

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Будівництво, архітектура та дизайн
(повне найменування факультету)

Підприємство торівля та біржова діяльність
(повне найменування кафедри)

Пояснювальна записка

до дипломного проекту (роботи)

Бакалавр

(ступінь вищої освіти)

на тему Інформаційна безпека в підприємстві
діяльності
(назва теми)

Виконав(ла): студент(ка) 4 курсу, групи БМД-410

Спеціальності 076 Підприємство та торівля
(код і найменування спеціальності)

Освітня програма (спеціалізація)

Економіка підприємства

Добродіє М.А.

(ПІРІЗВИЩЕ та ініціали)

Керівник Хаченко А.В.

(ПІРІЗВИЩЕ та ініціали)

Рецензент Гармідер А.Ф.

(ПІРІЗВИЩЕ та ініціали)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

Факультет Економіко-управлінський факультет
Кафедра Підприємств, управління та маркетингу
Степінь вищої освіти Диплом
Спеціальність Економіка підприємств та маркетинг
(код і вимовлення)
Освітня програма (спеціалізація) Економіка підприємств
(код і вимовлення)

ЗАТВЕРДЖУЮ

Завідувач кафедри П.Т.Б.Р.
Ткаченко А.М.
« » 20 року

ЗАВДАННЯ
НА ДИПЛОМНИЙ ПРОЄКТ (РОБОТУ) СТУДЕНТА(КИ)

Розділ Маріка Андріївна
(ПРИЗВИЩЕ, ім'я, по батькові)

1. Тема проекту (роботи) Інформаційна безпека в підприємстві
діяльності

керівник проекту (роботи) п.в.н., д-р Хомченко Алла Валеріївна
(науковий ступінь, вчене звання, ПРИЗВИЩЕ, ім'я, по батькові)

затверджені наказом закладу вищої освіти від «12» квітня 2024 року № 140

2. Строк подання студентом проекту (роботи) 03.06.24

3. Вихідні дані до проекту (роботи) Завдання і запитання з теми
Інформаційна безпека підприємства, статистика збитків, методи
захисту інформації, інформаційна безпека підприємства

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Сучасне інформаційне середовище підприємства
аналіз сучасного управління інформаційною безпекою підприємства
ТОВ «ОМІК», вихідні дані управління інформаційною безпекою
підприємства.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень, кількості слайдів, плакатів)

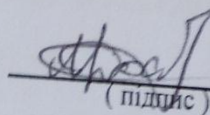
Розділ	ПРИЗВИЩЕ, ІМ'Я консультанта	Завдання
1-3	Н.С.Н., д-р Ханенко А.В.	
Переогляд роботи Н.А.		

7. Дата видачі завдання « 24 » травня 2024 року.

КАЛЕНДАРНИЙ ПЛАН

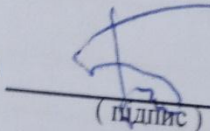
№ з/п	Назва етапів дипломного проекту (роботи)	Срок виконання етапів проекту (роботи)
1.	Визначення та узгодження зворотного зв'язку	24.05.2024
2.	Вибір статистичного матеріалу	24.05.2024
3.	Підготовка першого розділу	29.05.2024
4.	Підготовка другого розділу	30.05.2024
5.	Підготовка третього розділу	31.05.2024
6.	Подання на перевірку та переогляд	03.06.2024

Студент(ка)


(підпис)

Марина Касаріні
(Ім'я ПРИЗВИЩЕ)

Керівник проекту (роботи)


(підпис)

Алла Ханенко
(Ім'я ПРИЗВИЩЕ)

РЕФЕРАТ

Темою дослідження в дипломній роботі є: «Інформаційна безпека в підприємницькій діяльності». Містить 93 сторінок, 7 рисунків, 24 таблиць, 2 додатки та 34 літературних джерел.

Інформаційна безпека в підприємницькій діяльності є критично важливою складовою, яка забезпечує захист конфіденційної інформації, запобігає втраті даних та зменшує ризики, пов'язані з кіберзагрозами. В умовах сучасного інформаційного суспільства важливо мати надійну систему захисту даних для забезпечення стабільної та безпечної діяльності підприємства.

Метою даного дослідження є вивчення теоретичних засад та аналіз практичного досвіду підприємства у забезпеченні інформаційної безпеки в підприємницькій діяльності. Особлива увага приділяється розробці заходів щодо вдосконалення управління інформаційною безпекою на прикладі ТОВ "COMFY".

Завдання дослідження включають:

- аналіз сутності та складових інформаційної безпеки у сфері бізнесу;
- вивчення різноманітних інструментів для забезпечення інформаційної безпеки;
- розгляд методів оцінки рівня інформаційної безпеки на підприємстві;
- аналіз фінансово-економічної діяльності ТОВ "COMFY";
- дослідження системи управління інформаційною безпекою в компанії;
- розробка конкретних заходів для поліпшення управління інформаційною безпекою;
- оцінка ефективності впроваджених заходів.

ІНФОРМАЦІЙНА БЕЗПЕКА, ПІДПРИЄМНИЦЬКА ДІЯЛЬНІСТЬ, ЗАХИСТ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ, SWOT АНАЛІЗ.

ЗМІСТ

ВСТУП.....	6
ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	8
РОЗДІЛ 1 СУЧАСНЕ ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ.....	9
1.1 Інформаційний розвиток і його сучасні особливості.....	9
1.2 Особливості організації інформаційної безпеки підприємництва.....	20
1.3 Правові засади інформаційної безпеки суб'єктів підприємництва.....	30
РОЗДІЛ 2 АНАЛІЗ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ТОВ “COMFY”.....	37
2.1 Загальна характеристика підприємства ТОВ «COMFY»	37
2.2 Оцінка фінансово-економічного стану підприємства ТОВ «COMFY».....	46
2.3 Організація системи управління інформаційною безпекою ТОВ «COMFY».....	60
РОЗДІЛ 3 ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА	71
3.1 Заходи із вдосконалення інформаційною безпекою ТОВ «COMFY»..	71
3.2 SWOT-аналіз компанії ТОВ «COMFY».....	79
ВИСНОВКИ.....	88
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	90
ДОДАТКИ.....	93

ВСТУП

Актуальність теми. У сучасній економіці підприємства постійно працюють з великими обсягами даних, що робить інформацію цінним ресурсом. Однак зростання обсягів інформації супроводжується підвищенням ризиків її втрати або компрометації. Тому захист інформаційних ресурсів стає ключовою проблемою для багатьох організацій.

Сучасне управління підприємствами неможливе без ефективних інформаційних систем, які забезпечують підтримку усіх бізнес-процесів. В умовах швидкого розвитку технологій та збільшення кіберзагроз, забезпечення інформаційної безпеки є важливою складовою успішної діяльності компаній.

Інформаційна безпека включає захист конфіденційності, цілісності та доступності даних. Недостатня увага до цих аспектів може призвести до витоку інформації, фінансових втрат та інших серйозних наслідків, аж до зупинки бізнесу або банкрутства.[21]

Для забезпечення надійного захисту інформації необхідно застосовувати комплексні заходи: впроваджувати сучасні технології, розробляти політики безпеки та проводити навчання персоналу. Керівники підприємств повинні усвідомлювати, що ефективна система інформаційної безпеки є необхідною умовою для стабільного та успішного розвитку компанії.

Значущість вивчення інформаційної безпеки у сфері бізнесу обумовлена зростаючими ризиками, пов'язаними з розвитком сучасних технологій. Це потребує нових підходів до підвищення ефективності захисту даних на підприємствах в Україні.

Хоча існує багато наукових робіт на цю тему, питання інформаційної безпеки в бізнесі залишається актуальним і потребує подальших досліджень. Досвід компаній з України та інших країн показує, що для надійного захисту інформації необхідно впроваджувати цілісні системи безпеки, які включають технічні, організаційні та оперативні заходи.

Тема дослідження - аналіз стратегій забезпечення інформаційної безпеки в контексті діяльності компанії "COMFY".

Мета дослідження - вивчити теоретичні та практичні аспекти управління інформаційною безпекою на основі досвіду ТОВ "COMFY" та розробити рекомендації для покращення цієї системи.

Завдання дослідження включають:

- аналіз сутності та складових інформаційної безпеки у сфері бізнесу;
- вивчення різноманітних інструментів для забезпечення інформаційної безпеки;
- розгляд методів оцінки рівня інформаційної безпеки на підприємстві;
- аналіз фінансово-економічної діяльності ТОВ "COMFY";
- дослідження системи управління інформаційною безпекою в компанії;
- розробка конкретних заходів для поліпшення управління інформаційною безпекою;
- оцінка ефективності впроваджених заходів.

Моє дослідження базувалося на різноманітних методах та підходах до аналізу інформаційної безпеки в сфері підприємництва. Я використовувала не лише теоретичні концепції, але й практичні методи для вивчення ефективності систем управління безпекою.

Для аналізу системи управління інформаційною безпекою у ТОВ "COMFY" використовувалися економіко-математичні, структурологічні та графічні методи. Базою для дослідження послужили як законодавчі акти, так і публікації вітчизняних та зарубіжних авторів, а також фінансова звітність підприємства.

Отримані результати дослідження можуть глибше розкрити роль інформаційної безпеки у підприємницькій сфері та стати важливою основою для подальших досліджень. Розроблені заходи для підвищення ефективності систем управління інформаційною безпекою можуть бути успішно впроваджені в роботу підприємства "COMFY".

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

СУІБ - Система управління інформаційною безпекою

ІБ - Інформаційна безпека

ТОВ - Товариство з обмеженою відповідальністю

VPN - Віртуальна приватна мережа

MFA - Багатофакторна автентифікація

CISO - Chief Information Security Officer

ІТ - Інформаційні технології

NPS - Індекс підтримки споживача

AMP - Advanced Malware Protection

ESA - Email Security Appliance

РОЗДІЛ 1 СУЧАСНЕ ІНФОРМАЦІЙНЕ СЕРЕДОВИЩЕ ПІДПРИЄМНИЦЬКОЇ ДІЯЛЬНОСТІ

1.1 Інформаційний розвиток і його сучасні особливості

Сьогодні всі вже знають, що роль інформації у суспільстві набуває все більшого значення. Інформаційний розвиток, який пов'язаний з поширенням інформаційного компоненту завжди був присутнім у діяльності людства, і будь-який вид суспільного, економічного та технологічного розвитку в певних містах. Більше того, наукові відкриття, передбачення і гіпотези з'являлися задовго до їх матеріального втілення, служачи основою для прогресу. Чому саме сьогодні обговорюється мова про інформаційне суспільство, головну роль інформації в його розвитку? Які мають бути основні положення для удосконалення будь-яких політичних, технічних, економічних процесів?

Пояснюється це насамперед формуванням на сучасному етапі розвитку суспільства декількох факторів:

– Обсяги інформації значно збільшились. Для будь-якої діяльності, сфери або взаємовідносин характерне не лише велике число інформації. Було визначено, що один примірник газети "Нью-Йорк Таймс" містить більше інформації, ніж може отримати житель Англії за все своє життя. Збільшення знань почалося у 1900 році. Проводилось раз в 50 років, з 1950 р. Подвоєння відбувалось кожні 10 років, починаючи з 1970 року. — кожні 5 років, а з 1990 р.[2, 3]

– Щороку, якщо обсяг інформації зростає з такою швидкістю, то обсяг знань людини збільшується в мільйони разів. Розрив між кількістю інформації не тільки її засвоєнням а й розумінням. При цьому, властивості інформації є об'єктивними і існують одночасно. Природні або штучні чи навіть об'єктивні, вони значно доповнюють обсяг інформації.

– Швидкість зміни інформаційних атрибутів останнім часом зростає. На відміну від попередніх років, інформація повністю оновлена. Кожні 7 років,

така ситуація зумовлює необхідність швидкого прийняття соціальних дій та застосування духу. З іншого боку, швидке поширення інформації вимагає постійних досліджень. Необхідна інформація допомагає інформаційній індустрії залишатися в курсі справ. Невід'ємна складова будь-якої підприємницької діяльності в сучасних умовах;[5]

– За останні роки темпи обміну інформацією стрімко зросли. Зараз, на відміну від попередніх років, інформація оновлюється лише кожні 7 років. Воно вимагає швидкого здійснення соціальної діяльності та використання інтелектуальних благ. В результаті пошук необхідної інформації стає постійним, а робота з інформацією стає невід'ємною частиною будь-якої діяльності в сучасних умовах.[5]

– Враховуючи швидкі темпи обміну інформацією в сучасному світі, стає зрозуміло, що для успішного суспільного розвитку вже недостатньо лише збору фінансових і матеріальних ресурсів. Сучасні умови вимагають створення інформаційних ресурсів як невід'ємної складової ефективного функціонування суспільства.

– Сьогодні інформація існує не тільки як певна кількість інформації, а й як якась інформація відповідний технологічний процес разом з іншими технологіями може суттєво вплинути як на розвиток суспільства в цілому, так і на розвиток окремої людини. Ці технології здатні пришвидшити або, навпаки, уповільнити суспільний розвиток, надаючи переваги розвитку окремих галузей, чи концентрації суспільних зусиль у певних напрямках. До того ж, інформаційні технології мають здатність формувати характер відносин від мирного співіснування в суспільстві до великих конфліктів. Інформаційні технології, що впливають на характер взаємовідносин у суспільстві призвело до появи нового на сьогоднішній день виду зброї – її використання інформаційне не призводить до менших негативних наслідків, ніж зброя в загальноприйнятому розумінні цього слово.[6]

– Сучасний рівень демократизації та розвитку технологій призвів до значного розширення доступу до інформації. По-перше, збільшилося коло осіб,

які можуть отримати потрібну інформацію, по-друге знизився рівень конфіденційності інформації, значно збільшилась кількість джерел інформації. Глобалізація соціально-економічні відносини дають можливість навчатися майже з усіх частин інформаційного поля.

Враховуючи важливість інформаційних ресурсів для бізнес-організацій, інформаційна безпека стає важливим елементом успішної діяльності. Ось кілька прикладів:[21]

Захист конфіденційної інформації: підрозділи мають важливу конфіденційну інформацію, таку як права інтелектуальної власності, дані клієнтів і стратегічні плани. Захист цієї інформації виключає можливість несанкційованого доступу до цієї інформації, що допомагає запобігти втраті та пошкодженню зображення.

Запобігання кібератакам: у епоху цифрових технологій кібератаки стають серйозною загрозою для бізнес-організацій. Забезпечення належного захисту мереж, систем і даних допомагає запобігти знищенню інформаційних ресурсів і зберегти фінансову стабільність.

Захист репутації та іміджу: Порушення інформаційної безпеки може призвести до втрати довіри клієнтів і партнерів, що може негативно вплинути на позиції компанії на ринку. Забезпечення ефективної інформаційної безпеки допомагає запобігти таким ситуаціям і зберегти позитивний імідж.

Таким чином, ефективна інформаційна безпека не лише захищає інформаційні ресурси суб'єктів підприємництва, але і створює умови для стабільної діяльності, розвитку та забезпечення успішності на ринку.

Зазначені завдання мають бути інтегровані у повсякденну діяльність суб'єктів підприємництва шляхом планової роботи як спеціальних підрозділів інформаційної безпеки, так і всіх інших, що входять до складу організаційної структури суб'єктів. Останні мають забезпечувати свою інформаційну безпеку всією сукупністю своїх економічних, інтелектуальних, технічних, кадрових можливостей.

Організація інформаційної безпеки суб'єктів підприємництва здійснюється на основі принципу централізованого управління стратегічним розвитком суб'єктів і їх безпеки, як правило, у сукупності заходів, що виконуються ними у сфері забезпечення їх безпеки.[7]

Таблиця 1.1 – Основні принципи інформаційної безпеки

Вимога	Опис
1	2
Законність	заходи, що виконуються в межах організації та здійснення інформаційної безпеки мають вкладатись в межі чинного законодавства, не порушувати права та свободи громадян, законні інтереси інших суб'єктів та держави;
Самостійність та відповідальність	заходи інформаційної безпеки обираються суб'єктами підприємництва самостійно, в межах своїх можливостей і повинні бути адекватними загрозам їх інформаційній безпеці; за результати вжитих заходів відповідальність покладається на суб'єктів підприємництва та уповноважених ними на проведення таких заходів осіб;
Компетентність	виконання заходів інформаційної безпеки має здійснюватись грамотно, на високому професійному рівні, підготовленими для цього фахівцями;
Економічна доцільність	витрати на організацію та виконання заходів інформаційної безпеки повинні бути адекватними її ефективності, не завдавати шкоди економічному стану суб'єктів підприємництва;
Економічна доцільність	витрати на організацію та виконання заходів інформаційної безпеки повинні бути адекватними її ефективності, не завдавати шкоди економічному стану суб'єктів підприємництва;

Продовження таблиці 1.1

1	2
Цілеспрямованість	заходи інформаційної безпеки мають здійснюватись у строгій відповідності основним завданням і напрямком діяльності суб'єктів підприємництва;
Конфіденційність	переважна сукупність заходів інформаційної безпеки проводиться на конфіденційній основі, інформування про їх проведення та результати, здійснюється лише обмеженому колу осіб.

Надійність та ефективність інформаційної безпеки суб'єктів підприємництва визначається через її відповідність встановленим вимогам, якими можуть бути:

– безперервність забезпечення інформаційної безпеки – заходи інформаційної безпеки проводяться з початком її організації і продовжуються протягом всього часу існування суб'єкта підприємництва, посиляючи та послаблюючи в окремих ситуаціях, але без їх припинення;

– плановість інформаційної безпеки – встановлення відповідного порядку застосування заходів інформаційної безпеки, який б забезпечував запобіжний характер їх впливу на виникнення небезпек і загроз;

– конкретність інформаційної безпеки – заходами безпеки мають бути охоплені конкретні об'єкти та дії суб'єктів підприємництва; заходи безпеки повинні бути пов'язані з конкретними операціями, угодами, відносинами, які здійснюються на даний час суб'єктами підприємництва;

– активність інформаційної безпеки – в арсеналі заходів інформаційної безпеки повинні бути як такі, що забезпечують захист інформаційного ресурсу та іміджу суб'єктів підприємництва, так і ті, які спрямовуються на протидію заходом негативного впливу та розкриття їх джерел;

– комплексність інформаційної безпеки – передбачає необхідність застосування у забезпеченні безпеки різних форм, методів, засобів, заходів щодо різних видів інформації та інформаційних відносин.

Реалізація принципів і вимог до інформаційної безпеки неможлива без конкретизації самого об'єкта безпеки. Враховуючи багатофункціональність інформації можна бачити її присутність у будь-якому матеріальному чи нематеріальному об'єкті або у будь-якому виді діяльності. Тобто, будь-який об'єкт чи діяльність можна подати інформаційно, зробити уявлення про нього на основі його інформаційних характеристик. Таким чином, беручи за об'єкт інформаційної безпеки інформацію, маємо обов'язково пов'язати її з певним об'єктом (людиною, підприємством, установою, організацією, предметом) або ж з відповідним видом діяльності. Тоді об'єктом буде виступати уже не інформація як така, а інформація про щось (об'єкт чи діяльність). Разом з тим, інформація про щось може бути об'єктом інформаційної безпеки лише тоді коли вона буде мати певну цінність (для підприємництва – комерційну цінність) і щодо неї буде проявлена зацікавленість з боку інших осіб. Враховуючи наведене, інформацію як об'єкт інформаційної безпеки можна подати наступним чином – Рисунок 1.1.

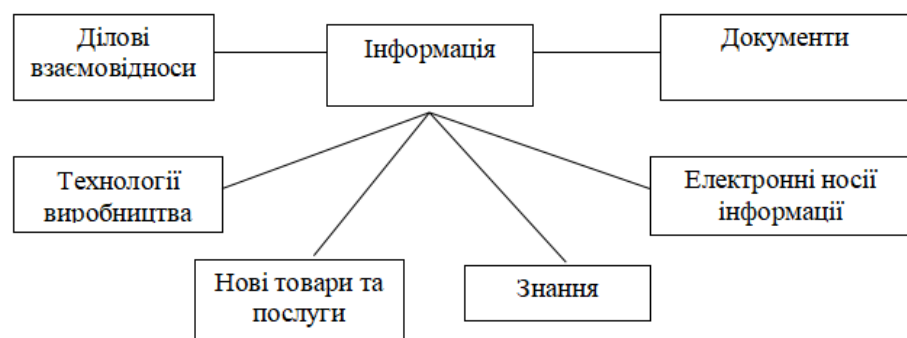


Рисунок 1.1 – Інформація як об'єкт інформаційної безпеки

У практиці забезпечення інформаційної безпеки суттєве значення має визначення її видів. Особливо це необхідно з т. з. організації інформаційної безпеки в діяльності суб'єктів підприємництва.

Аналізуючи практику інформаційних відносин суб'єктів підприємницької діяльності та беручи до уваги роль інформації в такій діяльності, можна говорити, що інформаційна безпека підприємництва включає наступні її види: комп'ютерну безпеку, інформаційно-психологічну безпеку, комунікаційну безпеку та документаційну безпеку.[21]

Комп'ютерна безпека передбачає: захист засобів комп'ютеризації, комп'ютерних технологій і інформації, що знаходиться на електронних носіях; отримання необхідної суб'єктам підприємництва інформації із глобального інформаційного простору (мережі Інтернет) для формування їх інформаційного ресурсу; протидія інформаційним загрозам в середовищі електронної інформації(комп'ютерні віруси, шкідливі програми, комп'ютерний тероризм і т. п.) [4]

Інформаційно-психологічна безпека зосереджує свої зусилля у сфері знань своєї інформації та її носіїв (працівників, клієнтів, споживачів продукції суб'єктів підприємництва). Основними напрямками забезпечення інформаційної безпеки є захист своєї інформації (організація захисту інтелектуальної власності, режиму використання інформації працівниками та іншими особами у процесі інформаційних відносин); збереження інформаційного здоров'я працівників суб'єктів підприємництва в умовах інформатизації виробництва; розробка технологій отримання знань своєї інформації (наукові дослідження, конференції, семінари, курси, симпозіуми і т. п.) для формування інформаційного ресурсу суб'єктів підприємництва; протидія технологіям маніпулювання інформацією, індивідуальною та колективною свідомістю.

Комунікаційна безпека включає захист інформації в процесі взаємообміну (електронна пошта, мобільний зв'язок) та ділового спілкування (зустрічі, перемовини); проведення заходів пропаганди, контр-пропаганди та агітації в інформаційному середовищі суб'єктів підприємництва; протидія поширенню негативної інформації засобами масової комунікації.

Документаційна безпека спрямована перш за все на захист документованої інформації та її носіїв, насамперед через запровадження надійної системи загального і спеціального діловодства, розробки нормативних документів з питань інформаційної безпеки; запровадження технологій отримання необхідних даних з різного роду документів (правових актів, звітів, звичайних публікацій, виступів, описів і т. п.) для формування інформаційного ресурсу суб'єктів підприємництва; документальне супроводження протидії інформаційним загрозам та інформаційно-психологічному впливу щодо суб'єктів підприємництва, їх діяльності та персоналу (документування фактів порушення інформаційного режиму, поширення неправдивої інформації чи маніпулювання нею, документальне спростування негативної інформації, документи щодо вимог відшкодування моральної шкоди і т. і.).

Розвиток інформаційних технологій призвів до значного збільшення обсягу доступної інформації та розширення сфери її використання, сприяючи виникненню нового етапу суспільного розвитку. Однією з головних характеристик цього етапу є значне зростання інтелектуального потенціалу в усіх сферах життя.

Економіка та менеджмент: завдяки доступу до великих обсягів даних та розвитку аналітичних інструментів сучасні економічні та управлінські процеси стають більш об'єктивними та ефективними. Аналітика дозволяє краще розуміти стан ринку, прогнозувати тенденції та приймати більш зважені рішення.

Виробництво та технології: такі інструменти ІІІ, як машинне навчання та розпізнавання образів, уже широко використовуються у виробничих процесах. Вони допомагають автоматизувати рутинні операції, покращити якість продукції та знизити витрати виробництва.

Творчість та інноваційність: широкий доступ до різноманітної інформації та інструментів для її обробки спонукає до творчого підходу до діяльності. Люди мають можливість використовувати нові ідеї та ресурси для створення інноваційних продуктів і послуг.

Отже, розвиток сучасних знань забезпечує створення сприятливих умов для розвитку суспільства, робить його діяльність більш обґрунтованою, ефективною та творчою.

Важливою характеристикою інформаційного розвитку є т. з. інформаційна експансія – активне поширення відповідними суб'єктами їх інформації, ідеології, поглядів, оцінок, інтерпретацій в межах конкретно обраного інформаційного простору. Інформаційна експансія може здійснюватись тривалий час забезпечуючи постійний вплив на суб'єктів інформаційного середовища або ж проводиться у вигляді інформаційних атак з метою пропаганди чи маніпулювання індивідуальною або громадською думкою. Прийнято вважати, що інформаційна експансія – прояв інформаційної політики країни у їх міжнародних відносинах. На сьогодні таку точку зору можна вже доповнювати тезою про застосування інформаційної експансії у конкурентній боротьбі суб'єктів підприємництва, в т.ч. і в межах однієї країни, внутрішнього ринку.

Використовуючи різного роду засоби пропаганди, маніпулювання інформацією, інформаційно-психологічного впливу та концентруючи їх заходи на окремому ринку, регіоні певні суб'єкти здобувають необхідні їм переваги за рахунок переконання потенційних споживачів їх продукції у вигідності взаємовідносин з такими суб'єктами. Окремо слід було б звернути увагу на те, що інформаційний розвиток, утворюючи сприятливі умови для суспільства та його суб'єктів, обумовив додатково різного роду проблеми, протиріччя, конфлікти, які здатні створювати значні небезпеки та загрози, причому як для окремих суб'єктів, так і для всього суспільства.

Спостереження показують, що інтенсивний розвиток інформаційних технологій в сучасному суспільстві і виробничому процесі породжує складні ситуації. При масовому поширенні цих технологій, вони випереджають можливості багатьох суб'єктів та громадян у вмінні грамотно ними користуватися, особливо в професійному плані. Навіть за наявності фахівців у

галузі інформаційних технологій, більшість громадян залишаються недостатньо підготовленими до життєдіяльності в умовах сучасної інформатизації.

Затрати на розробку та впровадження новітніх інформаційних технологій не завжди оправдовуються, іноді перевага перетворюється на збитки. Інформаційні технології можуть суперечити менталітету громадян та професійним навичкам фахівців, а також призводити до виникнення негативних або навіть небезпечних ситуацій, що вийшли з-під контролю.

У таких умовах існуючі тенденції інформаційного розвитку настійливо вимагають від громадян та керівників на всіх рівнях інформаційної грамотності та культури. Очевидно, що адаптація населення до рівня інформатизації суспільства стає нагальною потребою.

У світі, насиченому цифровими технологіями, стикаємося з безпрецедентними можливостями та викликами. Нові інформаційні технології, втілені в нашій щоденній діяльності, не лише спрощують рутинні завдання, але й перетворюють спосіб, яким ми спілкуємося, працюємо та живемо. Проте, зі зростанням впливу цифрового світу збільшується і потенційна загроза – від захоплення особистих даних до залежності від технологій.

Освоєння цього цифрового ландшафту вимагає від нас постійного оновлення наших знань та навичок. Нам необхідно не лише засвоювати нові інструменти, а й розвивати критичне мислення щодо їхнього використання. Навіть найпростіші програми можуть мати складні наслідки, якщо використовуються недбало.

У світлі цих викликів, необхідно розглядати інформаційну грамотність як необхідний навик для всіх членів суспільства. Навчання в цій галузі повинно стати складовою частиною освіти на всіх рівнях – від шкільної до професійної. Також, важливо забезпечити доступність навчальних ресурсів та підтримку для тих, хто потребує додаткової допомоги.

Збільшення інформаційної грамотності населення не лише допоможе уникнути негативних наслідків цифрового розвитку, але й сприятиме

створенню більш безпечного, збалансованого та рівного доступу до можливостей, які надають ці технології.

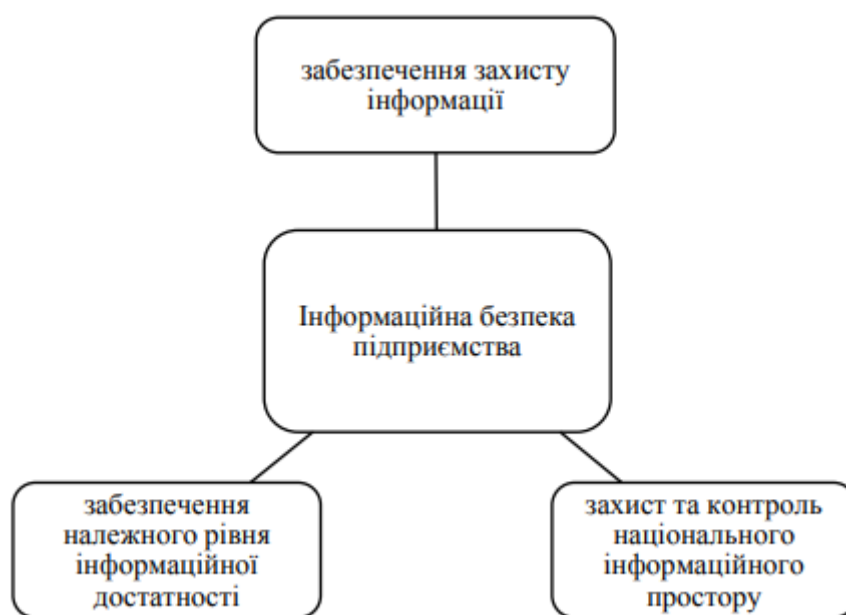


Рисунок 1.2 – Інформаційна безпека підприємства

Розвиток інформаційної грамотності є критично важливим в контексті сучасного світу. Крім розуміння технологій, потрібно акцентувати увагу на розвитку критичного мислення, етичності та здатності аналізувати та оцінювати інформацію.

Освіта в галузі інформаційної грамотності повинна починатися ще з раннього дитинства, і включати в себе навички розпізнавання дезінформації та фейків, здатність критично оцінювати джерела інформації, а також вміння захищати свої особисті дані в онлайн-середовищі.

У цьому процесі важливу роль відіграють і вчителі, і батьки. Вони повинні бути освіченими щодо цифрових технологій, щоб вони могли передати ці знання своїм учням та дітям. Батьки можуть бути партнерами в навчанні, надаючи дітям можливість практикувати безпечне використання Інтернету та соціальних мереж.

Окрім цього, важливо створити середовище, де кожен має доступ до навчальних ресурсів та підтримки для розвитку своєї інформаційної

грамотності. Це може включати в себе безкоштовні курси, вебінари та інші освітні ініціативи, спрямовані на підвищення обізнаності у сфері цифрових технологій.

Загальновизнано, що інформаційна грамотність є ключовою для успішного функціонування в сучасному цифровому світі. Інвестування у розвиток цього навчання не лише допоможе індивідуумам використовувати технології більш ефективно, а й сприятиме створенню більш безпечного та рівного суспільства.

1.2 Особливості організації інформаційної безпеки підприємництва

Сучасні тенденції розвитку інформації за останні роки істотно змінили всі сфери життя, в тому числі і бізнес. Формування взаємовідносин знань стало не лише важливою складовою, а й постійною ознакою існування суспільства, спільнот і компаній.

Такий розвиток призвів до появи нових типів ризиків і загроз щодо інформаційного поля. Інтенсивність цих ризиків залежить від якості взаємовідносин між суб'єктами господарювання. Інформаційні ризики мінімальні, коли співпраця ґрунтується на відкритості та довірі. Однак у ситуаціях, коли спілкування формується конфліктом і конкуренцією, інформаційні загрози стають ще більш важливими.[8]

У зв'язку з цим бізнес-організації повинні бути готові запровадити адекватні засоби захисту від інформаційних ризиків і загроз. Захист від цих загроз і протидія мають стати окремим аспектом безпеки бізнесу (інформаційної безпеки).

Дослідження, проведені авторами інформаційної безпеки виявили різні підходи до розуміння безпеки бізнесу, особливо безпеки інформації. Різні автори по-різному розуміють сутність і зміст інформаційної безпеки.

Проте дослідження показують, що більшість експертів віддають перевагу захисту інформації як основному елементу інформаційної безпеки

підприємства. Це загальноприйнятий підхід, який визначається насамперед багатофункціональністю інформації в контексті господарської діяльності.

Такий підхід до інформаційної безпеки заснований на визнанні важливості захисту конфіденційної інформації, відновленні даних та забезпеченні безперервності бізнес-процесів.

Як зазначалося раніше, інформація є основою інформаційно-інтелектуального потенціалу господарських організацій, що потребує законодавчої охорони. Водночас необхідно враховувати, що інформація також виступає як важливий фактор здійснення підприємницької діяльності: вона впливає на ринкову ситуацію, відносини між суб'єктами та має важливе ділове значення.[9]

Таким чином, може бути недоцільним обмежувати інформаційну безпеку лише захистом інформації в умовах, де її функції дуже різноманітні. На думку авторів, метою інформаційної безпеки також має бути мінімізація інформаційних ризиків і мати життєво важливе значення для управління та їх розвитку.

Інформаційні технології також можуть використовуватися як інтелектуальна зброя, яка може негативно вплинути на діяльність компаній. Тому інформаційна безпека повинна включати також заходи проти інформаційно-психологічного впливу та маніпулювання свідомістю.

Тому під інформаційною безпекою бізнесу можна розуміти стан інформаційної роботи, який забезпечує ефективну роботу компаній, надійний захист інформаційних ресурсів, успішне придушення негативних інформаційно-психологічних впливів.

Тобто, структуру інформаційної безпеки суб'єкта підприємництва складають три складові, наведені на рисунку 1.3.

Враховуючи динамічний характер сучасного інформаційного простору, такий підхід до розуміння суті та змісту інформаційної безпеки забезпечує суб'єктам підприємництва необхідний рівень живучості у їх конкурентній боротьбі, більш оптимальну поведінку у взаємовідносинах поміж собою,

іншими організаціями та інституціями. Інформаційна безпека у такому розумінні виступає формою існування суб'єктів підприємництва у інформаційному середовищі.

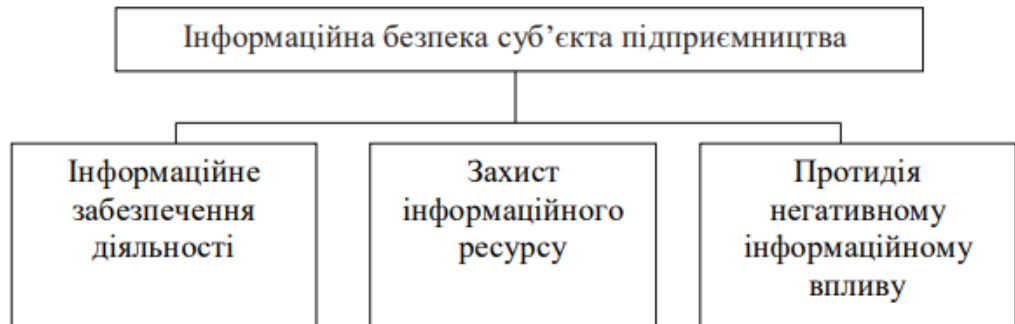


Рисунок 1.3 – Структура інформаційної безпеки суб'єкта підприємництва

Досягнення мети інформаційної безпеки вимагає виконання кількох завдань, спрямованих на запобігання втратам інформаційних ресурсів і шкоди репутації бізнес-організацій, а також створення умов для ефективної діяльності та отримання прибутку. Деякі з цих завдань включають:

- Регулювання належного функціонування інформації в діяльності господарських організацій, включаючи встановлення внутрішніх правил і процедур безпечної обробки, зберігання та передачі інформації.
- Створення необхідних інформаційних ресурсів, що включає створення та підтримку баз даних, програмного забезпечення та інших інформаційних ресурсів, необхідних для успішної діяльності.
- Своєчасне виявлення загроз інформаційним ресурсам та іміджу бізнес-організацій та загроз їх інформаційним відносинам, що вимагає систематичного аналізу та моніторингу можливих загроз і вразливостей.
- Швидке реагування на зміни та порушення умов інформаційних відносин, включаючи спроби проникнення в інформаційні ресурси та репутацію комерційних організацій.
- Забезпечення проникнення знань у необхідні сегменти ринку для підтримки та розвитку діяльності компаній.

- Навчання персоналу підприємницьких організацій з питань інформаційної безпеки, включаючи навчання та розвиток інформаційної компетентності.

- Оптимізувати заходи та витрати щодо забезпечення інформаційної безпеки господарської діяльності з метою ефективного використання ресурсів.

Ці завдання мають бути інтегровані в повсякденну діяльність. Господарські організації з плановою роботою як спеціальні підрозділи інформаційної безпеки та всі інші питання, які є частиною організаційної структури предметів. По-друге, він повинен забезпечувати інформаційну безпеку: економічні, інтелектуальні, технічні, все, що стосується персоналу можливості. Організація інформаційної безпеки комерційних організацій.

Це здійснюється за принципом централізованого стратегічного управління і, як правило, безпеки за допомогою різних заходів. Вони роблять це для власної безпеки.

Деякі дослідники розглядають інформаційну безпеку як захист важливих інтересів особи, суспільства і держави, метою якого є мінімізація негативного впливу інформаційних технологій і шкоди, яку може завдати неповна, несвоєчасна, недостовірна або негативна інформація.

Для багатьох дослідників інформаційна безпека суспільства визначається як соціальний сторожовий пес, який забезпечує захист інформаційної інфраструктури та інформації, що передається через неї, у спосіб, який не завдає шкоди духовній сфері, культурним цінностям чи поведінці людини.

На думку дослідників, неможливо передбачити всі можливі загрози інформаційній безпеці, оскільки вони постійно змінюються, а для забезпечення регуляторного нагляду необхідна стабільність.

Тому політика інформаційної безпеки спрямована не лише на пошук відповідей на конкретні загрози, а й на створення безпечних умов функціонування інформаційного простору. Він захищає інформаційне середовище від можливих негативних впливів. Експерти по-різному розуміють

термін «інформаційна безпека» і часто акцентують увагу на різних аспектах проблеми.

Наприклад, для керівників компаній серйозною загрозою є крадіжка конфіденційних файлів, тоді як для розробників антивірусного програмного забезпечення серйозною загрозою є злам цінних даних. Кожне з цих питань необхідно розглядати окремо, але для споживачів важливий не лише особистий ризик, але й загальна безпека.

Експерти вважають, що безпека корпоративної інформації включає конкретні заходи, спрямовані на виявлення, усунення та запобігання шкідливим джерелам, причинам і умовам, що впливають на інформацію. Це досягається системою заходів, спрямованих на запобігання, виявлення та усунення інформаційних загроз.

Проблеми інформаційної безпеки можуть серйозно вплинути на такі організаційні параметри, як конфіденційність, цілісність і доступність. Це може призвести до різних негативних сценаріїв, таких як функціональні збої в системах управління, розголошення конфіденційної інформації, фінансові збої та несанкційований доступ до особистої інформації. Наслідки можуть включати напружені ділові відносини, втрату контрактів, фінансові втрати і навіть банкрутство. Тому для створення ефективної системи захисту інформації важливо аналізувати загрози та ризики.

Людський фактор також відіграє ключову роль у ризиках інформаційної безпеки. Більшість нещасних випадків трапляється через помилки або неправильну поведінку співробітників. Керівники часто не розуміють внутрішніх загроз; Це свідчить про те, що потрібно приділяти більше уваги інформаційній безпеці. Це підкреслює важливість інформаційної безпеки як фактора виживання компаній.

Це справді важлива тема, яка стосується всіх компаній, незалежно від їх розміру. Недостатня увага до безпеки може призвести до серйозних проблем із захистом даних і бізнес-операціями в цифровому середовищі.

Дуже цікаво, як різні компанії сприймають безпеку. Зрозуміло, що випадкові кібератаки можуть бути серйознішими, оскільки їх важче передбачити та запобігти. Але керівники часто зосереджуються на навмисних ризиках, нехтуючи потенційними випадковими подіями, які можуть статися через помилки співробітників або технічні недоліки.

Тривожно чути, що багато компаній не знають джерел та причин внутрішніх загроз. Це свідчить про те, що інформаційна безпека не завжди отримує належну увагу. Але для подолання цієї проблеми кожна компанія повинна розробити свій власний підхід до безпеки, враховуючи свої потреби та можливі ризики.

Варто пам'ятати, що навіть найкращі заходи безпеки можуть бути обірвані випадковими помилками та неуважністю. Тому, незважаючи на витрати, належний рівень захисту є ключовим для забезпечення конкурентоспроможності та стійкості компанії у цифровому світі.

Таблиця 1.2 – Збитки, спричинені настанням інформаційних ризиків

Тип ризику	Потенційні збитки
1	2
Втрата конфіденційності	Фінансові втрати від розголошення конфіденційної інформації, втрата довіри клієнтів
Порушення цілісності	Фінансові збитки внаслідок маніпуляцій з даними або пошкодженням інформації
Недоступність	Втрати прибутку внаслідок припинення роботи систем або сервісів, репутаційні збитки

Один з найбільш очевидних наслідків відсутності політики інформаційної безпеки - негативні відгуки зовнішніх аудиторів. Це може суттєво підірвати

довіру до компанії, вплинути на її репутацію та позицію в рейтингах надійності. Немає сумніву, що рівень втрат, які може завдати компанії інформаційний ризик, залежить від конкретних об'єктів інформації.

Ці приклади демонструють різноманітні аспекти інформаційних ризиків та можливі наслідки для бізнесу. Надійна політика інформаційної безпеки може значно зменшити ймовірність виникнення таких ситуацій та мінімізувати їх наслідки.

Не слід забувати, що класифікація шкоди, спричиненої атакою, повинна здійснюватися власником інформації або персоналом, який використовує інформацію. Тільки вони можуть оцінити реальний вплив і наслідки порушення безпеки даних на діяльність компанії.

Також, можливість атаки багато в чому залежить від технічного персоналу компанії. Рівень умінь і навичок виявлення загроз і боротьби з ними значною мірою визначає загальний рівень інформаційної безпеки організації.

Залежно від організаційної структури за інформаційну безпеку компанії можуть відповідати різні відділи. Наприклад, функції підрозділу можуть бути передані системному адміністратору, а сам підрозділ може бути включений до складу служби інформаційної безпеки та підпорядкований вищому управлінському рівню. Також є організації, де відповідальність за економічну безпеку покладено на Службу економічної безпеки.

Вирішення цих проблем вимагає комплексного підходу та взаємодії різних відділів і персоналу для забезпечення найвищого рівня інформаційної безпеки в організації.

Таблиця 1.3 – Втрати від настання інформаційного ризику

Величина ризику	Опис
1	2
0,1-0,2	Оголошення інформації принесе незначні моральні і фінансові втрати підприємству

Продовження таблиці 1.3

1	2
0,2-0,3	Втрати від інформаційної атаки є, але вони незначні, основні фінансові операції і стан підприємства на ринку не порушено
0,3-0,4	Фінансові операції не ведуться протягом деякого часу, підприємство зазнає збитків, але його стан кількість клієнтів змінюються мінімально
0,4-0,6	Значні втрати на ринку й у прибутку. Підприємство втрачає значну частину клієнтів
0,6-0,8	Втрати дуже значні, підприємство на період до року втрачає можливості для відновлення

У контексті загальних завдань безпеки бізнесу найкращою стратегією вирішення проблем інформаційної безпеки є інтеграція цих проблем у загальну систему безпеки. У сучасних умовах інформаційна безпека стає не лише складовою внутрішнього управління компанією, а й важливим елементом, що впливає на її стабільність і конкурентоспроможність у реальному секторі економіки.

Забезпечення надійної інформаційної безпеки стає важливим етапом переходу економіки країни до моделі сталого розвитку. Він підкреслює не лише важливість індивідуальних заходів безпеки на рівні підприємства, а й розробку та впровадження комплексної національної стратегії інформаційної безпеки.

Особливу увагу слід приділити практичній реалізації запланованих заходів з захисту інформації. Вона повинна бути основою для розробки та реалізації інформаційної політики на рівні компанії, а також впровадження заходів щодо захисту інформації від можливих внутрішніх і зовнішніх загроз.

Впровадження системи захисту інформації в бізнес-організаціях потребує комплексного підходу та детального аналізу їх діяльності, ринкового середовища та правових умов. Перед початком процесу регулювання

інформаційної безпеки необхідно ретельно вивчити можливості суб'єкта щодо забезпечення належного рівня захисту та визначити його правовий статус.

Також важливо переконатися, що керівник компанії узгоджує структуру та зміст регламенту інформаційної безпеки. Оскільки перспектива керівника визначає стратегічний напрямок безпеки компанії, він повинен брати активну участь у процесах прийняття рішень з цього питання.

Важливим завданням у цьому процесі є створення ефективної системи захисту інформації. Ця система повинна включати різноманітні сили, засоби, заходи та технології, спрямовані на забезпечення стійкості компанії до інформаційних загроз та ефективне управління інформаційною діяльністю.

Таблиця 1.4 – Основні аспекти системи захисту інформації в бізнес-організаціях

Аспект	Опис
1	2
Політика безпеки інформації	Визначення основних принципів захисту, відповідальності працівників, процедур реагування на інциденти безпеки та інші важливі аспекти.
Свідомість персоналу	Навчання працівників з питань інформаційної безпеки та ризиків, пов'язаних з недбалістю. Навчальні програми та внутрішні інструкції.
Застосування технічних засобів захисту	Використання сучасних систем шифрування, антивірусного програмного забезпечення, захисту від витоку даних та інших інструментів.
Аудит та моніторинг	Регулярна перевірка та аналіз системи захисту для вчасного виявлення проблем та вразливостей, а також для вчасного реагування на них.

Продовження таблиці 1.4

1	2
Відповідність законодавству	Встановлення процедур відповідно до вимог GDPR, HIPAA та інших відповідних нормативно-правових актів з метою захисту персональних даних та інформації.
Реагування на інциденти безпеки	Розробка чіткого плану дій у випадку порушення безпеки, включаючи процедури повідомлення, відновлення даних та співпрацю з правоохоронними органами.

Отже, таблиця 1.4 відображає різні аспекти системи захисту інформації, необхідні для ефективного управління безпекою даних в бізнес-організаціях. Кожен з рядків у таблиці представляє важливий елемент, який потрібно врахувати при розробці та впровадженні стратегії захисту інформації. Отже, ця таблиця надає розгорнуту характеристику кожного аспекту:

Політика безпеки інформації: Цей аспект визначає основні принципи та стандарти, які будуть використовуватися для захисту інформації в організації.

Свідомість персоналу: Показує, що працівники повинні бути освічені щодо потенційних загроз безпеці та правил безпеки, щоб знизити ризик виникнення інцидентів.

Застосування технічних засобів захисту: Описує необхідність використання технологічних інструментів, таких як програмне забезпечення та обладнання, для захисту інформації.

Аудит та моніторинг: Цей аспект наголошує на важливості постійного контролю за системою захисту інформації для виявлення і виправлення слабких місць.

Відповідність законодавству: Показує, що організація повинна відповідати всім вимогам законодавства щодо захисту конфіденційної інформації.

Реагування на інциденти безпеки: Цей аспект описує процедури, які повинні бути реалізовані для виявлення, аналізу та відновлення після інцидентів безпеки.

Данна таблиця допомагає організаціям створити повну та комплексну стратегію захисту інформації, щоб забезпечити надійний захист даних.

1.3. Правові засади інформаційної безпеки суб'єктів підприємництва

Забезпечення інформаційної безпеки підприємницької діяльності здійснюються під впливом різноманітних умов, серед яких провідне місце займають правові умови. Останні, у свою чергу, утворюються чотирма джерелами правових норм: Конституцією України, законодавчими актами, підзаконними актами, нормативно-правовими актами суб'єктів підприємництва. Важливість правових умов у забезпеченні інформаційної безпеки полягає у тому, що без правових актів, які складають такі умови процес організації інформаційної безпеки неможливий взагалі.

Саме за допомогою зазначених актів здійснюється регулювання інформаційних відносин та застосування заходів інформаційної безпеки, визначається правомірність тих чи інших дій щодо інформації, формуються підстави для відповідальності за дії в інформаційному просторі. В решті решт правові норми забезпечують захист суб'єктів підприємництва від неправомірного посягання на їх права, інтелектуальну власність, інформацію, що може мати місце у процесі їх діяльності. Положення ст.55 Конституції України надають право будь-якими, не забороненими законом засобами захищати свої права і свободи від порушень і протиправних посягань.[10]

Під засобами, серед інших, можна розуміти і правові засоби (норми та положення Конституції та законів України, нормативно-правових актів органів влади, нормативних документів суб'єктів господарювання та інших організацій, рішення та ухвали судів, положення судових органів, Міністерства юстиції України, положення договорів, угод, укладених суб'єктами підприємництва,

рішення, приписи, накази органів нагляду та контролю). А права можуть поширюватись і на інформаційну сферу. Зокрема право на інформацію, передбачає можливість вільного одержання, використання, поширення, зберігання та захисту інформації, необхідної для реалізації своїх прав, свобод і законних інтересів.

До того ж, Конституцією України гарантується право судового захисту щодо спростування недостовірної інформації, право вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням та поширенням недостовірної інформації. Основний закон забороняє збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків визначених законом(ст. 32).

Конкретизуючи зміст конфіденційної інформації про особу слід зазначити, що до такої інформації належать, зокрема, дані про національність особи, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адресу, дату і місце народження. Тобто Конституція України встановлює загальні умови поведінки суб'єктів, і громадян в інформаційному просторі.[10]

Важливим моментом для забезпечення правової поведінки в інформаційному просторі і правомірних інформаційних відносин є регулювання доступу до інформації. Ці питання регулюються положеннями Закону України « Про інформацію» (Рисунку 1.4)[11].



Рисунок 1.4 – Режим доступу до інформації (Закон України «Про інформацію», ст. ст. 20, 21).

Будь-яка інформація є відкритою крім тієї, що віднесена законом до такої, що має обмежений доступ. Важливо знати, що обмеженню підлягає інформація, а не документ в якому вона міститься. Якщо документ містить таку інформацію, то він підлягає ознайомленню в частині, що не містить інформації з обмеженим доступом. Конфіденційною є інформація про фізичну особу, доступ до якої обмежений фізичною чи юридичною особою, крім суб'єктів владних повноважень.

Така інформація може поширюватись зазначеними особами за їхнім бажанням (згодою) у визначеному ними порядку відповідно до передбачених ними умов, інших випадках визначених законом. До суб'єктів владних повноважень законодавець відносить – органи державної влади, місцевого самоврядування, інших суб'єктів, що здійснюють владні управлінські функції відповідно до законодавства, в т.ч. і делеговані повноваження.

Важливим є з'ясування особи яка має право обмежувати доступ та надавати інформації категорію конфіденційної. Очевидно, що це може бути сам власник такої інформації, або особа яка отримує право розпоряджатись даною інформацією. У останньому випадку законодавець визначає перелік розпорядників інформації, види інформації, якими вони можуть розпоряджатись, їх обов'язки та функції (Закон України «Про доступ до публічної інформації» ст. ст. 13-18). [12]

Таємною є інформація, доступ до якої обмежується відповідно до вимог ст.6 Закону України «Про доступ до публічної інформації» і розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить відомості, що складають державну, професійну, банківську, комерційну та інші передбачені законом види таємниць. [12]

До службової інформації належить така, що міститься в документах суб'єктів владних повноважень, а також зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці. Доступ до таємної інформації визначається

відповідно до чинного законодавства установами, органами, які володіють такою інформацією.

Доступ до службової інформації визначається відповідно до Закону України «Про доступ до публічної інформації» в порядку передбаченому внутрішніми документами суб'єкта владних повноважень.

Відносини у сфері доступу до публічної інформації регулюються Законом України «Про доступ до публічної інформації». Зокрема, закон дає визначення поняття «публічна інформація» згідно з яким це відображена та задокументована будь-якими засобами та на будь-яких носіях інформація, що була отримана або створена в процесі виконання суб'єктами владних повноважень своїх обов'язків, передбачених чинним законодавством, або яка знаходиться у володінні таких суб'єктів, інших розпорядників, крім випадків встановлених законом. Відповідно до зазначеного вище закону, доступ до публічної інформації здійснюється шляхом її оприлюднення у встановленому порядку та шляхом подання запитів до розпорядників інформації. Інформація надається безкоштовно.[12]

Суб'єктами відносин у сфері доступу до публічної інформації є запитувачі інформації, розпорядники інформації, їх структурні підрозділи або відповідальні особи з питань виконання запитів. Окремо регулюється система відносин щодо доступу до інформації про особу. Тут маємо брати за основу положення Закону України «Про захист персональних даних», Закону України «Про доступ до публічної інформації», Закону України «Про інформацію». Зокрема передбачається, що збирання, зберігання, використання та поширення інформації про особу не можливе без згоди саме особи, крім випадків передбачених законом.[11, 12, 13]

Обсяг такої інформації має бути максимально обмеженим і використовуватись лише з метою та у спосіб, визначений законом. Суб'єктами відносин у сфері доступу до інформації про особу виступають самі особи, володільці та розпорядники баз персональних даних, треті особи (особи яким володільцями чи розпорядниками баз персональних даних здійснюється

передача персональних даних відповідно до закону), уповноважений державний орган з питань захисту персональних даних, інші державні органи, органи місцевого самоврядування, до повноважень яких належить здійснення захисту персональних даних.

Про збір даних про осіб, включення інформації про них в базу персональних даних особи мають повідомлятися про їх права володільцем, чи розпорядником бази даних протягом 10 днів з дня формування даних. Разом з тим, коли персональні дані збираються з загальнодоступних джерел таке повідомлення не здійснюється.

Поширення персональних даних здійснюється лише за згодою особи. Без згоди - у випадках визначених законом і лише в інтересах національної безпеки, економічного добробуту та прав людини. Порядок доступу до персональних даних та відносини суб'єктів з цих питань регулюються положеннями ст.ст. 16-19 Закону України «Про захист персональних даних» [13]. Питання правового регулювання доступу до персональних даних нормами міжнародного права, забезпечуються положеннями Конвенції Ради Європи «Про захист фізичних осіб при автоматизованій обробці персональних даних» від 28.01.1981р. зі змінами внесеними у 1999р., додаткового протоколу до Конвенції «Про захист фізичних осіб при автоматизованій обробці персональних даних щодо органів нагляду і транс-граничних потоків даних» від 08.11.2001 року., Директивою Ради Європейського Союзу «Про захист фізичних осіб при автоматизованій обробці персональних даних і про вільний обіг таких даних» 1995р., а також Директивою «Про обробку персональних даних і захист прав фізичних осіб у телекомунікаційному секторі» (1997р.).

Основними принципами захисту персональних даних викладених у зазначених правових актах є: збір і обробка персональних даних мають здійснюватись коректно і законно; використання персональних даних повинно бути адекватним визначеній меті, та обмежуватись за термінами; персональні дані повинні бути точними, оброблюватись лише з дозволу суб'єктів цих даних, бути доступними для них; персональні дані повинні бути надійно захищені. [4]

Таблиця 1.5 – Основні принципи захисту персональних даних [13]

Принцип захисту персональних даних	Опис
1	2
Коректність та законність збору та обробки даних	Збір та обробка персональних даних повинні відповідати законодавству та здійснюватися лише у випадках, передбачених законом або з дозволу суб'єкта даних.
Адекватність та обмеження обробки	Обробка даних повинна бути адекватною відповідно до визначеної мети та обмежена за часом та обсягом.
Точність та доступність для суб'єктів даних	Персональні дані мають бути точними, актуальними та доступними для перегляду та виправлення суб'єктами даних.
Захист даних	Персональні дані мають бути надійно захищені від несанкційованого доступу, втрати чи зміни.

Коректність та законність збору та обробки даних: Цей принцип вказує на необхідність збирати та обробляти персональні дані відповідно до законодавства, а також лише у випадках, які передбачені законом або з дозволу суб'єкта даних. Він підкреслює важливість дотримання правових норм та етичних стандартів при обробці особистої інформації.

Адекватність та обмеження обробки: Цей принцип стверджує, що обробка персональних даних повинна бути обмежена за метою, для якої вони були зібрані. Вона повинна бути адекватною цій меті та обмежена за часом та обсягом, щоб уникнути непропорційного втручання в приватне життя осіб.

Точність та доступність для суб'єктів даних: Цей принцип стверджує, що персональні дані повинні бути точними, актуальними та доступними для перегляду та виправлення суб'єктами даних. Це дає особам можливість контролювати та коригувати інформацію, що стосується їх особистості.

Захист даних: Цей принцип наголошує на важливості захисту персональних даних від несанкційованого доступу, втрати або зміни. Він передбачає вжиття відповідних заходів безпеки, включаючи технічні, організаційні та правові заходи, для забезпечення конфіденційності, цілісності та доступності даних. [13]

Отже, інформаційна безпека в підприємницькій діяльності — це комплекс заходів, процедур, методів і засобів, спрямованих на захист інформаційних ресурсів підприємства від несанкційованого доступу, втрат, змін, викрадення або пошкодження. Інформаційна безпека охоплює всі аспекти обробки, зберігання і передачі інформації в організації з метою забезпечення конфіденційності, цілісності та доступності даних.

РОЗДІЛ 2 АНАЛІЗ СИСТЕМИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА ТОВ «COMFY»

2.1. Загальна характеристика підприємства ТОВ «COMFY»

«COMFY» – провідна українська компанія у сфері електронної комерції та роздрібної торгівлі побутовою технікою та електронікою. COMFY є однією з найтехнологічніших компаній України та першим спеціалізованим ритейлером країни, який запровадив омніканальну бізнес-модель. Ця бізнес-модель поєднує мережу з 102 магазинів сучасного формату, сильну логістику з власною службою доставки COMFY Delivery та багаторічну E-Commerce-експертизу команди. [14]

Сьогодні компанія розвиває цифрову екосистему діджитал-комунікацій 360⁰, до якої окрім інтернет-магазину Comfy.ua входять також мобільні додатки для покупців та продавців, найкраща програма лояльності в сегменті та широкий набір каналів комунікації з покупцями – від персоніфікованих чат-ботів до унікального блогу компанії та соціальних медіа з найбільшим охопленням серед конкурентів. Все це дозволяє команді COMFY впевнено утримувати лідерські позиції щодо обсягів продажу та ефективності в галузі, а також входити до Топ-5 онлайн-гравців країни. [15]

Компанія незмінно входить до кола найбільших приватних компаній та найбільших платників податків, найкращих роботодавців та найкращих спеціалізованих ритейлерів України.

Цифри та факти:

- #1 Найбільша частка ринку серед конкурентів
- 10+ млн клієнтів
- 102 магазини
- Топ-5 онлайн-гравців України
- 92% всієї online-аудиторії України відвідали Comfy.ua
- Топ-50 найдорожчих брендів України 2021

- Топ-100 великих платників податків України
- #1 Ритейлер та e-commerce-ритейлер в Україні 2018-2023 від RAU Awards.[18]

Таблиця 2.1 – Характеристика компанії COMFY [14, 18]

Назва підприємства	COMFY
1	2
Форма власності	Недержавна власність
Термін присутності на ринку	Компанія заснована в 2005 році. На ринку 19 років
Кількість працівників	4000 осіб
Основні напрями діяльності	Продаж побутової техніки та електроніки в Україні
Продукція, що випускається (послуги, що надаються)	Побутова техніка (дрібна побутова техніка, велика побутова техніка, дрібна техніка для дому). Кондиціонери, вентилятори, зволожувачі повітря, очищувачі повітря, Водонагрівачі. Обігрівачі і конвертори, ніжки до обігрівачів, терморегулятори , метеостанції та цифрові термометри. Смартфони (Samsung, Apple, Huawei, vivo, Xiaomi). Гаджети та електротранспорт. PlayStation Store. Приставки PlayStation. Окуляри віртуальної реальності, PlayStation VR, аксесуари для PlayStation, ігри для PlayStation. Смарт-годинники. Фітнес-браслети. Квадрокоптери. Роботи і конструктори. Графічні планшети, графічні монітори і панелі, планшети для підпису, принтери і сканери. Ноутбуки, планшети комп'ютери; ТВ, аудіо та відео; фото, відеокамери; посуд, товари для дому; інструмент та витратники

Компанія “COMFY” заснована в 2005 році, її штаб-квартира знаходиться у Дніпрі. Адреса ТОВ "COMFY": 49100, Україна, Дніпро, бульвар Слави, 6б. Код ЄДРПОУ 36962487 [14].

Традиційній побутовій техніці від телевізорів до пральних машин також приділено багато простору. Гаджети та техніку можна замовити не тільки в магазині, але і по гарячій лінії, а також на сайті comfy.ua. COMFY розвивається і еволюціонує, пропонує своїм покупцям послуги і продукти, що йдуть в ногу з часом. COMFY – один з лідерів роздрібного ринку побутової техніки і електроніки в мережевому сегменті, яка працює понад 19 років.

На сьогоднішній день мережа магазинів являється однією з найбільших в Україні. Інтернет-магазин COMFY забезпечує доставку обраних товарів в більш ніж 1500 населених пункти України. Загальна торговельна площа торговельної мережі складає 130 тис. м², всі магазини відкриті в уніфікованому форматі.

Основні принципи діяльності COMFY – це клієнтоорієнтованість і високий рівень сервісу. Однією з суттєвих конкурентних переваг мережі є високі показники ефективності використання торговельної площі (приблизно \$500 з 1 кв. м, що в 1,5 разів більше, ніж в інших компаніях). Перший магазин COMFY був відкритий в Кривому Розі в грудні 2005 року. Через два роки, об'єднавшись з мережею «Побуттехніка», компанія увійшла до трійки лідерів серед ритейлерів з продажу побутової техніки та електроніки України. [14]

Компанія “COMFY” почала активний розвиток у 2007 році після об'єднання з компанією «Побуттехніка» Світлани Гуцул. Акціонери «Побуттехніки» і “COMFY” створили нову компанію на паритетних засадах. На час об'єднання мережа “COMFY”, що вийшла на ринок 2006 року, нараховувала 26 магазинів у 13 містах Дніпропетровської, Запорізької, Черкаської, Кіровоградської, Полтавської та Миколаївської областей. Мережа магазинів «Побуттехніка» була заснована у 1992 році в Донецьку, і на момент об'єднання складалась з 29 магазинів у 17 містах Донецької, Луганської областей та Криму.

У кризові роки 2008—2009, коли багато хто з ритейлерів вимушені були скоротити темпи розвитку або навіть піти з ринку, мережа “COMFY” стала найдинамічнішою з погляду розвитку — приріст кількості магазинів за 2 роки склав майже 65 % та найефективнішою з точки зору обороту продажів з кожного м² мережею магазинів побутової техніки та електроніки в Україні.[16, 17]

2010 року компанія відмовилася від контрабандної «сірої» техніки. Перехід на торгівлю тільки легально завезеною технікою підтримав також Фокстрот.

2011 року “COMFY” відкрила 15 нових і 50 оновлених магазинів по всій території України. 2013 року компанія зазнала тиску з боку податкової та прокуратури через відмову від контрабандної «сірої» техніки і як результат — несплата хабарів чиновникам.

2014 року інтернет-магазин comfy.ua входить до десятки найбільших онлайн-магазинів українського сегменту інтернету.

З 2006-го до 2016 року сайт “COMFY” (comfy.com.ua, згодом comfy.ua) мав виключно російськомовний інтерфейс. У вересні 2014 року компанія запустила тестову версію україномовного інтерфейсу. Наприкінці 2015 року в ЗМІ почала з'являтися інформація про впровадження інтерфейсу українською мовою, а 3 березня 2016 року, через 11 років після заснування, компанія оголосила про запуск повноцінної україномовної версії сайту в офіційному блозі.

Компанія ТОВ “COMFY” успішно здійснила перехід від методів масового і товарної-диференційованого маркетингу до цільового маркетингу, який допомагає повніше виявити маркетингові можливості. Для кожного цільового ринку компанія може розробити потрібний цьому ринку товар. Для забезпечення ефективного охоплення кожного такого ринку “COMFY” змінює ціни, канали розповсюдження, рекламні витрати і фокусується на покупцях, найбільш зацікавлених у придбанні товару. [18]

Основною метою діяльності підприємства є торгово-економічна діяльність по продажу переважно електроніки та інше. Ідеал організації – це результат, який в принципі є недосяжним, але до якого можна і треба наближатися компанії. До ідеалів організації зазвичай відносять її бачення. Стратегічне бачення – це керівна філософія бізнесу, обґрунтування існування компанії. Це не сама мета, а скоріше відчуття основної мети, тобто бачення – це ідеальна картина майбутнього, те становище, яке може бути досягнуте при найбільш сприятливих умовах.

Товарної асортимент формується на підприємстві в результаті спільної роботи різних підрозділів: відділу маркетингу, відділу збуту, планово - економічного відділу, фінансового відділу. Фактори, які потребують аналізу у внутрішньому середовищі та впливають на формування асортименту підприємства (таблиця 2.2.)

Таблиця 2.2 – Фактори, що впливають на формування асортименту

Фактори	Змістовність
1	2
Кадрові фактори	наявність і вартість оплати послуг кваліфікованих фахівців для виведення на ринок оновлених товарних груп; оплата послуг маркетологів
Технологічні наявність	технологічних потужностей для поновлення виробництва; умови зберігання для нового товару
Інфраструктурні наявність	підготовленої системи оновлення асортименту (від придбання ресурсів до реалізації)
Збутові наявність	налагоджених каналів збуту продукції; наявність оптових покупців
Фінансово-економічні	наявність власних або позикових фінансових ресурсів для оновлення асортименту; економічна доцільність нового товару; оцінка витрат на просування товару на ринок; сукупна економічна оцінка доцільності нового асортименту

Надзвичайно важливим засобом підвищення конкурентоспроможності підприємства та отримання очікуваних економічних результатів є розроблення та впровадження якісного і збалансованого асортименту товарів. У разі відсутності збалансованості асортименту товарів підприємство втрачає належний рівень прибутку, втрачає свої переваги на ринку.

Найбільший ритейлер побутової техніки та електроніки в Україні COMFY незмінно підтримує військових з перших днів російської агресії у 2014 році. 24 лютого 2022 року, коли ворог розпочав повномасштабне вторгнення, у “COMFY” лише посилили підтримку армії та територіальної оборони, лікарень та волонтерів. У перші години після відкриття Нацбанком спецрахунку для потреб армії компанія перевела перші 30 млн. гривень благодійного. За тиждень – перерахували ще 30 млн гривень.

З першого дня команда “COMFY” збільшила обсяги техніки, яку безкоштовно передає на запити організацій та волонтерів:

- для ЗСУ та осередків тер-оборони – смартфони, планшети, ноутбуки та принтери,
- лікарням, дитячим будинкам та волонтерам – побутову техніку, зокрема чайники, мультиварки, пральні та сушильні машини, обігрівачі.

Підтримали ці активності “COMFY” й провідні міжнародні виробники побутової техніки та електроніки – погодилися разом з “COMFY” понести витрати на безкоштовну передачу техніки на потреби армії, волонтерів та постраждалого населення. На сьогодні загальна сума допомоги через передачу техніки перевищила 15 млн гривень.



Рисунок 2.1 – Активність компанії “COMFY” у 2022 році

2023 рік розпочинався під шум генераторів та тривалих вимкнень світла. У магазинах продовжували купувати альтернативні джерела живлення: зарядні станції та повербанки. Разом з тим, від початку повномасштабного вторгнення компанія “COMFY” спостерігала зріст попиту на комп’ютерну електроніку. Велика частка запитів припала на планшети та потужні ноутбуки, адже наразі це допоміжні гаджети в обороні країни.

Ще одним трендом життя у війні став дистанційний формат навчання та роботи, який також вплинув на необхідність покупців у гаджетах.

У 2023 році до цього додалась потреба і у домашніх девайсах, зокрема, українці повернулись до більш звичних покупок: купували багато телевізорів, роботів-пилососів та кава-машин.

Цікавим трендом 2023 року став попит на великий побут. Лідери серед них — холодильники і пральні машини. Якщо у 2022 році покупці не інвестували у великі та дорогі покупки, то зараз все ж прагнуть стабільності і живуть майбутнім.

У 2023 році кількість оффлайн-магазинів “COMFY” зростала щомісяця. Ритейлер відкрив 21 новий магазин у 15 українських містах. 7 з них — флагманського формату. Також торік три магазини “COMFY” відновили свою роботу у Харкові, Одесі та Покровську. Ці магазини не працювали від початку вторгнення через ризики або руйнування.

Нові відкриття магазинів – це продовження реалізації стратегії “COMFY” на географічну експансію, яка була одним з бізнес-пріоритетів компанії у 2023

році. Як результат, за рік оффлайн-мережа компанії збільшилася з 78 до 102 магазинів.

Понад 10 років команда COMFY працює в омніканальній бізнес-моделі та активно розвиває онлайн-продажі. 2023 року компанія реалізувала багато ініціатив, спрямованих на розширення асортименту товарів, покращення якості контенту в інтернет-магазині, підвищення ефективності digital/цифрове-просування, пришвидшення обробки та отримання онлайн-замовлень в магазинах.

У результаті, онлайн-продажі зросли на понад 70%, частка онлайн-продажів перевищила 30% від загального обсягу продажів компанії, а частка мобільного додатку “COMFY” в онлайн-продажах зросла вдвічі.

На сьогодні “COMFY” є працедавцем для 4500 найманих працівників (новим співробітникам пропонується зрозумілі інструменти планування траєкторії кар’єрного росту від стажиста-продавця до директора магазину, а майже 70 % управлінців торговельної компанії починали свою кар’єру або в магазинах, або у call-центрі). Чисельність клієнтів торговельної мережі перевищує 10 млн. грн., а індекс підтримки споживача (NPS) складає більше 65 %.

Таблиця 2.3 – “COMFY” у цифрах станом на 01.01.2024 [18]

Кількість магазинів	102
Кількість працівників	4500
Кількість клієнтів	10+ млн
Налоги та збори оплачені на момент 2022 року	748 млн грн
Індекс підтримки споживача	65%
Топ онлайн-гравців на на ринку України	Топ5
Обсяг продажів у сегменті	#1
По ефективності продажів	#1

“COMFY” є соціально відповідальною компанією. На тлі гібридної агресії та повномасштабного вторгнення Росії компанія сконцентрувала зусилля на такому пріоритетному напрямку в сфері соціальної відповідальності, як допомога волонтерам та ЗСУ. На 2023 рік сукупний обсяг такої підтримки перевищив 120 млн. грн. [19]

У своєму сегменті підприємство є лідером як за обсягом продажів побутової техніки та електроніки, так і за ефективністю діяльності. Це є дуже важливим, оскільки бізнес має бути економічно стійким, ефективним і прибутковим, щоб мати можливість надавати допомогу і привносити у суспільство цінність.

У цей важкий період для країни, коли загроза з боку Росії стає все більш серйозною, роль підприємств, як COMFY, у підтримці волонтерів та ЗСУ надзвичайно важлива. Ця допомога не лише виражається у фінансовій підтримці, але й у наданні необхідної техніки та електроніки для підвищення ефективності виконання завдань волонтерами та військовослужбовцями.

COMFY, як лідер у сфері продажу побутової техніки та електроніки, несе відповідальність за якість продукції, яка потрапляє до споживачів. Надійність та ефективність їхніх товарів сприяють не лише задоволенню потреб клієнтів, а й підвищенню загального рівня технологічної культури в країні.

Такий підхід до бізнесу демонструє, що соціальна відповідальність не просто показова ініціатива для COMFY, але основний принцип їхньої діяльності. Вони усвідомлюють свою роль у формуванні стабільного та процвітаючого суспільства і активно працюють у цьому напрямку, роблячи значний внесок у підтримку та розвиток України.

Компанія COMFY розуміє, що успіх бізнесу пов'язаний не лише з фінансовими показниками, але й з довірою споживачів та відданістю принципам корпоративної відповідальності. Тому вони продовжують активно залучатися до ініціатив, спрямованих на підтримку волонтерів, ЗСУ та інших соціальних проектів. [19]

Наприклад, у 2023 році COMFY організувала серію тренінгів для волонтерів з використання сучасної техніки та електроніки, що сприяло підвищенню їхньої продуктивності та ефективності у виконанні завдань. Варто зазначити, що компанія постійно підтримує ініціативи з відновлення обладнання для військових підрозділів та надає спеціальні умови для ветеранів та учасників АТО.

Продовжуючи свою місію сприяти як соціальному, так і економічному розвитку країни, COMFY залишається прикладом позитивного впливу бізнесу на суспільство. Їхня зосередженість на соціально відповідальних ініціативах підтверджує, що успішний бізнес і соціальна відповідальність можуть і повинні існувати поруч, створюючи сприятливе середовище для розвитку кожного члена суспільства.

2.2. Оцінка фінансово-економічного стану підприємства ТОВ “COMFY”

Оцінка фінансово-економічного стану підприємства – це складний процес, який включає багато аспектів. Це включає аналіз стану нерухомості, структуру джерел майна, ліквідність, прибутковість, ділову активність та інші фактори. Особливості цього аналізу визначають характеристики та діяльність торгових підприємств.

Особливо важливий індекс оборотності акцій. Це відображає ефективність і швидкість управління запасами. Аналіз оборотності запасів дозволяє виявити проблеми в управлінні запасами та запобігти затримкам продажів.

Оскільки комерційні компанії часто працюють з кредиторами, оцінка кредитного ризику відіграє важливу роль. Це і аналіз платоспроможності клієнтів, і контроль платіжних операцій.

Також важливо враховувати сезонність і циклічність попиту на товари. Багато товарів мають сезонний попит, і для врахування цих коливань потрібне ретельне планування запасів і бюджет.

Оцінка торговельного обороту показує, наскільки ефективно підприємство використовує свої активи для генерації продажів. Аналіз обороту активів та капіталу допомагає виявити ефективність використання ресурсів.

Ризики валютних коливань є ще одним важливим аспектом, особливо для підприємств, які працюють з іноземними партнерами. Для цього необхідно застосовувати стратегії управління валютними ризиками.

Дослідження ринку та конкурентів дозволяє підприємству адаптувати свої стратегії та підвищувати конкурентоспроможність. Це особливо важливо у торгівлі, де конкуренція є високою.

Таким чином, комплексна оцінка фінансово-економічного стану торговельного підприємства допомагає виявити його сильні та слабкі сторони, сприяє прийняттю обґрунтованих управлінських рішень та стратегічному плануванню розвитку.

Оцінка майна товариства "COMFY", а також джерел формування майна, здійснюється за допомогою порівняльного аналітичного балансу, що будується на підставі фінансової звітності.

Сукупна вартість майна торговельного підприємства станом на початок 2023 року склала 4030799 тис. грн., що менше на 22,59 % у порівнянні з попереднім періодом. Скорочення активів свідчить про скорочення обсягів діяльності. Здебільшого це пояснюється наслідками повномасштабного вторгнення, окупацією частини Херсонської, Запорізької, Донецької і Луганської областей у 2022-ому році та активними бойовими діями на значній території країни, скороченням купівельної спроможності населення.

Протягом останніх двох років спостерігаються зміни не тільки у величині активів ТОВ "COMFY", а й у їх структурі. Найбільшу питому вагу у структурі активів займають оборотні активи – 87,75 %, 87,36 % і 88,86 % відповідно станом на початок 2023, 2022 і 2021 рр. На відміну від промислових підприємств, така структура активів не є «важкою» (питома вага необоротних активів у балансі підприємства < 60 %) і обумовлюється специфікою торговельного бізнесу.

Оборотні активи в першу чергу представлені такими складовими, як запаси і грошові кошти та їх еквіваленти. Станом на 01.01.2023 запаси становили 47,97 %, а грошові кошти та їх еквіваленти – 35,11 % від сукупних активів. У порівнянні з попереднім періодом питома вага запасів зросла на 13,55 в.п., а грошових коштів та їх еквівалентів, навпаки, трохи зменшилась – на 2,49 в.п.

У ТОВ "COMFY" відбулося скорочення дебіторської заборгованості. За 2022 рік ця стаття оборотних активів підприємства зменшилась на 310487 тис. грн. або на 40,4 %, у попередньому 2021 році – на 26412 тис. грн. або на 3,32 %. Питома вага дебіторської заборгованості у структурі активів також зменшилась, хоча і менш відчутно (у 2022 році проти 2021 року скорочення частки дебіторської заборгованості 2,26 в.п., у 2021 році проти 2020 року – 3,68 в.п.). Станом на 01.01.2023 питома вага дебіторської заборгованості становила 12,50 %. Зазвичай скорочення дебіторської заборгованості торговельного підприємства пов'язується з такими найважливішими аспектами фінансового здоров'я підприємства: ефективне управління кредитуванням; зменшення ризику неплатоспроможності; підвищення здатності підприємства перетворювати активи на грошові кошти; збільшення обсягу чистого прибутку за рахунок скорочення обсягів боргів і витрат на управління дебіторською заборгованістю. Важливо враховувати контекст та інші фактори при оцінці змін у рівні дебіторської заборгованості. Наприклад, збільшення обсягу продажів може супроводжуватися збільшенням дебіторської заборгованості, але це може бути прийнятною стратегією в контексті росту бізнесу. Для ТОВ «"COMFY" скорочення дебіторської заборгованості не можна однозначно розглядати у якості позитивної тенденції на тлі скорочення активів та чистого прибутку – результатного показника діяльності.

Основним джерелом формування майна підприємства є позиковий капітал, а саме – кредиторська заборгованість і поточні зобов'язання. Так, станом на 01.01.2023 питома вага цієї статті пасивів у сукупних джерелах формування майна становила 94,28 %, а власні джерела – 3,35 %. У порівнянні з

попереднім періодом обсяг кредиторської заборгованості ТОВ "COMFY" зменшився на 22,27 % і склав 3800185 тис. грн. Власний капітал, навпаки, збільшився на 4,24% до 135182 тис. грн. Приріст власного капіталу у першу чергу був обумовлений збільшенням нерозподіленого прибутку зі 129181 тис. грн. до 131182 тис. грн. Динаміка показників, що характеризують майновий стан ТОВ "COMFY", представлена у табл. 2.4 і на рис. 2.2.

Питома вага оборотних виробничих фондів в оборотних активах, у ТОВ "COMFY" – це співвідношення виробничих запасів, незавершеного виробництва та оборотних активів, протягом аналізованого періоду суттєво не змінилась. У порівнянні з початком 2021 року цей показник майнового стану зменшився всього на 0,04 відсоткових пункти і склав на 01.01.2023 усього 0,16 %.

У цілому ж скорочення показника у динаміці свідчить про збільшення більш ліквідної складової оборотних активів, що слід оцінювати позитивно.

Таблиця 2.4 – Показники майнового стану ТОВ "COMFY"

Показник	2021	2022	2023	Відхилення +/- у %	
				2022/2021	2022/2023
1	2	3	4	5	6
Питома вага оборотних виробничих фондів в оборотних активах	0,2	0,17	0,16	-15	-5,88
Питома вага основних засобів у сукупних активах	8,79	10,16	9,61	15,57	-5,42

Продовження таблиці 2.4

Коефіцієнт зносу основних засобів	56,70	54,40	62,20	-3,86	7,80
Коефіцієнт мобільності активів	7,97	6,91	7,17	-13,40	3,27
Коефіцієнт фінансової автономії	0,025	0,025	0,034	0	36
Коефіцієнт фінансового ризику	39,54	39,15	28,82	-0,98	-26,33

Складено автором на основі фінансової звітності на підприємстві COMFY [1]

Таблиця 2.4 показує фінансові показники компанії за 2021, 2022 та 2023 роки, разом із відхиленнями від попереднього року у відсотках.

Питома вага оборотних виробничих фондів в оборотних активах: Цей показник вказує на частку оборотних виробничих фондів у загальних оборотних активах компанії. За трьома роками спостерігається зменшення цієї частки на 15% від 2021 до 2022 року та на додаткові 5.88% від 2022 до 2023 року.

Питома вага основних засобів у сукупних активах: Цей показник вказує на частку вартості основних засобів у загальних активах компанії. За період 2021-2022 років ця частка зросла на 15.57%, але зменшилась на 5.42% у 2023 році порівняно з попереднім.

Коефіцієнт зносу основних засобів: Цей показник відображає швидкість, з якою основні засоби втрачають свою вартість через знос. У 2022 році цей

коефіцієнт зменшився на 3.86% відносно 2021 року, але підвищився на 7.80% у 2023 році порівняно з попереднім.

Коефіцієнт мобільності активів: Цей показник відображає, наскільки легко компанія може конвертувати свої активи у грошовий еквівалент. Він зменшився на 13.40% у 2022 році порівняно з 2021 роком, але зріс на 3.27% у 2023 році в порівнянні з попереднім роком.

Коефіцієнт фінансової автономії: Цей показник вказує на те, наскільки компанія фінансує свою діяльність за рахунок власних коштів. У 2023 році цей показник зріс на 36% порівняно з попереднім роком.

Коефіцієнт фінансового ризику: Цей показник відображає рівень ризику, пов'язаного з фінансовими зобов'язаннями компанії. У 2023 році цей показник зменшився на 26.33% відносно попереднього року.

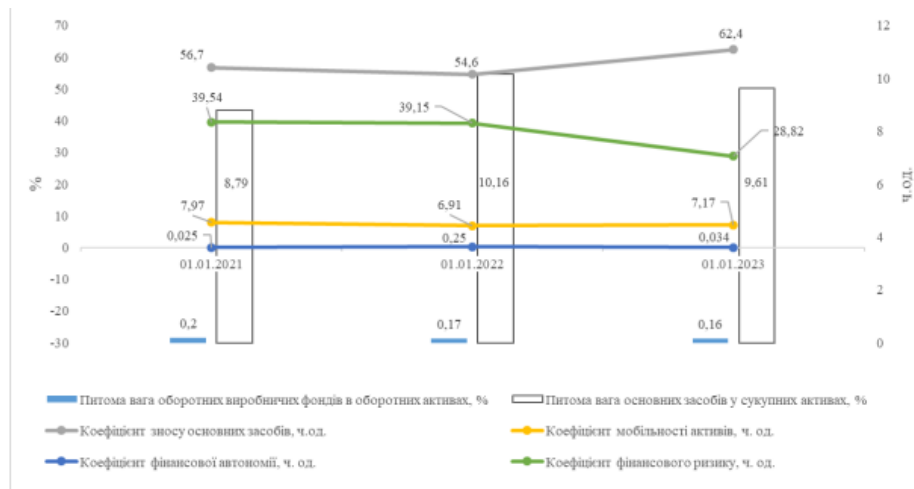


Рисунок 2.2 – Динаміка показників майнового стану ТОВ "COMFY"

Протягом останніх трьох періодів частка основних фондів в активах підприємства коливалася в межах 2 відсоткових пунктів. На початок 2022 року цей показник збільшився з 8,79% до 10,16%, але до початку 2023 року знову зменшився до 9,61%. Така структура активів є типовою для компаній, що діють у сфері торгівлі.

Негативно слід оцінювати коефіцієнт зносу основних засобів та його динаміку. Фактичні значення цього коефіцієнту (62,4% на початок 2023 року) не відповідають рекомендованому рівню (більше 50%).

Коефіцієнт мобільності активів у динаміці вказує на потенційну здатність активів перетворюватися у ліквідні кошти. На початок 2023 року цей коефіцієнт зростає на 0,26 відсоткових пунктів до 7,17.

Низькі значення показника фінансової автономії і високі показники коефіцієнта фінансового ризику свідчать про відсутність фінансової стійкості компанії. Коефіцієнт фінансової автономії не перевищував 3,4% за останні три періоди, тоді як коефіцієнт фінансового ризику, хоч і зменшився на 10,33 відсоткових пунктів, залишився на високому рівні - 28,82 на початок 2023 року, що може потенційно загрожувати фінансовому стану компанії.

Результати аналізу таблиці 2.5 вказують на помітне сповільнення ділової активності ТОВ "COMFY" протягом 2021-2022 років. Це виявляється у великих зниженнях оборотності активів (-13,70%), оборотності оборотних активів (-13,14%), оборотності запасів (-22,43%), та оборотності кредиторської заборгованості (-19,07%). Варто зауважити, що лише коефіцієнт оборотності дебіторської заборгованості показав зростання на 6,25%.

Підвищення рівня заборгованості ТОВ "COMFY" на тлі скорочення торговельної діяльності та виручки від реалізації створює низку потенційних загроз для фінансово-економічного стану підприємства у середньостроковій перспективі. Ці фактори можуть призвести до серйозних труднощів у забезпеченні фінансової стійкості, особливо з урахуванням ризиків, що виникають у зовнішньому середовищі.

Таблиця 2.5 – Показники ділової активності ТОВ “COMFY”

Показник	2021	2022	Зміна	
			Абсолютн е (+,-)	Темп приросту, %
1	2	3	4	5
1.Коефіцієнт оборотності загального капіталу (активів)	3,59	4,16	-0,57	-13,70
2.Коефіцієнт оборотності оборотних активів	4,10	4,72	-0,62	-13,14
3.Коефіцієнт оборотності матеріальних оборотних засобів (запасів)	9,34	12,04	-2,7	-22,43
4.Коефіцієнт оборотності дебіторської заборгованості	27,04	25,45	1,59	6,25
5.Середній період обороту дебіторської заборгованості	13	14	-1	-7,14
6.Коефіцієнт оборотності кредиторської заборгованості	3,82	4,72	-0,9	-19,07
7.Середній період обороту кредиторської заборгованості	96	77	19	24,68
8.Середній період обороту мобільних активів	99	77	12	15,58

Продовження таблиці 2.5

9.Середній період обороту запасів	39	30	9	30
10.Період операційного циклу	52	44	8	18,88
11.Період фінансового циклу	-44	-33	-11	33,33

Складено автором на основі фінансової звітності на підприємстві COMFY [1]

Фінансовий результат діяльності підприємства визначається його прибутком або збитком. За даними з таблиці 2.6, можна зробити наступні висновки: чистий прибуток ТОВ "COMFY" у 2022 році скоротився на 91,43%. Протягом 2022 року торговельне підприємство отримало чистий прибуток у розмірі 2001 тис. грн.

Таблиця 2.6 – Аналіз фінансових результатів ТОВ “COMFY”

Показник	2021	2022	Абсолютне (+,-)	Темп приросту, %
1	2	3	4	5
1.Чистий дохід	19795278	16579935	-3215343	-16,24
2.Інші операційні доходи	48375	129025	80650	166,72
3.Разом доходи	19843653	16708960	-3134693	-15,80
4. Собівартість	15966115	13113680	-2852435	-17,87
5.Інші операційні витрати	144813	322780	177967	122,89

Продовження таблиці 2.6

6.Разом витрати тис. грн.	3682468	3249483	-432985	-11,76
7. Фінансовий результат до оподаткування	29307	2819	-26488	-90,38
8. Податок на прибуток	5957	818	-5139	-86,27
9.Чистий прибуток	23350	2001	-21349	-91,43

Складено автором на основі фінансової звітності на підприємстві COMFY [1]

У порівнянні з попереднім періодом, виручка від реалізації підприємства за 2022 рік зменшилась на 3 215 343 тис. грн, що становить -16,24%. Приріст інших операційних доходів на 166,72% - з 48 375 тис. грн до 129 025 тис. грн - не суттєво вплинув на фінансові результати ТОВ "COMFY". Щодо інших операційних витрат, вони зросли на 177 967 тис. грн, досягнувши 322 780 тис. грн (зростання на 122,89%). Собівартість реалізованої продукції підприємства зменшилась на 17,87% до 13 113 680 тис. грн.

Зазначені зміни у фінансових результатах ТОВ "COMFY" не можна оцінити позитивно.

Для оцінки ефективності функціонування підприємства необхідно провести аналіз рентабельності, включаючи розрахунок та оцінку таких основних показників, як валова рентабельність продажів, рентабельність активів та рентабельність власного капіталу.

Таблиця 2.7 – Оцінка впливу факторів на зміну виручки від реалізації ТОВ “COMFY”

Показник	2021	2022	Відхилення, %
1	2	3	4
Чистий дохід (виручка) від реалізації продукції	19795278	19579935	-1,0908
Темп зростання	1,2112	0,8376	-30,8663
Валюта балансу середньорічна	4758798	4618885	-2,9392
Темп зростання	1,1620	0,9706	-16,4318
Ресурсовитратна	4,1597	3,5896	-13,7003

Складено автором на основі фінансової звітності на підприємстві COMFY [1].

Таблиця надає порівняльний аналіз ключових фінансових показників за 2021 та 2022 роки. Вона дозволяє керівництву компанії отримати уявлення про зміни в її фінансовому стані та ефективності за цей період.

Чистий дохід (ВР): Цей показник відображає загальний обсяг прибутку від реалізації продукції. Падіння на 1.0908% у 2022 році порівняно з 2021 роком може вказувати на різні фактори, такі як зміни в ціновій політиці, попиті на товари або ефективності виробництва.

Темп зростання ВР (ТВР): Цей показник показує, наскільки швидко зростає чистий дохід протягом року. Його спад на 30.8663% відображає значний спад зростання в 2022 році порівняно з попереднім роком.

Валюта балансу середньорічна: Цей показник вказує на середньорічний обсяг грошових коштів компанії. Зменшення на 2.9392% може відобразити зміни в інвестиційній політиці, співвідношенні між ліквідністю та іншими активами.

Темп зростання (Т): Цей показник вказує на темп зростання грошових коштів компанії. Його спад на 16.4318% може вказувати на меншу потребу в оборотних коштах або зниження інвестицій.

Ресурсовитратна (Рвідд.): Цей показник відображає ефективність використання ресурсів компанією. Спад на 13.7003% може вказувати на меншу ефективність використання активів або зміни в бізнес-моделі.

В цілому, аналіз цієї таблиці допомагає зрозуміти фінансове здоров'я та ефективність управління компанією COMFY та ідентифікувати області, які можуть потребувати уваги або коригувань у стратегії.

Таблиця 2.8 – Показники, що характеризують наявність/дефіцит у ТОВ “COMFY” джерел формування запасів

Показник	2021	2022	2023	Відхилення +/- у %	
				2022/2021	2023/2022
1	2	3	4	5	6
1.Власні оборотні кошти, ЕС	-374054	-528420	-358473	-41,27	32,16
2.Власні і довгострокові позикові джерела формування запасів, ЕТ	-222702	-339895	-263040	-52,62	22,61
3.Основні джерела формування запасів, Е□	-222702	-339895	-263040	-52,62	22,61

Складено автором на основі фінансової звітності на підприємстві COMFY [1].

У таблиці 2.8 наведено фінансові показники компанії «COMFY» за 2021, 2022 та 2023 роки. У таблиці також показано річне відхилення у відсотках для кожного показника. Основними показниками є оборотні кошти, власні та довгострокові джерела формування запасів та основні джерела формування запасів.

Оборотний капітал (ЕС) значно скоротився з 2021 по 2022 рік, зменшилися на -41,27%. Однак у 2023 році було досягнуто покращення на 32,16% порівняно з 2022 роком.

Власні і довгострокові позикові джерела формування запасів (ЕТ) також знизилися на -52.62% з 2021 до 2022 року, але в 2023 році вони показали покращення на 22.61%.

Основні джерела формування запасів (ЕΣ) мають аналогічні тенденції зниження на -52.62% у періоді 2021-2022 років та зростання на 22.61% у періоді 2022-2023 років.

У таблиці показана динаміка основних фінансових показників компанії, показуючи значні коливання у власних і позикових коштах, що вказує на потенційні фінансові труднощі або зміни у фінансовій стратегії ТОВ "COMFY".

Таблиця 2.9 – Показники забезпеченості запасів ТОВ “COMFY” різними джерелами їхнього формування

Показник	2021	2022	2023	Абсолютне відхилення, +/-	
				2022 до 2021	2023 до 2022
1	2	3	4	5	6
1. $E_c = E_c$ - ефективність управління запасами	-1870114	-2320570	-2116197	-450456	204373

Продовження таблиці 2.9

2. $E_T = E_T -$ ефективніс ть управління запасами	-3366174	-4112720	-3873921	-746546	238799
3. $E_{\Sigma} = E_T -$ ефективніс ть управління запасами	-3366174	-4112720	-3873921	-746546	238799

Складено автором на основі фінансової звітності на підприємстві COMFY [1]

У таблиці 2.9 представлений аналіз показників компанії ТОВ "COMFY" у періоди з 2021 по 2023 роки. Компанія спеціалізується на роздрібній торгівлі технікою для дому та електронікою.

Показник E_C (E_C - Запаси): Цей показник відображає ефективність управління запасами компанії. Аналіз показує, що від 2021 до 2022 року абсолютне відхилення склало -450,456 тис. одиниць, що відповідає зростанню на 24.07% відносно попереднього року. Проте з 2022 до 2023 року відхилення склало 204,373 тис. одиниць, що означає зниження на 8.80%.

Показник E_{Σ} (E_T - Запаси): Цей показник також відображає ефективність управління запасами компанії. Аналіз показує схожі тенденції з показником E_C . З 2021 до 2022 року абсолютне відхилення склало -746,546 тис. одиниць, зростання на 22.18% відносно попереднього року. З 2022 до 2023 року відхилення склало 238,799 тис. одиниць, що означає зниження на 5.81%.

Показник E_{Σ} (E_T - Запаси): Цей показник представляє загальне відхилення управління запасами. Аналогічно до показників E_C і E_T , він показує зростання з 2021 до 2022 року і подальше зниження з 2022 до 2023 року.

Аналіз цих показників може допомогти компанії "COMFY" в розумінні тенденцій управління запасами та розробці стратегій для оптимізації управління запасами у майбутньому.

2.3 Організація системи управління інформаційною безпекою ТОВ «COMFY»

Система управління інформаційною безпекою (СУІБ) ТОВ «COMFY» є невід'ємною частиною загальної системи менеджменту компанії. Вона заснована на ризик-орієнтованому підході і призначена для створення, впровадження, експлуатації, моніторингу, аналізу, підтримки та вдосконалення інформаційної безпеки (ІБ) компанії. СУІБ ТОВ «COMFY» спрямована на забезпечення захисту інформаційних ресурсів компанії, зменшення ризиків, пов'язаних з інформаційною безпекою, та підвищення загальної ефективності управління інформацією.

Таблиця 2.10 – Управління інформаційною безпекою ТОВ «COMFY»

Аспект	Діяльність/Відділ
1	2
Формування політики безпеки	Відділ стратегічного розвитку та політики безпеки
Організація відділу інформаційної безпеки	Відділ інформаційної безпеки
Розробка системи заходів щодо реагування на інциденти	Відділ кризового управління та реагування на інциденти
Проведення аудиту інформаційної безпеки	Відділ аудиту інформаційної безпеки

Компанія “COMFY” приділяє значну увагу захисту своїх інформаційних ресурсів. Одним з ключових аспектів є створення ефективного механізму управління доступом до інформації, що включає як розмежування доступу, так і визначення методів доступу.

Таблиця 2.11 – Основні принципи інформаційної безпеки в “COMFY”

Категорія	Опис
1	2
Розмежування доступу	
Ідентифікація та автентифікація	Впровадження процедур для підтвердження особи користувача перед наданням доступу до інформаційних систем.
Рольовий доступ	Визначення рівнів доступу відповідно до посадових обов'язків співробітників. Кожен співробітник має доступ лише до тієї інформації, яка необхідна для виконання його функцій.
Політики доступу	Встановлення чітких політик щодо того, хто і до яких даних має доступ. Це включає обмеження доступу до критичних систем і даних для мінімально необхідного числа співробітників.
Методи доступу	
Багатофакторна автентифікація (MFA)	Використання декількох методів перевірки особи користувача для підвищення безпеки (наприклад, паролі плюс одноразові коди, що надсилаються на мобільний телефон).
Шифрування даних	Захист даних під час зберігання і передачі за допомогою шифрування.
VPN (Віртуальна приватна мережа)	Забезпечення безпечного віддаленого доступу до внутрішніх систем компанії через зашифровані канали.

Продовження таблиці 2.11

1	2
Об'єкти захисту:	
Мовна інформація	Захист конфіденційної інформації, що передається усно, включаючи переговори і наради. Використання безпечних приміщень і пристроїв для таких комунікацій.
Інформація на електронних носіях	Дані, що зберігаються на серверах, комп'ютерах, мобільних пристроях, в хмарних сервісах. Впровадження політик резервного копіювання і відновлення даних.
Паперові документи	Захист паперових носіїв інформації через фізичну безпеку (наприклад, сейфи, замкнені приміщення), контроль доступу до них і регулярне знищення конфіденційних документів.
Ідентифікація та автентифікація	Впровадження процедур для підтвердження особи користувача перед наданням доступу до інформаційних систем.
Навчання та підвищення обізнаності	
Тренінги для співробітників	Регулярні навчання щодо політик інформаційної безпеки, нових загроз і методів захисту.
Симуляція інцидентів	Проведення навчань з реагування на інциденти безпеки для підготовки персоналу до можливих загроз.
Моніторинг і аудит	
Моніторинг систем	Постійне відстеження активності в інформаційних системах для виявлення і реагування на підозрілі дії.
Регулярні аудити	Проведення внутрішніх і зовнішніх аудитів інформаційної безпеки для перевірки відповідності політикам і стандартам безпеки.

Впровадження СУІБ в компанії “COMFY” дозволяє ефективно керувати всіма аспектами інформаційної безпеки. Це забезпечує чітке визначення взаємозв'язків між процесами і підсистемами, відповідальних за них осіб, а також необхідні ресурси для підтримки безпеки.

Таблиця 2.12 – Основні компоненти СУІБ “COMFY”

Категорія	Опис
1	2
Процеси та підсистеми інформаційної безпеки	
Політика безпеки	Визначення загальних принципів і підходів до інформаційної безпеки в компанії.
Управління доступом	Включає ідентифікацію, автентифікацію, авторизацію та аудит доступу до інформаційних ресурсів.
Управління ризиками	Оцінка і управління ризиками, пов'язаними з інформаційною безпекою.
Управління інцидентами	Процедури виявлення, реагування та усунення наслідків інцидентів інформаційної безпеки.
Безперервність бізнесу	Планування та забезпечення безперервної роботи критичних бізнес-процесів в разі інцидентів.
Навчання та обізнаність	Програми навчання персоналу з питань інформаційної безпеки.
Відповідальні особи	
CISO	Керівник служби інформаційної безпеки, відповідальний за загальну координацію та управління СУІБ.
Політика безпеки	Визначення загальних принципів і підходів до інформаційної безпеки в компанії.

Продовження таблиці 2.12

1	2
ІТ-відділ	Відповідальний за технічні аспекти безпеки, включаючи захист мереж, серверів та робочих станцій.
Спеціалісти з безпеки	Фахівці, відповідальні за впровадження та підтримку конкретних заходів безпеки.
Всі співробітники	Залучені в процеси дотримання політик і процедур інформаційної безпеки.
Ресурси для підтримки СУІБ	
Фінансові ресурси	Інвестиції в апаратне та програмне забезпечення, навчання персоналу та проведення аудитів.
Трудові ресурси	Кваліфікований персонал для розробки, впровадження і підтримки заходів інформаційної безпеки.
Технологічні ресурси	Сучасні ІТ-рішення для захисту даних, мережевої безпеки, резервного копіювання та відновлення.

Політика інформаційної безпеки компанії “COMFY” є внутрішнім нормативним документом, що формулює позицію компанії щодо інформаційної безпеки та визначає основні принципи і завдання СУІБ. Ця політика служить основою для захисту інформаційних активів компанії.

Основними принципами політики інформаційної безпеки є:

–Цілісність.Захист точності, коректності та повноти методів обробки інформації.

–Доступність.Забезпечення безперервного доступу до інформаційних активів і сервісів компанії відповідно до наданих повноважень і прав.

– Спостережуваність.Забезпечення можливості визначення користувачів і процесів, що працюють з інформаційними активами компанії, а також часу і

дати таких дій. Це включає забезпечення принципу неможливості відмови від виконаних дій.

Політика інформаційної безпеки компанії "COMFY" базується на вимогах законодавства України та міжнародних стандартів. Вона включає положення Законів України "Про інформацію"[11], "Про захист інформації в інформаційно-телекомунікаційних системах", "Про захист персональних даних" [13], а також стандартів ДСТУ ISO/IEC 2700x:2015 та інших нормативних документів з інформаційної безпеки. Політика поширюється на всю компанію та всі треті сторони, які мають доступ до інформаційних активів компанії. [21]

Основні цілі управління інформаційною безпекою компанії "COMFY" включають:

- Забезпечення безпеки персоналу та клієнтів компанії: Захист особистих даних і конфіденційної інформації.
- Управління інформаційною безпекою: Включає визначення ролей і обов'язків у галузі ІБ, створення і підтримку СУІБ.
- Класифікація інформаційних активів: Визначення важливості і категорій інформаційних активів для адекватного захисту.
- Оцінка ризиків інформаційної безпеки: Регулярна оцінка потенційних загроз і вразливостей.
- Моніторинг подій інформаційної безпеки та управління інцидентами: Виявлення, реагування і усунення наслідків інцидентів інформаційної безпеки.
- Забезпечення безперервності бізнес-діяльності: Підготовка планів і заходів для безперервної роботи бізнесу у випадку інцидентів.
- Безпечне управління життєвим циклом інформаційної системи: Включає всі етапи від проектування до знищення інформаційних систем та даних.

В цілому політика інформаційної безпеки компанії «COMFY» сприяє безпеці окремих осіб, клієнтів і всієї компанії, забезпечуючи системний підхід до захисту інформаційних активів.

Компанія "COMFY" прагне забезпечити комфорт і зручність не тільки у виборі техніки, а й у всіх сферах взаємодії з клієнтами та співробітниками. Місія компанії полягає в тому, щоб зробити покупки та використання технологій приємним і безпечним досвідом для всіх.

У "COMFY" вірять, що безпека та конфіденційність є ключовими елементами нашого бізнесу. Вони суворо дотримуються найвищих стандартів інформаційної безпеки, щоб забезпечити захист персональних даних своїх клієнтів і співробітників.

Команда "COMFY" прагне постійно вдосконалювати практики та процедури інформаційної безпеки. Забезпечення навчання та тренінгів для наших співробітників, щоб вони могли ефективно захищати дані та дотримуватися найкращих галузевих практик.

Бо створюють прозорі умови співпраці з контрагентами та третіми особами, які мають доступ до систем компанії. Кожен учасник ділиться стандартами безпеки та документами конфіденційності, щоб забезпечити взаємну підзвітність у цих питаннях.

Компанія завжди на шляху до покращення та інновацій, проте безпека завжди залишається їхнім пріоритетом. Компанія "COMFY" прагне забезпечити надійний та захищений середовище для своїх клієнтів та співробітників, де вони можуть відчувати себе комфортно та впевнено.

Таблиця 2.13 – Заходи забезпечення інформаційної безпеки, які використовує компанія "COMFY" у різних сферах своєї діяльності

Сфера діяльності	Заходи забезпечення інформаційної безпеки
1	2
Інформаційні ресурси	Захист конфіденційної інформації є пріоритетом для "COMFY". Компанія впроваджує заходи для забезпечення безпеки даних про продукцію, клієнтів та інших операційних процесів. Це включає в себе шифрування даних та обмеження доступу до них.

Продовження таблиці 2.13

1	2
Програмне забезпечення	"COMFY" використовує сучасне програмне забезпечення для автоматизації та оптимізації своїх бізнес-процесів. Компанія періодично проводить аудит з програмного забезпечення на предмет можливих вразливостей та вживає заходів для їх виправлення
Фізичні ресурси	Забезпечення безпеки робочих приміщень та обладнання є важливою складовою стратегії безпеки "COMFY". Вона використовує сучасні системи контролю доступу та встановлює безпечне обладнання для забезпечення безперебійної роботи
Сервісні ресурси	Компанія забезпечує доступ до надійних обчислювальних та комунікаційних сервісів для своїх працівників та клієнтів. "COMFY" також стежить за безпекою інших сервісів, таких як електронна пошта та Інтернет, для забезпечення захищеності від зовнішніх загроз.

Загальна стратегія безпеки «COMFY» базується на постійному аналізі можливих ризиків та вдосконаленні заходів їх запобігання. Компанія віддає перевагу проєктивним заходам замість реагування на інциденти, що дозволяє їй ефективно захищати свої ресурси та дані.

Продовжуючи успішну діяльність у сфері роздрібної торгівлі електронікою та побутовою технікою у 2022-2023 роках, «COMFY» став одним із провідних гравців українського ринку. Компанія, заснована в 2005 році, активно розвивалася, розширювала мережу магазинів і покращувала обслуговування клієнтів.

Протягом цього періоду, "COMFY" продовжувала впроваджувати нові технологічні рішення, спрямовані на забезпечення комфорту та зручності для своїх клієнтів. Це включало в себе не лише розширення асортименту товарів,

але й інноваційні онлайн-сервіси, які спрощували процеси покупки та забезпечували більш ефективне обслуговування.

У сфері інформаційної безпеки «COMFY» вважає дуже важливим захист конфіденційності та безпеки даних своїх клієнтів. Використання стандартів ISO 27001 і 27002 свідчить про серйозне ставлення компанії до цих питань. Розробка та підтримка систем управління інформаційною безпекою допомагає знизити ризик злому та зберегти впевненість клієнтів у захисті їхніх персональних даних.



Рисунок 2.3 - Процеси управління і забезпечення ІБ

"COMFY" — це провідна роздрібна мережа, що спеціалізується на реалізації побутової техніки, електроніки, меблів та інших товарів для дому. Заснована майже 20 років тому, компанія "COMFY" визнана за свою високу якість товарів, широкий асортимент та ефективну мережу магазинів.

У світі, де загрози кібербезпеки набувають все більшого значення, "COMFY" розуміє, наскільки важливо забезпечити захист інформації. Впровадження системи управління інформаційною безпекою на основі стандарту ISO 27001 стало стратегічним кроком для компанії.

Застосування стандарту ISO 27001 дозволяє "COMFY" забезпечити захист конфіденційної інформації про клієнтів та операції, мінімізувати ризики кібератак і зберігати довіру споживачів. Також, цей стандарт допомагає компанії ефективно управляти інформаційними ресурсами, виявляти потенційні загрози безпеки та розробляти стратегії їх запобігання. [20]

За допомогою системи управління інформаційною безпекою "COMFY" може підвищити свою авторитетність як на внутрішніх, так і на міжнародних ринках, демонструвати здатність ефективно захищати інформацію та відповідати стандартам безпеки. Це сприяє збільшенню довіри споживачів і партнерів, а також позитивно впливає на репутацію компанії перед регуляторами та органами влади.

До того ж, впровадження системи управління інформаційною безпекою на базі стандарту ISO 27001 дозволить "COMFY" підвищити ефективність своїх бізнес-процесів, зменшити витрати на підтримку системи безпеки та полегшить інтеграцію з іншими стандартами якості, наприклад, ISO 9001:2000. [21]

Основною метою системи управління інформаційною безпекою для компанії COMFY є захист її інформаційних ресурсів від зовнішніх та внутрішніх, навмисних та ненавмисних загроз.

Політика інформаційної безпеки COMFY описує та регламентує функціонування системи управління інформаційною безпекою відповідно до вимог національних та міжнародних стандартів, зокрема стандартів з інформаційної безпеки.

Метою цієї політики є забезпечення ефективного функціонування системи управління інформаційною безпекою, що забезпечить створення та постійну підтримку умов, при яких ризики, пов'язані з безпекою інформаційних активів компанії, будуть контролюватися та знаходитися на прийнятному рівні.

Результати оцінки рівня зрілості процесів інформаційної безпеки свідчать про те, що управління інформаційною безпекою компанії може мати деякі слабкі місця, такі як вразливості окремих ресурсів системи управління інформаційною безпекою, які можуть бути використані загрозами для

порушення конфіденційності, цілісності, доступності та спостережуваності інформації. Такі вразливості можуть виникати внаслідок збоїв в системі безпеки, які збільшують імовірність реалізації загроз.

Таким чином, для COMFY важливо постійно вдосконалювати свою систему управління інформаційною безпекою, виправляти виявлені вразливості та забезпечувати високий рівень захисту їхніх інформаційних ресурсів.

Метою цієї політики є забезпечення ефективного функціонування системи управління інформаційною безпекою, що забезпечить створення та постійну підтримку умов, при яких ризики, пов'язані з безпекою інформаційних активів компанії, будуть контролюватися та знаходитися на прийнятному рівні.

Результати оцінки рівня зрілості процесів інформаційної безпеки свідчать про те, що управління інформаційною безпекою компанії може мати деякі слабкі місця, такі як вразливості окремих ресурсів системи управління інформаційною безпекою, які можуть бути використані загрозами для порушення конфіденційності, цілісності, доступності та спостережуваності інформації. Такі вразливості можуть виникати внаслідок збоїв в системі безпеки, які збільшують імовірність реалізації загроз.

Отже, для COMFY важливо постійно вдосконалювати свою систему управління інформаційною безпекою, виправляти виявлені вразливості та забезпечувати високий рівень захисту їхніх інформаційних ресурсів.

РОЗДІЛ 3 ВДОСКОНАЛЕННЯ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ПІДПРИЄМСТВА

3.1 Заходи із вдосконалення інформаційною безпекою ТОВ “COMFY”

Компанія “COMFY” докладас значних зусиль для створення та підтримки надійної системи управління інформаційною безпекою. Його підхід базується на систематичному аналізі потенційних загроз і вразливостей, що дозволяє своєчасно виявляти та мінімізувати ризики. Для цього компанія розробляє та впроваджує ефективні стратегії захисту інформаційних ресурсів.

Одним із ключових компонентів цієї системи є постійне навчання персоналу. Компанія “COMFY” регулярно організовує тренінги, спрямовані на підвищення обізнаності співробітників щодо кращих практик інформаційної безпеки та правильного використання інформаційних систем.

Компанія активно співпрацює з провідними технологічними компаніями та експертами з кібербезпеки для захисту конфіденційних даних клієнтів і власної інформації компанії. Це дозволяє застосовувати передові технології та підходи для забезпечення високого рівня захисту даних.

Усвідомлюючи важливість постійного вдосконалення, “COMFY” прагне постійно вдосконалювати свою систему управління інформаційною безпекою. Він підтримує довіру та впевненість у безпеці ваших інформаційних ресурсів, забезпечуючи надійний захист як ваших власних даних, так і даних ваших клієнтів.

З точки зору процесів, систему інформаційної безпеки компанії можна розглядати як процес управління ризиками.

Метою кожного бізнес-процесу є отримання результату та винагорода за це у вигляді іншого результату. У цьому випадку вихід полягає в тому, щоб запобігти виникненню ризикованої ситуації або мінімізувати її наслідки, а винагородою - зберегти матеріальні та фінансові ресурси.

Таблиця 3.1 – Модель процесу управління ризиками для системи інформаційної безпеки ТОВ “COMFY”

Етап	Опис процесу
1	2
Опис процесів	Документування всіх бізнес-процесів, пов'язаних з інформаційними системами, включаючи операційні процедури та потоки даних
Збір ризиків	Ідентифікація потенційних ризиків та вразливостей шляхом аналізу інформаційних систем та консультацій з експертами
Оцінка вразливостей	Аналіз виявлених вразливостей для визначення рівня їх критичності та потенційного впливу на безпеку інформації
Оцінка загроз	Оцінка можливих загроз, що можуть використати вразливості, включаючи внутрішні та зовнішні загрози
Моніторинг	Постійне спостереження за станом безпеки, моніторинг ефективності впроваджених заходів та виявлення нових загроз
Оцінка ефективності	Оцінка поточних заходів безпеки та їх ефективності в протидії ідентифікованим загрозам і вразливостям
Планування заходів	Розробка плану заходів для мінімізації ризиків, включаючи технічні, адміністративні та організаційні заходи
Реалізація заходів	Впровадження запланованих заходів для зниження рівня ризику до прийнятного рівня
Оцінка збитків	Оцінка можливих фінансових та нефінансових збитків у випадку реалізації ризику, враховуючи вплив на репутацію та операційну діяльність

Серед основних загроз інформаційної безпеки ТОВ «Comfy Trade» в результаті аналізу були виділені загрози, пов'язані з несанкційованим доступом

до інформації (НСД) - несанкційований доступ до автоматизованого робочого місця (АРМ) співробітників.

Даний тип загрози характеризується:

Відсутністю регламенту доступу до АРМ

Відсутністю відеоспостереження

Відсутністю засобів захисту від несанкційованого доступу

Таблиця 3.2 – Організаційні заходи з підвищення інформаційної безпеки

Організаційний захист	Опис заходу
1	2
Організація режиму і охорони	Встановлення систем контролю доступу та відеоспостереження для забезпечення фізичної безпеки об'єктів.
Організація роботи зі співробітниками	Проведення процедур відбору персоналу, їх навчання правилам безпеки та систематичні перевірки на відповідність.
Організація роботи з документами	Контроль над створенням, обліком, зберіганням і знищенням документів для захисту від несанкційованого доступу.
Організація використання технічних засобів	Використання спеціалізованого програмного забезпечення та обладнання для шифрування та зберігання інформації.
Організація роботи з аналізом загроз	Застосування методів аналізу для виявлення потенційних загроз та розроблення стратегій їх запобігання.
Організація систематичного контролю	Встановлення процедур для регулярного контролю за діяльністю персоналу та станом заходів безпеки.

Забезпечення інформаційної безпеки в організації вимагає врахування різноманітних заходів залежно від характеристик і особливих умов організації.

Впровадження відеоспостереження: Захід спрямований на контроль за проникненням у приміщення з доступом до інформації з обмеженим доступом, а також за діяльністю працівників, які мають доступ до конфіденційних даних. Відеоспостереження допомагає вчасно виявити несанкційований доступ і може бути використано як доказ при розслідуванні справ.

Встановлення спеціальних програмно-технічних засобів захисту інформації: Цей захід спрямований на забезпечення технічної безпеки інформації. Програмне та апаратне забезпечення може включати шифрування даних, контроль доступу до системи, антивірус та інші технології, які запобігають несанкційованому доступу до конфіденційної інформації.

Обидва заходи можуть бути ефективними для забезпечення інформаційної безпеки в організації, але їх ефективність залежить від конкретних обставин і потреб організації. Для успішного впровадження таких заходів необхідно провести аналіз ризиків і вибрати найбільш оптимальний і відповідний підхід до захисту інформації.

Також можна розглянути ще такі додаткові заходи:

Навчання персоналу з питань інформаційної безпеки: Організувати регулярні навчання для персоналу щодо правил безпеки обробки інформації, виявлення фішингових атак, захисту паролів тощо. Налагодження культури безпеки серед персоналу може значно знизити ризики витоку конфіденційної інформації.

Аудит систем безпеки: Регулярно проводити аудит систем безпеки для виявлення слабких місць та потенційних загроз безпеці інформації. Це дозволить оперативно виявляти та виправляти можливі порушення безпеки.

Впровадження політики безпеки даних: Розробити та впровадити політику безпеки даних, яка визначатиме правила обробки, зберігання та передачі конфіденційної інформації. Ця політика повинна бути доступною для

всіх співробітників та включати процедури реагування на можливі інциденти безпеки.

- Advanced Malware Protection (AMP) - Захист від шкідливих програм, забезпечує моніторинг і контроль для виявлення та усунення шкідливого ПЗ.

- ETA_icon - Аналіз зашифрованого трафіку.

- Firepower 2100 series - Включає функції моніторингу і контролю додатків (AVC), систему запобігання вторгнень нового покоління (NGIPS), захист від складного шкідливого ПЗ (Cisco AMP) і фільтрацію URL-адрес.

- ESA-large Email Security Appliance (ESA) - Надає захист від спаму, фішингу, шкідливого коду і витоків інформації в електронній пошті.

Рішення Cisco (Web Security Appliance і Email Security Appliance) впроваджується без перерви в роботі сервісів і з мінімальним впливом на користувачів.

Введення в експлуатацію рішення для віддаленого доступу до внутрішніх сервісів компанії співробітників і зовнішніх партнерів - Основане на міжмережевих екранах Cisco ASA 5555 і серверах авторизації Cisco Identity Service Engine (ISE). Забезпечує безпечний доступ до корпоративних ресурсів, мінімізуючи ризики несанкційованого доступу.

Рішення Cisco Advanced Malware інтегровано в IT-інфраструктуру Endpoint Protection (для кінцевих точок AMP), технологія запобігання вторгненням нового покоління. Агенти AMP встановлюють разом із кінцевими точками як додатковий захід безпеки антивірусні програми. Рішення AMP для кінцевих точок відіграє важливу роль: Запобігання деяким атакам порушити зовнішню лінію захисту.

Архітектура Cisco SAFE забезпечує узгодженість інструментів і

дозволяє вирішувати оперативні завдання протягом усього життєвого циклу атаки - до, під час та після. Системи успішно працюють і створюють безпечне середовище.

Доступ до мережі Інтернет та корпоративної мережі компанії, обмін поштою для всіх співробітників. Експерти можуть безпечно спілкуватися із зовнішніми контактами контрагентів.

Спам-фільтри, захист електронної пошти, захист периметра від мережеских погроз - неповний список вирішених системою завдань. Блок аналізу мережевого трафіку Cisco StealthWatch встановлено для того, щоб оперативно отримувати інформацію про джерела і кінцеві об'єкти, що становлять загрозу для підприємства.

Таблиця 3.3 – Структура системи інформаційної безпеки Cisco Stealthwatch “COMFY”

Складова	Опис
1	2
Аналізатор трафіку	Відслідковує мережевий трафік і виявляє аномалії та загрози.
Система виявлення загроз (Threat Detection)	Аналізує виявлені аномалії та сповіщає про потенційні загрози.
Кореляція подій (Event Correlation)	Об'єднує різні події для виявлення складних атак або цілеспрямованих загроз.
Моніторинг мережі	Надає засоби для спостереження за мережевою активністю та аналізу її.
Виявлення аномалій (Anomaly Detection)	Спостерігає за несподіваними або незвичними змінами в мережі, що можуть свідчити про загрози.
Захист від загроз	Надає інструменти для захисту мережі від виявлених або потенційних загроз.
Система журналювання (Logging)	Збирає та архівує дані щодо мережевої активності та виявлених загроз для подальшого аналізу.
Інтеграція з іншими системами	Можливість інтеграції з іншими продуктами та рішеннями безпеки для ефективного захисту.

Система відеоспостереження (відеонагляду, відеоконтролю) призначена для організації отримання інформації про поточний стан об'єкту, що охороняється (технологічного процесу) шляхом збору, обробки, архівування, зберігання, відображення та аналізу цієї інформації. Метою установки системи відеоспостереження є перегляд місць, які важливо контролювати з точки зору збереження матеріальних цінностей, контролю за проникненням на об'єкт (прохідні, паркани, двері, ворота і ін.), стеження за переміщенням об'єктів.

Система відеоспостереження на підприємстві дозволяє забезпечити потрібний рівень захисту і безпеки як персоналу, так і майна підприємства.

Охоронне відеоспостереження на підприємстві ТОВ «COMFY» повинно стати невід'ємною частиною системи безпеки такого об'єкта. Установка відеоспостереження на підприємстві дуже важлива. Так як кількість працівників ТОВ «COMFY» досягає 4500 осіб, то забезпечення їх безпеки та безпеки підприємства займає головне місце адже дуже важливим є своєчасне реагування на будь-які загрози.

Виходячи з цього, ми рекомендуємо керівництву підприємств встановити охоронне внутрішнє та зовнішнє відеоспостереження. Зовнішнє відеоспостереження на підприємстві дозволяє вести відеоконтроль відкритої території підприємства. Так за допомогою вуличного відеоспостереження на підприємстві можна організувати контроль доступу центрального входу, а також забезпечити своєчасне реагування на будь-які зовнішні загрози.

Внутрішнє відеоспостереження покликане забезпечувати постійний контроль того, що відбувається всередині організації.

Якщо розглядати виробниче підприємство ТОВ «COMFY», то на таких об'єктах відеоспостереження часто використовується для контролю виробничого процесу та забезпечення інформаційної безпеки на підприємстві. Сучасні багатофункціональні відеокамери здатні фіксувати всі дрібні дії і надавати деталізоване відео. Для організації відеоспостереження на підприємстві необхідно визначити всі функціональні зони і необхідні відеокамери для виконання завдань у цих зонах. Так, якщо ми розглядаємо офіс

компанії, то відеокамери повинні забезпечувати контроль дій робітників. За допомогою відеоспостереження можна миттєво побачити появу різних загроз і оперативно відреагувати на них.

Система відеоспостереження підприємств створює можливість контролювати персонал та відвідувачів. Система відеоспостереження підприємства в цілому в рази підвищує ефективність роботи самого підприємства та суттєво впливає на продуктивність персоналу.

Впровадження системи відеоспостереження на виробничому підприємстві ТОВ «COMFY» є важливим кроком для забезпечення контролю та безпеки. Сучасні багатофункціональні відеокамери дозволяють фіксувати всі дрібні дії і надавати деталізоване відео, що забезпечує оперативне виявлення загроз і реагування на них.

Для організації ефективного відеоспостереження необхідно визначити всі функціональні зони підприємства і підібрати відповідні відеокамери для кожної з них. В офісних приміщеннях відеокамери повинні забезпечувати контроль дій працівників, що сприятиме підвищенню дисципліни і продуктивності.

Таблиця 3.4 – Основні функції відеоспостереження

Функція	Опис
1	2
Моніторинг виробничих процесів	Камери на ключових ділянках виробництва дозволяють контролювати дотримання технологічних процесів і швидко реагувати на відхилення.
Забезпечення безпеки працівників	Відеоспостереження допомагає контролювати дотримання правил техніки безпеки і попереджати травматизм.

Продовження таблиці 3.4

1	2
Контроль доступу	Інтеграція з системами контролю доступу дозволяє відстежувати переміщення персоналу по території підприємства і запобігати несанкційованому доступу до закритих зон.
Захист від крадіжок і розкрадань	Камери в зонах зберігання матеріальних цінностей, на складах і в офісах фіксують дії персоналу та відвідувачів, що попереджає крадіжки та зловживання.
Підвищення продуктивності праці	Знання про наявність відеоспостереження спонукає працівників бути більш дисциплінованими і зосередженими на виконанні своїх обов'язків.
Оперативне реагування на інциденти	Висока якість зображення сучасних систем відеоспостереження дозволяє миттєво виявляти і реагувати на інциденти або загрози, забезпечуючи своєчасне втручання.

Загалом, система відеоспостереження суттєво підвищує ефективність роботи підприємства та продуктивність персоналу. Впровадження цієї системи на підприємстві ТОВ «COMFY» сприяє зниженню ризиків, підвищенню рівня контролю та дисципліни, а також забезпечує захист всіх учасників виробничого процесу і матеріальних цінностей.

3.2 SWOT-аналіз компанії ТОВ "COMFY"

Збільшення коефіцієнта фінансової автономії на 36% говорить про те, що компанія змогла збільшити свої власні фінансові ресурси та зменшити залежність від зовнішніх джерел фінансування. Це свідчить про стабільність та

здатність компанії самостійно управляти своїми фінансами, що є важливим фактором для її довгострокового успіху.

Зменшення коефіцієнта фінансового ризику на 26.33% вказує на те, що компанія зуміла знизити свою вразливість до фінансових коливань та ризиків. Це може бути результатом диверсифікації портфелю, раціонального управління зобов'язаннями та ефективного ризик-менеджменту.

Висока питома вага оборотних активів (88,86%) свідчить про те, що компанія має значні оборотні активи, які можуть бути легко конвертовані в грошові кошти. Це дозволяє компанії швидко реагувати на зміни на ринку та забезпечує їй гнучкість у фінансовому плануванні.

Збільшення нерозподіленого прибутку на 2,49 відсоткових пункти свідчить про ефективне управління прибутком та збільшення капіталізації компанії. Це може збільшити довіру інвесторів та підвищити інвестиційний потенціал компанії.

Скорочення дебіторської заборгованості на 12,50% свідчить про те, що компанія ефективно управляє своїми активами та має добре організовану систему взаєморозрахунків з клієнтами. Це може покращити ліквідність компанії та зменшити ризик неплатоспроможності.

В цілому, ці позитивні зміни в фінансових показниках свідчать про те, що компанія ефективно управляє своїми ресурсами та здатна адаптуватися до змін на ринку, що робить її привабливою для інвесторів та конкурентноздатною на ринку.

Зменшення питомої ваги оборотних виробничих фондів та основних засобів може сигналізувати про зниження потужності компанії в сфері виробництва, що може вплинути на її конкурентоспроможність. Зменшення обсягів цих активів може свідчити про труднощі в оновленні або збереженні необхідного обладнання, що може призвести до зниження якості продукції та ефективності виробництва.

Збільшення коефіцієнта зносу основних засобів та зменшення коефіцієнта мобільності активів може свідчити про збільшення витрат на обслуговування

активів та складнощі у їх конвертації у грошовий еквівалент. Це може бути наслідком застарілості обладнання або неефективного управління активами, що може негативно вплинути на фінансову результативність компанії.

Скорочення сукупної вартості майна та обсягів діяльності на 22,59% може бути наслідком вторгнень та бойових дій на території країни. Це може призвести до руйнування майнових об'єктів, зниження виробничих потужностей та загального занепаду економіки країни.

Незначне збільшення питомої ваги запасів може свідчити про можливу затримку грошових потоків та зростання витрат на утримання запасів. Це може бути наслідком недооцінки попиту на товари або проблем з управлінням запасами, що може підірвати ліквідність компанії та її фінансову стійкість.

Збільшення кредиторської заборгованості може свідчити про залежність від зовнішніх джерел фінансування. Це може бути результатом стратегічного використання кредитів для фінансування діяльності компанії або погіршення її фінансової стабільності.

Таблиця 3.5 – SWOT-аналіз компанії ТОВ "COMFY"

Сильні сторони (Strengths)	Слабкі сторони (Weaknesses)	Можливості (Opportunities)	Загрози (Threats)
1	2	3	4
1.Широкий асортимент товарів побутової техніки та електроніки.	1.Висока конкуренція на ринку побутової техніки.	1.Розширення мережі магазинів в регіонах з високим попитом.	1.Зростання витрат на маркетинг та рекламу через конкурентний ринок.
2.Велика кількість роздрібних магазинів по всій країні.	2.Потреба в постійному оновленні технічного обладнання та інвестиціях.	2.Розширення асортименту товарів на ринку електронної комерції.	2.Зміни у споживчому попиті через економічні коливання.

Продовження таблиці 3.5

1	2	3	4
3.Добре розвинена логістика та система постачання.	3.Потреба в покращенні сервісу та підтримці клієнтів.	3.Використання цифрових технологій для покращення ефективності продажів та маркетингу.	3.Поява нових конкурентів з новими інноваційними підходами.
4.Висока рекламна активність та брендованість.	4.Обмежені можливості для розвитку у регіонах з низьким попитом.	4.Партнерство зі світовими виробниками для ексклюзивних угод та продуктів.	4.Політичні та економічні нестабільності в країні.

У таблиці 3.5 представлено SWOT-аналіз компанії ТОВ "COMFY", що допомагає проаналізувати її сильні та слабкі сторони, а також виявити можливості для розвитку та потенційні загрози, з якими вона може зіткнутися на ринку.

Сильні сторони (Strengths): У цьому розділі вказуються основні переваги компанії. Наприклад, широкий асортимент товарів, велика кількість роздрібних магазинів, розвинена логістика та сильний бренд.

Слабкі сторони (Weaknesses): Тут визначаються внутрішні недоліки компанії, які можуть завадити її розвитку. Наприклад, потреба в оновленні обладнання, обмежені можливості для розвитку у деяких регіонах, або нестача сервісу для клієнтів.

Можливості (Opportunities): У цьому розділі вказуються зовнішні фактори, які можуть стати підґрунтям для росту компанії. Наприклад, розширення

мережі магазинів, використання цифрових технологій для покращення продажів, чи укладання ексклюзивних угод зі світовими виробниками.

Загрози (Threats): Тут розглядаються зовнішні чинники, які можуть загрожувати успішному функціонуванню компанії. Це можуть бути конкуренція на ринку, зміни у споживчому попиті, політичні або економічні нестабільності тощо.

Таблиця 3.6 – SWOT-аналіз інформаційної безпеки компанії ТОВ "COMFY"

Сильні сторони (Strengths)	Слабкі сторони (Weaknesses)	Можливості (Opportunities)	Загрози (Threats)
1	2	3	4
Ефективні системи захисту даних	Вразливість застарілих систем	Вдосконалення систем безпеки	Кібератаки та злочинні дії в Інтернеті
Проективний моніторинг та реагування	Недостатня освіта персоналу	Партнерство зі спеціалізованими фірмами	Розширення кількості кіберзагроз
Інвестиції у безпеку	Недостатня усвідомленість про безпеку серед працівників	Регулярне навчання персоналу	Регуляторні вимоги та вимоги до відповідності

Отже, у таблиці 3.6 показані сильні сторони, слабкі сторони, можливості та загрози інформаційної безпеки компанії.

Сильні сторони: Ефективні системи захисту даних: Компанія має належно розвинуті системи захисту даних, що дозволяють їй ефективно протистояти різноманітним кіберзагрозам, таким як віруси, шкідливі програми та несанкціонованість доступу.

Проективний моніторинг та реагування: Наявність процесів для раннього виявлення та реагування на інциденти безпеки дозволяє компанії оперативно реагувати на потенційні загрози.

Інвестиції у безпеку: Компанія активно інвестує ресурси у покращення рівня безпеки, що включає в себе оновлення програмного забезпечення, навчання персоналу та інші заходи.

Слабкі сторони: Вразливість застарілих систем: Використання застарілого програмного чи апаратного забезпечення може поставити компанію в небезпечне положення через відомі слабкі місця, які можуть бути використані зловмисниками.

Недостатня освіта персоналу: Відсутність належного навчання з кібербезпеки серед персоналу може призвести до неналежної реакції на потенційні загрози та збільшити ризик для компанії.

Недостатня усвідомленість про безпеку серед працівників: Якщо працівники не розуміють важливості безпеки даних та не дотримуються встановлених процедур, це може стати джерелом загрози через людський фактор.

Можливості: Вдосконалення систем безпеки: Використання новітніх технологій та методів дозволить компанії підвищити рівень безпеки та забезпечити кращу захищеність від кіберзагроз.

Партнерство зі спеціалізованими фірмами: Співпраця з фахівцями з кібербезпеки допоможе компанії виявити та усунути слабкі місця в її системах безпеки, а також отримати консультації щодо запобігання кібератак.

Регулярне навчання персоналу: Забезпечення періодичного навчання персоналу з питань кібербезпеки допоможе підвищити їх усвідомленість та зменшити ризик людського фактору у безпеці.

Загрози: Кібератаки та злочинні дії в Інтернеті: Зростаюча кількість кібератак та злочинної діяльності в Інтернеті може ставити під загрозу конфіденційність та цілісність даних компанії.

Розширення кількості кіберзагроз: Поява нових видів кіберзагроз, таких як поширення шкідливого програмного забезпечення або розкрадання конфіденційної інформації, може стати серйозною загрозою для компанії.

Регуляторні вимоги та вимоги до відповідності: Зміни у законодавстві або регуляторних вимогах можуть збільшити витрати на забезпечення відповідності та безпеки даних для компанії.

Зважаючи на вищезазначені можливості, компанія може розглядати додаткові стратегії для посилення своєї кібербезпеки:

Використання штучного інтелекту та машинного навчання: Впровадження інноваційних технологій, таких як системи засновані на штучному інтелекті та машинному навчанні, дозволить компанії автоматизувати процеси виявлення та відповіді на кіберзагрози, що зробить її більш відповідальною та реактивною.

Розвиток політик безпеки та процедур: Встановлення чітких політик та процедур у сфері кібербезпеки та їх систематичне оновлення допоможе компанії збільшити свою стійкість до загроз та забезпечити єдність підходів до захисту даних.

Впровадження двофакторної аутентифікації: Використання двофакторної аутентифікації для доступу до систем компанії зменшить ризик несанкційованого доступу навіть у випадку, якщо пароль був скомпрометований.

Аудит безпеки та тестування на проникнення: Проведення регулярних аудитів безпеки та тестування на проникнення дозволить компанії ідентифікувати потенційні слабкі місця в своїх системах та вжити відповідних заходів щодо їх усунення.

З огляду на вищенаведені загрози, компанія може також розглядати наступні заходи:

Реагування на інциденти: Розробка та впровадження планів реагування на кіберінциденти дозволить компанії ефективно та швидко реагувати на загрози, мінімізуючи їх вплив на діяльність.

Співпраця з правоохоронними органами: Встановлення зв'язків з правоохоронними органами може допомогти компанії у виявленні та протистоянні кіберзлочинності, а також виявленні зловмисників.

Моніторинг нових загроз: Постійне відстеження та аналіз нових методів кібератак допоможе компанії бути завжди готовою до нових викликів у сфері кібербезпеки.

Всі ці заходи разом з регулярними оновленнями та навчанням персоналу допоможуть компанії забезпечити високий рівень кібербезпеки та захисту даних у довгостроковій перспективі.

Збільшення коефіцієнта фінансової автономії дійсно може мати значний вплив на інформаційну безпеку підприємства. Коли компанія має більше власних коштів порівняно з боргами, це надає їй більшу гнучкість і можливості в інвестуванні в заходи забезпечення інформаційної безпеки. Наприклад, з додатковими ресурсами вона може проводити оновлення своєї інфраструктури, впроваджувати нові технології безпеки та навчати персонал.

Зменшення коефіцієнта фінансового ризику також може позитивно вплинути на інформаційну безпеку. Менші фінансові ризики означають меншу ймовірність фінансових проблем, які можуть виникнути внаслідок кібератак або втрати даних. Таким чином, компанія може мати змогу виділити більше ресурсів на заходи забезпечення безпеки та реагування на потенційні загрози.

Загрози, такі як політична нестабільність або зменшення купівельної спроможності населення, також можуть вплинути на інформаційну безпеку. Наприклад, політична нестабільність може збільшити ризик кібератак або кібершпигунства, тому важливо мати належні заходи захисту для захисту важливої інформації компанії.

Можливості, такі як збільшення обсягів продажів або привернення нових інвесторів, можуть стати основою для вкладення в додаткові заходи забезпечення інформаційної безпеки. Наприклад, компанія може використовувати додаткові прибутки для впровадження нових технологій безпеки або підвищення кваліфікації персоналу з питань безпеки даних.

У сфері інформаційної безпеки, компанія "COMFY" має свої переваги, включаючи ефективне управління кредитуванням та зменшення дебіторської заборгованості. Однак, вона також стикається з викликами, пов'язаними з політичною та економічною нестабільністю. Для забезпечення подальшого успіху, важливо розглядати можливості для диверсифікації бізнесу та залучення нових джерел фінансування. Наприклад, це може включати оновлення технологічної інфраструктури для забезпечення високого рівня захисту інформації, встановлення сучасних засобів шифрування та захисту від кібератак.

Також важливо проводити навчання персоналу з питань кібербезпеки та встановлювати строгі правила доступу до конфіденційної інформації, щоб запобігти витоку даних та інших інцидентів безпеки.

ВИСНОВОК

У результаті нашого дослідження ми зробили кілька важливих висновків:

Інформаційна безпека повинна розглядатися як перший пріоритет для будь-якої підприємницької діяльності. Це означає захист від несанкційованого доступу, збереження конфіденційності та цілісності даних. Для цього необхідно використовувати комплекс заходів, спрямованих на запобігання будь-яким загрозам інформаційній безпеці.

Забезпечення інформаційної безпеки вимагає системного і комплексного підходу. Нам важливо не лише виявляти потенційні загрози, а й реагувати на них у реальному часі. Це означає безперервний контроль за подіями, які можуть вплинути на безпеку даних, від їх створення до знищення.

Управління інформаційною безпекою важливо для забезпечення безпеки всіх властивостей інформаційних ресурсів та послуг. Для досягнення цієї мети потрібні різноманітні засоби та заходи управління, які враховують конкретні загрози і вразливості підприємства.

Щоб забезпечити ефективну роботу в умовах зміни ринкових умов, ТОВ "COMFY" повинно також удосконалити свою стратегію щодо основних засобів. Це може включати ремонт, заміну або модернізацію активів для забезпечення ефективної діяльності.

Для досягнення цієї мети, ТОВ "COMFY" може розглянути впровадження програми ефективного управління ризиками. Це допоможе зменшити негативний вплив зовнішніх факторів та максимізувати можливості в умовах економічної нестабільності.

Окрім цього, компанія може розвивати стратегічне партнерство з іншими гравцями на ринку, щоб забезпечити собі доступ до нових ресурсів та технологій. Це може включати спільні дослідження та розробки, обмін ноу-хау та інші форми співпраці.

Необхідно також активно працювати над підвищенням рівня обслуговування та задоволеності клієнтів. Залучення нових клієнтів та

збереження існуючих є ключовими для збільшення обсягів продажів та збереження лідерської позиції на ринку.

Загалом, для ТОВ "COMFY" важливо постійно адаптуватися до змін у внутрішньому та зовнішньому середовищі, вдосконалювати свої стратегії та процеси, щоб забезпечити стабільність та успішний розвиток в майбутньому.

У контексті інформаційної безпеки, ТОВ "COMFY" повинно також приділити особливу увагу захисту своїх інформаційних ресурсів та даних. Забезпечення цілісності, конфіденційності та доступності інформації є критичними для ефективної діяльності підприємства.

Підприємство повинно впровадити строгі політики безпеки, які включають у себе захист від несанкційованого доступу до даних, захист від вірусів та інших кіберзагроз, а також забезпечення регулярних резервних копій даних.

Ретельна перевірка стану безпеки мережі і систем забезпечить безперебійну роботу і захист від можливих кібератак. Проведення навчання та тренінгів для персоналу з питань інформаційної безпеки також є необхідним кроком для запобігання витоку чи недозволеного доступу до важливої інформації.

Також, компанія може розглядати можливість отримання сертифікатів та впровадження стандартів безпеки, щоб підтвердити свою відданість захисту інформації та збереженню довіри клієнтів.

Загалом, інформаційна безпека має стати невід'ємною частиною стратегії розвитку ТОВ "COMFY", щоб забезпечити стійкість, надійність та успішну діяльність компанії в сучасному цифровому світі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Фінансова звітність ТОВ "COMFY". [Електронний ресурс]. – Режим доступу: https://clarity-project.info/edr/36962487/finances?current_year=2022
2. Прибутько П.С., Лук'янець І.Б. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах. –К.: Видавець ПАЛИВОДА А.В., Київ 2007. – 252с
3. Інформаційно-психологічна безпека в епоху глобалізації: навч. посіб./В.М. Петрик, / В.В. Остроухов, А.А. Штоквіш та ін – К.: ГУІКТ, Київ 2008. – 544с
4. Кібертероризм, інформаційні війни та безпека.-К.: ТОВ «Консалтингова компанія «СІДКОН» Київ р. 2014. – 60с.
5. Кастельс, М. Інформаційна епоха: економіка, суспільство і культура. – Київ: ВД "Києво-Могилянська академія", 2012. – 640 с.
6. Вінер, Н. Кібернетика або управління і зв'язок у тварині і машині. – Київ: Либідь, Київ 1968. – 448 с.
7. Масуда, Й. Інформаційне суспільство як постіндустріальне суспільство. – Київ: ВД "Києво-Могилянська академія", Київ 2004. – 512 с.
8. Петров О.О. Управління інформаційними ризиками в бізнесі. Видавництво: Видавництво "Альфа-прес" Харків 2022.
9. Сидоренко М.М. Концепції та стратегії інформаційної безпеки підприємств. Видавництво: Видавництво "Світ знань".Львів 2021
10. Конституція України. [Електронний ресурс]. – Режим доступу: www.rada.gov.ua
11. Про інформацію, Закон України. ВВР, 1992, №48, ст.65
12. Про доступ до публічної інформації, Закон України. ВВР, 2011, №32, ст.314
13. Про захист персональних даних, Закон України. ВВР, 2010, №34, ст.481
14. Мережа «Домотехніка» припинила своє існування. Сайт українського інформаційного агентства "РБК-Україна". [Електронний ресурс]. – Режим доступу:

https://daily.rbc.ua/rus/show/set_domotekhnika_prekratila_svoe_sushchestvovanie_240620091

15. Торгові мережі «Биттехніка» та Comfy вирішили об'єднатися. Сайт українського бізнес-порталу Delo.ua. [Електронний ресурс]. – Режим доступу:
<https://web.archive.org/web/20191206204716/https://delo.ua/business/torgovye-seti-byttehnika-i-com-44034/>
16. Retail&Development Business Awards 2017: переможці, експерти, гості та багато іншого. Сайт Асоціації рітейлерів України. [Електронний ресурс]. – Режим доступу: <https://rau.ua/novyni/retail-development-business-awards-fotootchet/>
17. Ритейлер електроніки Comfy відкрив у Києві три магазини нового формату – Comfy-точки. До кінця року компанія планує відкрити ще чотири такі ж магазини. [Електронний ресурс]. – Режим доступу:
<https://biz.nv.ua/ukr/consmarket/comfy-vidkriv-tri-magazini-novogoformatu-novini-kiyeva-50194869.html>
18. Про компанію Comfy. Офіційний сайт Comfy. [Електронний ресурс]. – Режим доступу: <https://comfy.ua/ua/aboutus.html>
19. Допомога ЗСУ. Офіційний сайт Comfy. [Електронний ресурс]. – Режим доступу: <https://help.comfy.ua/braveukraine/>
20. Журавель М.Ю. Формування системи показників оцінки рівня інформаційної безпеки підприємства. Вісник економіки транспорту і промисловості. Київ, 2011. № 33. С. 171-177.
21. Система менеджменту інформаційної безпеки [Електронний ресурс]. – Режим доступу: <https://tic-ua.com/uk/services/it-servisi-i-bezpeka/>
22. Парфенцева Н.О., Голубова Г.В. Моделювання фінансових ризиків на основі статистичних методів оцінювання. Науковий вісник Національної академії статистики, обліку та аудиту. Київ, № 1-2, 2022. С. 14 – 20. [Електронний ресурс]. – Режим доступу: <https://doi.org/10.31767/nasoa.1-2-2022.02>

23. Синчук І. В. Вплив SWOT-аналізу на прийняття управлінських рішень в умовах фінансової кризи. Молодий вчений. Одеса, 3 (30). 2016. С. 174 – 178. [Електронний ресурс]. – Режим доступу: <http://molodyvcheny.in.ua/files/journal/2016/3/41.pdf>
24. Тихомиров О.О. Діяльнісний підхід у дослідженнях забезпечення інформаційної безпеки. Київ, 2012. № 3(10). С. 11-17
25. Кулініч О. А. Структурні чинники економічної безпеки України. Харків, 2007. С. 59-63.
26. Гуцу С.Ф. Правові основи інформаційної діяльності: навч. посібник. Харків «ХАІ» 2009. [Електронний ресурс]. – Режим доступу: <https://dspace.library.khai.edu/xmlui/bitstream/handle/123456789/6747/GutzuPravovi.pdf?sequence=1&isAllowed=y>
27. Харченко Л.С., Ліпкан В.А., Логінов О.В. Інформаційна безпека України: глосарій. Київ: Текст, 2004. 136 с
28. Корченко О.Г., Дрейс Ю.О. Нормативно-правове забезпечення інформаційної безпеки: збірник нормативно-правових документів. Житомир : ЖВІ НАУ, 2019. 280 с.
29. Логінова Н. І. Правовий захист інформації: навч. посібник. Одеса: Фенікс, 2015. 264 с
30. Аванесова Н. Е., Марченко О. В. Стратегічне управління підприємством та сучасним містом: теоретико-методичні засади : монографія. Харків : Щедра садиба плюс, 2015. 196 с.
31. Батракова Т. І., Калюжна Ю. В. Банківські операції : навч. посіб. Запоріжжя : ЗНУ, 2017. 130 с
32. Аніловська Г. Я., Марушко Н. С., Стоколоса Т. М. Інформаційні системи і технології у фінансах : навч. посіб. Львів : Магнолія 2006, 2015. 312 с.
33. Бікулов Д. Т, Чкан А. С., Олійник О. М., Маркова С. В. Менеджмент : навч. посіб. Запоріжжя : ЗНУ, 2017. 360 с.
34. Горбунова А. В. Управління економічною захищеністю підприємства: теорія і методологія : монографія. Запоріжжя : ЗНУ, 2017. 240 с.

ДОДАТОК А

Аналіз балансу ТОВ "COMFY"

Статі активу (пасиву)	01.01.2021 тис. грн.	Питома вага	01.01.2022 тис. грн.	Питома вага	01.01.2023 тис. грн.	Питома вага
Майно усього	4310624	100	520671	100	4030799	100
1. Необоротні активи	480384	11,14	658101	12,64	4936855	12,25
2. Оборотні активи	383024	88,86	4548870	87,36	3537144	87,75
2.1 Запаси	149060	34,71	1792150	34,42	1757724	47,97
2.2 Дебіторська заборгованість	794881	18,44	768469	14,76	457982	12,50
2.3 Витрати майбутніх періодів	818	0,02	1171	0,02	349	0,01
2.4 Грошові кошти та їх еквіваленти	1515361	35,15	1957672	37,60	1286606	35,11
2.5 Інші оборотні активи	23120	0,54	29408	0,56	4030799	0,94
Джерела майна, всього	4310624	100	5206971	100	135182	100
1. Власний капітал	106330	2,47	129681	2,49	4000	3,35
1.1 Зареєстрований капітал	500	0,01	4000	0,08	34483	0,10
1.2 Нерозподілений прибуток	105830	97,53	129181	2,48	13182	3,25
1.3 Інші джерела	0	0,00	-3500	-0,07	0	0,00
2. Позиковий капітал	4204294	2,46	5077290	97,51	3895617	96,65
2.1 Кредиторська заборгованість та поточні зобов'язання	4052942	94,02	4888765	93,89	3800185	94,28