцільність використання наведеної в роботі створеної та впровадженої СУІБ на підприємстві.

Новизна дослідження полягає в тому, що розроблені рекомендації зі створення системи управління інформаційною безпекою торговельних підприємств.

ЗАХИСТ ІНФОРМАЦІЇ, ТОРГІВЕЛЬНЕ ПІДПРИЄМСТВО, ЗАГРОЗА, РИЗИКИ, СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ, КОНТРЗАХОДІВ, РЕКОМЕНДАЦІЇ.

ABSTRACT

Explanatory note: 116 p., _5_ pic., 10_ tabl., _4_ app., _16_ sources.

Object of research: information flows at typical trading enterprises.

Subject of research: protection of information of trading enterprises.

Purpose of work: creation of information security management system of trade enterprises.

In the special part developed a set of measures and recommendations for the creation of information security management system of trade enterprises. The trading enterprise "Autochemistry" is considered as an object of research. This ISMS was implemented at the enterprise. Recommendations on information security of trade enterprise were developed.

The economic section substantiates the economic feasibility of using the created and implemented ISMS at the enterprise.

The novelty of the study is that recommendations for the creation of an information security management system for trade enterprises have been developed.

INFORMATION SECURITY, TRADE ENTERPRISE, THREAT, RISKS, INFORMATION SECURITY MANAGEMENT SYSTEMS, COUNTERMEASURES, RECOMMENDATIONS.

СПИСОК УМОВНИХ СКОРОЧЕНЬ

АРМ – автоматизоване робоче місце;

ВВБ – високий вплив на бізнес;

ДСТУ – Державний стандарт України;

ЕОМ – електронна обчислювальна машина;

ЗБПД – загроза безпеки персональних даних;

ЗЗІ – засоби захисту інформації;

ЗПД – загрози персональним даним;

ІБ – інформаційна безпека;

ІС – інформаційна система;

ІТ – інформаційні технології;

НСД – несанкціонований доступ;

ПД – персональні дані;

ПЕМВН – побочні електромагнітні випромінювання;

ПЗ – програмне забезпечення;

ПК – персональний комп’ютер;

СЗІ – система захисту інформації;

СУІБ – система управління інформаційною безпекою ;

ТЗІ – технічний захист інформації.

ЗМІСТ

ВСТУП

У зв'язку з прискоренням темпу розвитку людської діяльності інформація стає робочим інструментом як економічної діяльності, що призводить в дію і регулюючої її механізми, а також застосовується в багатьох інших областях. Процес розвитку обумовлює вихід на новий рівень інформаційного забезпечення. Притому, вимоги до нього ростуть набагато швидше, ніж вони вдосконалюються.

Інформація стає найважливішим з компонентів діяльності торгівельних підприємств. В даний час необхідність в якісному інформаційному забезпеченні значно зростає. Роль інформації виходить на перший план. У цих умовах формуються інформаційні системи, які й покликані забезпечити вихід на новий рівень, який був здатний оптимізувати інформаційне забезпечення підприємств в умовах динамічного розвитку. З цих причин і виявляється реальна необхідність створення ефективної системи управління інформаційної без-пеки торгівельних підприємств.

Важливість інформаційної безпеки торгівельних підприємств для підвищення ефективності їх роботи обумовлює актуальність теми даного дослідження.

Інформаційна безпека включає в себе заходи по захисту процесів створення даних, їх введення, обробки і виведення. Метою інформаційної безпеки є убезпечити цінності системи, захистити і гарантувати точність і цілісність інформації, і мінімізувати руйнування, які можуть мати місце, якщо інформація буде модифікована або зруйнована. Інформаційна безпека вимагає врахування всіх подій, в ході яких інформація створюється, модифікується, до неї забезпечується доступ або вона поширюється.

Метою роботи є створення системи управління інформаційної безпеки торгівельних підприємств. Для досягнення поставленої мети в роботі були поставлені і вирішені наступні завдання:

1 Проаналізувати нормативні документи про систему управління інформаційною безпекою, а також етапи її створення;

2 Проаналізувати структуру, інформаційні потоки, існуючі загрози для типових торгівельних підприємств;

3 Розрахувати ризики ІБ;

4 Розробити на їх основі комплекс заходів та рекомендацій щодо створення системи управління інформаційної безпеки;

5 Провести впровадження створеної СУІБ на підприємстві;

6 Розрахувати ризики ІБ на підприємстві.

РОЗДІЛ 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

1.1 Аналіз нормативних документів стосовно системи управління інформаційної безпеки

Під управлінням інформаційною безпекою розуміється захищеність інформації і підтримуючої її інфраструктури від будь-яких випадкових або зловмисних впливів, результатом яких може з'явитися нанесення збитку інформації, її власникам або підтримуючій інфраструктурі. Завдання інформаційної безпеки зводяться до мінімізації збитку, а також до прогнозування і запобігання таких впливів.

Параметри інформаційних систем, які потребують захисту, можна розділити на наступні категорії: забезпечення цілісності, доступності та конфіденційності інформаційних ресурсів.

– доступність - це можливість отримання, за короткий проміжок часу, необхідної інформаційної послуги;

– цілісність - це актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни;

– конфіденційність захисту від несанкціонованого доступу до інформації.

Інформаційні системи, насамперед, створюються для отримання певних інформаційних послуг. Якщо отримання інформації з якихось причин стає неможливим, це приносить шкоду всім суб'єктам інформаційних відносин. З цього можна визначити, що доступність інформації стоїть на першому місці.

Цілісність є основним аспектом інформаційної безпеки тоді, коли точність і правдивість будуть головними параметрами інформації.

Найбільш відпрацьованою складовою інформаційної безпеки в нашій країні є конфіденційність. Але практична реалізація заходів щодо забезпечення конфіденційності сучасних інформаційних систем стикається з труднощами. По-перше, відомості про технічні канали витоку інформації є закритими, так що більшість користувачів позбавлені можливості скласти уявлення про потенційні

ризики. По-друге, на шляху користувальницької криптографії як основного засобу забезпечення конфіденційності стоять численні законодавчі перешкоди і технічні проблеми.

У ході роботи над роботою проаналізовані нормативні документи, ДСТУ та ISO. Зокрема нас цікавить документ ДСТУ СУІБ 1.0/ISO/IEC 27001 (далі Стандарт). У цьому документі сформульовані вимоги до системи управління інформаційною безпекою (СУІБ), включаючи загальну методологію створення, впровадження та оцінки ефективності механізмів СУІБ.

Даний стандарт застосовується в різних галузях, в тому числі і для торгівельних підприємств. Відповідність йому стає важливим фактором комерційного успіху організації завдяки цілому ряду переваг, які вона отримує, таким як:

– конкурентні переваги;

– підвищення становища компанії в міжнародних рейтингах, необхідне для залучення закордонних інвестицій і виходу на міжнародні ринки;

– підвищення вартості акцій компанії;

– демонстрація партнерам і клієнтам високого рівня надійності за рахунок адекватної захисту інформації, включаючи інформацію клієнтів і партнерів;

– зниження ризиків, пов'язаних з можливими збитками для активів компанії;

– підвищення прозорості процесу управління інформаційною безпекою в організації:

а) чіткий поділ повноважень і відповідальності за забезпечення інформаційної безпеки;

б) критерії оцінки ефективності виконуваних заходів щодо забезпечення інформаційної безпеки;

в) обґрунтування витрат на інформаційну безпеку.

Переваги здобуваються в результаті отримання сертифіката відповідності СУІБ організації вимогам ISO/IEC 27001, який видається незалежним органом з сертифікації при успішному проходженні сертифікаційного аудиту СУІБ.

Управління інформаційною безпекою - це циклічний процес, що включає усвідомлення ступеня необхідності захисту інформації та постановку завдань; збір та аналіз даних про стан інформаційної безпеки в організації; оцінку інформаційних ризиків; планування заходів з обробки ризиків; реалізацію та впровадження відповідних механізмів контролю, розподіл ролей і відповідальності, навчання і мотивацію персоналу, оперативну роботу по здійсненню захисних заходів; моніторинг функціонування механізмів контролю, оцінку їх ефективності та відповідні коригуючи дії.

Самим трудомістким і складним етапом на шляху до сертифікації є власне створення системи управління ІБ і впровадження її механізмів у компанії.

Проаналізований стандарт являє собою модель системи менеджменту в області інформаційної безпеки. СУІБ - це набір організаційних заходів і процедур управління, вона не є за своєю суттю технічним стандартом.

Стандарт приймає процес ний підхід до розробки, впровадження, функціонування, моніторингу, перегляду, підтримки і вдосконалення СУІБ організації. Застосування системи процесів в рамках організації разом з ідентифікацією цих процесів та їх взаємодією, а також менеджмент можна розглядати як « процесний підхід».

Процесний підхід до управління інформаційною безпекою, запропонований цим стандартом, заохочує користувачів робити упор на важливості:

1) розуміння вимог інформаційної безпеки організації і необхідності розробки політики і цілей інформаційної безпеки;

2) впровадження контролів і їх функціонування для управління ризиками інформаційної безпеки організації в контексті загальних бізнес - ризиків організації;

3) моніторингу та перегляді продуктивності та ефективності СУІБ

4) постійному вдосконаленні, заснованому на об'єктивному вимірі.

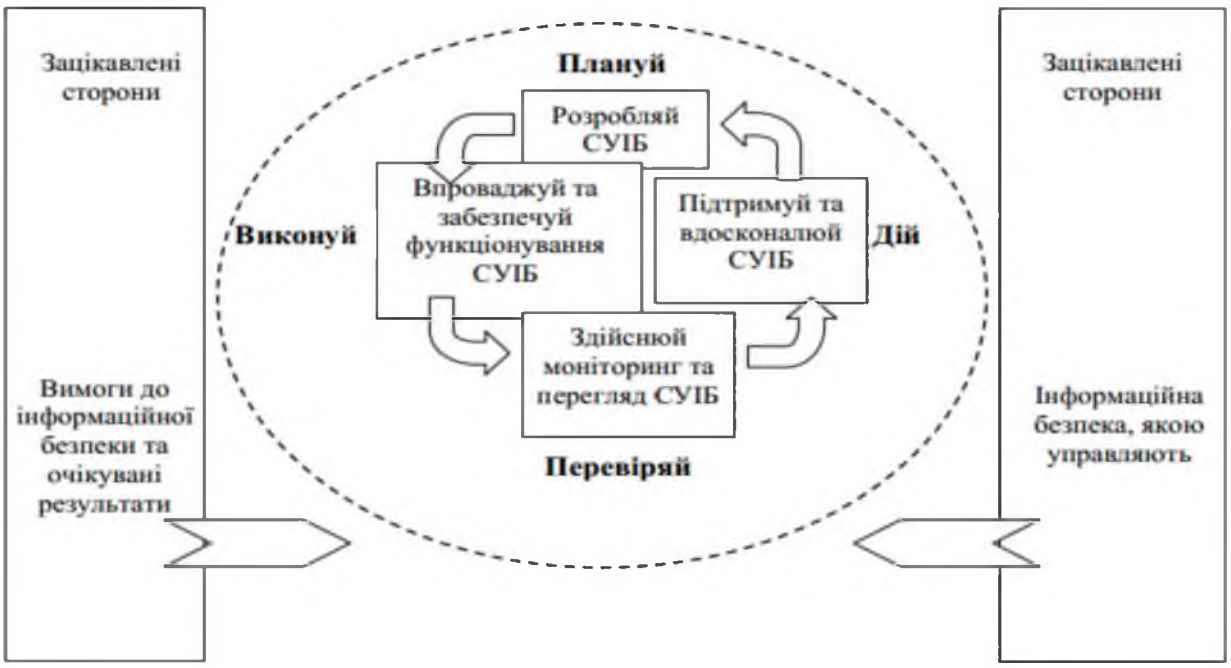

Рисунок 1.1 – Процесний підхід в рамках СУІБ

Модель «Плануй Виконуй Перевіряй Дій» («Plan Do Check Act»), надалі ПВПД (PDCA), яку застосовують для структуризації всіх процесів СУІБ. На рисунку 1.1 представлений процесний підхід до створення СУІБ.

В якості вхідних даних будуть вимоги інформаційної безпеки та очікування зацікавлених сторін, за допомогою необхідних дій і процесів виробляє вихідні дані інформаційної безпеки, що відповідають цим вимогам та очікуванням.

У таблиці 1.1 представлені етапи створення СУІБ, а також дії, що виконуються на кожному з них.

Таблиця 1.1 – Етапи створення СУІБ

Етап	Дія
Плануй (розробляй СУІБ)	Розробити політику СУІБ, цілі, процеси та процедури,суттєві для управління ризиками та вдосконалення інформаційної безпеки, щоб одержати результати, які відповідають загальній політиці та цілям організації.
Виконуй (впроваджуй та забезпечуй функціонування СУІБ)	Впроваджувати та забезпечувати функціонування політики інформаційної безпеки, контролів, процесів та процедур СУІБ.

Перевіряй (здійснюй моніторинг та перегляд СУІБ)	Оцінювати і, за можливості, вимірювати продуктивність процесів згідно з політикою, цілями і практичним досвідом СУІБ та звітувати про результати керівництву для перегляду.
Дій (підтримуй та вдосконалюй СУІБ)	Вживати коригувальні та запобіжні дії на підставі результатів внутрішнього аудиту і перегляду СУІБ з боку керівництва або іншої суттєвої інформації для досягнення постійного вдосконалення СУІБ.

У проаналізованому стандарті представлена комплексна система, що включає і механізми управління, і механізми захисту інформації.

Організація повинна розробляти, впроваджувати, забезпечувати функціонування, здійснювати моніторинг, переглядати, підтримувати та вдосконалювати задокументовану СУІБ в контексті загальної бізнес-діяльності організації і ризиків, з якими вона стикається.

Основним рушійним механізмом СУІБ є періодичний аналіз ризиків інформаційної безпеки. Вище керівництво організації також втягується в процес управління СУІБ шляхом прийняття рішень на основі результатів аналізу ризиків, результатів внутрішніх аудитів та інших механізмів СУІБ. З точки зору процесів управління СУІБ входить в загальну систему менеджменту організації та надає додаткові механізми управління в частині забезпечення захисту критичної інформації.

1.2 Аналіз створення СУІБ з урахуванням специфіки торгівельного підприємства

Торгівельне підприємство повинно розробляти, впроваджувати, забезпечувати функціонування, здійснювати моніторинг, переглядати, підтримувати та вдосконалювати задокументовану СУІБ в контексті загальної бізнес-діяльності організації і ризиків, з якими вона стикається. Процес, використаний для цього стандарту, базується на моделі ПВПД (PDCA), яку наведено на рисунку 1.1.

1.2.1 Етапи розроблення СУІБ

1 Визначити сферу і межі використання СУІБ виходячи з характеристик бізнесу, організації, її розташування, активів і технологій, охоплюючи подробиці та обґрунтування будь-яких винятків із галузі застосування;

2 Визначити політику СУІБ, виходячи з характеристик бізнесу, організації, її розташування, активів і технологій, яка:

1) охоплює основи для встановлення цілей і розробляє загальний зміст регулювання та принципів діяльності щодо інформаційної безпеки;

2) враховує вимоги бізнесу, правові чи нормативі вимоги, а також контрактні зобов'язання щодо безпеки;

3) узгоджена з контекстом стратегічного управління ризиками торгівельного підприємства, в якому будуть розробляти та підтримувати СУІБ;

4) встановлює критерії, за якими будуть оцінювати ризики;

5) повинна бути затверджена керівництвом.

3 Визначити підхід торгівельного підприємства до оцінки ризику.

1) ідентифікувати методологію оцінки ризику, пристосовану до СУІБ і ідентифікованої інформаційної безпеки бізнесу, правових і нормативних вимог.

2) розробити критерії прийняття ризиків та ідентифікувати прийнятні рівні ризику.

3) вибрана методологія оцінки ризику повинна забезпечувати, що оцінки ризику дають порівнювані та відтворювані результати.

4 Ідентифікувати ризики:

1) ідентифікувати активи в межах галузі застосування СУІБ та власників цих активів.

2) ідентифікувати загрози цим активам.

3) ідентифікувати вразливості, які можуть бути використані загрозами.

4) ідентифікувати значні впливи, які втрата конфіденційності, цілісності та доступності можуть справити на активи.

5 Проаналізувати та оцінити ризики:

1) оцінити значні бізнес-впливи на торгівельне підприємство, які можуть бути наслідком порушення безпеки, враховуючи наслідки втрати конфіденційності, цілісності або доступності активів.

2) оцінити реальну ймовірність порушень безпеки, що виникають, беручи до уваги переважаючі загрози і вразливості, та значні впливи, пов'язані з цими активами, і впроваджені на цей момент контролі.

3) визначити величину рівнів ризиків.

4) використовуючи критерії прийнятності ризиків, визначити є ризики прийнятними чи вимагають оброблення.

6 Ідентифікувати та оцінити альтернативні варіанти оброблення ризиків. Можливі дії охоплюють:

1) застосування належних контролів;

2) свідоме та об'єктивне прийняття ризиків, забезпечуючи, що вони чітко задовольняють політику організації та критерії прийняття ризиків;

3) уникнення ризиків;

4) перенесення відповідних бізнес-ризиків на інші сторони, наприклад, страхувальників, постачальників.

7 Вибрати цілі контролів та контролі для оброблення ризиків.

8 Цілі контролів та контролі треба вибирати та впроваджувати таким чином, щоб задовольняти вимоги, ідентифіковані оцінкою ризиків і процесом їх оброблення. Цей вибір повинен враховувати як критерії для прийняття ризиків, так і правові, нормативні та контрактні вимоги. Як частину цього процесу треба вибирати цілі контролів та контролі, що підходять для задоволення ідентифікованих вимог.

9 Отримати від керівництва затвердження запропонованих залишкових ризиків.

10 Отримати санкцію керівництва на впровадження та функціонування СУІБ;

11 Підготувати Положення щодо застосовності. Положення щодо застосовності треба підготувати таким чином, щоб воно включало:

1) цілі контролів і контролі, та обґрунтування їх вибору;

2) цілі контролів і контролі, впроваджені на теперішній час;

3) будь-які вилучені цілі контролів і обґрунтування їх вилучення.

1.2.2 Впровадження та функціонування СУІБ

Торгівельне підприємство повинно діяти таким чином:

1 Сформулювати план оброблення ризиків, який ідентифікує належні управлінські дії, ресурси, відповідальності та пріоритети щодо управління ризиками інформаційної безпеки;

2 Впровадити план оброблення ризиків для досягнення ідентифікованих цілей контролю, який містить розгляд фінансових питань та розподілу ролей і відповідальності;

3 Для досягнення цілей контролів впровадити контролі;

4 Визначити, як вимірювати ефективність вибраних контролів або груп контролів, і встановити, як треба використовувати такі вимірювання для оцінки ефективності контролів, щоб отримувати порівнювані та відтворювані результати;

5 Впровадити програми з навчання та поінформованості;

6 Управляти функціонуванням СУІБ;

7 Управляти ресурсами СУІБ;

8 Впровадити процедури та інші контролі для уможливлення термінового виявлення подій безпеки та реагування на інциденти безпеки.

1.2.3 Моніторинг та перегляд СУІБ

Торгівельне підприємство повинно діяти таким чином:

1 Виконувати процедури моніторингу та перегляду, а також інші контролі для того, щоб:

1) терміново виявляти помилки в результатах оброблення;

2) терміново ідентифікувати вдалі та невдалі спроби порушень безпеки і інциденти безпеки;

3) надати можливість керівництву встановити, чи є діяльність щодо безпеки, яку доручено персоналу або впроваджено за допомогою інформаційних технологій, очікувано продуктивною;

4) сприяти виявленню подій безпеки і, таким чином, запобігати інцидентам безпеки, використовуючи показники;

5) встановити, чи були ефективними дії, вжиті для усунення порушення безпеки.

2 Проводити регулярні перегляди ефективності СУІБ (включаючи перевірку відповідності політиці і цілям СУІБ та перегляд контролів безпеки), враховуючи результати аудитів безпеки, інциденти, результати вимірювань ефективності, пропозиції і зворотній зв'язок з усіма зацікавленими сторонами.

3 Вимірювати ефективність контролів, щоб підтвердити відповідність вимогам безпеки.

4 В заплановані терміни переглядати оцінки ризиків, а також переглядати залишкові ризики та ідентифіковані прийнятні рівні ризиків, враховуючи зміни в:

1) організації;

2) технології;

3) цілях та процесах бізнесу;

4) ідентифікованих загрозах;

5) ефективності впроваджених контролів; та

6) зовнішніх подіях, наприклад, змінах правового чи нормативного середовища, змінених контрактних зобов'язаннях та змінах соціального клімату.

5 В заплановані терміни проводити внутрішні аудити СУІБ

6 Здійснювати на регулярній основі перегляд СУІБ з боку керівництва, щоб забезпечити, що галузь застосування залишається адекватною і вдосконалення в процесах СУІБ є ідентифікованими.

7 Оновлювати плани безпеки для врахування результатів діяльності з моніторингу та перегляду.

8 Реєструвати дії та події, що можуть мати значний вплив на ефективність чи продуктивність СУІБ

1.2.4 Підтримування та вдосконалення СУІБ

Торгівельне підприємство повинно регулярно виконувати таке:

1 Впроваджувати в СУІБ ідентифіковані вдосконалення;

2 Здійснювати відповідні коригувальні та запобіжні дії;

3 Доводити до відома всіх зацікавлених сторін інформацію щодо дій та вдосконалень СУІБ із ступенем деталізації, що відповідає обставинам, і, що суттєво, погоджувати подальші дії;

4 Забезпечувати, що вдосконалення досягають намічених цілей.

1.2.5 Вимоги до документації

Документація повинна містити записи щодо управлінських рішень, забезпечуючи відстежуваність дій відповідно до управлінських рішень і політик, а також забезпечувати, що задокументовані результати відтворювані.

Важливо бути в змозі продемонструвати зворотній зв'язок від вибраних контролів до результатів оцінки ризику і процесу оброблення ризику, а потім і до політики та цілей СУІБ [13].

Документація СУІБ повинна містити:

- задокументовані положення щодо політики та цілей СУІБ;
- галузь застосування СУІБ;
- процедури та контролі, що підтримують СУІБ;
- опис методології оцінки ризиків;
- звіт щодо оцінки ризиків;
- план оброблення ризиків;
- задокументовані процедури, необхідні організації для забезпечення ефективного планування, функціонування і контролю її процесів інформаційної безпеки, та опису того, як вимірювати ефективність контролів;
- записи, яких вимагає цей стандарт;

– положення щодо застосовності.

1.2.6 Відповідальність керівництва

Керівництво повинно надати докази виконання своїх зобов'язань щодо розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення СУІБ шляхом:

1) розроблення політики СУІБ;

2) забезпечення, що цілі та плани СУІБ розроблено;

3) розроблення ролей і відповідальностей щодо інформаційної безпеки;

4) доведення до відому організації інформації щодо важливості досягнення цілей інформаційної безпеки та відповідності політиці інформаційної безпеки, відповідальності перед законом та потреби постійного вдосконалення;

5) надання достатніх ресурсів для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення СУІБ;

6) винесення рішення щодо критеріїв прийняття ризиків і прийнятних їх рівнів;

7) забезпечення проведення внутрішніх аудитів СУІБ;

8) проведення переглядів СУІБ з боку керівництва.

Організація повинна визначити та забезпечити ресурси, потрібні щоб:

1) розробляти, впроваджувати, забезпечувати функціонування, здійснювати моніторинг, перегляд, підтримку та вдосконалення СУІБ;

2) забезпечувати підтримку вимог бізнесу процедурами інформаційної безпеки;

3) ідентифікувати і враховувати правові та нормативні вимоги, а також контрактні зобов'язання з безпеки;

4) підтримувати адекватний рівень безпеки шляхом коректного застосування усіх впроваджених контролів;

5) за необхідності виконувати перегляди та відповідним чином реагувати на результати таких переглядів; і

6) за потреби, підвищувати ефективність СУІБ.

Організація повинна забезпечити, щоб весь персонал, для якого встановлено визначені в СУІБ відповідальності, був компетентним для виконання необхідних завдань шляхом:

1) визначення необхідної компетентності персоналу, який виконує роботи, що впливають на СУІБ;

2) забезпечення навчання або вжиття інших заходів (наприклад, наймання компетентного персоналу) для задоволення цих потреб;

3) оцінювання ефективності вжитих заходів; та

4) підтримування записів щодо освіти, навчання, навиків, досвіду та кваліфікації персоналу.

Організація повинна також забезпечити, що весь відповідний персонал поінформовано щодо значущості та важливості їх діяльності з інформаційної безпеки і їх внеску в досягнення цілей СУІБ.

Організація повинна в заплановані терміни проводити внутрішні аудити СУІБ для встановлення чи цілі контролю, контролі, процеси та процедури її СУІБ:

- відповідають вимогам цього стандарту та відповідному законодавству або нормативам;
- відповідають вимогам ідентифікованої інформаційної безпеки;
- є ефективно впровадженими та підтримуваними;
- виконуються як очікувалося.

Програма аудиту повинна плануватися з урахуванням статусу і важливості процесів і областей, що підлягають аудиту, а також результатів попередніх аудитів. Повинні бути визначені критерії, галузь застосування, частота і методи аудиту. Відбір аудиторів і проведення аудитів повинні забезпечувати об'єктивність і неупередженість процесу аудиту. Аудитори не повинні проводити аудит своєї власної роботи.

Відповідальності та вимоги до планування і проведення аудитів, а також звітування про результати і підтримування записів повинні бути визначені в задокументованій процедурі.

Керівництво, відповідальне за область, що підлягає аудиту, повинне забезпечити, що дії для усунення виявлених невідповідностей та їх причин виконуються без недоречних затримок. Подальша діяльність повинна містити верифікацію виконаних дій і звітування про результати верифікації.

Коригувальні дії

Організація повинна здійснювати дії для усунення причин невідповідностей вимогам СУІБ, щоб запобігати їх повторенню. Задокументована процедура коригувальних дій повинна визначати вимоги до:

– ідентифікації невідповідностей;

– встановлення причин невідповідностей;

– оцінювання потреби у діях для забезпечення того, що невідповідності не будуть повторюватись;

– встановлення та впровадження потрібних коригувальних дій;

– реєстрування результатів виконаних дій;

– перегляд виконаних коригувальних дій.

Запобіжні дії

Організація повинна встановити дії для усунення причини потенційних невідповідностей вимогам СУІБ для запобігання їх появі. Здійснені запобіжні дії повинні відповідати значущості впливу потенційних проблем. Задокументована процедура запобіжних дій повинна визначити вимоги до:

– ідентифікації потенційних невідповідностей та їх причин;

– оцінювання потреби в діях для запобігання виникненню невідповідностей;

– встановлення та впровадження необхідних запобіжних дій;

– реєстрування результатів виконаних дій;

– перегляду виконаних запобіжних дій.

– організація повинна ідентифікувати ризики, що змінилися, та ідентифікувати вимоги до запобіжних дій, зосередивши увагу на ризиках, що істотно змінилися.

Пріоритети запобіжних дій повинні бути встановлені на основі результатів оцінки ризику.

Для створення СУІБ на типовому торгівельному підприємстві почнемо з етапу розробки. Першим завданням якого є аналіз типового торгівельного підприємства.

1.3 Аналіз типового об'єкта

Головною метою сучасного етапу економічних перетворень, що проводяться в торгівлі, є створення сприятливих умов для ефективної діяльності торгівельних підприємств.

Досягнення цієї мети, з одного боку, передбачає вдосконалення середовища, в якому працюють торгівельні підприємства, а з іншого - вимагає кардинального поліпшення роботи самих підприємств в умовах ринкових відносин [8].

Складність поставлених завдань викликає необхідність всебічного вивчення сутності та змісту такого поняття, як підприємство торгівлі, яке в якості самостійного господарюючого суб'єкта стає основною ланкою ринкового механізму галузі.

Під торгівельним підприємством у даний час розуміється незалежний господарюючий суб'єкт, що володіє правовим статусом юридичної або фізичної особи, створений з метою отримання прибутку і здійснює діяльність за свій ризик із закупівлі, зберігання, реалізації товарів, спрямовану на задоволення потреб ринку. Це майновий комплекс, використовуваний організацією для купівлі-продажу товарів і надання послуг торгівлі.

Майновий комплекс торгівельного підприємства включає земельні ділянки, будівлі, споруди, обладнання, інвентар, товари, борги, права, фірмове найменування, товарні знаки і знаки обслуговування.

Торгівельне підприємство, виходячи на споживчий ринок, де в конкурентній боротьбі здійснюється продаж товарів, повинно дотримуватись певних правил, основне з яких свідчить: чим краще будуть враховуватися

можливості та побажання покупців, тим більше можна продати товарів і прискорити їх оборотність.

Торгівельні підприємства мають право створювати відокремлені підрозділи у вигляді представництв або філій, які не є юридичними особами і діють на підставі затверджених ними положень.

Торгівельні підприємства виконують такі функції: прогнозування, планування, організацію торгівельно-технологічного процесу, аналіз і контроль.

Всі торгівельні підприємства можуть бути класифіковані по ряду ознак. Така класифікація дозволяє визначити місце, цілі, завдання кожного підприємства в загальній системі торгівельної галузі; дає можливість згрупувати їх за певними критеріями; дозволяє судити про масштаби, спрямованості, різних характеристиках діяльності конкретних підприємств торгівлі; аналізувати, оцінювати, порівнювати результати їхньої діяльності.

Основні класифікаційні ознаки торгівельних підприємств (рис. 1.2):

- форма власності;
- вид діяльності;
- чисельність зайнятих працівників;
- спеціалізація;
- організаційно-правова форма.

За формами власності (приналежності капіталу) виділяють державні та (або) муніципальні, приватні та спільні торгівельні підприємства.

У державних і (або) муніципальних підприємствах засновниками і відповідно власниками капіталу виступають влади різних рівнів. До державним (муніципальним) підприємствам торгівлі відносяться ряд підприємств роздрібної, в тому числі відомчої, торгівлі, але в основному підприємства оптової торгівлі.

До приватних підприємств торгівлі відносять індивідуальні, приватні, сімейні підприємства, що займаються торгівлею, колективні підприємства (причому сюди можна включити підприємства торгівлі, утворені як групою

фізичних, так і юридичних осіб); приватизовані підприємства, що належать трудовим колективам.

Рисунок 1.2 – Класифікація торгівельних підприємств

Особливо слід виділити торгівельні підприємства змішаної форми власності. Їх важко класифікувати, так як форма власності, в якій вони утворені, являє собою комбінацію інших видів і типів власності (наприклад, приватна і державна). Але, як правило, в більшості випадків подібні торгівельні підприємства відносять до приватної форми власності.

Спільні підприємства торгівлі, тобто об'єкти, створюються російськими та іноземними або фізичними, або юридичними особами (резидентами або нерезидентами). Можна виділити торгівельні підприємства повністю з іноземним капіталом. Такі підприємства торгівлі представлені як у роздрібній, так і в оптовій торгівлі, переважно у великих містах.

За видами діяльності виділяють три відносно самостійних ланки: оптову торгівлю, роздрібну торгівлю.

Відповідно можна виділити і підприємства, що займаються оптовою, роздрібною торгівлею, внедомашне харчуванням.

Оптова торгівля включає в себе будь-яку діяльність з продажу товарів або послуг тим, хто купує їх з метою перепродажу або подальшого використання у виробничих процесах.

Роздрібна торгівля являє собою будь-яку діяльність з продажу товарів або послуг безпосередньо кінцевим споживачам для їх особистого некомерційного використання. Відповідно, головною метою роздрібних торгівельних підприємств є реалізація товарів, обслуговування безпосередньо кінцевих споживачів.

Однією з причин відносного відокремлення підприємств торгівлі різних видів діяльності (підгалузей) служить спеціалізація. Торгівельні підприємства кожної підгалузі покликані виконувати цілком певні функції, вирішувати власні завдання на ринку; відповідно, вони змушені використовувати у своїй діяльності різні за структурою ресурси, і в результаті отримують неоднакові результати. Спеціалізація в чому визначається складом споживачів, впливає на розміри і стратегію окремих підприємств, впливає на формування підсумків господарської діяльності.

Спеціалізовані торгівельні підприємства реалізують товари певного асортименту, наприклад, однієї товарної групи (одяг), підгрупи, іноді навіть виду (краватки), але ці товари представлені у повній номенклатурі.

Вузькоспеціалізовані підприємства реалізують обмежений асортимент продукції масового або багатосерійного виробництва.

Універсальні торгівельні підприємства реалізують універсальний асортимент продовольчих і (або) непродовольчих товарів.

Комбіновані торгівельні підприємства реалізують кілька груп товарів, пов'язаних спільністю попиту і задовольняють окремі потреби.

Змішані торгівельні підприємства реалізують окремі види продовольчих і непродовольчих товарів.

За чисельністю підприємства можуть бути малі, середні і великі. Класифікаційними факторами, що визначають ставлення підприємства до малому, середньому або великому, є: кількість працівників, річний оборот,

розмір основного капіталу, кількість робочих місць, витрати на оплату праці, використання вихідних матеріалів.

За організаційно-правовою формою торгівельні підприємства бувають комерційні і некомерційні. Комерційними є ті, які переслідують одержання прибутку як основної мети своєї діяльності, а некомерційні не ставлять своєю метою вилучення прибутку та його розподіл між учасниками.

Товариство з обмеженою відповідальністю (загальноприйняте скорочення - ТОВ) - засноване одним або кількома юридичними та / або фізичними особами господарське товариство, статутний капітал якого розділений на частки; учасники товариства відповідають за його зобов'язаннями і несуть ризик збитків, пов'язаних з діяльністю товариства, у межах вартості належних їм часток у статутному капіталі товариства.

Публічні Акціонерні Товариства (загальноприйняте скорочення ПАТ) - форма публічного торгівельного підприємства; акціонерне товариство, акціонери якого користуються правом відчужувати свої акції. Організація і діяльність відкритих акціонерних товариств регулюється законом України. Оскільки відкрите акціонерне товариство розглядається законодавцем як публічне, для нього передбачається обов'язок щодо розкриття інформації в більш широкому форматі в порівнянні з закритим акціонерним суспільством. Дана норма призначена для підвищення публічності та прозорості процесів інвестування.

Приватні Акціонерні Товариства - форма організації публічної компанії; (загальноприйняте скорочення - ПрАТ) - акціонерне товариство, акції якого розподіляються тільки серед засновників або заздалегідь певного кола осіб (на противагу відкритому).

Товариство (спільна діяльність) - це форма діяльності, здійснюваної особами, які зобов'язуються спільно діяти без створення юридичної особи для досягнення певної мети, що не суперечить закону.

Некомерційна організація (НКО) - організація, яка не має в якості основної мети своєї діяльності одержання прибутку і не розподіляє отриманий прибуток

між учасниками. Некомерційні організації можуть створюватися для досягнення соціальних, благодійних, культурних, освітніх, політичних, наукових та управлінських цілей, в сферах охорони здоров'я громадян, розвитку фізичної культури і спорту, задоволення духовних та інших нематеріальних потреб громадян, захисту прав, законних інтересів громадян і організацій, вирішення спорів та конфліктів, надання юридичної допомоги, а також в інших цілях, спрямованих на досягнення суспільних благ. Некомерційні організації мають право займатися підприємницькою діяльністю, тільки якщо дана діяльність спрямована на досягнення цілей організації.

Некомерційні споживчі кооперативи - це один з різновидів кооперативів. Споживчим кооперативом є добровільне об'єднання громадян і юридичних осіб на основі членства з метою задоволення власних потреб у товарах і послугах, початкове майно якого складається з пайових внесків.

1.3.1 Особливості підприємств торгівлі

Інформацію, що потрапляє в торгівельне підприємство, можна класифікувати за різними критеріями. Основним критерієм, що дозволяє вважати те або інше повідомлення інформацією, є його цінність, корисність для досягнення цілей. Таке розуміння інформації призводить до виділення в ній якостей відносності: одні й ті ж відомості можуть вважатися інформацією для однієї системи і бути перешкодою, інформаційним шумом - для іншої [21].

Інформацію, яка використовується в процесі управління торгівельним підприємством, можна класифікувати по ряду ознак.

1 За характером призначенням та формами закріплення вся інформація ділиться на три великих класи: науково-технічна, управлінська та обліково-статистична інформація. Управлінська інформація утворюється безпосередньо в процесі управління. Це планова, нормативна та інша економічна інформація, яка використовується в цілях організації процесу управління підприємством. Така інформація міститься в установчих документах підприємства, договорах з постачальниками і покупцями, в організаційно-розпорядчих документах.

Обліково-статистична інформація виникає як результат господарської діяльності підприємства і фіксується в спеціально створених документах (формах).

2 За об'єктами, що відображаються вся інформація ділиться на інформацію про трудові, матеріальні ресурси, фінанси, про основні фонди підприємства, про постачальників, конкурентів, попит на товари і т.п.

3 За організаційною ознакою інформація підрозділяється на систематизовану, тобто регламентовану за складом показників, періодичності, формам подання (наприклад, баланс, звіт про прибутки і збитки, рахунок - фактура), і несистематизованими, тобто що має вільну форму подання.

4 У напрямку передачі інформація поділяється на низхідну, спрямовану від об'єкта до суб'єкта управління, що сходить (від об'єкта до суб'єкта) і горизонтальну.

1.3.2 Вимоги до інформації

Однією з найбільш важливих вимог до інформації, використовуваної в системах управління, є цінність інформації, під якою розуміється її здатність сприяти цілям управління. Цінність інформації визначається характером об'єкта та умов середовища, в якій він функціонує. Ця якість інформації не є постійною. Вона може з часом досягати максимального значення або, навпаки, втрачати силу [24].

Велике значення має достовірність інформації. В інформаційний обмін в системі управління можуть бути залучені неправдиві відомості, що багато в чому ускладнює її функціонування. Достовірність висловлює точність відповідності даних про якусь подію реальним фактам. На достовірність значно впливають як засоби так і способи відображення реальних фактів, так і засоби і способи зберігання і передачі інформації.

Наступною вимогою до інформації є своєчасність. Ця властивість тісно пов'язана з цінністю, так як саме своєчасністю найчастіше визначається цінність тієї чи іншої інформації.

До обов'язкових вимог відноситься також повнота інформації. Під повнотою розуміється достатність інформації для вирішення поставлених завдань. При цьому слід пам'ятати, що надлишок інформації (зайві деталі і подробиці) може утруднити прийняття рішення, як і її недолік.

І нарешті, важливою вимогою є компактність інформації. Вона дозволяє збільшити пропускну спроможність каналів зв'язку, робить інформацію більш наочною і легкою для сприйняття, що, в свою чергу, підвищує якість її використання.

1.3.3 Інформаційні потоки торгівельних підприємств

Одним з важливих понять при розгляді інформаційного забезпечення процесу управління підприємством є поняття інформаційного потоку.

Інформаційний потік - це сукупність циркулюючих між окремими структурними елементами системи (підрозділами підприємства, окремими особами), а також між системою і зовнішнім середовищем повідомлень, необхідних для управління. Інформаційний потік може існувати у вигляді паперових і електронних документів.

Залежно від пов'язують потоком систем потоки діляться на горизонтальні і вертикальні; залежно від місця проходження - на зовнішні і внутрішні і залежно від напряму - на вхідні та вихідні.

Інформаційний потік характеризується наступними показниками:

- джерело виникнення;
- напрямок руху потоку;
- швидкість передачі і прийому інформації;
- інтенсивність потоку, тобто кількість інформації, що надходить в одиницю часу.

На рисунку 1.3 представлена типова схема інформаційних потоків торгівельного підприємства. Розглядається центральний офіс фірми і його філії. Філії відправляють в центральний офіс звіти про проведену роботу і заборгованість замовників. У свою чергу відділ закупівель разом з відділом

логістики відправляють заявки постачальникам. Постачальники відправляють товар і з ним звіти про доставку. Оплата постачальнику проходить через банк.

Замовник може звернутися зі своїм замовленням або в центральний офіс, або в філію. Якщо він звернувся в центральний офіс, то оплата йде або офіс або в банк. Якщо замовник звернувся до філії, то оплата у філію, а після переводиться в центральний офіс, а після в банк.

1.3.4 Існуючі загрози торгівельних підприємств

Зроблено аналіз існуючих загроз інформаційної безпеки для типового торгівельного підприємства [28]. Інформація на торгівельному підприємстві класифікована наступним чином:

По режиму доступу:

- відкрита;
- з обмеженим доступом (за правовим режимом).

Відкрита інформація поділяється на:

- відкриту, яка не потребує захисту (відомості про сплату податків і обов'язкових платежів, відомості про ліквідність підприємства, відомості про чисельність, склад працюючих, фонд заробітної плати, умови праці та наявність вільних робочих місць);
- відкриту, яка потребує захисту (правила та інструкції роботи в ІКС, відомості з установчих документів статуту, відомості з документів, що дають право на підприємницьку діяльність, відомості по статутним формами звітності про фінансово-господарської діяльності).

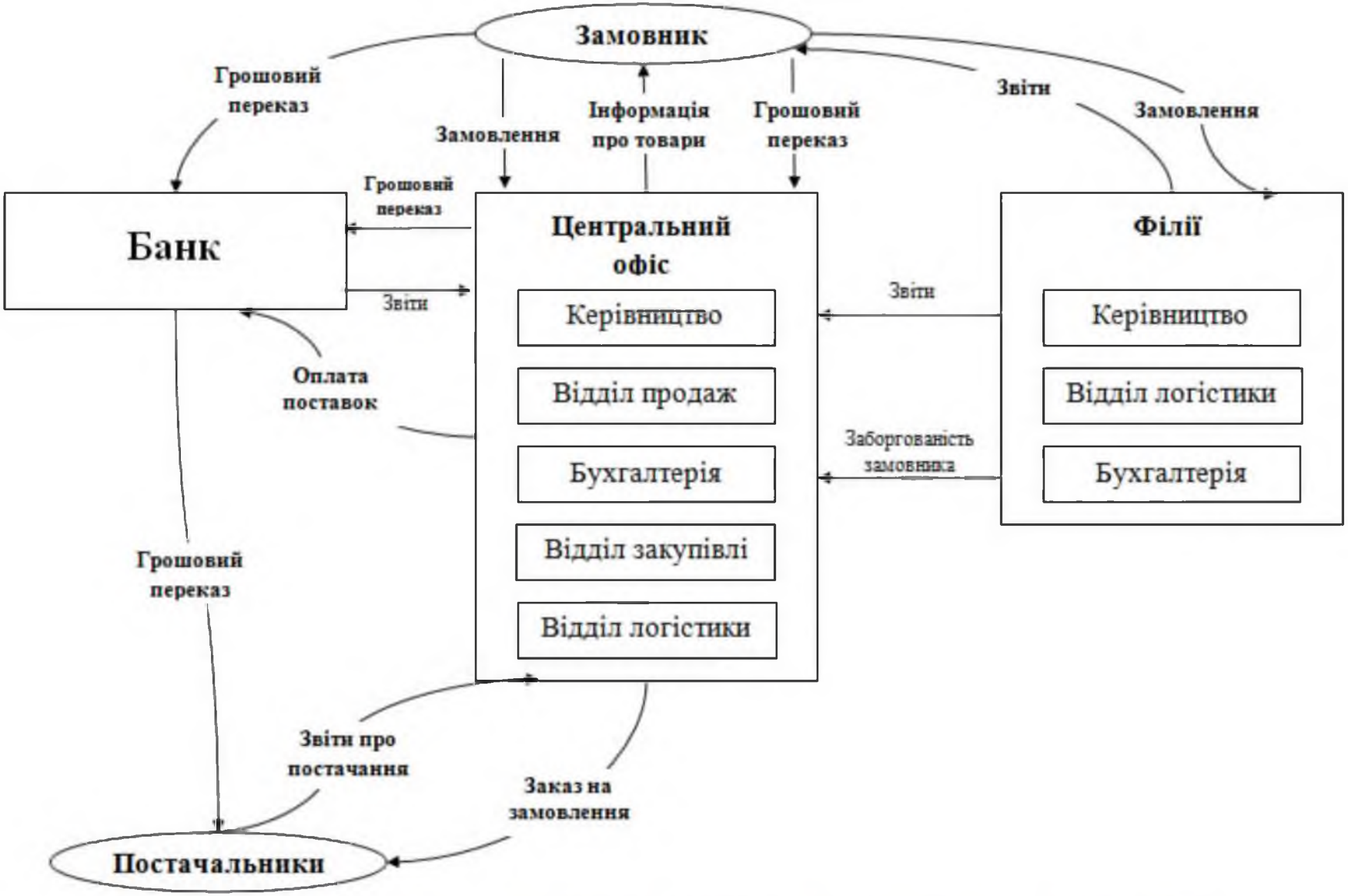

Рисунок 1.3 – Типова схема інформаційних потоків торгівельного підприємства

До відкритої інформації належить:

– техногенні и антропогені загрози;

– відомості, що містяться в статуті організації;

– фінансова звітність;

– склад керівництва тощо;

– інформація про вакансії та відомості про чисельність і склад працівників, про умови їх праці, про систему оплати праці;

– контакти менеджерів компанії.

До інформації з обмеженим доступом на підприємстві відноситься конфіденційна інформація. Конфіденційна інформація - інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, та яка може поширюватися у визначеному ними порядку за їхнім бажанням відповідно до передбаченими ними умовами.

Розпорядники інформації, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди - лише в інтересах національної безпеки, економічного добробуту та прав людини.

Цілі захисту інформації:

– запобігання витоку, розкрадання, спотворення, підробки інформації;

– запобігання загрозам безпеки особистості, суспільства, держави;

– запобігання несанкціонованих дій по знищенню, модифікації,

– копіювання, блокування інформації; запобігання інших форм незаконного втручання в інформаційні ресурси та інформаційні системи, забезпечення правового режиму як об'єкта власності;

– захист конституційних прав громадян на збереження особистої таємниці, конфіденційності персональних даних, наявних в інформаційних системах;

– конфіденційності документованої інформації згідно з законодавством.

На торгівельних підприємствах до конфіденційної відноситься наступна інформація:

У сфері управління:

– про перспективні методи управління;

– планові відомості;

– розвиток підприємства;

– інвестиції фірми;

– закупівля і продаж;

– про проекти річних і перспективних експортно-імпортних планах по зовнішньоекономічним організаціям;

– обсяг майбутніх закупівель за термінами, асортименту, цінам, країнам, фірмам.

У сфері фінансів:

– планові та фактичні показники фінансового плану;

– вартість товарних запасів;

– дані про баланси підприємства;

– майновий стан;

– бюджет, обороти, дані про обороти грошових потоків підприємства;

– банківські операції, дані про фінансові операції;

– банківські зв'язки;

– специфіка міжнародних розрахунків з інофірмами;

– планові та звітні дані по валютних операціях;

– рівень доходів;

– боргові зобов'язання;

– стан кредиту;

– розміри та умови банківських кредитів;

– джерела кредитів;

– генеральна лінія і тактика у валютних та кредитних питаннях.

У ринковій сфері:

– містять висновки та рекомендації фахівців щодо стратегії і тактики діяльності фірми;

– комерційно-аналітичні цілі фірми;

– про час виходу на ринок при закупівлях товарів і виборі фірм для ведення комерційних переговорів;

– політика зовнішньоекономічної діяльності в цілому і по регіонах;

– про продажі товару на новому ринку;

– місця закупівлі товару.

Про партнерів:

– коло клієнтів;

– списки представників і посередників;

– комерційні зв'язки;

– дані про постачальників і клієнтів;

– про фінансовий стан, репутацію та інші дані, що характеризують ступінь надійності фірми або представників як торгівельного партнера.

У сфері переговорів:

– про одержувані та оброблювані замовлення та пропозиція;

– про факти підготовки та ведення переговорів;

– терміни, які виділені для опрацювання та ведення угоди;

– директиви з проведення переговорів, включаючи тактику, межі повноважень посадових осіб за цінами, знижкам;

– про заходи, що проводяться перед переговорами;

– про хід і результати комерційних переговорів та результати зовнішньоекономічних угод;

– про ділові прийоми.

Про контракти:

– умови контрактів, що включають особі умови контракту (знижки, доплати, розстрочки платежів);

– умови платежу за контрактами.

Про ціни:

– розрахунок цін;

– структура ціни і калькуляції;

– дані для калькуляції цін;

– внутрішні прейскуранти і тарифи;

– про собівартість і контрактні ціни товарів і послуг.

Про співробітників:

– домашні адреси, телефони, паспортні дані, ідентифікаційний код та інші особисті дані;

– стан здоров'я.

Серед конфіденційної інформації, що циркулює на підприємстві, необхідно виділити критичну інформацію, тобто інформацію, що вимагає підвищеного ступеня захисту, так як порушення її властивостей призведе до найбільших збитків.

До критичної інформації відносяться:

– інформація про клієнтів, їх контактні і особисті дані;

– інформація про проекти, терміни і умови договорів;

– інформація про постачальників, споживачів, ціни;

– інформація про доходи і т.д.

Розглянемо перелік загроз та їх опис на основі стандарту ISO/IEC PDTR 13335.

1 Підробка ідентифікатора користувача. Підробка пароль та ідентифікатор працівника з метою отримання доступу до його інформації.

Об'єкт нападу - суттєва інформація.

Тип втрати: затруднення (ускладнення) в діяльності, втрати продуктивності, грошові втрати, цілісність інформації.

Масштаб збитку - високий

Джерело загрози: хакери.

Досвід: професійний досвід.

Знання: спеціалізовані.

Доступні ресурси, необхідні для реалізації загрози: відповідне програмне та апаратне забезпечення ПК.

Можлива мотивація дій: навмисне.

2 Доступ до мережі неавторизованих користувачів. Проникнення в електромережу організації з метою отримання доступу до інформації.

Об'єкт нападу - конфіденційна інформація.

Тип втрати: грошові втрати, труднощі в діяльності, втрата продуктивності, цілісність інформації.

Масштаб збитку - високий

Джерело загрози: хакери.

Досвід: професійний досвід.

Знання: спеціалізовані.

Доступні ресурси, необхідні для реалізації загрози: відповідне програмне та апаратне забезпечення ПК.

Можлива мотивація дій: навмисне.

3 Шкідливе програмне забезпечення. Віруси, що ускладнюють роботу системи та програми.

Об'єкт нападу - конфіденційна інформація.

Тип втрати: грошові втрати, труднощі в діяльності, втрата продуктивності, цілісність інформації.

Масштаб збитку: попередньо високі.

Джерело загрози: віруси.

Досвід: професійний.

Знання: спеціалізовані.

Доступні ресурси, необхідні для реалізації загрози: відсутні.

Можлива мотивація дій: відсутня.

4 Помилки користувачів. Ненавмисне видалення, редагування інформації користувачами.

Об'єкт нападу - суттєва інформація.

Тип втрати: утруднення в діяльності, втрата продуктивності, цілісність, доступність.

Масштаб збитку: попередньо високий.

Джерело загрози: персонал.

Досвід: початковий.

Знання: відсутні.

Доступні ресурси, необхідні для реалізації загрози: відповідне програмне забезпечення ПК.

Можлива мотивація дій: халатність, недбалість.

5 Перезавантаження трафіку. Дія, спрямована на виявлення контактів організації з іншими фізичними особами і організаціями.

Об'єкт нападу - конфіденційна інформація.

Тип втрати: втрата конфіденційності.

Масштаб збитку-високий

Джерело загрози: хакери.

Досвід: професійний.

Знання: спеціалізовані.

Доступні ресурси, необхідні для реалізації загрози: ПК і спеціалізоване устаткування.

Можлива мотивація дій: навмисне.

6 Перехоплення. Дія, спрямована на виявлення контактів організації з іншими фізичними особами і організаціями, а також викрадення важливої інформації (несанкціоноване копіювання).

Об'єкт нападу - інформація про клієнтів, продажі і т.д.

Тип втрати: втрата конфіденційності.

Масштаб збитку - високий

Джерело загрози: хакери.

Досвід: професійний.

Знання: спеціалізовані.

Доступні ресурси, необхідні для реалізації загрози: відповідне ПК і ПЗ.

Можлива мотивація дій: навмисне.

7 Пошкодження в лініях зв'язку. Фізичне пошкодження в лініях зв'язку, розриви.

Об'єкт нападу - робочий процес, мережа.

Тип втрати: зниження продуктивності, доступність.

Масштаб збитку: середній.

Джерело загрози: персонал.

Досвід: відсутній.

Знання: відсутні.

Доступні ресурси, необхідні для реалізації загрози: відсутні.

Можлива мотивація дій: халатність, недбалість.

8 Технічна несправність компонентів мережі. Вихід з ладу компонентів мережі (комутатор, маршрутизатор, сервери).

Об'єкт нападу - робочий процес, мережа.

Тип втрати: зниження продуктивності, доступність.

Масштаб збитку – високий.

Джерело загрози: хакери

Досвід: професійний.

Знання: спеціалізовані.

Доступні ресурси, необхідні для реалізації загрози: відсутні.

Можлива мотивація дій: відсутній.

9 Помилка технічного обслуговування. Дія представляє собою зниження продуктивності і пошкодження (несправності) обладнання і апаратури.

Об'єкт нападу - робочий процес.

Тип втрати: зниження продуктивності, доступність.

Масштаб збитку-високий.

Джерело загрози: системний адміністратор.

Досвід: початковий.

Знання: відсутні.

Доступні ресурси, необхідні для реалізації загрози: відсутні.

Можлива мотивація дій: недбалість, ненавмисно.

10 Збій програмного забезпечення. Ця загроза є незапланованою втратою доступності частини робочого процесу у зв'язку з неполадками.

Об'єкт нападу - робочий процес.

Тип втрати: зниження продуктивності.

Масштаб збитку: середній.

Джерело загрози: відсутній.

Досвід: відсутній

Знання: відсутні.

Доступні ресурси, необхідні для реалізації загрози: відсутні.

Можлива мотивація дій: відсутній.

11 Неправильна маршрутизація повідомлень. Помилкове перенаправлення повідомлень.

Об'єкт нападу - суттєва інформація.

Тип втрати: втрата продуктивності, доступність, конфіденційність.

Масштаб збитку - високий.

Джерело загрози: системний адміністратор.

Досвід: не обов'язковий.

Знання: не обов'язкові.

Доступні ресурси, необхідні для реалізації загрози: мережеві засоби, ПК.

Можлива мотивація дій: ненавмисно.

12 Помилки при передачі. Помилкове перенаправлення повідомлень і невірна передача, пошкодження повідомлення.

Об'єкт нападу - суттєва інформація.

Тип втрати: втрата продуктивності, доступність, конфіденційність.

Масштаб збитку - високий.

Джерело загрози: системний адміністратор.

Досвід: не обов'язковий.

Знання: не обов'язкові.

Доступні ресурси, необхідні для реалізації загрози: мережеві засоби, ПК.

Можлива мотивація дій: ненавмисно.

13 Умисне пошкодження. Навмисна псування, обладнання, апаратури.

Об'єкт нападу - робочий процес.

Тип втрати: зниження продуктивності, доступність.

Масштаб збитку - середній.

Джерело загрози: персонал.

Досвід: не обов'язковий.

Знання: не обов'язкові.

Доступні ресурси, необхідні для реалізації загрози: не обов'язкові.

Можлива мотивація дій: злий умисел.

Термін зона локальної уразливості використовується для позначення нестачі у систему, використовуючи яку, можна навмисно порушити її цілісність і викликати неправильну роботу. Розглянемо відомі зони локальної вразливості інформаційної безпеки торгівельних підприємств:

1 Персонал

Вразливість цієї зони зв'язані зі службовцями, постачальниками і персоналом, що працює за контрактом. Вони стосуються навичок службовця, а також його обізнаності та проходження відомчих операційних процедур та захисним заходам.

2 Обладнання та апаратура

Вразливість цієї зони пов'язана з фізичною безпекою робочих зон і апаратури, а також доступу до них.

3 Комунікації

Вразливість цієї зони пов'язані з електронним рухом інформації між двома кінцевими точками.

4 Програмне забезпечення, що відноситься до середовища і операційні системи

Вразливість цієї зони пов'язані з програмним забезпеченням операційних систем і підсистем, у межах яких програми розробляються і виконуються.

5 Поштовий сервер

Вразливість цієї зони пов'язані з низькою захищеністю протоколів (POP3).

6 Інтернет

Вразливість цієї зони пов'язані з можливістю проникнення шкідливого ПЗ і несанкціонованого доступу.

7 Лінії зв'язку

Вразливість цієї зони пов'язані з можливістю фізичного пошкодження. Існує кілька категорій можливих втрат. Розглянемо їх:

1) грошова втрата.

Грошова втрата визначається як втрата цінностей або збільшення вартості або витрат. У сумнівних випадках необхідно класифікувати більш високий ризик грошової втрати або більш високе можливе значення втрати, більш високий ризик функціонування бізнесу.

2) втрата продуктивності.

Втрата продуктивності відбувається тоді, коли персонал не здатний продовжувати виконання своїх обов'язків або коли необхідно повторювати службові обов'язки. Переривання роботи або дублювання зусиль можуть призводити до недоступності бізнес-функцій або до некоректності результатів.

3) труднощі для організації.

Ця категорія стосується ситуацій, що впливають на встановлення суспільної довіри. Слід враховувати також конфіденційність, точність і узгодженість [7].

У таблиці 1.2 надані види загроз інформаційної безпеки, зони уразливості, а також ризики, до яких вони можуть призвести.

Таблиця 1.2 – Види загроз, що впливають на діяльність торгівельного підприємства

Вид загрози	Зона уразливості	Ризик
Підробка ідентифікатора користувача	Персонал, обладнання та апаратура	Труднощі в діяльності, втрати продуктивності, грошові втрати, цілісність інформації
Доступ до мережі неавторизованих користувачів	Мережеві засоби, обладнання і апаратура	Труднощі в діяльності, втрати продуктивності, грошові втрати, цілісність інформації
Вид загрози	Зона вразливості	Ризик

Вид загрози	Зона уразливості	Ризик
Шкідливе програмне забезпечення	Поштовий сервер, носій інформації, Інтернет, ПЗ, ОЗ	Грошові втрати, труднощі в діяльності, втрата продуктивності, цілісність інформації
Помилки користувачів	Персонал	Труднощі в діяльності, втрата продуктивності, цілісність, доступність
Перезавантаження трафіку	Мережеві засоби, обладнання і апаратура	Втрата конфіденційності
Перехоплення	Мережеві засоби, обладнання і апаратура	Втрата конфіденційності
Пошкодження ліній зв'язку	Персонал, мережа, лінія зв'язку	Зниження продуктивності, доступність
Технічна несправність компонентів мережі	Системний адміністратор, обладнання апаратура, комунікація	Зниження продуктивності, доступність
Помилка технічного обслуговування	Адміністратор, обладнання апаратура, комунікація	Зниження продуктивності, доступність
Збій програмного забезпечення	Програмне забезпечення, операційна система	Зниження продуктивності
Неправильна маршрутизація повідомлень	Мережеве обладнання, ПЗ, ОЗ	Втрата продуктивності, доступність, конфіденційність
Помилки при передачі	Мережеве обладнання, ПЗ, ОЗ	Втрата продуктивності, доступність, конфіденційність
Умисне пошкодження	Персонал, обладнання, апаратура	Зниження продуктивності, під'їзд
Некомпетентність персоналу	Персонал	Зниження продуктивності

В таблиці 1.3 наведено ступінь впливу загроз на ризики, зокрема ступінь ризику грошової втрати, ступінь ризику втрати продуктивності та ступінь ризику труднощів.

Таблиця 1.3 – Ступінь впливу загрози на певні ризики

Загроза	Ступінь ризику грошової втрати	Ступінь ризику втрати продуктивності	Ступінь ризику труднощів виконання	Загальний ризик
Підробка ідентифікатора користувача	Високий	Середній	Високий	Високий
Доступ до мережі неавторизованих користувачів	Високий	Високий	Високий	Високий
Шкідливе програмне забезпечення	Середній	Високий	Високий	Високий
Помилки користувачів	Високий	Середній	Середній	Середній
Перезавантаження трафіку	Високий	Низький	Високий	Високий
Перехоплення	Високий	Середній	Високий	Високий
Пошкодження ліній зв'язку	Низький	Високий	Середній	Середній
Технічна несправність компонентів мережі	Низький	Високий	Середній	Середній
Помилка технічного обслуговування	Низький	Високий	Середній	Середній
Збій програмного забезпечення	Низький	Високий	Середній	Середній
Неправильна маршрутизація повідомлень	Низький	Середній	Середній	Середній
Помилки при передачі	Низький	Високий	Високий	Високий
Умисне пошкодження	Високий	Середній	Високий	Високий
Некомпетентність персоналу	Низький	Середній	Середній	Середній

1.4 Аналіз ризиків інформаційної безпеки

Однією з найбільш відповідальних і складних завдань, що вирішуються в процесі створення СУІБ, слід назвати проведення аналізу ризиків інформаційної безпеки щодо активів організації в обраній галузі діяльності і прийняття вищим керівництвом рішення про вибір заходів протидії виявленим ризикам.

Аналіз ризиків - це основний рушійний процес СУІБ. Він виконується не тільки при створенні СУІБ, але і періодично при зміні бізнес-процесів організації та вимог з безпеки.

У процедурі аналізу ризиків повинні бути ідентифіковані критерії прийняття ризиків і прийнятні рівні ризику. Ці критерії мають базуватися на досягненні стратегічних, організаційних і управлінських цілей організації.

Керівництво компанії використовує дані критерії, приймаючи рішення щодо прийняття контрзаходів для протидії виявленим ризикам. Якщо виявлений ризик не перевищує встановленого рівня, він є прийнятним, і подальші заходи по його обробці не проводяться. У разі ж, коли виявлений ризик перевищує прийнятний рівень критичності загрози, вище керівництво повинне прийняти одне з таких можливих рішень:

- зниження ризику до прийнятного рівня за допомогою застосування відповідних контрзаходів;
- прийняття ризику;
- уникнути ризику;
- переклад ризику в іншу область, наприклад, за допомогою його страхування [23].

Після проведення аналізу можливих підходів до оцінювання ризиків ІБ був обраний цей метод розрахунку рівня ризиків на основі критичності та ймовірності реалізації загрози [22].

Розрахуємо рівень ризиків Th_i на основі критичності та ймовірності реалізації i загрози через дану уразливість. Рівень ризиків показує, наскільки критичним є вплив i загрози на ресурс з урахуванням ймовірності її реалізації.

$$Th_i = \frac{ER_i}{100} \cdot \frac{P(V_i)}{100}, \quad (1.1)$$

де ER_i - критичність реалізації i загрози (вказується у %); $P(V_i)$- ймовірність реалізації i загрози через дану уразливість (вказується у %).

Сумарний ризик розраховується:

$$Th_{\Sigma} = \frac{\sum_{i=1}^{n} Th_i}{n}, \quad (1.2)$$

де n - кількість загроз.

Отримуємо значення рівня загрози по уразливості в інтервалі від 0 до 1. Розрахуємо для кожної загрози окремо (табл. 1.4).

Таблиця 1.4 – Аналіз ризиків інформаційної безпеки типового торгівельного підприємства

Загроза інформаційної безпеки (i)	Критичність реалізації загрози (ER_i)	Імовірність реалізації загрози ($P(V_i)$)	Загальний ризик (Th_i)
Підробка ідентифікатора користувача	65%	100%	0,65
Доступ до мережі неавторизованих користувачів	50%	100%	0,50
Шкідливе програмне забезпечення	70%	80%	0,56
Помилки користувачів	30%	60%	0,18
Перезавантаження трафіку	80%	100%	0,80
Перехоплення	80%	100%	0,80
Пошкодження ліній зв'язку	20%	30%	0,06
Технічна несправність компонентів мережі	15%	40%	0,06

Продовження таблиці 1.4

Помилка технічного обслуговування	30%	50%	0,15
Збій програмного забезпечення	50%	50%	0,25
Неправильна маршрутизація повідомлень	70%	100%	0,70
Помилки при передачі	40%	20%	0,08
Умисне пошкодження	80%	100%	0,80
Некомпетентність персоналу	60%	80%	0,48
Сумарний ризик (Th_{Σ})			0,43

Отриманий показник $Th_{\Sigma} = 0,43$, трохи менше половини, що вимагає вдосконалення системи інформаційної безпеки на торгівельних підприємствах.

1.5 Висновок. Постановка задачі

Таким чином, можна зробити висновок, що існує висока потреба удосконалення існуючої системи інформаційної безпеки торгівельних підприємств.

Основними цілями захисту інформації на типовому торгівельному підприємстві є:

– запобігання загроз безпеки підприємства внаслідок несанкціонованих дій по знищенню, модифікації, спотворення, копіювання, блокування інформації або інших форм незаконного втручання в інформаційні ресурси та інформаційних системах;

– збереження конфіденційної інформації, що обробляється з використанням засобів обчислювальної техніки;

– захист конституційних прав громадян на збереження особистої таємниці та конфіденційності персональних даних, наявних в інформаційних системах.

– завдання формування системи управління інформаційної безпеки в організації є: цілісність інформації, достовірність інформації та її конфіденційність. При виконанні поставлених завдань, мета буде реалізована.

Задачі роботи:

1 Розробити комплекс заходів та рекомендацій щодо створення системи управління інформаційної безпеки;

2 Провести впровадження створеної СУІБ на торгівельному підприємстві «Автохімія»;

3 Розрахувати ризики інформаційної безпеки.

РОЗДІЛ 2. СПЕЦІАЛЬНА ЧАСТИНА

2.1 Розробка узагальнених рекомендацій щодо впровадження СУІБ

Розробка та виконання політики ІБ організації є найбільш ефективним способом мінімізації ризиків порушення ІБ для власника. Політика безпеки являє собою звід принципів і правил безпеки для найбільш важливих областей діяльності і зон відповідальності персоналу. Політика інформаційної безпеки є планом високого рівня, в якому описуються цілі і завдання заходів у сфері безпеки.

Торгівельне підприємство має забезпечувати захист інформаційних, обчислювальних, комунікаційних і апаратних ресурсів, стежити за функціонуванням систем, створювати захисні заходи для ефективної працездатності та якісної продуктивності.

Вся інформація, що знаходиться в торгівельному підприємстві, повинна бути конфіденційною, цілісної, надійної, якісної, захищеною. Їй управляє адміністратор, захищає – адміністратор ІБ. У відділенні повинні забезпечуватися:

– функціонування системи парольного захисту електронних обчислювальних машин і локальних обчислювальних мереж. Повинна бути організована служба централізованої парольного захисту для генерації, зміни, видалення паролів, розробки необхідних інструкцій, контролю за діями персоналу по роботі з паролями;

– формування унікальних ідентифікаторів повідомлень і ідентифікаторів користувачів;

– здійснення перевірки запитів даних по паролів, ідентифікаторам;

– функціонування системи обмеженого доступу до сервера і використанню ресурсів Інтернет;

– зберігання БД та копій БД в певних захищаються місцях;

– застосування шифрування інформації криптографічними і стеганографічними методами і засобами;

– забезпечення ефективного захисту каналах і засобам зв'язку (проводи, телефони та ін.)

– взаємодії кількох АРМ один з одним, що виконують однакові повноваження;

– створення сприятливих умов і місце праці співробітникам відділення;

– відсутність можливої появи шкідливого ПЗ або застосування боротьби з ним.

На етапі оцінювання загроз інформаційної безпеки необхідно звернути увагу на основні зони вразливості ІБ та види захисних заходів:

1 Пожежа. Обладнати пожежну сигналізацію; встановити необхідну кількість вогнегасників; призначити відповідального за пожежну безпеку; провести інструктаж з пожежної безпеки з працівниками відділення; виконувати планові та позапланові перевірки справності проводки.

2 Умисне пошкодження. Створити скрутний доступ до проводами ін каналах зв'язку, забезпечити відділення камерами спостереження та додаткової сигналізацією, попередити про покарання у разі навмисної поломки.

3 Несправності апаратних засобів. Своєчасна заміна та ремонт обладнання; ізолювати від сторонніх осіб важливі апаратні засоби, щоб виключити навмисне і випадкове пошкодження; проводити періодичні перевірки справності апаратних засобів.

4 Знос середовища зберігання. Здійснення поновлення БД та апаратної частини; зберігання копій БД на окремому комп'ютері.

5 Збій програмного забезпечення. Створювати резервні копії; постійно оновлювати ПЗ; обмежити користування неліцензійними копіями ПЗ.

6 Підробка ідентифікатора користувача. Забезпечити кожен ПК унікальним паролем. Паролі повинні відповідати наступним вимогам:

1) Довжина пароля повинна бути не менше 8 символів;

2) В числі символів пароля обов'язково повинні бути присутніми букви, цифри і спеціальні символи;

3) Пароль не повинен включати в себе легко обчислювані поєднання символів (імена, прізвища, і т.д.);

4) При зміні пароля нове значення має відрізнятися від попереднього не менш, ніж в 4 позиціях;

5) Зміна паролів повинна проводитися регулярно не рідше одного разу на місяць;

6) Однакових паролів не повинно бути.

7 Шкідливе програмне забезпечення. Захист ПЗ за допомогою антивірусних програм; ніколи не копіювати на свій диск програми, що не перевірені на наявність вірусу; не копіювати програми з ненадійних джерел; вести уважне спостереження за новою програмою (бажано експлуатувати її на спеціальному комп'ютері); мати копії всіх цінних програм і зберігати їх на захищених дисках; встановити по можливості системних файлів атрибут «тільки для читання»; мати системний диск з антивірусними програмами [12].

8 Доступ до мережі неавторизованих користувачів. Контролювати дії неавторизованого користувача; покласти відповідальність за будь-які несправності; повідомляти адміністратора про відомих входах в мережу неавторизованим способом.

9 Помилка персоналу. Обмежити рівень допуску відповідно з необхідністю; набір тільки кваліфікованого персоналу; проведення семінарів з навчання роботи з новим ПЗ.

10 Технічна несправність компонентів мережі. Постійно стежити за компонентами мережі; своєчасний ремонт і заміна обладнання; заборонити доступ до компонентів мережі, крім технічного обслуговування.

11 Помилки при передачі. Використання різних алгоритмів поділу файлів при передачі; перевірка контрольних сум.

12 Пошкодження в лініях зв'язку. Забезпечити скрутний доступ до ліній зв'язку; розташувати проводи ближче до стелі і прибрати їх у коробки.

13 Перехоплення. Унеможливити прямий доступ до мережі; кодувати всю інформацію при передачі; аналізувати трафік.

14 Помилкова маршрутизація повідомлень. Виключити помилкову передачу відомостей з локальної мережі по мережі Інтернет; вести таблицю маршрутизації і постійно її оновлювати, відсилаючи запити.

15 Повторна маршрутизація повідомлень. Виключити помилкову передачу відомостей з локальної мережі по мережі Інтернет; вести таблицю маршрутизації і постійно її оновлювати, відсилаючи запити.

16 Неправильне використання ресурсів. Встановити пріоритет на запити; обмежити доступ до них для всіх на певній час; використовувати багатоканальний доступ.

Розглянемо декілька *певних* загроз торгівельних підприємств:

1) Антивірусне програмне забезпечення. Необхідно, щоб на торговому підприємстві використовувалася хороша антивірусна програма. Але співробітники мають низьку кваліфікацію в сфері інформаційних технологій. Отже, виникають проблеми з оновленням антивірусу, з конфігурацією антивірусу, або з виконанням видаленням вірусом. Ризики пов'язані з низькою кваліфікацією персоналу виходить на перший план;

2) Халатність персоналу при роботі з конфіденційною інформацією, інсайд, промислове шпигунство і багато іншого. Співробітник компанії, не обізнана про правила роботи з конфіденційною корпоративною інформацією або нехтує базовими принципами безпечної роботи, вже несе в собі потенційну загрозу. А до більшості співробітників на регулярній основі не доносяться правила безпечної роботи в цілому і з конфіденційними даними зокрема. Змушувати співробітників виконувати якісь правила і сподіватися, що це забезпечить захист не має сенсу. Набагато правильніше провести аудит власної системи безпеки і створити такі умови роботи, щоб у співробітника не було і можливості нашкодити. Тут ще позначаються особливості менталітету, коли головний бухгалтер, фінансовий або навіть генеральний директор можуть дозволяти собі ігнорувати обмеження, які IT-спеціалісти вводять в цілях забезпечення безпеки;

3) Спам дійсно може стати причиною серйозних втрат. Досить часто зустрічаються випадки, коли через поштові розсилки співробітники компанії потрапляють на сайти, з яких на їх робочі комп'ютери закачується програмне забезпечення або для доступу до корпоративних файлових серверів, або для підготовки DDoS-атаки;

4) Поширення шкідливого ПЗ (віруси, черв'яки, трояни). Якщо з шкідливим ПЗ можливо боротися, то не варто вважати цю загрозу не небезпечною. Адже за допомогою такого ПЗ може відбутися витік конфіденційної інформації.

У торгівельних підприємствах обов'язково необхідно стежити і забезпечувати безпеку інформації за складеними правилам і вимогам. У цьому випадку підвищиться ймовірність уникнути небажаних наслідків і зменшаться ризики втрат.

Після проведення аналізу загроз ІБ необхідно розробити контрзаходи по їх знищенню. Ґрунтуючись на аналізованих раніше загрозах розроблені наступні більш розгорнуті контрзаходи [27].

Підробка ідентифікатора користувача може бути використана для того, щоб обійти аутентифікацію і пов'язані з нею послуги і функції забезпечення безпеки. Це може привести до порушення конфіденційності всякий раз, коли така підробка забезпечує доступ до конфіденційної інформації. Захисні заходи від цієї загрози включають в себе:

– ідентифікацію і аутентифікацію

Підробка під особу законного користувача утруднюється, якщо захисні заходи ідентифікації і аутентифікації засновані на комбінації того, що відомо користувачеві, або того, чим він володіє, або властивих тільки йому характеристиках;

– логічне керування і аудит доступу

Логічне керування доступом не здатна робити різницю між санкціонованим користувачем і будь-ким, маскуються під санкціонованого користувача, але застосування механізмів управління доступом на робочому

місці може зменшити зону впливу. Розгляд та аналіз контрольних журналів реєстрації дозволить виявити несанкціоновані дії;

– захист від шкідливого коду

Так як один із способів отримання паролів пов'язаний з впровадженням шкідливого коду для їх перехоплення, то слід встановити місцеву захист від таких програм;

– управління мережею

Іншим способом захоплення секретного матеріалу є підробка під законного користувача в трафіку, наприклад електронною поштою. В даний час міжнародна організація по стандартизації (ISO) розробляє кілька документів, що містять додаткову інформацію про докладних захисних заходи щодо забезпечення безпеки мереж;

– збереження конфіденційності даних

Якщо з якоїсь причини згаданий вище спосіб забезпечення безпеки неможливий або недостатній, то додаткова захист може бути забезпечений шляхом зберігання конфіденційних даних у зашифрованому вигляді.

Доступ до мережі неавторизованих користувачів може стати загрозою, якщо можливий доступ до будь-якого секретного матеріалу. Захисні заходи від несанкціонованого доступу включають в себе відповідне упізнання й перевірку реєстрації, логічне керування доступом, аудит на рівні системи IT і поділ мереж на мережевому рівні:

– ідентифікацію та аутентифікацію

Захисні заходи шляхом відповідного впізнання та перевірки реєстрації слід використовувати в комбінації з логічним управлінням доступом для попередження несанкціонованого доступу;

– логічне керування і аудит доступу

Захисні заходи, повинні використовуватися для логічного керування доступом через використання механізмів управління доступом. Розгляд та аналіз контрольних журналів реєстрації дозволяє виявляти несанкціоновані види діяльності користувачів з правами доступу в систему;

– поділ мереж

Для утруднення несанкціонованого доступу, повинно застосовуватися місцеве поділ мереж;

– фізичне управління доступом

Крім логічного, може застосовуватися фізичне управління доступом;

– управління носіями даних

Якщо конфіденційна інформація зберігається на портативних чи інших носіях, то організація повинна встановити місцеве управління носіями даних для їх захисту від несанкціонованого доступу;

– збереження конфіденційності даних

Якщо з якоїсь причини управління носіями даних неможливо або недостатньо, то додаткова захист може забезпечуватися шляхом зберігання конфіденційних даних у зашифрованому

– цілісність даних

Засоби криптографії можна використовувати для захисту цілісності інформації в пристрої або під час її передачі.

Шкідливе програмне забезпечення створює загрозу цілісності інформації в пристрої і при обробці її в системі, якщо ці програми і дані використовуються для незаконної зміни інформації або містять шкідливий код. Захисні заходи у цій галузі включають в себе:

– обізнаність та навчання з питань безпеки

До відома всього персоналу повинна бути доведена інформація про заборону встановлення і використання будь-якого програмного забезпечення без дозволу адміністратора системи ІТ або відповідального за безпеку цієї системи;

– резервні копії

Резервні копії слід використовувати для відновлення пошкодженої інформації;

– ідентифікацію та аутентифікацію

Відповідні захисні заходи за допомогою ідентифікації і аутентифікації повинні використовуватися спільно з логічним управлінням доступом для попередження несанкціонованого проникнення;

– логічне керування і аудит доступу

Логічне керування доступом повинно забезпечувати застосування програмного забезпечення для обробки та зміни інформації тільки уповноваженими користувачами. Перегляд та аналіз журналів реєстрації дозволяє виявляти несанкціоновані види діяльності;

– захист від шкідливого коду

Помилки користувачів може порушити цілісність інформації. Захисні заходи для цілісності інформації включають в себе:

– обізнаність у питаннях безпеки і відповідне навчання

Організація повинна провести навчання всіх користувачів для того, щоб вони не допускали помилок при обробці інформації. У програму навчання має бути включено вивчення певних методик для спеціальних дій, наприклад процедури з експлуатації і забезпечення безпеки;

– резервні копії

Резервні копії, наприклад попереднє покоління програмного забезпечення, можуть бути використані для відновлення цілісності інформації, пошкодженої в результаті помилок користувача.

Перезавантаження трафіку загрожує доступності інформації, переданої через надані послуги. Захисні заходи у цій галузі включають в себе:

– резервування і резервні копії

Впровадження резервування компонентів комунікаційних послуг може застосовуватися для зниження ймовірності перевантаження трафіку. Залежно від максимального допустимого часу вимушеного простою може бути передбачено резервне обладнання для виконання встановлених вимог. Дані про конфігурацію і компонувальному плані повинні резервуватися для забезпечення їх доступності в аварійних ситуаціях.

– управління мережею

Організація повинна використовувати правильну конфігурацію, менеджмент і адміністрування;

– мереж і послуг зв'язку

В даний час міжнародна організація по стандартизації (ISO) розробляє кілька документів, що містять додаткову інформацію про докладних захисних заходи щодо забезпечення безпеки мережі, застосовну для захисту від перевантаження трафіку.

Перехоплення може загрожувати збереженню конфіденційності, якщо вкрадений компонент містить конфіденційну інформацію, яка може виявитися доступною. Захисні заходи проти розкрадання включають в себе:

– фізичну захист

Це може бути технічний захист, що утрудняє доступ в будівлю, зону або приміщення з обладнанням ІТ, або спеціальні захисні заходи від розкрадання;

– персонал

Захисні заходи для персоналу (управління доступом персоналу та / або сторонніх осіб, угоди про збереження конфіденційності і т.д.) повинні підтримуватися в робочому стані, утруднюючи можливість розкрадання;

– збереження конфіденційності даних

Такий захист слід впровадити, якщо існує ймовірність викрадення обладнання ІТ, що містить конфіденційну інформацію, наприклад невеликий портативний комп'ютер.

– засоби контролю носіїв інформації

Будь-які носії інформації, що містять секретні матеріали, повинні охоронятися від розкрадання.

Пошкодження ліній зв'язку загрожують доступності інформації, переданої через ці комунікаційні послуги. Залежно від причини несправності або порушення комунікаційних послуг корисно звернути увагу на збої програмного забезпечення, подачі електроживлення або інші технічні несправності. Захисні заходи доступності включають в себе:

– резервування і резервні копії

Впровадження резервування компонентів комунікаційних послуг може застосовуватися для зниження ймовірності порушення їх роботи. Залежно від максимального допустимого часу вимушеного простою може бути передбачено резервне обладнання для виконання встановлених вимог. Дані про конфігурацію і компонувальному плані повинні резервуватися для забезпечення їх доступності в аварійних ситуаціях;

– управління мережею

В даний час міжнародна організація по стандартизації (ISO) розробляє кілька документів, що містять додаткову інформацію про докладних захисних заходи щодо забезпечення безпеки мережі, застосовну для захисту від збоїв в роботі комунікаційних апаратури і послуг;

– прокладку кабелів

Планування і відповідна прокладка кабелів дозволяють уникнути пошкоджень. У разі підозри несправності на лінії зв'язку її слід перевірити;

– неспростовності

Якщо потрібне підтвердження мережевих передач, відправлення або прийому повідомлень, організація повинна забезпечити неспростовності. У цьому випадку легко можуть бути виявлені несправності зв'язку або пропущена інформація.

Технічна несправність компонентів мережі [18] можуть порушувати доступність будь-якої інформації, що зберігається або обробляється в мережі. Захисні заходи цій області включають в себе:

– експлуатаційні питання

Управління конфігурацією і змінами, а також управління пропускною здатністю повинні використовуватися для того, щоб не допускати несправностей в системі ІТ або мережі. Документація і технічне обслуговування застосовуються для забезпечення безаварійної роботи системи;

– управління мережею

Організація повинна використовувати операційні процедури, планування системи і правильну конфігурацію мережі для того, щоб звести до мінімуму ризик від технічних несправностей;

– план безперервності бізнесу

Для захисту бізнесу від згубних впливів технічних несправностей, організація повинна розробити і впровадити план безперервності бізнесу, а також створити доступні резерви всієї важливої інформації, послуг і ресурсів.

Помилка технічного обслуговування. Якщо технічне обслуговування проводиться нерегулярно або з помилками, то цілісність всієї порушеної інформації знаходиться під загрозою. Захисні заходи цілісності в цьому випадку включають в себе:

– технічне обслуговування

Правильне технічне обслуговування є найкращим способом уникнути помилок при огляді і ремонті. Технічне обслуговування включає в себе документовані верифіковані процедури з технічного обслуговування, і відповідний контроль за проведенням робіт;

– резервні копії

Якщо в процесі технічного обслуговування мали місце помилки, то організація може використовувати резервні копії для відновлення цілісності ушкодженої інформації;

– захист цілісності даних

Організація може використовувати засоби криптографії для збереження цілісності інформації.

Збій програмного забезпечення можуть порушувати цілісність даних та інформації [14], яка обробляється за допомогою такого програмного забезпечення. Заходи для захисту цілісності включають в себе:

– повідомлення про збої в програмному забезпеченні

Швидке повідомлення про збої програмного забезпечення допомагає знизити можливий збиток;

– експлуатаційні питання

Тестування безпеки може бути використано для забезпечення коректного функціонування програмного забезпечення. За допомогою управління змінами програмного забезпечення можна уникнути проблем, які виникають у зв'язку з удосконаленням або іншими коригуваннями програмного забезпечення;

– резервні копії

Резервні копії, наприклад програмне забезпечення попереднього покоління, можна використовувати для відновлення цілісності даних, оброблених за допомогою програмного забезпечення, функціонуючого зі збоями;

– захист цілісності даних

Засоби криптографії можуть бути використані для захисту цілісності інформації.

Неправильна маршрутизація повідомлень - це навмисне чи випадкове неправильний напрямок повідомлень, а зміна маршруту може переслідувати позитивні та деструктивні мети. Зміна маршруту повідомлень може бути, наприклад, зроблено для підтримки безперервності готовності до роботи. Напрямок повідомлень по хибному / іншому маршруту може призвести до втрати конфіденційності, якщо воно допускає несанкціонований доступ до цих повідомлень. Захисні заходи від цієї загрози включають в себе:

– управління мережею

Опис способів захисту від напрямків повідомлень по хибному / іншим маршрутом буде приведена в інших документах ІСО, що знаходяться на стадії розробки. У них буде міститися додаткова інформація щодо забезпечення безпеки мережі;

– збереження конфіденційності даних

Для недопущення несанкціонованого доступу в разі помилкового або зміненого напрямки повідомлень вони можуть бути зашифровані.

– захист цілісності даних

Для недопущення несанкціонованих коригувань у разі помилкового або зміненого напрямки повідомлень можна використовувати хеш-функції та цифрові підписи.

Помилки при передачі можуть порушити цілісність переданої інформації. Заходи щодо забезпечення цілісності в цьому випадку включають в себе:

– прокладку кабелів

Планування і відповідна прокладка кабелів дозволяють виключити помилки при передачі, якщо, наприклад, помилка викликана перевантаженням;

– управління мережею

Мережеве обладнання повинно правильно експлуатуватися і технічно обслуговуватися для того, щоб уникнути помилок при передачі. В даний час міжнародна організація по стандартизації (ISO) розробляє кілька документів, що містять додаткову інформацію щодо забезпечення безпеки мережі, яка може бути застосована для захисту від помилок при передачі;

– збереження цілісності даних

Контрольні суми і циклічне кодування в протоколах зв'язку може бути використано для захисту від випадкових помилок передачі. Засоби криптографії можна застосовувати для збереження цілісності переданих даних у разі навмисного впливу на дані.

Умисне пошкодження може наражати на небезпеку доступність інформації, так як в цьому випадку можливе несанкціоноване знищення інформації, записаної на цих носіях. Захисні заходи у цій галузі включають в себе:

– експлуатаційні питання

Організація може керувати носіями інформації, наприклад для фізичного захисту та підзвітності носіїв інформації для того, щоб не допустити несанкціонований доступ до інформації, записаної на цих носіях. Особлива увага повинна приділятися захисту легко знімаються носіїв інформації, наприклад зовнішні HDD із записами резервних копій і паперових носіїв;

– фізичну безпеку

Відповідна захист приміщень (міцні стіни і вікна, а також фізичне управління доступом) та офісне обладнання можуть захистити від несанкціонованого доступу.

Розглянуті контрзаходи зведені у таблицю 2.1.

Таблиця 2.1 – Контрзаходи проти загроз ІБ

Загроза	Контрзаходи
Підробка ідентифікатора користувача	- ідентифікацію та аутентифікацію. - логічне керування і аудит доступу. - захист від шкідливого коду. - управління мережею. - збереження конфіденційності даних.
Доступ до мережі неавторизованих користувачів	- ідентифікацію та аутентифікацію. - логічне керування і аудит доступу. - поділ мереж. - фізичне управління доступом. - управління носіями даних. - збереження конфіденційності даних. - цілісність даних.
Шкідливе програмне забезпечення	- обізнаність та навчання з питань безпеки. - резервні копії. - ідентифікацію та аутентифікацію. - логічне керування і аудит доступу. - захист від шкідливого коду.
Помилки користувачів	- обізнаність у питаннях безпеки і відповідне навчання. - резервні копії.
Перезавантаження трафіку	- резервування та резервні копії. - управління мережею.
Перехоплення	- фізичний захист. - персонал. - збереження конфіденційності даних. - засоби контролю носіїв інформації.
Пошкодження ліній зв'язку	- резервування та резервні копії. - управління мережею. - прокладку кабелів. - неспростовності.
Технічна несправність компонентів мережі	- експлуатаційні питання. - управління мережею. - план безперервності бізнесу.
Помилка технічного обслуговування	- технічне обслуговування. - резервні копії. - захист цілісності даних.

Загроза	Контрзаходи
Збій програмного забезпечення	- повідомлення про збої в програмному забезпеченні. - експлуатаційні питання. - резервні копії. - захист цілісності даних.
Неправильна маршрутизація повідомлень	- управління мережею. - збереження конфіденційності даних. - захист цілісності даних.
Помилки при передачі	- прокладку кабелів. - управління мережею. - збереження цілісності даних.
Умисне пошкодження	- експлуатаційні питання. - фізичну безпеку.

Для того, щоб уникнути втрату інформації необхідно забезпечувати захист і виконувати загальні вимоги.

Адміністративні заходи - це перший засіб забезпечення безпеки, т. к. ІБ - це процес, а в процесі важлива в першу чергу організація. Програмні засоби дозволяють автоматизувати процес забезпечення ІБ практично у галузі контролю: програми, робочі місця, БД або цілі мережі. Апаратні засоби використовуються в основному в двох випадках - потрібен серйозний рівень продуктивності (десятки тисяч підключень в хвилину, наприклад), або коли рішення вже типове, легко масштабується для продажу і затребуване ринком, наприклад, домашні бездротові точки з мережевим екраном і т. п.

На етапі створення системі управління інформаційної безпеки торгівельних підприємств пропонується запровадити наступні заходи:

1 Необхідно запровадити заходи адміністративного рівня в політиці безпеки фірми. На адміністративному рівні пропонується:

– створити ряд інструкцій по інформаційній безпеці усередині фірми для окремих категорій працівників:

1) інструкція по внесенню змін до списків користувачів;
2) інструкція про порядок дій в нештатних ситуаціях
3) інструкція щодо забезпечення працездатності ЛОС організації
4) інструкція з організації антивірусного захисту
5) інструкція з організації парольного захисту

6) інструкція по регламентації роботи адміністратора безпеки

7) інструкція користувачеві АС

8) модель порушника

9) деякі процедурні та організаційні вимоги

10) обов'язки адміністратора ІБ

11) приклад правил роботи та інструкцій

– передбачити низку мотиваційних заходів для зацікавленості працівників у дотриманні політики безпеки, а так само покарання за грубе порушення політики безпеки фірми:

1) преміювання за притримування політики безпеки;

2) своєчасне оновлення ПЗ;

3) стягнення штрафу за невиконання інструкцій з безпеки;

4) мотивуючі наради для директорів філій, відділів і т.д.

2 Для вдосконалення системи безпеки на процедурному рівні пропонується наступний ряд заходів:

– обмежити доступ сторонніх людей у деякі відділи фірми (відділ продаж, відділ маркетингу, відділ служби безпеки, відділ планування, ІТ-служба та інші);

– провести ряд консультаційних заходів з працівниками організації з питань інформаційної безпеки та інструкцій з дотримання політики безпеки. Ці заходи потрібно проводити з співробітниками торгівельного підприємства у яких є доступ до конфіденційної інформації, а також для підвищення їх рівня обізнаності у сфері інформаційних технологій;

– провести аудит безпеки, який включає в себе проведення обстеження, ідентифікацію загроз безпеки, виявлення ресурсів, що потребують захисту та оцінку ризиків. У ході аудиту необхідно провести аналіз поточного стану ІБ, виявити уразливості і найбільш чутливі до погроз ІБ бізнес-процеси. В результаті аудиту безпеки збираються та узагальнюються відомості, необхідні для розробки політик безпеки. Якщо своїми силами дану задачу конкретна організація

виконати утруднюється, то найбільш правильним рішенням буде звернутися до професіоналів;

– необхідно провести зовнішній аудит системи управління ІБ. Аудит повинен бути обов'язково зовнішнім, тому що 80% політик безпеки розробляється компаніями виходячи з умовиводів власних відділів ІТ або ІБ. Рекомендується доручати аудит найбільш важливих компонентів ІБ (таких як мережева безпека) професійним організаціям, що мають широкий досвід аудиту та впровадження систем ІБ.

3 На програмно-апаратному рівні пропонується запровадити наступні заходи:

– зобов'язати всіх співробітників використовувати паролі для доступу до бази програмного комплексу бухгалтерського обліку (наприклад, M.E.DOC, 1С Бухгалтерія, тощо) і більш ретельно розмежувати доступ до певних даних бази (довідників, документів і звітів) всіх співробітників;

– необхідно змінити всі стандартні логіни і паролі для доступу до інтернету, необхідно щоб паролі відповідали рівню складності;

– ввести обмеження на що передаються через Інтернет формати і розміри файлів окремим співробітникам, шляхом створення фільтрів за допомогою антивірусних програм (наприклад, avast!, NOD 32, AVG і тощо).

Загальні контрзаходи до забезпечення інформаційної безпеки зведені у таблицю 2.2.

Таблиця 2.2 – Контрзаходи забезпечення інформаційної безпеки

Сфера	Контрзаходи
Розробка політики в області ІБ	формування відповідного комплекту організаційно-розпорядчої та нормативно-методичної документації, положень щодо забезпечення ІБ компанії і методики проведення внутрішнього аудиту ІБ
Організаційні питання ІБ	– розробка моделі організаційно-штатної структури супроводу СУІБ; – розробка рольового складу структурних підрозділів, що беруть участь у забезпеченні ІБ

Сфера	Контрзаходи
Відповідність вимогам стандартів	проведення аналізу СУІБ на відповідність вимогам національним та міжнародним стандартам у галузі ІБ
Класифікація і управління інформаційними активами	роботи з визначення, аналізу та оцінці існуючих в компанії інформаційних ризиків
Підготовка персоналу до виконання процедур забезпечення ІБ	– розробка положення про структуру підрозділу та проєкту посадових інструкцій персоналу, що у забезпеченні ІБ; – навчання персоналу процедурам забезпечення ІБ
Фізичний захист ІС	проєктування та впровадження систем безперебійного та гарантованого електроживлення, контролю та управління доступом в приміщення і до обладнання, відеоконтролю і телеспостереження
Управління інцидентами в системі ІБ	– проєктування та впровадження систем моніторингу, реєстрації та управління інцидентами ІБ; – проведення тестів на проникнення
Управління доступом до інформаційних ресурсів та систем	впровадження служб каталогу, інфраструктури відкритих ключів (PKI), систем розмежування доступу; систем 2х-факторної аутентифікації; систем управління персональною інформацією та систем віддаленого доступу
Управління безперервністю бізнесу компанії	– створення планів відновлення роботи ІС після надзвичайних ситуацій; – створення планів забезпечення безперервності ведення бізнесу

Таким чином, визначимо із змінами в існуючій системі інформаційної безпеки. Серед цих змін ключовим є робота з персоналом, оскільки які б досконалі програмні засоби захисту інформації не впроваджувалися, тим не менш, всю роботу з ними здійснює персонал та основні збої в системі безпеки організації викликаються, як правило, персоналом. Правильно мотивований персонал, націлений на результат діяльності - це вже половина того, що необхідно для ефективної діяльності будь-якої системи.

2.2 Впровадження та застосування рекомендацій на ОІД

Датою введення СУІБ в експлуатацію є дата затвердження вищим керівництвом компанії положення про застосовність засобів управління. Даний

документ є публічним і декларує цілі та засоби, обрані організацією для управління ризиками. Положення включає:

– засоби управління і контролю, вибрані на етапі обробки ризиків;

– існуючі в організації засоби управління і контролю;

– засоби, що забезпечують виконання вимог законодавства та вимог регулюючих організацій;

– засоби, що забезпечують виконання вимог замовників;

– кошти, що забезпечують виконання загальних вимог;

– будь-які інші відповідні засоби управління і контролю.

При введенні СУІБ в експлуатацію задіяні всі розроблені процедури та механізми, що реалізують обрані цілі і засоби управління.

Впровадження системи управління інформаційною безпекою процес досить тривалий і трудомісткий. У загальному випадку, він включає в себе ряд послідовних етапів, які виконуються організацією, як правило, за допомогою зовнішніх консультантів.

На першому етапі проводиться попередній аудит СУІБ, в ході якого оцінюється поточний стан, здійснюється інвентаризація та документування всіх основних складових СУІБ, визначаються область і межі сертифікації і виконується ще цілий ряд необхідних підготовчих дій. За результатами аудиту розробляється детальний план заходів з підготовки до сертифікації.

На другому етапі виконується оцінка інформаційних ризиків, основною метою якої є визначення застосовності описаних у стандарті механізмів контролю в даній конкретній організації, підготовка декларації про застосовність та плану оброблення ризиків.

На третьому етапі виконується аналіз розбіжностей з вимогами стандарту, в результаті якого оцінюється поточний стан механізмів контролю в організації та ідентифікуються розбіжності з декларацією про застосовність.

На наступних етапах здійснюється планування та впровадження відсутніх механізмів контролю, по кожному з яких розробляється стратегія і план впровадження. Роботи з впровадження механізмів контролю включають в себе

три основні складові: підготовка співробітників організації: навчання, тренінги, підвищення обізнаності; підготовка документації СУІБ: політики, стандарти, процедури, регламенти, інструкції, плани; підготовка свідоцтв функціонування СУІБ: звіти, протоколи, накази, записи, журнали подій і т.п.

Торгівельним підприємствам рекомендується пройти попередній аудит, який допоможе оцінити готовність до сертифікаційного аудиту. Попередній аудит зазвичай проводиться тим же органом з сертифікації, в якому передбачається проходження сертифікаційного аудиту.

За результатами попереднього аудиту орган по сертифікації складає звіт, в ньому зазначаються всі позитивні сторони створеної СУІБ, виявлення невідповідності та рекомендації щодо їх усунення.

Для проведення сертифікаційного аудиту рекомендується, щоб СУІБ компанії функціонувала від трьох до шести місяців. Це мінімальний період, необхідний для первинного виконання внутрішніх аудитів та аналізу СУІБ з боку керівництва, а також для формування записів за результатами виконання всіх процедур СУІБ, які аналізуються в ході сертифікаційного аудиту.

Розглянувши основні етапи створення СУІБ, відзначимо, що цей процес досить складний і тривалий, однак застосувавши цей метод можна створити ефективну і реально працюючу систему.

Зусилля, витрачені на створення системи управління інформаційною безпекою, дозволять торгівельному підприємству вийти на новий рівень відносин з клієнтами, партнерами, акціонерами, продемонструвати надійність компанії і нададуть можливість успішної конкуренції з провідними підприємствами на міжнародному ринку.

Головною метою робіт з впровадження системи управління інформаційною безпекою в компанії є досягнення надійного рівня захищеності інформаційних систем і значне зниження ризиків реалізації загроз інформаційної безпеки. СУІБ є каркасом, який пов'язує різні технічні засоби та організаційні заходи забезпечення інформаційної безпеки і дозволяє надійно і прозоро управляти інформаційною безпекою в компанії.

Впровадження в Компанії СУІБ, відповідно до вимог стандарту ДСТУ СУІБ 1.0/ISO/IEC 27001, привнесе цілий ряд переваг, як для бізнесу Компанії, в цілому, так і для окремих структурних підрозділів. В цілому для Компанії можна відзначити наступні переваги:

- підвищення керованості і надійності;
- підвищення захищеності ключових бізнес - процесів;
- підвищення довіри до Компанії з боку контрагентів;
- підтвердження прозорості;
- підвищення авторитету Компанії як на внутрішньому, так і на зовнішніх ринках;
- спрощення процедури виходу на зовнішні ринки;
- підвищення прибутковості і капіталізації.

Для структурних підрозділів Компанії, таких, як підрозділи інформаційних технологій, це:

- систематизація процесів забезпечення ІБ;
- розстановка пріоритетів у сфері ІБ;
- управління ІБ в рамках єдиної корпоративної політики;
- своєчасне виявлення і управління інформаційними ризиками;
- зниження ризиків від зовнішніх і внутрішніх загроз;
- оптимізація управлінських процесів;
- істотне підвищення захищеності інформаційних систем.

Етапи 1 та 2 (аудит торгівельного підприємства та оцінка інформаційних ризиків) вже проведено.

Розглянемо на третьому етапі виконується аналіз розбіжностей з вимогами стандарту, в результаті якого зможемо оцінити поточний стан механізмів контролю в організації та ідентифікуються розбіжності з декларацією про застосовність.

2.2.1 Загальні відомості про організацію

Торговельне підприємство «Автохімія» входить у групу компаній «Біохім» - найбільшого оператора по дистиляції та продажу гліцерину на ринку України.

ТП «Автохімія» за формою власності приватна, спеціалізована, оптова, по чисельності працівників середня, а також комерційна організація.

ТП «Автохімія» розвивався на базі виробничих потужностей «Дніпропетровського заводу хімічних виробів» та є одним з лідерів на ринку охолоджуючих рідин та автохімії. Підприємство володіє розгалуженою інфраструктурою, великим ємнісним парком і серйозним науковим і технологічним потенціалом в області удосконалення рецептур і виробництва охолоджуючих рідин.

Основним напрямком діяльності підприємства є імпорт, переробка гліцерину для подальшого його використання в промисловості. ТП «Автохімія» виробляє високоякісні, екологічно чисті продукти, які мають основу сучасних органічних присадок, без додавання нітритів, нітратів, амінів, фосфатів, боратів, силікату.

Компанія має ряд автономних джерел постачання (води, електроенергії тощо), що забезпечує безперебійну роботу.

На рис. 2.2 представлена організаційна схема торгівельного підприємства. Розглянемо її окремо.

Генеральний директор - керівника комерційної організації, орган управління організацією. Він виконує наступні функції:

– організація, координація та контроль роботи підприємства;

– організація ефективної взаємодії структурних підрозділів компанії;

– стратегічне планування розвитку підприємства і реалізація цих планів;

– участь у формуванні бюджету та контроль його виконання;

– забезпечення ефективного документообігу та своєчасного руху інформації в компанії.

Рисунок 2.2 – Організаційна структура підприємства

Директор з маркетингу розробляє маркетингову політику підприємства, ґрунтуючись на аналізі споживчих якостей товарів, прогнозуванні попиту споживачів, а також даних про споживчі якості продукції конкурентів. У його підкоренні знаходяться наступні відділи:

– відділ планування розробляє довгострокові або короткострокові плани розвитку ринку, його місткості;

– відділ логістики забезпечує оптимальну доставку готової продукції до споживачів;

– відділу маркетингу ведеться постійний моніторинг та аналіз ринку охолоджуючих рідин України, з метою визначення найбільш вигідних пропозицій для кінцевого споживача. На основі аналізу ринку та вивчення споживчих переваг розширюється асортимент торгових марок;

– відділ продажів формує дилерську мережу.

Комерційний директор відповідає за роботу з клієнтами і загальний прибуток компанії. У його підкоренні знаходяться наступні відділи:

– відділ приймання перевіряє відповідність замовленого товару з доставленим постачальником, а також кількість і якість;

– обліково-операційний відділ займається організацією і контролем ведення бухгалтерського обліку, складання звітності та оформлення арбітражних операцій, операцій з цінними паперами тощо;

– відділ сертифікації займається організацією процесу контролю якості продукції.

Виконавчий директор - це керівник, який підпорядковується тільки генеральному директору. Функції виконавчого директора включають в себе ретельний контроль за фінансовими потоками, управління персоналом компанії та вирішення всіх організаційних завдань реалізації товарів або послуг. У його підкоренні знаходяться наступні відділи:

– відділ кадрів займається обліком особового складу підприємства (прийом на роботу, переведення, звільнення тощо);

– IT відділ підтримує правильну роботу комп'ютерної техніки та програмного забезпечення, а також відповідає за інформаційну безпеку організації;

– відділ служби безпеки займається охороною і захистом підприємства.

Бухгалтерія виконує такі посадові обов'язки:

– ведення первинного бухгалтерського обліку. Прийом, контроль та обробка первинної документації (товарно-транспортних накладних, касових, кадрових документів, договорів з контрагентами тощо);

– нарахування заробітної плати, виплат за цивільними договорами;

– ведення податкового та управлінського обліку;

– складання та здача податкової звітності;

– мінімізація податкових виплат;

– взаємодія з банками і кредитними організаціями.

На даний момент компанія випускає тосоли та антифризи 5 торгових марок:

ТМ «TRIOL» - преміум сегмент, високоякісна продукція на основі органічних присадок.

ТМ «PROFI» - продукція для професійного використання.

ТМ «Стандарт» - продукція, призначена для використання в автомобілях у стандартних кліматичних умовах.

ТМ «NordWay» - продукція відповідає співвідношенню ціна-якість.

ТМ «Тайфун» - тосоли для використання та експлуатації при не дуже низьких температурах навколишнього середовища.

2.2.2 Обґрунтування необхідного створення комплексу технічного захисту інформації

Деякі з загроз інформаційної безпеки, такі як несанкціоноване отримання доступу ззовні, некоректна робота програмного забезпечення або технічні збої, досить успішно нейтралізуються грамотним налаштуванням і адмініструванням мережі, однак заходів для запобігання внутрішніх загроз не існує [29].

У процесі аналізу існуючої системи інформаційної безпеки в ТП «Автохімія» були виділені наступні недоліки:

– Не повне використання функціональних можливостей 1С. Не повністю розмежовані права доступу до даних в базі, а так само паролі не відповідають вимогам складності або у деяких співробітників просто не використовуються.

– Відсутні обмеження щодо форматів та розмірів переданих даних через інтернет (*.mp3,*.avi,*.rar) для певних працівників.

– Деякі співробітники зберігають конфіденційну інформацію в загальнодоступних папках просто через власну неуважність, а так само зберігають логін / пароль від інформаційних систем, що вимагають авторизації в легкодоступних місцях на робочому столі.

– Практично не охороняється інформація на паперових носіях, за винятком найбільш важливою (кредитні договори, договори ренти, результати перевірок тощо).

Серед конфіденційної інформації, що циркулює на підприємстві, необхідно виділити критичну інформацію, тобто інформацію, що вимагає підвищеного ступеня захисту, так як порушення її властивостей призведе до найбільших збитків.

До критичної інформації відносяться:

– інформація про клієнтів, їх контактні і особисті дані;
– інформація про проєкти, термінах і умовах договорів;
– інформація про постачальниках, споживачах, цінах;
– інформація про доходи і т.д.

Ступінь впливу на інформацію, що відноситься до комерційної таємниці, може бути наступних рівнів:

1 Висока

Доступ до всієї інформації та можливість її зміни.

2 Середня

Доступ до всієї інформації без можливості її зміни.

3 Низька

Частковий доступ без можливості зміни.

У таблиці 2.3 представлені дані про те, хто і в якій мірі має доступ до інформації, яка відноситься до комерційної таємниці.

Основною метою захисту інформації є забезпечення заданого рівня її безпеки. Під заданим рівнем безпеки інформації розуміється стан захищеності інформації від загроз, при яких забезпечується допустимий ризик її знищення, зміни і розкрадання. При цьому під знищенням інформації мається на увазі не тільки її фізичне знищення, але й стійке блокування санкціонованого доступу до неї.

Таблиця 2.3 – Доступ і ступінь впливу на конфіденційну інформацію на ТП «Автохімія»

Підрозділ	Інформація	Ступінь впливу
Генеральний директор	1) інформація про клієнтів, їх контактні і особисті дані; 2) інформація про проєкти, термінах і умовах договорів; 3) інформація про постачальниках, споживачах, цінах; 4) інформація про доходи і т.д.	Висока
Директор з маркетингу	1) інформація про клієнтів, їх контактні і особисті дані; 2) інформація про проєкти, термінах і умовах договорів; 3) інформація про постачальниках, споживачах, цінах; 4) інформація про доходи і т.д.	Висока
Комерційний директор	1) інформація про клієнтів, їх контактні і особисті дані; 2) інформація про проєкти, термінах і умовах договорів; 3) інформація про постачальниках, споживачах, цінах; 4) інформація про доходи і т.д.	Висока
Виконавчий директор	1) інформація про клієнтів, їх контактні і особисті дані; 2) інформація про проєкти, термінах і умовах договорів; 3) інформація про постачальниках, споживачах, цінах; 4) інформація про доходи і т.д.	Висока
Бухгалтерія	1) інформація про клієнтів, їх контактні і особисті дані; 2) інформація про проєкти, термінах і умовах договорів; 3) інформація про постачальниках, споживачах, цінах; 4) інформація про доходи і т.д.	Середня
Відділ планування	1) інформація про проєкти, термінах і умовах договорів	Низька
Група логістики	1) інформація про постачальниках, споживачах, цінах	Низька
Відділ маркетингу	1) інформація про проєкти, термінах і умовах договорів	Низька
Відділ продажів	1) інформація про клієнтів, їх контактні і особисті дані; 2) інформація про проєкти, термінах і умовах договорів; 3) інформація про постачальниках, споживачах, цінах; 4) інформація про доходи і т.д.	Середня
Відділ закупівлі	1) інформація про постачальників, ціни	Низька
Обліково-операційний відділ	1) інформація про постачальниках, споживачах, цінах; 2) інформація про доходи і т.д.	Низька
Відділ служби безпеки	1) інформація про клієнтів, їх контактні і особисті дані; 2) інформація про проєкти, термінах і умовах договорів; 3) інформація про постачальниках, споживачах, цінах; 4) інформація про доходи і т.д.	Висока

У загальному випадку при блокуванні інформації в результаті несправності замку або втрати ключа сейфа, забуття пароля комп'ютера,

спотворення коду завантажувальний сектор HDD і інших факторах інформація не спотворюється і не викрадається і при певних зусиллях доступ до неї може бути відновлений. Отже, блокування інформації прямої загрози її безпеки не створює. Однак при неможливості доступу до неї в потрібний момент її користувач втрачає інформацію так само, як якщо б вона була знищена.

До інформаційних ресурсів фірми належить документи і акти на паперових носіях, локальна обчислювальна мережа.

2.2.3 Оцінка існуючого стану захищеності

Не вся інформація в організації вимагає забезпечення максимального рівня безпеки. Необхідно визначити, якою захисту, яка інформація потребує. Тому треба розділити інформацію за різними критеріями.

Інформація в організації класифікується на критичну і чутливу [3].

Критичність інформації передбачає, що інформація повинна бути доступна там і тоді, коли вона потрібна для безперервності та живучості бізнесу. Критичність інформації прямо пов'язана з критичністю процесів доступу до інформації.

За ступенем критичності інформація може бути, наприклад, такою:

- суттєва: інформація або інтенсивність обробки інформації, втрата якої може завдати серйозної або непоправної шкоди організації;

- важлива: інформація або інтенсивність обробки інформації, втрата якої може завдати середній, але виправити шкоду організації;

- нормальна: інформація або інтенсивність обробки інформації, втрата якої представляє мінімальну руйнування.

За ступенем чутливості можуть бути виділені наступні види інформації:

- високо чутлива: інформація вищої чутливості, неправильне поводження з якого ймовірно призведе до значного збитку для організації. Прикладами є інформація про придбання/продажу, стратегічні бізнес-плани, криптографічні ключі та матеріали.

- чутлива: інформація, неправильне поводження з якою може призвести до істотного збитку для організації. Прикладами є персональна дані, інформація про клієнтів, бюджети департаментів.

- внутрішня: інформація, неправильне поводження з якою може завдати певної шкоди організації. Прикладами є телефонні книги, функції підрозділів організації.

- відкрита: інформація, схвалена для опублікування. Відкрита інформація не створюється відразу як відкрита, а отримує таку класифікацію після опублікування.

За ступенем критичності щодо доступності види інформації можуть бути наступні:

- критична: інформація, без якої робота суб'єкта зупиняється;

- дуже важлива: інформація, без якої суб'єкт може працювати, але дуже короткий час;

- важлива інформація, без якої суб'єкт може працювати деякий час, але рано чи пізно вона знадобиться;

- корисна інформація, без якої суб'єкт може працювати, але її використання економить ресурси;

- несуттєва: застаріла або невживана інформація, не впливає на роботу суб'єкта.

За ступенем критичності щодо цілісності види інформації можуть бути наступні:

- критична: інформація, несанкціоноване зміна якої призведе до неправильної роботи суб'єкта; наслідки модифікації незворотними;

- дуже важлива: інформація, несанкціоноване зміна якої призведе до неправильної роботи суб'єкта через деякий час, якщо не будуть зроблені деякі дії; наслідки модифікації незворотними;

- важлива інформація, несанкціоноване зміна якої призведе до неправильної роботи суб'єкта через деякий час, якщо не будуть зроблені деякі дії; наслідки модифікації оборотні;

- значуща: інформація, несанкціоноване зміна якої позначиться через деякий час, але не призведе до збою в роботі суб'єкта; наслідки модифікації оборотні;

- незначна: інформація, несанкціоноване зміна якої не позначиться на роботі системи.

За ступенем критичності щодо конфіденційності види інформації можуть бути наступні:

- критична: інформація, розголошення якої призведе до неможливості реалізації цілей системи або до значних збитків;

- дуже важлива: інформація, розголошення якої призведе до значного збитку, якщо не будуть зроблені деякі дії;

- важлива: інформація, розголошення якої призведе до незначного збитку, якщо не будуть зроблені деякі дії;

- значуща інформація, розголошення якої призведе тільки до морального збитку;

- незначна: інформація, розголошення якої не впливає на роботу системи.

Одна і та ж інформація може одночасно поділяється за різними класифікаціями, тому в роботі була розглянута вся класифікація. Об'єктом захисту є конфіденційна інформація. Специфіка діяльності організації ТД по розробці та продажу товарів така, що розкриття саме суттєвої інформації (інформація про клієнтів, їх контактні дані, інформація про проєкти, термінах і умовах договорів, технічне завдання, інформація про постачальників, споживачів, ціни, виробництві, інформація про доходи тощо) може завдати серйозної шкоди організації. У таблиці 2.4 подано класифікацію інформації, яка підлягає комерційної таємниці, за різними критеріями.

Таблиця 2.4 – Класифікація інформації за різними критеріями

Класифікація оцінювання	Вид інформації			
	про клієнтів, їх контактні і особисті дані	про проєкти, термінах і умовах договорів	про постачальниках, споживачах, цінах	про доходи і т.д.
За ступенем критичності	Суттєва	Суттєва	Суттєва	Суттєва
За ступенем чутливості	Чуттєва	Високо чутлива	Високо чутлива	Високо чутлива
За ступенем критичності щодо доступності	Дуже важлива	Критична	Дуже важлива	Критична
За ступенем критичності щодо цілісності	Дуже важлива	Критична	Критична	Критична
За ступенем критичності щодо конфіденційності	Критична	Критична	Дуже важлива	Критична

Ґрунтуючись на табл.2.4 можемо зробити висновок, що інформація, яка є конфіденційною, істотно важлива, робота без якої практично неможлива, неправильне поводження або втрата її призведе до значного збитку для організації.

2.2.4 Аналіз ризиків інформаційної безпеки на ТП «Автохімія»

Розрахуємо рівень ризиків Th_i на основі критичності та ймовірності реалізації i загрози через дану уразливість. Рівень ризиків показує, наскільки критичним є вплив i загрози на ресурс з урахуванням ймовірності її реалізації.

$$Th_i = \frac{ER_i}{100} \cdot \frac{P(V_i)}{100}, \qquad (2.1)$$

де ER_i - критичність реалізації i загрози (вказується у %); $P(V_i)$- ймовірність реалізації i загрози через дану уразливість (вказується у %).

Сумарний ризик розраховується:

$$Th_{\Sigma} = \frac{\sum_{i=1}^{n} Th_i}{n}, \qquad (2.2)$$

де, n - кількість загроз.

Отримуємо значення рівня загрози по уразливості в інтервалі від 0 до 1 для ТД «Автохімія». Розрахуємо для кожної загрози окремо (табл. 2.5).

Таблиця 2.5 – Аналіз ризиків інформаційної безпеки ТП «Автохімія»

Загроза інформаційної безпеки (i)	Критичність реалізації загрози (ER_i)	Імовірність реалізації загрози ($P(V_i)$)	Загальний ризик (Th_i)
1	2	3	4
Підробка ідентифікатора користувача	80%	100%	0,80
Доступ до мережі неавторизованих користувачів	55%	100%	0,55
Шкідливе програмне забезпечення	80%	80%	0,64
Помилки користувачів	50%	60%	0,30
Перезавантаження трафіку	80%	100%	0,80
Перехоплення	80%	100%	0,80
Пошкодження ліній зв'язку	40%	30%	0,12
Технічна несправність компонентів мережі	25%	40%	0,10
Помилка технічного обслуговування	30%	50%	0,15
Збій програмного забезпечення	50%	50%	0,25
Неправильна маршрутизація повідомлень	70%	100%	0,70

Загроза інформаційної безпеки (i)	Критичність реалізації загрози (ER_i)	Імовірність реалізації загрози ($P(V_i)$)	Загальний ризик (Th_i)
1	2	3	4
Помилки при передачі	50%	20%	0,10
Умисне пошкодження	80%	100%	0,80
Некомпетентність персоналу	60%	80%	0,48
Сумарний ризик (Th_Σ)			0,47

Отриманий показник $Th_\Sigma = 0,47$ - трохи менше половини, що вимагає вдосконалення системи інформаційної безпеки на ТП «Автохімія».

2.2.5 Розробка політики ІБ ТП «Автохімія»

Розробка організаційно-нормативної бази, необхідної для функціонування СУІБ, може проводитися паралельно з реалізацією заходів плану обробки ризиків.

На цьому етапі розробляються документи, необхідність реалізації яких випливає з результатів аналізу ризиків та з власних вимог компанії до захисту інформації. У запропонований перелік входять наступні основні політики та процедури:

- область діяльності СУІБ;
- політика СУІБ;
- подполітики за основними механізмам забезпечення інформаційної безпеки, що застосовується до обраної галузі діяльності, яка охоплюється СУІБ, такі як:
- політика антивірусного захисту;
- політика надання доступу до інформаційних ресурсів;
- політика використання засобів криптографічного захисту;
- інші політики;
- процедури СУІБ:

- управління документацією;
- управління записами;
- внутрішні аудити;
- коригувальні дії;
- запобіжні дії;
- управління інцидентами;
- аналіз функціонування СУІБ керівництвом організації;
- оцінка ефективності механізмів управління СУІБ;
- інші процедури та інструкції.

Розроблені політики та процедури повинні охоплювати наступні ключові процеси СУІБ:

- управління ризиками;
- управління інцидентами;
- управління ефективністю системи;
- управління персоналом;
- управління документацією та записами системи управління ІБ;
- перегляд і модернізація існуючої системи;
- управління безперервністю бізнесу і відновлення після переривань.

Крім того, в посадові інструкції відповідального персоналу, положення про підрозділи, контрактні зобов'язання організації повинні бути включені обов'язки щодо забезпечення інформаційної безпеки.

Обов'язки з виконання вимог СУІБ допомогою відповідних наказів і розпоряджень покладаються на відповідальних співробітників підрозділів, які охоплюються СУІБ.

Всі розроблені положення політики СУІБ, подполітик, процедур та інструкцій доводяться до відома рядових співробітників при їх початковому і наступному періодичному навчанні та інформуванні.

Таким чином, в результаті не тільки створюється документальна база СУІБ, але й відбувається реальний розподіл обов'язків щодо забезпечення

безпеки інформації серед персоналу організації.

В основі організаційних заходів захисту інформації лежить політика безпеки, від ефективності якої найбільшою мірою залежить успішність заходів щодо забезпечення інформаційної безпеки.

Політика безпеки будується на основі аналізу ризиків. З урахуванням ризиків, проаналізованих у торгівельному підприємстві, політика інформаційної безпеки для організації повинна містити сім розділів:

– «Вступ». Необхідність появи політики безпеки на підставі виявлених недоліків в інформаційній безпеці ТП;

– «Мета політики». У цьому розділі документа для ТП необхідно відобразити цілі створення даного документа (зокрема, для пральний політики - «встановлення стандартів для створення «сильних» паролів, їх захисту та регулярної зміни »);

– «Область застосування». У даному розділі необхідно описати об'єкти або суб'єкти ТП, які повинні виконувати вимоги даної політики (наприклад, «дана політика застосовується до всіх співробітників, які мають будь-яку форму доступу до будь інформаційних ресурсів компанії»);

– «Політика». У даному розділі необхідно описати самі вимоги до інформаційної безпеки (наприклад, парольний політика повинна містити п'ять підрозділів: «Створення паролів», «Зміна паролів», «Захист паролів», «Використання паролів при розробці додатків», «Використання паролів при віддаленому доступі»);

– «Відповідальність». Описує покарання за порушення зазначених у попередньому розділі вимог;

– «Історія змін даної політики». Дає можливість відстежити всі внесені в документ зміни (дата, автор, коротка суть зміни).

Така структура дозволить лаконічно описати всі основні моменти, пов'язані з предметом політики безпеки організації, що не «прив'язуючись» до конкретних технічних рішень, продуктам і виробникам. Інакше зміна політичної

ситуації в компанії і т. п. призведе до необхідності зміни концепції ІБ, а цього відбуватися не повинно.

Крім того, в політиці безпеки організації повинні бути визначені обов'язки посадових осіб з вироблення програми безпеки та проведення її в життя. У цьому сенсі політика безпеки є основою підзвітності персоналу.

2.2.5.1 Адміністративний рівень ІБ

До адміністративного рівня інформаційної безпеки відносяться дії загального характеру, що починаються керівництвом організації.

Головна мета заходів адміністративного рівня сформувати програму робіт в області інформаційної безпеки і забезпечити її виконання, виділяючи необхідні ресурси і контролюючи стан справ.

Основою програми є політика безпеки, що відображає підхід організації до захисту своїх інформаційних активів. Керівництво компанії має усвідомити необхідність підтримки режиму безпеки і виділення на ці цілі значних ресурсів, а також призначити відповідальних за розробку, впровадження і супровід системи безпеки.

З практичної точки зору політику безпеки доцільно розглядати на трьох рівнях деталізації. До верхнього рівня можна віднести рішення, що зачіпають організацію в цілому. Вони носять досить загальний характер і виходять від керівництва організації. Список рішень цього рівня включає в себе наступні елементи:

– рішення сформувати або переглянути комплексну програму забезпечення інформаційної безпеки, призначення відповідальних за просування програми;

– формулювання цілей, які переслідує організація в області інформаційної безпеки, визначення загальних напрямків у досягненні цих цілей;

– забезпечення бази для дотримання законів і правил;

– формулювання адміністративних рішень з тих питань реалізації програми безпеки, які повинні розглядатися на рівні організації в цілому.

Для політики верхнього рівня мети організації в галузі інформаційної безпеки формулюються в термінах цілісності, доступності та конфіденційності. Так як компанія відповідає за підтримання критично важливою бази даних бухгалтерії, то на першому плані стоїть завдання зменшення числа втрат, пошкоджень або спотворень даних.

На верхній рівень виноситься керування захисними ресурсами і координація використання цих ресурсів, виділення спеціального персоналу для захисту критично важливих систем і взаємодію з іншими організаціями, що забезпечують або контролюючими режим безпеки.

Політика верхнього рівня має справу з трьома аспектами законослухняності та виконавської дисципліни. По-перше, організація повинна дотримуватися існуючих законів. По-друге, слід контролювати дії осіб, відповідальних за вироблення програми безпеки. Нарешті, необхідно забезпечити певний ступінь старанності персоналу, а для цього потрібно виробити систему заохочень і покарань.

Взагалі кажучи, на верхній рівень слід виносити мінімум питань. Подібне винесення доцільно, коли вона обіцяє значну економію коштів або коли інакше вчинити просто неможливо.

У документ, що характеризує політику безпеки компанії необхідно включити такі розділи:

– вступний, що підтверджує стурбованість вищого керівництва проблемами інформаційної безпеки;

– організаційний, що містить опис підрозділів, комісій, груп і т.д., що відповідають за роботи в галузі інформаційної безпеки;

– класифікаційний, що описує наявні в організації матеріальні та інформаційні ресурси та необхідний рівень їх захисту;

– штатний, що характеризує заходи безпеки, що застосовуються до персоналу (опис посад з точки зору інформаційної безпеки, організація навчання та перепідготовки персоналу, порядок реагування на порушення режиму безпеки тощо);

– розділ, що висвітлює питання фізичного захисту;

– керуючий розділ, що описує підхід до управління комп'ютерами та комп'ютерними мережами;

– розділ, що описує правила розмежування доступу до виробничої інформації;

– розділ, що характеризує порядок розробки та супроводу систем;

– розділ, що описує заходи, спрямовані на забезпечення безперервної роботи організації;

– юридичний розділ, що підтверджує відповідність політики безпеки чинному законодавству.

До адміністративних заходів захисту, необхідним для проведення в бухгалтерії торгівельного підприємства, відносяться:

– підтримка правильної конфігурації ОС;

– створення, ведення та контроль журналів роботи користувачів в ІС за допомогою вбудованих механізмів програми M.E.DOC;

– виявлення «проломів» у системі захисту;

– проведення тестування засобів захисту;

– контроль зміни паролів.

2.2.5.2 Організаційний рівень ІБ

До організаційних засобів захисту можна віднести організаційно-технічні та організаційно-правові заходи, здійснювані в процесі створення і експлуатації ІС з метою забезпечення захисту інформації. Організаційні заходи охоплюють усі структурні елементи ІС та системи захисту на всіх етапах їх життєвого циклу. При цьому організаційні заходи відіграють двояку роль у механізмі захисту: з одного боку, дозволяють повністю або частково перекривати значну частину каналів витоку інформації, а з іншого - забезпечують об'єднання всіх використовуваних в ІС коштів в цілісний механізм захисту.

Організаційні заходи захисту базуються на законодавчих і нормативних документах з безпеки інформації. Вони повинні охоплювати всі основні шляхи збереження інформаційних ресурсів і включати:

– обмеження фізичного доступу до об'єктів ІВ і реалізацію режимних заходів;

– обмеження можливості перехоплення інформації внаслідок існування фізичних полів;

– обмеження доступу до інформаційних ресурсів та іншим елементам ІС шляхом встановлення правил розмежування доступу, криптографічне закриття каналів передачі даних, виявлення та знищення «закладок»;

– створення твердих копій важливих з точки зору втрати масивів даних;

– проведення профілактичних та інших заходів від впровадження вірусів.

До організаційно-правових заходів захисту, необхідними для проведення в бухгалтерії ТП відносяться:

– організація та підтримку надійного пропускного режиму і контроль відвідувачів;

– надійна охорона приміщень компанії і території;

– організація захисту інформації, тобто призначення відповідального за захист інформації, проведення систематичного контролю за роботою персоналу, порядок обліку, зберігання та знищення документів.

Організаційні заходи при роботі з співробітниками компанії включають в себе:

– бесіди при прийомі на роботу;

– ознайомлення з правилами та процедурами роботи з ІС на підприємстві;

– навчання правилам роботи з ІС для збереження її цілісності та коректності даних;

– бесіди з людьми які звільняються.

В результаті бесіди при прийомі на роботу встановлюється доцільність прийому кандидата на відповідну вакансію.

Навчання співробітників передбачає не тільки придбання і систематичне підтримання на високому рівні виробничих навичок, а й психологічне їх виховання в глибокої переконаності, що необхідно виконувати вимоги промислової (виробничої) секретності, інформаційної безпеки. Систематичне навчання сприяє підвищенню рівня компетентності керівництва і співробітників в питаннях захисту комерційних інтересів свого підприємства. Бесіди з звільняються мають головною метою запобігти розголошення інформації або її неправильне використання. У ході бесіди слід особливо підкреслити, що кожен звільняється співробітник має тверді зобов'язання про нерозголошення фірмових секретів і ці зобов'язання, як правило, підкріплюються підпискою про нерозголошення відомих співробітнику конфіденційних відомостей.

Організаційно-технічні заходи захисту включають такі основні заходи:

– резервування (наявність всіх основних компонентів операційної системи та програмного забезпечення в архівах, копіювання таблиць розподілу файлів дисків, щоденне ведення архівів змінюваних файлів);

– профілактика (систематична вивантаження вмісту активної частини HDD, SSD, роздільне зберігання компонентів програмного забезпечення та програм користувачів, зберігання не використовуваних програм в архівах);

– ревізія (обстеження знову одержуваних програм на дисках на наявність вірусів, систематична перевірка довжин файлів, що зберігаються на вінчестері, використання і постійна перевірка контрольних сум при зберіганні і передачі програмного забезпечення, перевірка вмісту завантажувальних секторів вінчестера і використовуваних flash системних файлів);

– фільтрація (поділ вінчестера на логічні диски з різними можливостями доступу до них, використання резидентних програмних засобів стеження за файлової системою).

Всі ці заходи, в тій чи іншій мірі, включають використання різних програмних засобів захисту. До їх числа необхідно віднести програму-архіватор

WinRar, програми резервування важливих компонентів файлової системи, перегляду вмісту файлів і завантажувальних секторів, підрахунку контрольних сум і власне програм захисту. Резервування даних ІС повинно проводитися з використанням вбудованих засобів програми M.E.DOC.

2.2.5.3 Технічний рівень ІБ

Інженерно-технічне забезпечення безпеки інформації шляхом здійснення необхідних технічних заходів повинно виключати:

– неправомочний доступ до апаратури обробки інформації шляхом контролю доступу в приміщенні бухгалтерії;

– неправомочний винос носіїв інформації персоналом, що займаються обробкою даних, за допомогою вихідного контролю;

– несанкціоноване введення даних в пам'ять, зміна або стирання інформації, що зберігається в пам'яті;

– неправомочне користування системами обробки інформації та незаконне отримання в результаті цього даних;

– доступ в системи обробки інформації за допомогою саморобних пристроїв і незаконне отримання даних;

– можливість неправомочною передачі даних через комп'ютерну мережу;

– безконтрольний введення даних в систему;

– неправомочне зчитування, зміна або стирання даних у процесі їх передачі або транспортування носіїв інформації.

Інженерно-технічний захист використовує такі засоби [16]:

– фізичні засоби;

– апаратні засоби;

– програмні засоби.

Методи захисту інформації від більшості загроз базуються на інженерних та технічних заходах. Інженерно-технічний захист - це сукупність спеціальних органів, технічних засобів і заходів, що функціонують спільно для виконання певного завдання по захисту інформації.

Для побудови системи фізичної безпеки необхідні наступні засоби:

– апаратура тривожної сигналізації, забезпечує виявлення спроб проникнення і несанкціонованих дій, а також оцінку їх небезпеки;

– системи зв'язку, що забезпечують збір, об'єднання та передачу тривожної інформації та інших даних;

– персонал охорони, що виконує щоденні програми безпеки, управління системою та її використання в нештатних ситуаціях.

До інженерних заходам, необхідним для проведення в бухгалтерії ТП, відносяться:

– захист акустичного каналу;

– екранування приміщення бухгалтерії.

До апаратних засобів відносяться прилади, пристрої, пристосування та інші технічні рішення, використовувані в інтересах забезпечення безпеки.

У бухгалтерії необхідно:

– в терміналах користувачів розміщувати пристрої, призначені для попередження несанкціонованого включення терміналу в роботу (блокатори);

– забезпечити ідентифікацію терміналу (схеми генерування ідентифікаційного коду);

– забезпечити ідентифікацію користувача (магнітні індивідуальні картки).

Програмні засоби - це спеціальні програми, програмні комплекси та системи захисту інформації в інформаційних системах різного призначення і засобах обробки даних.

До завданням програмних засобів захисту відносяться:

– ідентифікація та аутентифікація;

– управління доступом;

– забезпечення цілісності і збереження даних;

– контроль суб'єктів взаємодії;

– реєстрація і спостереження.

2.2.6 Рекомендації до інформаційної безпеки торгівельного підприємства

З точки зору адміністративних заходів були розроблені наступні рекомендації:

– система захисту інформації повинна відповідати законодавству України та державним стандартам;

– класифікація та категорування захищаємих інформаційних ресурсів та встановлення порядку доступу до них повинні бути закріплені в документах підприємства;

– будинки та приміщення, де встановлені або зберігаються засоби обробки інформації, проводяться роботи з захищається інформацією, повинні охоронятися і бути захищені засобами сигналізації та пропускного контролю;

– проведення навчання персоналу з питань інформаційної безпеки (пояснювати важливість парольного захисту та пред'являємих до паролю вимог, проводити інструктаж з антивірусного ПЗ і т.п.) слід організовувати при прийомі співробітника на роботу;

– кожні 6-12 місяців проводити тренінги, спрямовані на підвищення грамотності співробітників в сфері інформаційної безпеки;

– аудит системи і коректування розроблених регламентів повинна проводитися щорічно, 1 жовтня, або негайно після впровадження серйозних змін в структуру підприємства;

– права доступу кожного користувача до інформаційних ресурсів повинні оформлятися документально (при необхідності доступ запитується у керівника письмовою заявою);

– забезпечення політики інформаційної безпеки повинні забезпечувати адміністратор з програмного забезпечення і адміністратор з апаратного забезпечення, їхні дії координуються начальником групи.

Сформулюємо політику щодо паролів:

– не зберігати їх в незашифрованому вигляді (не записував їх на папір, у звичайний текстовий файл і т.п.);

– змінювати пароль в разі його розголошення або підозри на

розголошення;

– довжина повинна бути не менше 8 символів;

– в числі символів пароля повинні бути присутніми букви у верхньому і нижньому регістрах, цифри і спеціальні символи, пароль не повинен включати в себе легко обчислювані послідовності символів (імена, клички тварин, дати);

– змінювати один раз на 6 місяців (позапланова заміна пароля повинна проводитися негайно після отримання повідомлення про подію, який ініціював заміну);

– при зміні пароля можна вибирати ті, які використовувалися раніше (паролі повинні відрізнятися, щонайменше, на 6 позицій).

Сформулюємо політику щодо антивірусних програм і виявлення вірусів:

– на кожній робочій станції має бути встановлено ліцензійне антивірусне ПЗ;

– оновлення антивірусних баз на робочих станціях з виходом в Інтернет - 1 раз на добу, без виходу в Інтернет - не рідше 1 разу на тиждень;

– встановити автоматичну перевірку робочих станцій на виявлення вірусів (частота перевірок - 1 раз на тиждень: п'ятниця, 12:00);

– перервати оновлення антивірусних баз або перевірку на віруси може тільки адміністратор (слід встановити на вказане дію користувача парольний захист).

Сформулюємо політику щодо фізичного захисту:

– технічне зондування та фізичне обстеження на предмет несанкціонованих пристроїв, підключених до кабелів, проводити кожні 1-2 місяці;

– мережеві кабелі повинні бути захищені від несанкціонованого перехоплення даних;

– записи про всі передбачуваних і дійсних збоях, що сталися з обладнанням повинні зберігатися в журналі;

– кожна робоча станція повинна бути забезпечена джерелом

безперебійного живлення.

Визначимо політику щодо резервування інформації:

– для резервних копій слід відвести окреме приміщення, що знаходиться за межами адміністративного будинку (приміщення має бути обладнане електронним замком та сигналізацією);

– резервування інформації слід проводити щоп'ятниці, о 16:00.

Політика щодо прийому / звільнення співробітників повинна мати наступний вигляд:

– про будь кадрові зміни (прийом, підвищення, звільнення співробітника тощо) повинно протягом 24 годин повідомлятися адміністратору, який, у свою чергу, в строк, що дорівнює половині робочого дня повинен внести відповідні зміни в систему розмежування прав доступу до ресурсів підприємства;

– новий співробітник повинен проходити інструктаж у адміністратора, що включає ознайомлення з політикою безпеки і всіма необхідними інструкціями, рівень доступу до інформації новому співробітнику призначається керівником;

– при звільненні співробітника з системи видаляються його ідентифікатор та пароль, проводиться перевірка робочої станції на наявність вірусів, аналіз цілісності даних, до яких у співробітника був доступ.

Політика щодо роботи з локальною внутрішньою мережею (ЛОМ) та базами даних (БД):

– при роботі на своїй робочій станції і в ЛВС співробітник повинен виконувати тільки завдання, що безпосередньо стосуються його службової діяльності;

– про повідомлення антивірусних програм про появу вірусів співробітник повинен ставити до відома адміністратора;

– нікому, крім адміністраторів, які не дозволяється вносити зміни в конструкцію чи конфігурацію робочих станцій та інші вузли ЛВС, проводити встановлення будь-якого програмного забезпечення, залишати без контролю робочу станцію або допускати до неї сторонніх осіб;

– адміністраторам рекомендується постійно тримати запущеними дві програми: утиліту виявлення атаки ARP - spoofing і сніффер, використання якого дозволить побачити мережу очима потенційного порушника, виявити порушників політики безпеки;

– слід встановити ПЗ, що перешкоджає запуску інших програм, окрім призначених адміністратором, виходячи з принципу: «Будь-якій особі надаються привілеї, необхідні для виконання конкретних завдань». Всі порти комп'ютера повинні бути апаратно або програмно дезактивовані;

– ПЗ слід регулярно оновлювати.

Політика щодо роботи з Інтернет:

– за адміністраторами закріплюється право обмежувати доступ до ресурсів, зміст яких не має відношення до виконання службових обов'язків, а так само до ресурсів, зміст і спрямованість яких заборонені міжнародним і Українським законодавством;

– співробітнику забороняється завантажувати і відкривати файли без попередньої перевірки на наявність вірусів;

– вся інформація про ресурси, відвідуваних співробітниками компанії, повинна зберігатися в журналі і, при необхідності, може бути надана керівникам відділів, а також керівництву.

Крім цього, сформулюємо основні вимоги до складання паролів для співробітників.

Пароль все одно що ключі від будинку, тільки є ключем до інформації. Для звичайних ключів вкрай небажано бути втраченими, вкраденими, переданими в руки незнайомої людини. Те ж саме і з паролем. Звичайно, збереження інформації залежить не тільки від пароля, для її забезпечення потрібно встановити цілий ряд спеціальних налаштувань і, бути може, навіть написати програму, що захищає від злому. Але вибір пароля - це саме те дію, де тільки від користувача залежить, наскільки сильним буде це ланка в ланцюзі заходів, спрямованих на захист інформації.

При виборі пароля слід керуватися такими правилами:

– пароль повинен бути довгий (8-12-15 символів);

– містити як ЗАГОЛОВНІ, так і прописні латинські букви;

– містити цифри;

– не повинен бути словом зі словника (будь-якого, навіть словника спеціальних термінів і сленгу), ім'ям власним або словом кирилицею, набраними в латинській розкладці;

– його не можна пов'язати з власником;

– він змінюється періодично або в міру потреби;

– не використовується в цій якості на різних ресурсах (тобто для кожного ресурсу - для входу в поштову скриньку, операційну систему чи базу даних - повинен використовуватися свій, відмінний від інших, пароль);

– його можливо запам'ятати.

Використання великих і великих літер, а також цифр значно ускладнює завдання зловмисника з підбору пароля.

Пароль слід зберігати в секреті, а якщо ви запідозрили, що пароль став комусь відомий, змініть його. Також дуже корисно міняти їх час від часу.

2.2.7 Рекомендації начальнику СБ по розробці моделі зовнішніх і внутрішніх загроз

1 Для аналізу та, згодом для моніторингу стану зовнішніх і внутрішніх загроз підприємству доцільно, розробити ієрархічну систему таблиць окремо для обліку зовнішніх загроз і окремо для обліку внутрішніх.

2 Для опису зовнішніх загроз таблиці бажано проранжувати наступним чином:

– перша таблиця повинна містити дані всіх юридичних і фізичних осіб з перерахуванням можливих варіантів атак і на які цілі.

– друга і наступні таблиці повинні містити дані конкретної юридичної або фізичної особи, статистку атак і стан системи загроз.

– підсумкова таблиця повинна являти собою матрицю загроз, яка відображає ймовірність і величину потенційного збитку підприємству чи окремих об'єктах, або окремим бізнес-проєктам.

3 Для опису внутрішніх загроз також розробляються таблиці. Ці таблиці повинні бути прив'язані до певних технологічних ліній, наприклад:

– потенційні внутрішні загрози інформаційних ресурсів.

– потенційні внутрішні загрози в збиральному цеху.

– потенційні внутрішні загрози на складі і т.д.

Обов'язково повинна бути окрема таблиця, в якій би фіксувалася частота спроб реалізації загроз, який був нанесений збиток і, який збиток вдалося запобігти.

Важливо мати такі характеристики загроз: ймовірність здійснення (за даними статистики, можна використовувати статистику аналогічних підприємств, розташованих у цьому ж регіоні), усереднений збиток за однорідними цілям, основне джерело загроз і залучені сили і засоби.

2.2.8 Рекомендації керівнику торгівельного підприємства

Для підприємця, абсолютно ясно, що успіх у бізнесі забезпечений, якщо він будується на сучасній виробничій базі, на підприємстві працює висококваліфікований колектив, мотивований на ефективну роботу, залучені вигідні кредитні ресурси і т.д [30].

Зі сказаного випливає висновок, що бізнес успішний, якщо при інших сприятливих умовах, він організований як узгоджена ефективна система виробництва товарів або послуг, що користуються стабільним попитом. Звертаю вашу увагу на поєднання - «ефективна система». Інформаційна безпека бізнесу, підприємства той же буде забезпечена, тобто підприємство і бізнес будуть працювати в стані захищеності від зовнішніх і внутрішніх загроз, якщо буде організована ефективна система інформаційної безпеки на підприємстві або в бізнесі в цілому. Система інформаційної безпеки будуватиметься в залежності

від формату підприємства, умов виробничої діяльності, застосовуваних технологій, стану інфраструктури та багато чого іншого, про що йшлося вище.

2.2.9 Аналіз ризиків на підприємстві після впровадження

Розрахуємо рівень ризиків Th_i на основі критичності та ймовірності реалізації загрози через дану уразливість. Рівень ризиків показує, наскільки критичним є вплив даної загрози на ресурс з урахуванням ймовірності її реалізації.

Отримуємо значення рівня загрози по уразливості в інтервалі від 0 до 1 для ТП «Автохімія». Розрахуємо для кожної загрози окремо (табл. 2.6).

Таблиця 2.6 – Аналіз ризиків інформаційної безпеки

Загроза інформаційної безпеки (i)	Критичність реалізації загрози (ER_i)	Імовірність реалізації загрози ($P(V_i)$)	Загальний ризик (Th_i)
Підробка ідентифікатора користувача	20%	50%	0,10
Доступ до мережі неавторизованих користувачів	25%	60%	0,15
Шкідливе програмне забезпечення	10%	50%	0,05
Помилки користувачів	15%	50%	0,08
Перезавантаження трафіку	30%	50%	0,15
Перехоплення	60%	75%	0,45
Пошкодження ліній зв'язку	20%	30%	0,06
Технічна несправність компонентів мережі	15%	20%	0,03
Помилка технічного обслуговування	10%	30%	0,03
Збій програмного забезпечення	20%	30%	0,06
Неправильна маршрутизація повідомлень	40%	60%	0,24
Помилки при передачі	50%	20%	0,10

Умисне пошкодження	30%	50%	0,15
Некомпетентність персоналу	20%	30%	0,06
Сумарний ризик (Th_{Σ})			0,12

Отриманий показник $Th_{\Sigma} = 0,12$ нижче 15% - показує що заходи вдосконалення системи інформаційної безпеки на даному підприємстві зведені до мінімуму, що і було потрібно.

2.3 Висновок

У ході виконання роботи було розроблено систему управління інформаційної безпеки для типових торгівельних підприємств. Виконання запропонованої СУІБ дозволить торгівельному підприємству підвищити ефективність засобів захисту і скоротити ризик втрати інформації.

Дана система управління інформаційною безпекою була впроваджена на ТП «Автохімія». Були розроблені рекомендації до інформаційної безпеки торгівельного підприємства, рекомендації начальнику СБ по розробці моделі зовнішніх и внутрішніх загроз, рекомендації керівнику торгівельного підприємства. Показник ризиків інформаційної безпеки на підприємстві значно знизився, це показує що дані заходи ефективні.

РОЗДІЛ 3. ЕКОНОМІЧНИЙ РОЗДІЛ

Вступ

У роботі створена система управління інформаційною безпекою для типового торгівельного підприємства.

Загальна площа торгівельного підприємства складає 600 м^{2,} яка є власністю підприємства. Об'єм продаж складає 25 тисяч штук на рік. Продуктивність 20000000 грн на рік. Загальна численність персоналу 40 чоловік, з котрих 2 є системними адміністраторами.

Метою економічного розділу є визначення:

– капітальних витрат на створення та впровадження систем управління інформаційної безпеки;

– експлуатаційних витрат на підтримку функціонування СУІБ;

– визначення річного економічного ефекту від впровадження СУІБ.

3.1 Визначення капітальних витрат

Капітальні вкладення – це кошти, призначені для створення і придбання основних фондів і нематеріальних активів, що підлягають амортизації.

Капітальні (фіксовані) витрати на проектування та впровадження системи управління ІБ складають:

$$K = K_{пр} + K_{зпз} + K_{навч} + K_{н}, \qquad (3.1)$$

де $K_{пр}$ – вартість розробки проекту системи управління ІБ та залучення для цього зовнішніх консультантів, тис. грн.;

$K_{зпз}$ – вартість закупівель ліцензійного основного й додаткового ПЗ, тис. грн.;

$K_{навч}$ – витрати на навчання технічних фахівців і обслуговуючого персоналу, тис. грн.;

$K_н$ – витрати на встановлення та налагодження системи управління ІБ, тис. грн.

Для розробки СУІБ не потребує залучення зовнішніх спеціалістів, а буде використовувати власний персонал або персонал інших підрозділів торгівельного підприємства. Тому потрібно визначити лише вартість розробки проекту, наприклад, витрати на розробку політики, яка регулює діяльність системи управління ІБ. Вартість буде складати 25 000 грн.

Для використання впровадженої СУІБ потрібне придбання ліцензії:

1) M.E.DOC;
2) Avast!;
3) Програму-архіватор WinRar.

Покупка програми M.E.DOC коштує 19474 грн., сертифікат ключа електронного цифрового підпису та шифрування (печатки підприємства) на 1 рік коштує 811 грн., сертифікат відкритого ключа електронного цифрового підпису директора на 1 рік коштує 811 грн, сертифікат відкритого ключа електронного цифрового підпису бухгалтера на 1 рік коштує 811 грн., сертифікат відкритого ключа електронного цифрового підпису співробітника на 1 рік – 811 грн

Програма Avast! – ключ з терміном дії 1 рік коштує 559 грн.

Ключ Avast! Premier та усі ключі к M.E.DOC відносяться до експлуатаційних витрат.

Програма-архіватор WinRar коштує 950 грн.

Отже:

$$K_{зпз} = 19474 + 950 = 20424 \text{ грн.}$$

Витрати на навчання $K_{навч}$ технічних фахівців і обслуговуючого персоналу не визначаються, тому що є детальні рекомендації щодо процесу використання системи управління інформаційною безпекою, тому під час роботи співробітники, які будуть займатися цим процесом, отримуватимуть нові знання, якщо вони будуть недостатніми.

Витрати на впровадження та налагодження системи управління ІБ $K_н$, складаються з заробітної платні співробітників, які займалися створенням СУІБ, та кількості часу витраченого на це. Впровадженням системи управління інформаційною безпекою займалися 2 співробітників, заробітна платня одного працівника складає 180 грн. за годину, на процес впровадження може бути витрачено 5 днів, що дорівнює 40 робочим годинам. Таким чином розрахуємо $K_н$ та K за формулою (3.1):

$$K_н = 2 \cdot 180 \cdot 40 = 14400 \text{грн.}$$

Отже, капітальні витрати на створення та впровадження системи управління ІБ складають:

$$K = 25000 + 20424 + 14400 = 59864 \text{ грн.}$$

3.2 Розрахунок поточних (експлуатаційних) витрат

Експлуатаційні витрати – це поточні витрати на експлуатацію та обслуговування об'єкта проектування за визначений період (наприклад, рік), що виражені у грошовій формі.

Річні поточні витрати на функціонування системи визначаються за формулою (3.2):

$$C = C_{кл} + C_н + C_з + C_с + C_{ел} + C_о + C_{тос}, \text{ грн.} \quad (3.2)$$

де $C_{кл}$ - витрати на купівлю ліцензійних ключів необхідного ПЗ;

$C_н$ - витрати на навчання адміністративного персоналу й кінцевих користувачів;

$C_з$ - річний фонд заробітної плати інженерно-технічного персоналу;

$C_с$ - на соціальні відчислення;

$C_{ел}$ - вартість електроенергії;

$C_{о}$ - витрати на залучення сторонніх організацій;

$C_{тос}$ - витрати на технічне й організаційне адміністрування та сервіс.

Витрати на купівлю ліцензійних ключів необхідного ПЗ дорівнює:

$$C_{КЛ} = 559 + 811 + 811 + 811 + 811 = 3803 \text{ грн.}$$

Витрати на навчання адміністративного персоналу й кінцевих користувачів ($C_{н}$) визначаються за даними організації з проведення навчання з підвищення кваліфікаційного рівня, що буде коштувати 19 000 грн., для трьох співробітників, які займаються цим процесом.

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує СУІБ ($C_{з}$), складає:

$$C_{з} = З_{осн} + З_{дод}, \text{ грн.}, \quad (3.3)$$

де $З_{осн}$, $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн на рік.

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 8-10% від основної заробітної плати.

До річного фонду заробітної плати додається єдиний внесок на загальнообов'язкове державне соціальне страхування – консолідований страховий внесок, збір якого здійснюється відповідно до класів професійного ризику виробництва, до яких віднесено платників єдиного внеску, з урахуванням видів їх економічної діяльності.

$$З_{осн} = Ч_{г} \cdot Т_{г} \cdot n \cdot 12, \quad (3.4)$$

де $Ч_{г}$ – кількість годин, що працює робітник,

n – кількість робітників, які підтримують процес,

$Т_{г}$ – погодинна тарифна ставка.

Робітник працює 8 годин у день, 22 дні у місяць, погодинна тарифна ставка 180 грн., над підтримкою систем управління ІБ протягом року працюють 2 співробітника.

Обчислимо заробітну плату за формулами (3.3) та (3.4):

$$З_{осн} = 22 \cdot 8 \cdot 180 \cdot 2 \cdot 12 = 760320 \text{ грн.}$$

$$З_{дод} = 0{,}08 \cdot З_{осн} = 0{,}08 \cdot 760320 = 60825{,}60 \text{ грн}$$

$$С_з = З_{осн} + З_{дод} = 760320 + 60825{,}60 = 821145{,}60 \text{ грн.}$$

До річного фонду заробітної плати додається єдиний внесок на загальнообов'язкове державне соціальне страхування $С_с$, що є консолідованим страховим внеском, збір якого здійснюється відповідно до класів професійного ризику виробництва, до яких віднесено платників єдиного внеску, з урахуванням видів їх економічної діяльності. Відрахування на соціальні заходи від заробітної плати обчислюються за формулою, з урахуванням, що єдиний соціальний внесок складає 22%:

$$С_с = 0{,}22 \cdot С_з = 0{,}22 \cdot 821145{,}60 = 180625{,}03 \text{ грн.}$$

Витрати на технічне й організаційне адміністрування СУІБ – $С_{тос}$, визначаються у відсотках від вартості капітальних витрат $К$, 1-3% від витрат:

$$С_{тос} = 0{,}02 \cdot К = 0{,}02 \cdot 59864 = 1197{,}28 \text{ грн.}$$

$$С_о = 0$$

$$С_{ел} = 0$$

Отже, після отриманих результатів можливо визначити за формулою (3.2) річні поточні витрати:

$$C = 3803 + 19000 + 821145{,}60 + 180625{,}03 + 1197{,}28 + 0 + 0 =$$
$$1025770{,}91 \text{ грн.}$$

3.3 Оцінка величини збитку

Кінцевим результатом впровадження й проведення заходів щодо забезпечення інформаційної безпеки є величина *відвернених втрат*, що розраховується, виходячи з імовірності виникнення інциденту інформаційної безпеки й можливих економічних втрат від нього. По суті, ця величина відображає ту частину прибутку, що могла бути втрачена.

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

Необхідні *вихідні дані* для розрахунку:

$t_п$ – час простою вузла або сегмента мережі внаслідок атаки, годин;

$t_в$ – час відновлення після атаки персоналом, що обслуговує мережу, годин;

$t_{ви}$ – час повторного введення загубленої інформації співробітниками атакованого вузла або сегмента мережі, годин;

$З_о$ – місячна заробітна плата обслуговуючого персоналу (адміністраторів та ін.) з нарахуванням єдиного соціального внеску, грн на місяць;

$З_с$ – місячна заробітна плата співробітника атакованого вузла або сегмента мережі з нарахуванням єдиного соціального внеску, грн на місяць;

$Ч_о$ – чисельність обслуговуючого персоналу (адміністраторів та ін.), осіб.;

$Ч_с$ – чисельність співробітників атакованого вузла або сегмента мережі, осіб.;

$О$ – обсяг чистого прибутку/дохід від реалізації/ атакованого вузла або сегмента мережі, грн у рік, або оподаткований прибуток атакованого вузла або сегмента мережі;

$П_{зч}$ – вартість заміни встаткування або запасних частин, грн;

I – число атакованих вузлів або сегментів мережі;

N – середнє число можливих атак на рік.

Упущена вигода від простою атакованого вузла або сегмента мережі становить:

$$U = П_п + П_в + V, \tag{3.5}$$

де $П_п$ – оплачувані втрати робочого часу та простої співробітників атакованого вузла або сегмента мережі, грн;

$П_в$ – вартість відновлення працездатності вузла або сегмента мережі (переустановлення системи, зміна конфігурації та ін.), грн;

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

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

$$П_п = \frac{\sum З_с * Ч_с}{F} \cdot t_п, \tag{3.6}$$

де F – місячний фонд робочого часу (при 40-а годинному робочому тижні становить 160-176 ч).

Витрати на відновлення працездатності вузла або сегмента мережі включають кілька складових:

$$П_в = П_{ви} + П_{пв} + П_{зч}, \tag{3.7}$$

де $П_{ви}$ – витрати на повторне уведення інформації, грн;

$П_{пв}$ – витрати на відновлення вузла або сегмента корпоративної мережі, грн;

$П_{зч}$ – вартість заміни устаткування або запасних частин, грн.

Витрати на повторне введення інформації $П_{ви}$ розраховуються виходячи з розміру заробітної плати співробітників атакованого вузла або сегмента корпоративної мережі $З_с$, які зайняті повторним введенням втраченої інформації, з урахуванням необхідного для цього часу $t_{ви}$:

$$П_{ви} = \frac{\sum З_с * Ч_с}{F} \cdot t_{ви} \qquad (3.8)$$

Витрати на відновлення вузла або сегмента мережі $П_{пв}$ визначаються часом відновлення після атаки $t_в$ і розміром середньогодинної заробітної плати обслуговуючого персоналу (адміністраторів):

$$П_{пв} = \frac{\sum З_о * Ч_о}{F} \cdot t_в \ . \qquad (3.9)$$

Втрати від зниження очікуваного обсягу продажів за час простою атакованого вузла або сегмента мережі визначаються виходячи із середнього динного обсягу продажів і сумарного часу простою атакованого вузла або сегмента мережі:

$$V = \frac{О}{F_г} \cdot (t_п + t_в + t_{ви}) \quad , \qquad (3.10)$$

де $F_г$ – річний фонд часу роботи торгівельного підприємства (52 робочих тижні, 5-ти денний робочий тиждень, 8-ми годинний робочий день) становить близько 2080 ч.

Таким чином, загальний збиток від атаки на вузол або сегмент мережі торгівельного підприємства складе

$$B = \sum\sum U \cdot I \,. \qquad (3.11)$$

Отже вихідні дані:

- $t_п = 26$ годин;
- $t_в = 9$ годин;
- $t_{ви} = 13$ годин;
- $З_о = 8 \cdot 22 \cdot 180 \cdot 1{,}195 \cdot 1{,}22 = 46186{,}27$ грн.;
- $З_с = 8 \cdot 22 \cdot 100 \cdot 1{,}195 \cdot 1{,}22 = 25659{,}04$ грн.;
- $Ч_о = 2$ людини;
- $Ч_с = 40$ людин;
- $О = 20\,000\,000$ грн.;
- $П_{зч} = 0$ грн.;
- $I = 40$.

Згідно формулою (3.5) – (3.11):

$$П_п = \frac{25659{,}04 \cdot 40}{160} \cdot 26 = 166783{,}76 \text{ грн.}$$

$$П_{ви} = \frac{25659{,}04 \cdot 40}{160} \cdot 13 = 83391{,}88 \text{ грн.}$$

$$П_{пв} = \frac{46186{,}27 \cdot 2}{160} \cdot 9 = 5195{,}96 \text{ грн.}$$

$$П_в = П_{ви} + П_{пв} + П_{зч} = 83391{,}88 + 5195{,}96 + 0 = 88597{,}84 \text{ грн.}$$

$$V = \frac{20000000}{2080} \cdot (29 + 9 + 13) = 490384{,}38$$

Згідно з формулою (3.5) та (3.11) отримаємо:

$$U = П_п + П_в + V = 166783{,}76 + 88597{,}84 + 490384{,}38 = 695765{,}98 \text{ грн.}$$

$$B = 27\,830\,639{,}20 \text{ грн.}$$

3.4 Загальний ефект від впровадження системи управління інформаційної безпеки

Загальний ефект від впровадження системи управління інформаційної безпеки визначається з урахуванням ризиків порушення інформаційної безпеки і становить:

$$E = B \cdot R - C, \tag{3.12}$$

де B – загальний збиток від атаки на вузол або сегмент мережі, тис. грн;

R – очікувана імовірність атаки на вузол або сегмент мережі, частки одиниці;

C – щорічні витрати на експлуатацію системи управління інформаційної безпеки, тис. грн.

Розрахуємо загальний ефект згідно з формулою (3.15):

$$E = 27\,830\,639{,}20 \cdot 0{,}12 - 1025770{,}91 = 2313905{,}80 \text{ грн.}$$

3.5 Висновок

У цьому розділі обґрунтована економічна доцільність використання приведеної у роботі створеної та впровадженої СУІБ. Для обґрунтування доцільності були визначені наступні фактори:

– капітальні витрати на впровадження системи управління ІБ на торгівельному підприємстві;

– експлуатаційні витрати на підтримку функціонування системи управління ІБ під час її використання;

– загальний ефект від впровадження СУІБ.

За отриманими результатами можна зробити висновок, що капітальні витрати на впровадження системи управління ризиками складають 59864 грн., а експлуатаційні витрати на підтримку функціонування системи складають

1025770,91 грн., загальний ефект від впровадження складає 2313905,80 грн., що значно менше ніж можливі збитки.

Враховуючи ці показники очевидно, що використовуючи впроваджену СУІБ, можливо значно зменшити збитки від реалізації загроз ІБ активам торгівельного підприємства. Але потрібно зазначити, що окрім визначених витрат, будуть витрат на впровадження елементів контролю, які дозволяють нейтралізувати ризики, а відповідно й збитки.

ВИСНОВКИ

Способи щодо вдосконалення інформаційної безпеки підприємства є мало витратними і досить ефективними, щоб убезпечити торгівельне підприємство від безлічі загроз інформаційної безпеки як ззовні, так і з середини. Хоча існують і інші способи, начебто тотального стеження за співробітниками, їх ефективність значно нижче і не потрапляє під категорію простих засобів. Крім того, не варто забувати, що забезпечення систем управління інформаційної безпеки не повинно завдавати шкоди діяльності підприємства або створювати перешкоди для роботи співробітникам.

Проведене дослідження дозволило зробити наступні висновки та сформулювати рекомендації.

Виділені особливості торгівельних підприємств у сфері забезпечення ІБ. Виділені найбільш вагомі ризики: шкідливе програмне забезпечення, перехоплення, підробка ідентифікатора користувача, доступ до мережі неавторизованих користувачів, помилки користувачів, перезавантаження трафіку, помилки при передачі і тощо.

Встановлено, що основною причиною проблем підприємства в галузі захисту інформації є відсутність політики забезпечення інформаційної безпеки, яка включала б організаційні, технічні, фінансові рішення з наступним контролем їх реалізації та оцінкою ефективності.

У процесі виконання роботи було проведено аналіз типового торгівельного підприємства для створення системи управління інформаційної безпеки. Був проведений аналіз інформаційних ресурсів ТП, аналіз загроз ІБ, і були виявлені відповідні недоліки. Також був проведений аналіз ризиків інформаційної безпеки типового торгівельного підприємства.

В ході виконання роботи також була створена системи управління інформаційної безпеки. Виконання запропонованої СУІБ дозволить торгівельному підприємству підвищити ефективність засобів захисту і

скоротити ризик втрати інформації. Слід зазначити, що процес організації або реорганізації інформаційної безпеки це комплексний процес, в якому взаємодіють одночасно програми, персонал і техніка.

Дана система управління інформаційною безпекою була впроваджена на підприємстві. Були розроблені рекомендації до інформаційної безпеки торгівельного підприємства, рекомендації начальнику СБ по розробці моделі зовнішніх и внутрішніх загроз, рекомендації керівнику торгівельного підприємства. Показник ризиків інформаційної безпеки на підприємстві значно знизився, це показує що дані заходи ефективні.

Новизна дослідження полягає в тому, що розроблені рекомендації зі створення системи управління інформаційною безпекою торговельних підприємств.

ПЕРЕЛІК ПОСИЛАНЬ

1 Домарев В. В. Захист інформації і безпека комп'ютерних систем - К.: ДіаСофт, 1999. – 443 стр.

2 ISO/IEC 27003 Методи і засоби забезпечення безпеки. Системи менеджменту інформаційної безпеки. Керівництво по реалізації системи менеджменту інформаційної безпеки.

3 Домарев В. В. Безпека інформаційних технологій. Системний підхід. Київ.2004.

4 Журнал «Захист інформації. INSIDE», №1, 2007 г., стр. 23-26 стаття «Методологія створення об'єктів інформатизації різного призначення в захищеному виконанні».

5 СУІБ 1.0/ISO/IEC 27001:2010 Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). Київ. 2010.

6 НД ТЗИ 2.5-006-99 и НД ТЗИ 2.7-002-99 Методичні вказівки з використання засобів копіювально-розмножувальної техніки.

7 НД ТЗИ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

8 НД ТЗИ 2.5-004-99. Критерії оцінювання захищеності інформації в комп’ютерних системах від несанкціонованого доступу. Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захист інформації Служби безпеки України від 28 квітня 1999 р. № 22. // Офіційний сайт Служби безпеки України. Спосіб доступу: URL: http: // www.dstszi.gov.ua/. – Загол. з екрана.

9 Буров Є. Комп'ютерні мережі. 2-ге оновлене і доповнене видання. Львів: БаК, 2003. – 584 с., іл.

10 Журнал «Захист інформації. INSIDE», №2, 2007 г., стр.64 – 67, Безпека комп’ютерних систем.

11 Глатенко В.А. Стандарти інформаційної безпеки / Відкрите видання 2006.- 264с

12 Староверов Д. Оцінювання загроз впливу конкурента на ресурси організації // Конфидент. Захист інформації. - №2. - 2005. - С. 58-62.

13 Сімонов С.В. Методологія аналізу ризиків в інформаційних системах / / Конфідент. захист інформації. - №1. - 2008. - С. 72-76.

14 Шпак В.Ф. Методологічні основи забезпечення інформаційної безпеки об'єкта // Конфідент. Захист інформації.- №1. - 2000. - С. 75-86.

15 Скот Бармен. Розробка правил інформаційної безпеки. Вильямс, 2002, - 208 с.

16 Ярочкін В.И. «Інформаційна безпека»; Гаудеамус, 2004; ISBN 5-98426-008-5.

ДОДАТОК А. Відомість матеріалів кваліфікаційної роботи

№	Формат	Найменування	Кількість листів	Примітка
1	А4	Реферат	2	
2	А4	Список умовних скорочень	1	
3	А4	Зміст	2	
4	А4	Вступ	2	
5	А4	1 Розділ	39	
6	А4	2 Розділ	50	
7	А4	3 Розділ	11	
8	А4	Висновки	1	
9	А4	Перелік посилань	2	
10	А4	Додаток А	1	
11	А4	Додаток Б	1	
12	А4	Додаток В	1	
13	А4	Додаток Г	1	

ДОДАТОК Б. Перелік документів на оптичному носії

1 Титульна сторінка.doc

2 Завдання.doc

3 Реферат.doc

4 Список умовних скорочень.doc

5 Зміст.doc

6 Вступ.doc

7 Розділ 1.doc

8 Розділ 2.doc

9 Розділ 3.doc

10 Висновки.doc

11 Перелік посилань.doc

12 Додаток А.doc

13 Додаток Б.doc

14 Додаток В.doc

15 Додаток Г.doc

Презентація.pptx

ДОДАТОК В. Відгуки керівників розділів

Відгук керівника економічного розділу:

Керівник розділу _____ _____

(підпис) (ініціали, прізвище)

ДОДАТОК Г. ВІДГУК
на кваліфікаційну роботу магістра на тему:
Розробка системи управління інформаційною безпекою
торгівельного підприємства «Автохімія»
Данильченка Олексія Ігоровича

Пояснювальна записка складається з титульного аркуша, завдання, реферату, списку умовних скорочень, змісту, вступу, трьох розділів, висновків, переліку посилань та додатків, розташованих на 116 сторінках та містить 5 рисунків, 10 таблиць, 16 джерел та 4 додатка.

Об'єкт дослідження: потоки інформації на типових торгівельних підприємствах.

Мета роботи: створення системи управління інформаційною безпекою торговельних підприємств.

У спеціальній частині розроблені комплекс заходів та рекомендацій щодо створення системи управління інформаційною безпекою торговельних підприємств. Розглянуто як об'єкт дослідження торгівельне підприємство «Автохімія». Дана СУІБ була впроваджена на підприємстві. Були розроблені рекомендації з інформаційної безпеки торгового підприємства.

В економічному розділі обґрунтована економічна доцільність використання наведеної в роботі створеної та впровадженої СУІБ на підприємстві.

Студент показав достатній рівень володіння теоретичними положеннями з обраної теми, показав здатність формувати власну точку зору (теоретичну позицію).

Робота оформлена та написана грамотною мовою. Містить необхідний ілюстрований матеріал. Автор добре знає проблему, уміє формулювати наукові та практичні завдання і знаходить адекватні засоби для їх вирішення.

В цілому робота задовольняє усім вимогам і може бути допущена до захисту, а його автор заслуговує на оцінку «_____».

Керівник