Ф А 2.2.1-32-367

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ
Факультет фармацевтичних технологій та менеджменту
Кафедра управління та забезпечення якості у фармації

КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«РОЗРОБКА ПРОЦЕДУРИ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ РИЗИКАМИ В ОРГАНІЗАЦІЇ»

Виконав: здобувач вищої освіти
групи ЯССм22(1,5д)-02
спеціальності: 073 Менеджмент
освітньої програми Якість,
стандартизація та сертифікація
Сергій ОБЛОГ

Керівник: доцент закладу вищої
освіти кафедри управління та
забезпечення якості у фармації,
канд. фармац. наук, доцент
Тетяна ЗБОРОВСЬКА

Рецензент: професор закладу вищої
освіти кафедри фармацевтичного
менеджменту і маркетингу,
д-р. фармац. наук, професор
Оксана ТКАЧОВА

Харків – 2024 рік

АНОТАЦІЯ

Сергія ОБЛОГА на тему "Розробка процедури управління інформаційними ризиками в організації"

Мета дослідження: розробка процедури управління інформаційними ризиками, що виникають у діяльності комерційних підприємств.

Завдання: аналіз сучасних підходів до інформаційної безпеки; вивчення вимог ДСТУ ISO 31000:2018 та ДСТУ ISO 27001:2023; аналіз діяльності вітчизняної компанії ПП «IT МАСТЕР-СЕРВІС»; розробка заходів щодо побудови системи управління інформаційної безпеки.

Об'єктом дослідження є діяльність вітчизняного приватного підприємства «IT МАСТЕР-СЕРВІС».

Предметом дослідження є підходи до формування процедури управління інформаційними ризиками.

Розроблені рекомендації для побудови системи управління інформаційною безпекою, в основу якої покладено процеси управління ризиками інформаційної безпеки. На основі розроблених рекомендацій надана можливість оцінки ризиків інформаційної безпеки комерційного підприємства для подальшого зменшення їх руйнівного впливу.

Структура і обсяг кваліфікаційної роботи: кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, переліку посилань 33 найменування, 2 додатки, і містить 9 рисунків, 9 таблиць. Повний обсяг кваліфікаційної роботи складає 68 сторінки, з яких перелік посилань займає 4 сторінки, додатки – 7 сторінок.

Ключові слова: ризик-орієнтований підхід, інформаційна безпека, кібербезпека, стандарт ДСТУ ISO 31000, стандарт ДСТУ ISO 27001.

ABSTRACT

Serhii OBLOH on the topic "Development of the information risk-management procedure in the organization".

The purpose of the study: development of a procedure for managing information risks arising in the activities of commercial enterprises.

Task: analysis of modern approaches to information security; studying the requirements of ISO 31000:2018 and ISO 27001:2023; analysis of the activities of the domestic company PE "IT MASTER-SERVICE"; development of measures to build an information security management system.

The object of the study is activity of the domestic private enterprise "IT MASTER-SERVICE".

The subject of the study is approaches to the formation of information risk management procedures.

Recommendations for building an information security management system based on information security risk-management processes have been developed. Based on the developed recommendations, it is possible to assess the information security risks of a commercial enterprise in order to further reduce their destructive impact.

Structure and scope of the qualification work: the qualification work consists of an introduction, three sections, general conclusions, a list of references, 33 names, 2 appendices, and contains 9 figures, 9 tables. The full scope of the qualification work is 68 pages, of which the list of references occupies 4 pages, the appendices - 7 pages.

Key words: risk-oriented approach, information security, cyber security, standard ISO 31000, standard ISO 27001.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

DDoS – вид кібератаки, під час якої зловмисники намагаються порушити роботу веб-сайту, мережі чи інших онлайн-сервісів, перевантажуючи їх великою кількістю підроблених чи небажаних запитів

ESET – міжнародний розробник антивірусного програмного забезпечення і рішень в області комп'ютерної безпеки для корпоративних і домашніх користувачів

Gartner, Inc – провідна світова дослідницька і консалтингова компанія у сфері інформаційних технологій

IBM – International Business Machines Corporation – американська електронна корпорація, один із найбільших світових виробників усіх видів комп'ютерів і програмного забезпечення

ISO – International Organization for Standardization (міжнародна організація зі стандартизації)

PDCA Plan-Do-Check-Act – Цикл Шухарта-Демінга: планування – виконання запланованого – перевірка і аналіз – коригування та удосконалення

PwC – Price water house Coopers – міжнародна мережа компаній, що пропонує професійні послуги у сфері менеджмент-консалтингу та аудиту

SWOT-аналіз – Strengths (сильні сторони), Weaknesses (слабкі сторони), Opportunities (можливості) та Threats (загрози)

ДБЖ – джерело безперебійного живлення

ЗМІ – засоби масової інформації

ІБ – інформаційна безпека

ІТ – інформаційні технології

НП – надзвичайна подія

ПЗ – програмне забезпечення

ПП – приватне підприємство

СУЯ – система управління якістю

ЦОД – центр обробки даних

ВСТУП

Актуальність роботи. У сьогоднішніх умовах фінансової, політичної нестабільності в Україні, підвищеної конкуренції між підприємствами, актуальним постає питання вивчення сучасних підходів до управління та розвитку, які б допомогли оперативно, в режимі реальному часу, реагувати на непередбачувані зміни, впливи зовнішнього та внутрішнього середовища.

З кожним днем комерційні організації все більше приділяють увагу захисту інформації. Грамотна побудова системи безпеки з урахуванням потенційних ризиків є дуже важливим етапом на шляху до збереження таємниці своєї комерційної інформації, втрата або розповсюдження якої може фатально вплинути на діяльність компанії та її позиції на ринку.

Дослідження, які провела компанія IBM у 2022 році, показали, що середній розмір збитків від інформаційних кібератак для підприємств становив 3,66 мільйона доларів США. Більше половини підприємств, які зазнали кібератак – втратили ділову репутацію [1].

Інше дослідження, яке проводилось компанією PwC у 2022 році, також вказує, що 60 % підприємств зазнали кібератак. При цьому 40 % підприємств повідомили про втрату даних в результаті цих атак. Найбільшою загрозою для підприємств становлять кібератаки, спрямовані на крадіжку даних. У 2022 році 40 % підприємств, які зазнали кібератак, повідомили про крадіжку даних. При цьому найчастіше крадуть конфіденційну інформацію, таку як особисті дані клієнтів, фінансову інформацію або інформацію, що відноситься до комерційної таємниці [2].

За підсумками дослідження, проведеного компанією ESET у 2022 році, в Україні 77 % підприємств зазнали кібератаки. Це на 10 % більше, ніж у 2021 році [5]. Серед найпоширеніших видів атак в Україні були:

- зловмисні програми (78 %);
- фішинг (65 %);
- знищення даних (57 %);
- розкрадання даних (55 %);

– атака розподілених відмов у обслуговуванні (DDoS) (49 %).

Наслідками кібератак в Україні можуть бути перебої у роботі критичної інфраструктури. Це можуть бути енергетичні об'єкти, медичні установи та системи життєзабезпечення, що може призвести до дуже серйозних проблем у нормальному функціонуванні держави в цілому. Щоб мінімізувати можливість виникнення інформаційних ризиків, підприємства повинні впровадити ефективні системи управління інформаційною безпекою. Ці системи повинні включати в себе заходи щодо запобігання, виявлення та реагування на інформаційні ризики.

Основні ризики, які можуть бути розглянуті щодо інформації підприємства, пов’язані з неправильним підходом до керування інцидентами інформаційної безпеки; незахищеністю активів IT-інфраструктури; неналежним захистом інформації у мережах та на носіях з використанням технічних уразливостей цих самих носіїв тощо. Аналіз стандартів з інформаційної безпеки дозволяє виявити основні елементи ризиків, які описуються інформаційною структурою та визначають вплив на діяльність інформаційних систем [7].

Під ризиками ми розуміємо незаплановані події або ймовірність настання подій, які не є частиною діяльності підприємства та можуть призвести до негативних наслідків. Інколи, у результаті певних рішень або дій, ризики можуть призвести до позитивного розвитку непередбаченої ситуації. Тому ідентифікація та оцінка ризиків – це дуже важливий процес у сучасній діяльності комерційних організацій.

Для того, щоб ефективно організувати захист інформації, треба побудувати ефективну та надійну систему управління інформаційною безпекою (ІБ), а це, в свою чергу, потребує проаналізувати ризики, запланувати заходи запобігання порушенню ІБ, вирішити, які програмні та апаратні комплекси необхідні для забезпечення безпеки. Усі ці заходи повинні бути об’єднані Політикою інформаційної безпеки організації. З перелічених етапів побудови системи інформаційної безпеки найскладнішим є етап

ідентифікації та аналізу ризиків. На цьому етапі нам треба ідентифікувати загрози відповідно до специфіки діяльності та визначити об'єкти інформації, що потребують захисту, виявити та ідентифікувати джерела загроз, а також оцінити інформаційні ризики за ймовірністю настання, виявлення та ступеню впливу.

Сучасні підприємства приділяють все більше уваги аналізу ризиків ІБ. Це пов’язано з тим, що постійно збільшується використання інформаційних технологій, і, як наслідок, постійно зростають об’єми та цінності комерційної інформації, яка генерується самими підприємствами, а також інтеграція нових програмно-технічних комплексів з метою автоматизації та удосконалення діяльності підприємства.

Постійне розгортання та удосконалення комерційної діяльності підприємств вимагає ще більшого впровадження захисних заходів для збереження інформації, що, в свою чергу, призводить до того, що на сьогодні ІБ є дуже важливим фактором, що забезпечує конкурентоспроможність, репутацію та прибутковість комерційних структур.

Для багатьох користувачів комп’ютерні засоби є обмеженням зони інформаційних ризиків. Дуже часто при розгляданні теми ризиків пропускаються такі аспекти, як отримання та обробка, зберігання та передача інформації. Отже, дуже важливими аспектами інформаційної безпеки можна вважати цілісність інформації, її конфіденційність та можливість доступу й обробки певним колом співробітників.

Комерційні підприємства впроваджують та використовують інноваційні рішення, постійно впроваджують та розгортають новітні інформаційні технології, але при цьому ми повинні розуміти, що і інноваційні рішення, і новітні інформаційні технології вимагають особливих підходів до Системи управління ІБ, яка базується на управлінні ризиками.

Мета роботи. Аналізуючи цей напрям управління ми визначили метою роботи розробку процедури управління інформаційними ризиками, що виникають у діяльності комерційних підприємств.

Об’єкт та предмет дослідження. Як об’єкт було вибрано діяльність вітчизняного приватного підприємства «ІТ МАСТЕР-СЕРВІС»; предметом дослідження стали підходи до формування процедури управління інформаційними ризиками.

Основні завдання роботи. Для досягнення раніше встановленої мети нам необхідно здійснити дії, направлені на:

- аналізування сучасних підходів до ІБ;
- вивчення вимоги ДСТУ ISO 31000:2018 та ДСТУ ISO 27001:2023;
- аналізування діяльності компанії «ІТ МАСТЕР-СЕРВІС»;
- розробку заходів щодо побудови системи управління ІБ.

Методи дослідження, що використовувалися нами: системно-аналітичний метод; метод структурно-логічного моделювання; аналіз міжнародних стандартів; проблемно-орієнтований.

Практичне значення отриманих результатів роботи полягає в можливості використання розроблених рекомендацій для побудови системи управління інформаційною безпекою, в основу якої покладено процеси управління ризиками ІБ. Також на основі розроблених рекомендацій розглядається можливість оцінки ризиків інформаційної безпеки комерційного підприємства для подальшого зменшення їх руйнівного впливу.

Апробація результатів роботи. Матеріали роботи опубліковані в матеріалах ІІІ Всеукраїнської науково-практичної конференції з міжнародною участю (7-8 грудня 2022 р., м. Харків) та матеріалах І Науково-практичної internet-конференції з міжнародною участю «Актуальні проблеми якості, менеджменту і економіки у фармації і охороні здоров’я» (19 травня 2023 р., м. Харків).

Структура і обсяг кваліфікаційної роботи: кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, переліку посилань 33 найменувань, 2 додатки, і містить 9 рисунків, 9 таблиць. Повний обсяг магістерської роботи складає 68 сторінок, з яких перелік посилань займає 4 сторінок, додатки – 7 сторінок.

РОЗДІЛ І

ВПРОВАДЖЕННЯ РИЗИК-ОРІНТОВАНОГО ПІДХОДУ В ІНФОРМАЦІЙНУ ДІЯЛЬНІСТЬ ОРГАНІЗАЦІЙ

1.1 Досвід побудови інформаційної діяльності організації на основі ризик-орієнтованого підходу

Останніми роками можна спостерігати зростання кількості приватних підприємств малого та середнього бізнесу, з якою зростає і кількість впроваджуваних інформаційних технологій. Розширення інформаційних технологій, які використовує бізнес, призводить до актуалізації потреб в області інформаційної безпеки, що стає ключовим в організації діяльності підприємства. Опитування, проведене IBM Ponemon [8] показує, що незважаючи на те, що підприємства збільшили витрати на кібербезпеку, середній час виявлення та нейтралізації витоку даних не покращився за останні кілька років. Це дослідження вказує на те, що з підвищенням витрат та уваги, яка приділяється кібербезпеці, самі ризики для організацій не зменшуються. Розглядаючи інформаційні ризики, деякі автори (Фон Солмс, та Ван Нікерк) розрізняють кібербезпеку та інформаційну безпеку. Кібербезпека відноситься як до інформаційних, так і до неінформаційних активів, впливати на які можна через кіберпростір. Неінформаційними активами можуть бути співробітники, яких можна скомпрометувати, а також фізичні активи, які можуть бути пошкоджені через систему взаємопов’язаних комп’ютерних пристроїв, об’єктів, які наділені унікальними ідентифікаторами та здатні передавати дані через мережу без взаємодії між людьми та комп’ютерами. Проте інформаційна безпека стосується лише захисту інформаційних активів незалежно від того, зберігаються вони в кіберпросторі чи за його межами [9].

Із зростанням кількості центрів обробки даних та об’ємів самої інформації, що обробляється, виникають різні моделі, які допоможуть ефективніше ідентифікувати кіберризики. Одна з таких моделей – це

використання методів спостереження за поведінкою та аналізу великих об’ємів даних для виявлення аномалій, які можуть становити загрозу для ІТ-інфраструктури [10]. Інша модель, коли кіберзлочинці вигадують нові та сучасні методи зламу систем, передбачає більш проактивний підхід до ідентифікації ризиків. Ця модель розглядає концепцію «приманки» щодо активного залучення кіберзлочинців за допомогою систем-приманок задля розуміння та виявлення нових типів та принципів атак, перш ніж таки атаки набудуть широкого розповсюдження [11].

Одним з цікавих прикладів боротьби з загрозами є страхування в рамках управління кіберризиками. В рамках цієї ідеї розглядається можливість обмеження управління кіберризиками та здійснення перенаправлення ресурсів на страхування. Але тут виникає декілька проблем, одна з яких є незрозумілість ціноутворення. Вона полягає у тому, що неможливо знайти компроміс між фінансовими витратами, які слід вкласти в кібербезпеку, та витратами для придбання кіберстрахування [3, 4].

Розглядаючи організації в розрізі чисельності співробітників та рівня розвитку ІТ-інфраструктури, можна виділити кілька типів порушень кібербезпеки. Це можуть бути інциденти, спричинені як внутрішніми, так і зовнішніми сторонами. Доведено, що ймовірність порушень є меншою для великих компаній. Поясненням цього факту є те, що великі компанії можуть мати кращу інфраструктуру ІБ, яка більш ефективно перешкоджає кіберзлочинцям здійснювати атаки [12]. Але, водночас, розглядаючи корпоративне управління і незважаючи на розмір компанії, організації, що мають небагато управлінців, проте з великим фінансовим досвідом,мають меншу ймовірність зіткнутися з порушенням. Крім того, корпоративна відповідальність допомагає зменшити ймовірність порушення кібербезпеки, оскільки кіберзлочинці часто атакують соціально безвідповідальні фірми, обґрунтовуючи свої дії своєрідним покаранням за їх діяльність щодо навколишнього середовища чи, наприклад, безпеки продукції [12].

Однак у нещодавньому дослідженні щодо порушень кібербезпеки за період 2005-2017 років не було знайдено доказів того, що показники корпоративного управління, такі як: розмір правління, кількість членів правління, кількість управляючих філіями, мають вплив на ймовірність витоку даних, спричиненого іншими сторонами. Це дослідження вказує на те, що впливає на кількість кібератак фінансова міцність організації, тобто ймовірність кібератак збільшується на фінансово здорові організації [13].

На відміну від цього, дослідження чисельних втрат даних та їх розповсюдження за період 2005-2016 років мають обґрунтовані докази того, що організації, які часто кредитують свій бізнес, частіше повідомляють про порушення кібербезпеки. Пояснення цьому лежить в недостатній кількості ресурсів цих організацій для інвестування в системи кібербезпеки, і як наслідок, це робить їх більш уразливими до кібератак [14]. Схожі результати були отримані в дослідженні кіберінцидентів, які відбулися в періоді з 2005 по 2018 роки. У ньому повідомляється, що порушення кібербезпеки імовірніше трапляються в організаціях з обмеженими фінансами, ніж у фінансово незалежних організаціях [15].

Сучасні витрати організацій на інфраструктуру інформаційних технологій становлять значну частину інвестицій і надалі продовжуватимуть зростати (табл.1.1), оскільки комерційні організації і надалі намагатимуться підвищити свою операційну ефективність [8].

Таблиця 1.1.

Прогноз витрат на IT у всьому світі у 2024р. (мільйони доларів США)

	2022 Витрати	**2022 Зростання (%)**	**2023 Витрати**	**2023 Зростання (%)**	**2024 Витрати**	**2024 Зростання (%)**
Системи ЦОД	227,021	19,7	237,703	4,7	260,221	9,5
Пристрої	766,279	-6,3	689,288	-10,0	722,472	4,8
Програмне забезпечення	811,314	10,7	916,240	12,9	1,042,386	13,8
IT-послуги	1,305,699	7,5	1,401,038	7,3	1,547,349	10,4
Послуги зв'язку	1,423,128	-1,9	1,449,286	1,8	1,497,345	3,3
Загалом IT	**4,533,441**	**2,9**	**4,693,556**	**3,5**	**5,069,773**	**8,0**

У своїх дослідженнях глобального набору даних про порушення кібербезпеки, де організації зазнавали фінансові втрати, понесені з 1995 по 2014 роки, Елінг і Вірфс підкреслюють, що людський фактор є одним із головних факторів кіберризику [17].

Розділивши організації за галузевим напрямком можна побачити, що організації, які працюють у роздрібній торгівлі або високотехнологічних галузях як правило, мають більшу ймовірність зазнати кібератак або втратити дані при кіберінцидентах [13, 16, 18].

Окрім кіберпорушень, націлених на одну конкретну організацію, бувають порушення кібербезпеки, які мають побічні ефекти. Інакше кажучи, вплив кібератак може поширюватися від організації, на яку націлена атака, на інші споріднені організації в тій самій галузі або на організації, які розташовані в тому самому географічному регіоні [13, 19, 20]. Прикладом цього може бути те, що розробники систем безпеки зацікавлені в отриманні вигоди від інцидентів кібербезпеки шляхом зростання вартості їх послуг чи продукції або компанії в цілому [19].

1.2 Вимоги стандартів ДСТУ ISO 31000:2018 та ДСТУ ISO 27001:2023

Огляд стандарту ДСТУ ISO 31000

Управління ризиками повинно бути системним процесом, в якому беруть участь усі співробітники організації. За мету управління ризиками треба ставити збільшення ймовірності настання позитивних наслідків та звести до мінімуму негативні наслідки кризової ситуації. Сам процес управління ризиками від ідентифікації загрози до запобігання або нейтралізації наслідків зводиться до усунення або зменшення ефекту від кризової ситуації з мінімальним вкладенням ресурсів [22, 23].

Впровадження вимог міжнародних стандартів переважно базується на використанні циклу Демінга-Шухарта (PDCA). Стандарт ISO 31000:2018 Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT) не є виключенням та розглядає: ідентифікацію, аналіз та оцінку ризиків; далі,

після оцінки ризику, пропонується обробка або запобігання ризику. Останнім кроком є моніторинг та огляд ризикових ситуацій.

Стандарт ISO 31000:2018 може бути застосований до будь-яких організацій незалежно від типу, розміру, виду діяльності та місцезнаходження. Цей стандарт покриває всі види ризиків. ISO 31000:2018 є своєрідною інструкцією для організацій щодо створення систем управління ризиками [26].

Незважаючи на те, що ISO 31000:2018 надає загальне керівництво, він не є універсальним в управлінні ризиками в організаціях, а використовується як допоміжний стандарт для побудови системи управління ризиками, щоб гарантувати досягнення організацією виробничих цілей з ощадливим використанням ресурсів. Стандарт ISO 31000:2018 надає принципи управління ризиками, визначає межі та допомагає виділити процеси, які можна використовувати як базу ефективного управління ризиками [24].

Проте цей стандарт не надає опис механізмів, які організація може використати для того, щоб відстежити та ідентифікувати загрозу. Тому кожна організація, виходячи зі своїх цілей і можливостей, повинна обирати для себе найпридатніші та ефективні механізми та ресурси, за допомогою яких, в умовах невизначеності, зможе зменшити ризики для своєї діяльності [27].

Як у всіх стандартах ISO, у першому розділі стандарту ISO 31000:2018 визначаються ключові терміни. Термінів всього вісім, включаючи визначення ризику як «вплив невизначеності на цілі» який зосереджується на впливі неповного розуміння або знання подій та обставин на прийняття рішень організацією [24].

Розділи стандарту були переглянуті з ціллю спрощення розуміння, щоб зробити його більш доступним для всіх зацікавлених сторін. У версії 2018 року більша увага приділяється постійному вдосконаленню, залученню зацікавлених сторін, розглядання специфіки діяльності організації та врахування людських і культурних факторів. Виходячи з цього, ключовою

перевагою стандарту є адаптація організації до управління ризиками у відповідності до власних потреб і цілей.

Нова версія ISO 31000 представляє загальний огляд управління ризиками та процесами побудови і реалізації системи управління ризиками. Ця версія стандарту представляє собою невеликий посібник, який надає організаціям можливість використовувати принципи управління ризиками для більш кращого планування своєї діяльності. Ключові особливості нової редакції полягають у [28]:

– перегляді принципів управління ризиками, які є ключовими критеріями його успішності;

– підвищені уваги щодо лідерства з боку вищого керівництва, яке має забезпечити інтеграцію управління ризиками в усі організаційні заходи, починаючи з управління організацією;

– збільшені акценту на процесний підхід в управління ризиками, залучення нового досвіду, знань і аналізу для перегляду елементів процесу. Контроль дій на кожному етапі процесу;

– зосередженості на моделі, яка регулярно використовує зворотний зв’язок із зовнішнім середовищем, щоб відповідати його численним потребам.

Технічний комітет з управління ризиками, який розробив стандарт ISO 31000 в новій версії, зосередився на інтеграції з організацією та звернув більшу увагу на роль лідерів та їх відповідальність. В організаційному менеджменті питанню ризиків приділяється не так багато уваги, тому акцент на лідерство та відповідальність допоможе звернути увагу на те, що управління ризиками є невід’ємною частиною бізнесу. Такий підхід надає організаційну стійкість інформаційним технологіям (IT), відповідність, якість та безпеку, безперервність бізнесу, антикризове управління.

ISO 31000:2018 – це не просто стандарт – це погляд у майбутнє керування ризиками. Цей стандарт не пристосований до сертифікації, він

надає не вимоги, а рекомендації, що, в свою чергу, дає менеджерам гнучкість у впровадженні у відповідності до потреб і цілей організації [24, 28].

Огляд стандарту ДСТУ ISO 27001

Стандарт ДСТУ ISO 27001:2023 висуває вимоги щодо створення, впровадження, обслуговування і постійного вдосконалення системи управління інформаційною безпекою організації. Цей стандарт забезпечує структурований підхід до управління ІТ інфраструктурою організації, захисту інформаційних активів, включаючи конфіденційну інформацію. Стандарт ДСТУ ISO 27001:2023 включає в себе вимоги до процесу управління ризиками інформаційної безпеки, а також встановлює вимоги до засобів та заходів щодо зниження ризиків і захисту інформації, безперервності бізнесу.

Стандарт ДСТУ ISO 27001:2023 може бути застосовано в організаціях усіх розмірів і типів для захисту інформації та побудові ефективної системи управління ризиками ІБ. Система управління інформаційною безпекою представляє собою набір політик, процедур, засобів контролю та інших заходів для виявлення, оцінки та управління ризиками ІБ.

Принципи стандарту ISO 27001

Стандарт ДСТУ ISO 27001:2023 заснований принципах, які допомагають створити, впровадити, підтримувати й постійно вдосконалювати систему управління ІБ. Ці основоположні принципи полягають у наступному:

Оцінка ризиків: Стандарт ДСТУ ISO 27001:2023 вказує на важливість проведення оцінок ризиків ІБ які можуть вплинути на конфіденційність, цілісність і доступність інформаційних ресурсів організації [25].

Обробка ризиків: Стандарт ДСТУ ISO 27001:2023, для ефективного управління виявленими ризиками, вимагає від організацій впровадження заходів по обробці ризиків. Це може бути впровадження засобів контролю ІБ, таких як політики, процедури та технічні заходи для запобігання виникненню ризиків, або їх зниження до прийнятного рівня.

Контекстний підхід: ДСТУ ISO 27001:2023 приділяє увагу контексту організації, включаючи його внутрішні та зовнішні фактори, нормативні

вимоги, враховуючи інтереси усіх зацікавлених сторін. Такий підхід надає гарантії, що система управління ІБ відповідає цілям, завданням й напрямку стратегічного розвитку організації.

Цикл PDCA: Стандарт відповідає циклу PDCA, головна ідея якого полягає в постійному вдосконаленні процесів. Такий підхід гарантує, що система управління ІБ постійно оцінюється, переглядається і вдосконалюється [25].

Лідерство: В стандарті підкреслена важливість лідерства і прагненні вищого керівництва у створенні, впровадженні й підтримці ефективної системи управління ІБ. На вищому керівництві полягає відповідальність за забезпечення лідерства, встановленню пріоритетних напрямків та створенню культури ІБ всередині організації.

Процесний підхід: Стандарт ДСТУ ISO 27001:2023 підтримує процесний підхід при створенні системи управління ІБ. Процесний підхід включає в себе ідентифікацію, документування та впровадження процесів для ефективного управління ризиками ІБ на основі системного підходу. Це надає впевненості, що методи забезпечення інформаційної безпеки інтегруються у процеси організації [25].

Прийняття рішень, заснованих на фактах. Документування: Стандарт вимагає від організацій документування діяльності побудованої системи ІБ, включаючи політики й процедури. Приймати рішення спираючись на фактичні дані для забезпечення ефективності методів побудови інформаційної безпеки та відповідності цих методів вимогам та цілям організації.

Перелічені принципи допомагають організаціям побудувати основу для створення і підтримання ефективної системи управління ІБ, заснованої на вимогах стандарту ДСТУ ISO 27001:2023. Дотримання організацією цих принципів дозволить систематично і структуровано управляти ризиками ІБ а також постійно поліпшувати свій стан в області інформаційної безпеки [25].

1.3 Процес реалізації управління інформаційними ризиками

Управління ризиками ІБ – це процес управління ризиками, які виникають при використанні інформаційних технологій. Інакше кажучи, це процес, при якому організації повинні ідентифікувати і оцінити ризики розповсюдження конфіденційних даних, а також ризики втрати доступності та цілісності своїх інформаційних активів. Процес реалізації залежить від розміру організації, ресурсів, які організація може використати і цілей яких прагне досягти.

Впровадження системи управління ризиками представляє собою безперервний процес інтеграції бізнес-стратегій, які повинні пом'якшити або оптимізувати ризики організації. Цей процес можна представити так:

– Перший крок: організація повинна створити основу системи управління ризиками, визначити обсяг реалізації, зацікавлені сторони. Призначити керівників проекту.

– Другий крок: організація повинна визначити та провести оцінку ризиків на основі розроблених критеріїв.

– Третій крок: зменшення або оптимізація ризиків за допомогою розробленого підходу реагування на ризик.

– Четвертий крок: моніторинг і звіт про реагування. Покращення та вдосконалення процесів реагування.

Перший крок: фундамент системи управління ризиками.

У процесі реалізації системи управління ризиками організація повинна визначити, яку структуру системи використовувати. Це може бути власноруч розроблена внутрішня структура або обрана одна зі стандартизованих моделей управління ризиками. В обох випадках головна мета – це мінімізація наслідків кризової ситуації. Об'єднавши сильні сторони добре відомих систем управління в спрощену, засновану на простих циклах зворотного зв'язку, можна отримати систему з чотирьох компонентів: це політика управління, оцінка ризиків, управління ризиками та звітність і моніторинг. Це дасть можливість розподілити відповідальність, побудувати ланцюги рішень

реагування на кризові ситуації, проаналізувати систему управління ризиками за допомогою зворотного зв'язку [29, 31].

Визначивши зацікавлені сторони, організація може розподілити відповідальність за конкретні цілі управління ризиками, а також те, як ці сторони повинні вирішувати ускладнення, що виникають під час впровадження системи управління ризиками. Головний акцент при цьому робиться на цілях і результатах впровадження системи.

Другий крок: Визначення та оцінка ризику.

Оцінка ризику – це процес ідентифікації, оцінки та визначення пріоритетів ключових ризиків для конкретних бізнес-цілей. Оцінювати ризик можна за типом ризику, сферою впровадження, складністю та впливу на цілями [29].

На цьому етапі керівництво розробляє критерії оцінки, порівнюючи поточний ризик з порогом допустимого ризику для організації. Далі керівництво створює звіти про оцінку ризиків, в яких окреслюються події ризику, і оцінюється потенційний вплив на діяльність організації. Ці звіти допомагають виконавцям розподілити обов'язки та розробити план дій у разі настання кризової ситуації. Також, на цьому етапі припустимо використання інструменту моделювання ризиків який допомагає прогнозувати ймовірність настання різних ризиків за різних умов [29, 30]. Дуже важливим для розробки критеріїв оцінки є аудит ризиків. Цей механізм забезпечує виявлення ризиків, вивчення граничних значень ризику, який шкодить діяльності організації та документування першопричин кризових ситуацій.

Третій крок: реагування на ризики та їх оптимізація.

Реагування на ризик базується на вивченні звітів про оцінки ризиків та реагування у відповідності до розроблених процедур, щоб зменшити або збільшити можливості ризику, в залежності від цілей впровадження системи управління ризиками. Метою цього кроку є визначення пріоритетності основних ризиків, встановлених на попередніх етапах впровадження і пошуку шляхів для усунення цих ризиків. Неспроможність організації

виконати плани попередження ризиків та інтегрувати методи управління ризиками в IT інфраструктуру знижує цінність самої системи управління ризиками і наражає організацію на нові непередбачені загрози.

Четвертий крок: Моніторинг, покращення.

Щоб отримати високу ефективність системи управління ризиками, треба постійно аналізувати та мати зворотній зв'язок щодо дій з управління ризиками [30]. Результати аналізу середовища можуть допомогти прийняти ті або інші рішення щодо управління внутрішніми та зовнішніми загрозами, а також розробити альтернативні підходи корпоративного управління. Інформація, отримана від циклів зворотного зв'язку та виконаних антикризових дій, може допомогти скорегувати поточні процеси управління ризиками,а також визначити майбутні бізнес-цілі.

Якщо організація не буде аналізувати результати діяльності з управління ризиками, вона може створити хибні прогнози для найгірших сценаріїв ризику. У свою чергу це призведе до неточного аналізу ймовірності та серйозності ризику. Інформування повинно бути цілісним процесом системи управління ризиками, який торкається всіх зацікавлених сторін в межах цього етапу впровадження. Інформування повинно торкатися найвищого керівництва, але більш за все воно націлене на співробітників найближчих до технологій та бізнес-процесів [30]. Головна мета полягає в тому, щоб усвідомити конкретні ризики, пов'язані процесами конкретних відповідальних осіб, щоб вони працювали таким чином, щоб мінімізувати загрози та оптимізувати ризик.

Висновки до розділу 1

В цьому розділі було проаналізовано джерела літератури, які допомогли визначити, що впровадження новітніх інформаційних технологій допомагає підприємствам розвиватись та додає їм можливостей у конкурентній боротьбі, проте ускладнює надійність захисту IT інфраструктури. Постійна модернізація IT інфраструктури вимагає переглядати підходи до подолання виникаючих загроз, вивчати їх та розробляти новітні та сучасні алгоритми

протидії. У свою чергу, кіберзлочинці також використовують новітні технології та удосконалюються, і тим самим протидіють розробленим системам кіберзахисту. Тому у новій редакції стандарту ISO 31000 приділяється більше уваги постійному вдосконаленню та зворотному зв'язку з зацікавленими сторонами.

Стандарт ISO 31000:2018 приділяє більше уваги лідерству, що в свою чергу допоможе забезпечити інтеграцію управління ризиками в усі організаційні заходи, починаючи з управління організацією. Враховуючи основні підходи стандарту ISO 31000:2018, менеджери отримують багато різноманітних інструментів, які допомагають досягти цілей. Саме це робить доцільним компіляцію процесу управління ризиками та формування системи інформаційної безпеки для сучасних організацій.

Відрізняючись від стандарту ISO 31000:2018, ДСТУ ISO 27001:2023 – це стандарт, який встановлює саме вимоги до системи управління інформаційною безпекою, структуруючи підхід до захисту інформаційних активів організації. До основних цілей стандарту ДСТУ ISO 27001:2023 входить забезпечення конфіденційності, цілісності та доступності інформації, зниження ризиків ІБ, підвищення довіри до організації з боку зацікавлених сторін. Стандарт ґрунтується на циклі PDCA, який забезпечує постійний контроль та покращення системи управління ІБ. Отже, сертифікація за цим стандартом може допомогти організаціям підвищити свою інформаційну безпеку та зменшити ризик виникнення інцидентів.

РОЗДІЛ ІІ

АНАЛІЗ ДІЯЛЬНОСТІ ПП «ІТ МАСТЕР СЕРВІС»

2.1 Особливості діяльності ПП «ІТ МАСТЕР СЕРВІС»

Одним з елементів управління торгівельною організацією є управління комерційною діяльністю. Комерційну діяльність слід розглядати як сукупність процесів, пов'язаних з купівлею і реалізацією товарів, вивченням та задоволенням попиту клієнтів, розширенням ринку збуту товарів, зменшенням витрат та отриманням прибутку. У комерційній діяльності приватного підприємства «ІТ МАСТЕР СЕРВІС» даним напрямком займається керівний склад підприємства. Деякі процеси, такі як розширення ринку збуту, частково розподіляються і на менеджерів (Рис. 2.1).

Рис. 2.1 Організаційна структура приватного підприємства «ІТ МАСТЕР СЕРВІС»

Закупівля товарів здійснюється паралельно з вивченням ринку та потреб клієнтів. У цьому процесі відбувається налагоджування нових та підтримка існуючих господарських відносин з постачальниками, відбувається здійснення комерційних операцій. Ці процеси, а також безпосередньо укладання контрактів постачання, покладені на відділ закупівлі, в якому

працює два менеджери, які займаються закупівлею товарів та послуг. Кожен менеджер має свій напрямок діяльності та особисті групи постачальників.

Комерційна діяльність – особливий вид діяльності, пов'язаний із реалізацією товарів та послуг. У діяльності приватного підприємства «ІТ МАСТЕР СЕРВІС» реалізація товарів та послуг здійснюється підрозділом збуту. Цей підрозділ поділяється на два відділи: відділ гуртової та роздрібної торгівлі. Гуртовий відділ веде господарську діяльність з організаціями та підприємствами, які мають потреби в оновленні або розширенні власної ІТ інфраструктури. Відділ роздрібної торгівлі спрямовано на роботу з покупцями в магазині та прийняттям і обробкою інтернет замовлень через інтернет-магазин. Також інтернет-магазин має спеціальні форми від банків-партнерів, які надають можливість оформлення онлайн кредитування покупок. Ці форми можуть використовуватись кіберзлочинцями для отримання несанкціонованого доступу до ІТ інфраструктури підприємства.

В процесі оцінки ризиків ПП «ІТ МАСТЕР СЕРВІС» саме інтернет-магазин був ідентифікований як одне з вразливих місць організації, оскільки має відкриту інтернет адресу та водночас синхронізує дані з базою даних підприємства.

Однією з особливостей в діяльності приватного підприємства «ІТ МАСТЕР СЕРВІС» є його сервісний центр. Сервісний центр виконує гарантійне та післягарантійне обслуговування техніки клієнтів, здійснення повернень товарів постачальникам, заміну товарів кінцевому споживачеві. Особливістю роботи сервісного центру є те, що база даних підприємства синхронізується з деякими базами постачальників за допомогою зовнішніх каналів зв'язку, що, в свою чергу, може бути точкою втручання кіберзлочинців в нормальну діяльність організації.

Документообіг організації покладено на бухгалтерів. Підприємство має в штаті двох бухгалтерів, один з яких працює віддалено. Обидва бухгалтери використовують мережу Інтернет та зовнішні каналі зв'язку для обміну інформацією з постачальниками, клієнтами та контролюючими органами.

Канали обміну бухгалтерською інформацією також можуть розглядатися як потенційна вразливість, яка може використовуватись для несанкціонованого доступу до внутрішньої мережі підприємства.

Отже, розглядаючи особливості діяльності приватного підприємства «ІТ МАСТЕР СЕРВІС» можна виділити те, що використання підрозділами організації зовнішніх каналів зв'язку, мережі Інтернет або підключення клієнтських пристроїв для діагностування сервісним центром, можуть нести загрозу ІТ інфраструктурі підприємства. Також потенційною точкою несанкціонованого доступу можуть бути файли або посилання, отримані кожним співробітником організації через електронну пошту.

2.2 Аналіз економічної діяльності підприємства

Базою дослідження були опрацьована звітність щодо діяльності приватного підприємства «ІТ МАСТЕР СЕРВІС», а саме: бухгалтерська звітність і фінансовий аналіз за 2020 р. [32].

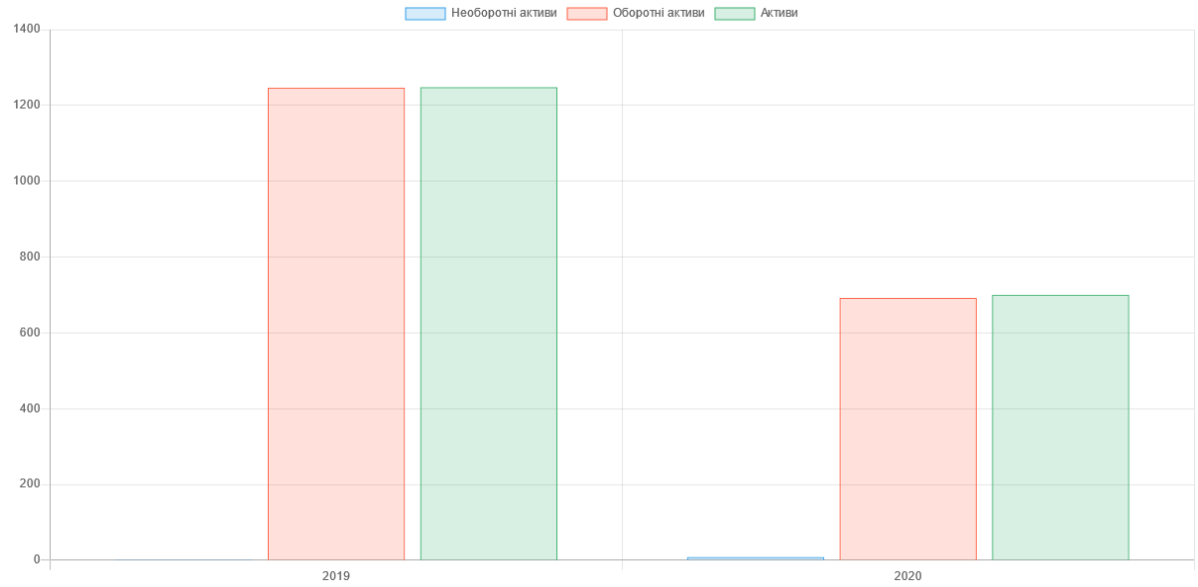

Рис. 2.2 Динаміка активів «ПП «ІТ МАСТЕР СЕРВІС» у 2019-2020 рр., тис. грн.

На рисунку 2.2 можна побачити зменшення суми активів приблизно на 45 %, що вказує на послаблення господарського потенціалу. Це означає, що у підприємства скорочується обсяг наявного у розпорядженні майна. Проте, зростання доходу від продажу товарів і послуг в той час, коли активи

знижуються, вказує на зростання ефективності управління при обмежених ресурсах.

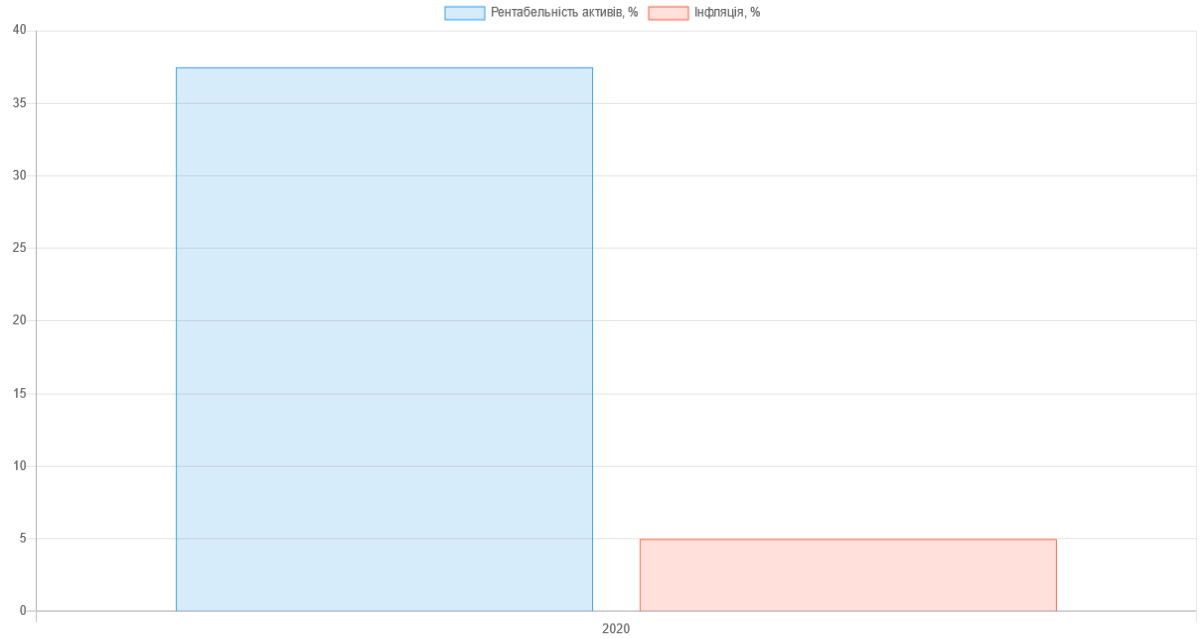

Рис 2.3 Співставлення рентабельності активів «ПП «ІТ МАСТЕР СЕРВІС» з інфляцією в Україні у 2020 р., %

Рисунок 2.3 вказує на те, що рентабельність активів підприємства у 2020 р. суттєво перевищувала інфляцію, а це говорить про реальне зростання вартості активів підприємства, не зважаючи на їх скорочення.

Таблиця 2.1

Звіт про фінансові результати ПП «ІТ МАСТЕР СЕРВІС»

Назва показника	Код	2020	2019
Чистий дохід від реалізації продукції (товарів, робіт, послуг)	2000	11244,2	10242,4
Інші доходи	2160	16,2	22,6
Разом доходи	2280	11260,4	10265
Собівартість реалізованої продукції (товарів, робіт, послуг)	2050	10290,3	9077,3
Інші витрати	2165	524,9	499
Разом витрати	2285	10815,2	9576,3
Фінансовий результат до оподаткування	2290	445,2	688,7
Податок на прибуток	2300	80,1	124
Чистий прибуток (збиток)	2350	365,1	564,7

Проаналізувавши Звіт про фінансові результати, зведений у Таблиці 2.1 можна побачити наступне: чистий дохід приватного підприємства

«ІТ МАСТЕР СЕРВІС» за основним напрямком діяльності зріс, незважаючи на падіння вторинних доходів, зросла собівартість продукції, але разом з тим зросли і витрати, у зв'язку з чим спостерігається зменшення чистого прибутку у порівняльний період.

Підсумовуючи аналіз економічної діяльності можна сказати, що за проаналізований період економічний стан приватного підприємства «ІТ МАСТЕР СЕРВІС» погіршився, про що свідчить зменшення кількісті активів та зменшення чистого прибутку. Також можна побачити зростання якості управління, про що свідчить суттєве перевищення вартості наявних активів підприємства щодо інфляції. Також на ефективність управління вказує зростання доходу від продажу товарів і послуг при суттєвому скороченні вартості активів підприємства.

2.3 SWOT аналіз поточного стану підприємства

Для того, щоб зробити компанію успішною, прибутковою та конкурентоспроможною, треба, щоб керівництво вміло приймати об'єктивні та добре виважені рішення. Необхідно чітко розуміти, які позиції компанія займає на ринку, які можливі перспективи та які можуть виникнути проблеми. Одним з найкращих інструментів для розуміння позицій, перспектив та проблем є SWOT-аналіз. Найважливіше завдання SWOT-аналізу – допомогти організації побачити та оцінити всі чинники, що впливають на прийняття рішень, а також визначити можливості розвитку. Цей метод протягом багатьох років залишається одним з найефективніших інструментів стратегічного планування.

Перші букви елементів аналізу складають саму назву SWOT і розшифровується наступним чином:

- Strengths (сильні сторони);
- Weaknesses (слабкі сторони);
- Opportunities (можливості);
- Threats (загрози).

Метод використовує чотири елементи, які можна об’єднати до двох груп – це внутрішні чинники: сильні та слабкі сторони; та зовнішні чинники: можливості та загрози.

Внутрішні чинники, сильні (S) та слабкі сторони бізнесу (W), визначаються ресурсами, якими володіє організація, а також процесами, на які організація має безпосередній вплив. Це може бути:

– фізичні ресурси: обладнання, нерухомість;

– фінансові ресурси: джерела фінансування, інвестиції, дохід компанії;

– людські ресурси: співробітники, клієнти;

– розробки, патентна документація;

– внутрішні процеси: програми лояльності для клієнтів та співробітників, виробництво.

Зовнішніми чинниками, це можливості (O) та загрози (T), можуть бути:

– ринкові тенденції: поява нових продуктів чи технологій, зміни потреб клієнтів;

– господарські відносини з контрагентами;

– економічні тенденції: конкуренція, зміна попиту, купівельна спроможність споживачів;

– зовнішнє фінансування;

– законодавчі обмеження, взаємодія з органами влади.

Правильно проведений SWOT-аналіз дасть змогу зрозуміти, чи всі ресурси компанії задіяні та використовуються раціонально, які сильні сторони можуть стати конкурентними перевагами, які поточні загрози є критичними та які загрозі є у майбутньому та як уникнути цих загроз.

Для вивчення загроз ПП «ІТ МАСТЕР СЕРВІС» нами було проведено SWOT-аналіз підприємства (табл 2.2):

Проаналізувавши діяльність приватного підприємства «ІТ МАСТЕР СЕРВІС» ми дійшли висновку, що підприємство має конкурентні переваги, маючи торгівельні точки та кваліфікованих співробітників. Маючи власний

сайт та розширюючи географію продажів, організація має можливості розширення своїх переваг серед конкурентів. Розглядаючи слабкі сторони, а саме залежність від сторонніх організацій, таких як постачальники та логістичні компанії, ми можемо бачити перешкоди для розширення господарської діяльності.

Таблиця 2.2

SWOT-аналіз ПП «ІТ МАСТЕР СЕРВІС»

Сильні сторони (S)	**Слабкі сторони (W)**
Наявність торгівельних площ Наявність Інтернет магазину Сертифіковані співробітники Велика клієнтська база Участь у державних закупівлях Орієнтованість на споживача Налагоджена мережа збуту Наявність сервісного центру та виробництва	Залежність від постачальників Залежність від логістичних компаній Залежність цін від курсу валют Відсутність реклами в ЗМІ Мало залучених оборотних коштів Високі оперативні витрати
Можливості (O)	**Загрози (T)**
Анонс новинок на власному сайті Розширення асортименту Продаж товарів по всій країні Заснування власної торгової марки	Велика конкуренція Зниження попиту на продукцію Загрози втручання в ІТ інфраструктуру Залежність від наявності ресурсів (електропостачання) Залежність від якості каналів зв’язку Цілодобове використання серверного та мережевого обладнання Зниження платоспроможності клієнтів

Розглядаючи загрози, підкреслені в SWOT-аналізі, окремо можна звернути увагу на загрози в ІТ секторі діяльності підприємства. Ці види загроз є не індивідуальні, вони притаманні більшості організацій, оскільки майже кожна організація використовує комп’ютерне, мережеве обладнання та безпосередньо мережу Інтернет. Тому цим видам загроз треба постійно

приділяти увагу, аналізувати й удосконалювати методи та підходи для запобігання протидії та їм.

2.4 Підходи до ідентифікації та оцінки ймовірності настання кризових ситуацій на ПП «ІТ МАСТЕР СЕРВІС»

Підхід до аналізу ризиків повинен бути комплексним, тому розробка, підтримка та удосконалення системи управління ризиками є дуже важливим процесом у ризик-менеджменті. Існує дуже багато класифікацій ризиків [34], і узагальнивши деякі з них, можна сформувати наступні (таблиця 2.3):

Таблиця 2.3

Класифікація ризиків

Класифікація ризиків	**Види ризиків**
За циклічністю	Систематичні – ризики, пов'язані із коливаннями цін на ресурси і а також інфляційні, податкові
	Несистематичні – ризики, які впливають на конкретний процес
За терміном настання	Ретроспективні
	Поточні
	Перспективні
За рівнем дії	Невпливові
	Помірні
	Дуже впливові
Залежно від джерела дії	Зовнішні – екологічний вплив, втручання сторонніх осіб, соціально-економічний влив
	Внутрішні – виробничі ризики, кадрові, управлінські

Отже, розглянемо зовнішні та внутрішні ризики для ІТ інфраструктури приватного підприємства «ІТ МАСТЕР СЕРВІС» (таблиця 2.4).

Вивчаючи свій минулий досвід успіхів та невдач, організація може багато чому навчитися. Аналіз завжди дає інформацію щодо ефективності

попередньо впроваджених заходів, якісних характеристик процесів, питань щодо контролю якості процесів, тощо

Таблиця 2.4

Складові інформаційних ризиків

Небажана подія	**Причина (фактор впливу)**	**Ризик за рівнем дії**
Отримання недостовірної інформації	• Неуважність персоналу • Відсутність синхронізації даних • Зовнішнє втручання	Помірний
Оприлюднення комерційної інформації	• Людський фактор (саботаж) • Відсутність розмежування між публічною та комерційною інформацією. • Відсутність порядку зберігання та утилізації інформації	Дуже впливовий
Втрата інформації	• Відсутність енергопостачання • Фізична втрата інформації • Втрата інформації на програмному рівні. • Помилкові дії співробітників	Дуже впливовий
Втручання в канали зв'язку	• Технічний збій • Людський фактор	Помірний
Відмова обладнання	• Технічний збій • Людський фактор • Зовнішнє втручання	Дуже впливовий
Відсутність електропостачання	• Людський фактор • Зовнішнє втручання	Невпливові
Фізичне втручання в роботу обладнання	• Людський фактор (саботаж) • Некоректні дії персоналу	Дуже впливовий
Помилка в роботі сервісів (бухгалтерських, хостінгу)	• Технічні роботи у постачальника послуг • Збій в роботі обладнання	Помірний

Грамотна та послідовна організація, а також систематичний підхід до аналізу свого досвіду з успіхів і невдач, можуть принести велику користь підприємству в оцінюванні ризиків. Такий підхід можна назвати аналізом причин. Його принципи полягають у наступному:

– організація однаково вивчає свої успіхи та невдачі;

– спочатку чітко визначаємо проблему, потім шукаємо її рішення;

– важливо зрозуміти причини, а тільки після розуміння робити аналіз подій впливу;

– розроблені заходи повинні вести до покращення процесів на підприємстві.

Аналіз причин є дуже вагомим інструментом в управлінні ризиками. Оцінюючи ризики, організація робить своєрідний погляд у майбутнє, де намагається передбачити події та спланувати свої дії. Проте, аналіз причин полягає у використанні ретроспективних даних та вивчення досвіду минулих подій. Організація багато чому може навчитися зі свого минулого позитивного чи негативного досвіду для того щоб покращити якість і ефективність своїх процесів і систем.

Аналіз причин у процесі управління ризиками є своєрідним етапом моніторингу та перевірки. На етапі аналізу причин організація може підтримувати в актуальному стані реєстр ризиків, засоби їх контролю та оновлювати плани вирішення кризових ситуацій. Метод аналізу причин дозволяє нам визначити не лише прямі причини виникнення кризової ситуації, але й приховані, фіксувати досягнені результати та вести реєстр усіх подій.

Одним із підходів проведення аналізу причин може бути побудова діаграми Ісікави або «риб'ячого скелету». Завдяки цьому підходу організація може віднести кілька можливих причин до однієї події. Це може допомогти класифікувати декілька потенційних небажаних подій і визначити основні причини їх виникнення. Таким чином, для небажаної події можна створити діаграму, щоб визначити та упорядкувати можливі причини її виникнення.

Отже, розглянувши як приклад ризик втрати інформації в організації, нами була побудована діаграма Ісікави, (рис 2.4) на якій графічно зображені причини виникнення кризової ситуації, а саме втрати інформації, а також фактори, які можуть ці причини викликати.

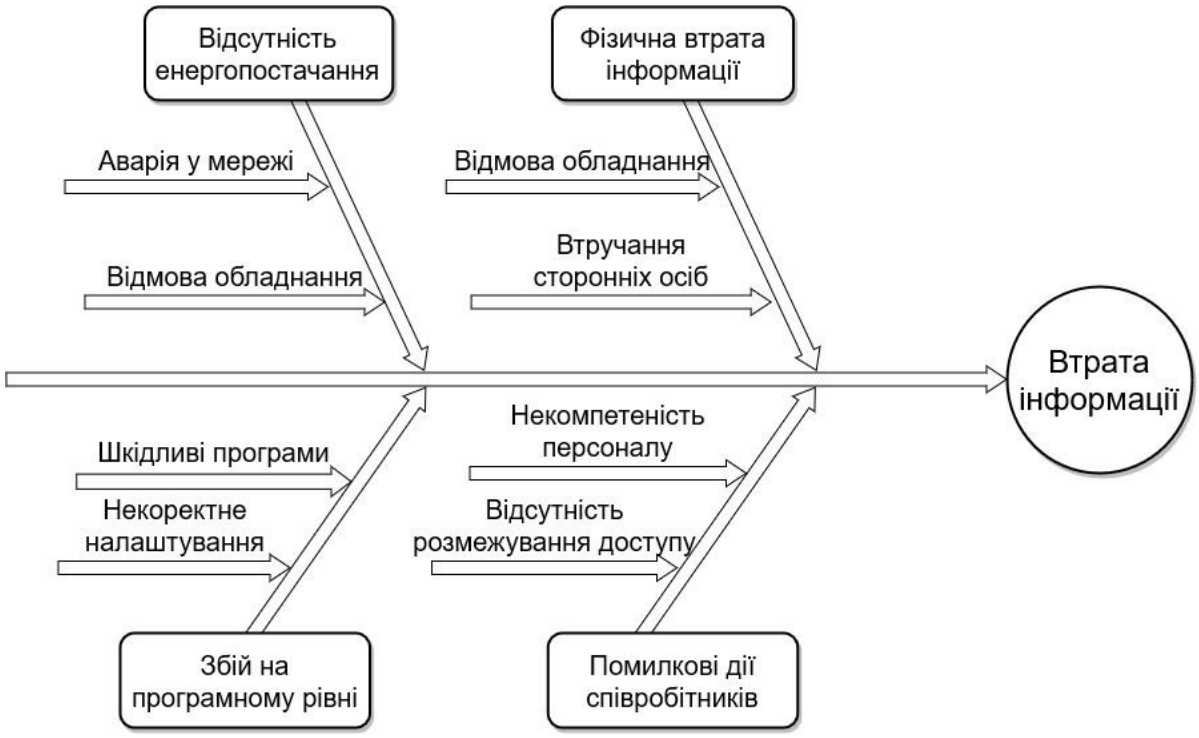

Рис. 2.4 Діаграма Ісікави. Втрата Інформації

Проаналізувавши за допомогою діаграми кожну причину та фактор, який може викликати її, можна розробити план дій, який допоможе звести небажані наслідки до мінімуму або зовсім уникнути небажаної кризової ситуації.

2.4.1 Причини виникнення інформаційних ризиків діяльності

Проаналізувавши складові інформаційних ризиків можна виділити дві основні групи причин їх виникнення: внутрішні та зовнішні. Кожна з цих груп складається з набору конкретних причин, які ми розглянемо.

Внутрішні причини. Ця група пов'язана з недоліками в системі управління організації та технічному забезпеченні інформаційної інфраструктури. До них можна віднести:

– відсутність розмежування між публічною та комерційною інформацією, а також відсутність порядку зберігання та утилізації інформації, що використовується підприємством. Виникнення цієї причини пов’язане з нечіткими процедурами управління конфіденційною інформацією, недостатньою увагою до інформаційної безпеки в стратегії організації. Це може призводити до збоїв в роботі систем, втрати інформації,

несанкціонованого доступу до інформації як співробітників, так і сторонніх осіб.

– неуважність персоналу, людський фактор (саботаж), а також помилкові дії співробітників. Ця причина свідчить про недостатній рівень кваліфікації працівників, які мають доступ до інформації або до обладнання. Також ця причина може вказувати на неналежне розмежування як фізичного доступу до конкретного обладнання або інфраструктури в цілому, так і програмного доступу до налаштування обладнання або центрів зберігання даних. Це може призводити до помилок в обробці інформації, втраті інформації, а також несанкціонованого доступу до інформації.

– збій в роботі обладнання, втрата інформації на програмному та фізичному рівні – призвести до цього можуть деякі фактори. У разі недотримання правил експлуатації комп'ютерного та мережевого обладнання можуть відбутися відмови та поломки обладнання, які, в свою чергу, призведуть до фізичної втрати інформації. Використання неліцензійного програмного забезпечення або програмного забезпечення з неподовженою ліцензією може призвести до зупинки роботи програм або їх компонентів і, як наслідок цього, може бути втрата інформації на програмному рівні.

Зовнішні причини. Ця група пов'язана з впливом зовнішніх факторів, які можуть завдати шкоди інформаційній безпеці організації та її активам. До них можна віднести:

– збій в роботі зовнішнього обладнання, відсутність енергопостачання. Загалом, це будь-які технологічні фактори, які не залежать від самої організації, але можуть вплинути на її діяльність або на інформаційну безпеку. Конкретні наслідки залежать від самого обладнання, яке використовується організацією. Якщо організація використовує обладнання для зберігання даних, то збій в енергопостачанні може призвести до втрати або знищення інформації. Якщо організація використовує обладнання для обробки інформації, то відсутність енергопостачання може призвести до несанкціонованого доступу до інформації сторонніми особами.

– зовнішнє втручання – це будь-які дії або їх відсутність, спрямовані на порушення інформаційної безпеки організації, які здійснюються ззовні. Метою таких дій може бути злочинна діяльність, яка здійснюється задля заволодіння або знищення інформації. Також, такий вид втручання може мати цілі щодо заволодіння можливостями обладнання організації, щоб створити більш потужну хакерську атаку на третю організацію. У будь-якому випадку, зовнішнє втручання призведе до часткової або повної втрати інформації та (або) її розповсюдження.

– відсутність синхронізації даних або послуг сторонніх сервісів можуть бути викликані декількома факторами. Це можуть бути технічні роботи у постачальників інформаційних послуг, аварії на каналах зв'язку, наслідки погодних умов. Також це можуть бути регламентні роботи, про які відомо заздалегідь. У будь-якому випадку, ці загрози мають помірний вплив на інформаційну безпеку організації. Пов'язано це з тим, що немає порушень у нормальній роботі обладнання організації, що розглядається. Тому до пошкодження обладнання або повної втрати даних такі загрози не призведуть, але можуть викликати затримку у нормальній діяльності організації.

Розглядаючи діяльність організації можна побачити, що основними причинами виникнення інформаційних ризиків є людський фактор. Людський фактор криється у діяльності або бездіяльності співробітників, цілеспрямованих дій сторонніх осіб. Не менш впливовим може бути і поломки або відмова обладнання, викликані його некоректною експлуатацією як всередині організації, так і ззовні. Відсутність сервісів, таких як зв'язок, інтернет послуги, енергозабезпечення, хостинг від провайдерів та сервісів бухгалтерських послуг, мають помірний вплив на діяльність організації. Але об'єднує всі ці загрозі одне – все це причини, наслідками яких може бути втрата конфіденційної інформації або її розголошення.

2.4.2 Наслідки впливу інформаційних ризиків на бізнес-процеси ПП «ІТ МАСТЕР СЕРВІС»

Розглядаючи діяльність приватного підприємства «ІТ МАСТЕР СЕРВІС», можна виділити декілька основних процесів:

- організація діяльності керівним складом;
- закупівля товарів та послуг;
- збут продукції корпоративним клієнтам;
- продаж товарів та послуг роздрібним клієнтам;
- організація роботи сервісного центру;
- виробництво;
- документообіг.

Деякі з цих процесів можуть складатися з більш простих субпроцесів, наприклад: продаж роздрібним клієнтам складається з продажів в торгівельному залі та продажів в інтернет магазині.

Розглянемо вплив інформаційних ризиків на основні процеси, оскільки вплив на них так само спричиняє небажану дію і на субпроцеси.

Отримання недостовірної інформації. Ця небажана подія може оказати найбільший вплив на управлінські процеси та процеси збуту. Недостовірна інформація може призвести до прийняття організацією невірних рішень у маркетингу, виробництві, фінансах, що в свою чергу призведе до фінансових втрат та погіршенні репутації. Іншими наслідками може бути те, що співробітники будуть працювати неефективно. Отримавши недостовірну інформацію про потреби клієнтів, вони можуть прийняти невдалі рішення щодо закупівлі товарів та послуг та їх продажів. Ще одним небажаним наслідком для організації при отриманні недостовірної інформації може бути порушення закону, наприклад при участі у державних тендерах.

Оприлюднення комерційної інформації. У даному випадку розглянемо як негативні, так і позитивні сторони цієї небажаної події. Негативними наслідками буде зниження конкурентних переваг організації, а

також велика вірогідність збільшення ризику шахрайства та маніпуляцій. Оприлюднення комерційної інформації ПП «ІТ МАСТЕР СЕРВІС» також може мати негативний вплив на відносини з клієнтами та співробітниками, оскільки більшість Договорів між організаціями мають угоду про не розголошення інформації щодо цих Договорів.

Позитивним наслідком розголошення комерційної інформації може бути підвищення конкуренції, внаслідок чого ймовірна можливість зниження цін та підвищення якості товарів та послуг.

Втрата інформації може призвести до порушення бізнес-процесів приватного підприємства «ІТ МАСТЕР СЕРВІС», оскільки кожен співробітник не зможе отримати доступ до робочої інформації. В першу чергу буде порушена нормальна робота підрозділів збуту та закупівлі, а також бухгалтерська діяльність.

Іншими наслідками втрати інформації може бути зниження конкурентоспроможності та погіршення репутації приватного підприємства «ІТ МАСТЕР СЕРВІС», оскільки підприємство не зможе виконувати свої зобов'язання перед клієнтами та постачальниками. Невиконання зобов'язань може накласти фінансові обмеження та викликати втрату активів підприємства.

Втручання в канали зв'язку та відсутність електропостачання. Ці події мають вплив на всі процеси підприємства, але їх наслідки не завжди можуть мати великий вплив на нормальну роботу процесів. Оскільки більшість процесів діяльності ПП «ІТ МАСТЕР СЕРВІС» внутрішні, то втручання в роботу каналів зв'язку може частково перервати комунікацію з клієнтами та постачальниками. Так само і енергопостачання, відсутність якого не буває надто довгою. Вплинути на репутацію підприємства та призвести до значних фінансових втрат ці небажані події не зможуть.

Відмова обладнання або фізичне втручання в роботу обладнання являє собою дуже впливовий ризик щодо нормальної діяльності ПП «ІТ МАСТЕР СЕРВІС». Наслідки дії такої небажаної ситуації можуть

стосуватись усіх бізнес процесів підприємства, як внутрішніх так і зовнішніх. Відмова роботи обладнання призведе, по-перше до повної або часткової втрати даних, неможливості вести підприємством подальшу господарську діяльність та виконувати зобов'язання перед контрагентами. По-друге, ця подія потягне за собою фінансові втрати підприємства, які будуть складатися з неотриманого прибутку, витрат на відновлення обладнання, витрат на відновлення програмного забезпечення, виплат пені за прострочені терміни поставки та погашення заборгованостей перед постачальниками. Отже відмова обладнання – це дуже впливова кризова ситуація, наслідки якої об'єднують фінансові та репутаційні втрати підприємства.

Помилки в роботі сервісів (бухгалтерських, хостінгу) мають не дуже великий вплив на нормальну діяльність підприємства. Обумовлено це тим, що ці сервіси надаються сторонніми організаціями, які в свою чергу зацікавлені в безперебійності роботи власних послуг. Але ці небажані події також можуть призвести до фінансових втрат підприємства. При помилках роботі в бухгалтерських сервісах можливі затримки в подачі звітів та первинної документації, що в свою чергу може стати причиною накладання штрафів. Збій в роботі хостингу впливатиме на роботу інтернет магазину, за нестабільною роботою якого прослідує втрата частини потенційних замовлень.

Виділивши основні процеси діяльності приватного підприємства та проаналізувавши ризики, які можуть виникнути та впливати, можна зробити підсумок, що кожна кризова ситуація має економічний та репутаційній вплив на підприємство. Вплив може бути як короткочасним, так і довгостроковим; при цьому він супроводжується фінансовими втратами підприємства.

Висновки до розділу 2

У другому розділі описано організаційну структуру приватного підприємства «ІТ МАСТЕР СЕРВІС», робота підрозділів якого залежить від зовнішніх каналів зв'язку, мережі Інтернет. Використання зовнішніх каналів зв'язку може бути потенційною точкою втручання в нормальну діяльність

підприємства. Розглядаючи більшість загроз ІТ інфраструктурі підприємства, можна побачити, що ці загрози не є притаманними конкретному підприємству. Вони існують для багатьох організацій, оскільки майже кожна організація використовує комп'ютерне, мережеве обладнання та безпосередньо мережу Інтернет. Аналіз економічної діяльності підприємства вказує на зростання якості управління, що в свою чергу можна протиставити потенційним можливостям виникнення кризових ситуацій.

Розглядаючи діяльність приватного підприємства «ІТ МАСТЕР СЕРВІС» стає зрозумілим, що основним джерелом виникнення кризової ситуації може бути людський фактор. Він криється у діяльності або бездіяльності співробітників, цілеспрямованих дій сторонніх осіб. Другою за впливовістю є загроза поломки або відмова обладнання як всередині організації, так і ззовні. Обидві ці загрози можуть призвести до критичної ситуації, а саме – втрати або розголошенню комерційної інформації. Щоб звести до мінімуму розвиток таких загроз, треба постійно приділяти їм увагу, аналізувати та удосконалювати методи для запобігання їх виникненню. Після проведення аналізу причин виникнення кризових ситуацій, підприємство може розробити план дій, який допоможе звести небажані наслідки до мінімуму або зовсім їх уникнути.

РОЗДІЛ ІІІ

ПРАКТИЧНІ АСПЕКТИ ФОРМУВАННЯ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ В ПП «ІТ МАСТЕР СЕРВІС»

3.1 Формування процедури ризик-орієнтованого підходу в інформаційну діяльність підприємства

Оскільки на приватному підприємстві «ІТ МАСТЕР СЕРВІС» немає впровадженої системи ризик-орієнтованого підходу, ми можемо скористатись рекомендаціями стандарту ISO 31000:2018, в якому більше звертається увага на роль лідерів та їх відповідальності. Як було сказано раніше, цей стандарт не пристосований до сертифікації, він надає не вимоги, а рекомендації, що більше підходить нам відповідно до потреб і цілей підприємства.

Другим стандартом, на який ми спираємось при побудові системи управління кіберризиками – це ДСТУ ISO 27001:2023, який встановлює вимоги до системи управління інформаційною безпекою. У відповідності до нього ми можемо виділити п’ять елементів циклу управління кібербезпекою, які впроваджуються у нашу систему управління ризиками. Ці елементи представлені на схемі (рис. 3.1). Також наша система доповнюється вимогами цього стандарту щодо компетенції персоналу, який самостійно виконує роботу, що впливає на результативність інформаційної безпеки. Цих співробітників забезпечують навчанням, додатковими тренінгами та вивченням відповідного досвіду споріднених організацій.

Завдання та цілі ризик-орієнтованого підходу можуть і будуть змінюватись у відповідності до вдосконалення процесу управління ризиками. У відповідності до вимог 8.2 та 8.3 стандарту ДСТУ ISO 27001:2023 нами була проведена оцінка ризиків інформаційної безпеки через заплановані інтервали часу або якщо відбулись зміни в системі управління, які можуть суттєво покращити цю систему. Оптимальними термінами перегляду завдань та цілей обрано один раз на два роки. Після оцінки ризиків запланована обробка ризиків та відновлення стану безпеки підприємства.

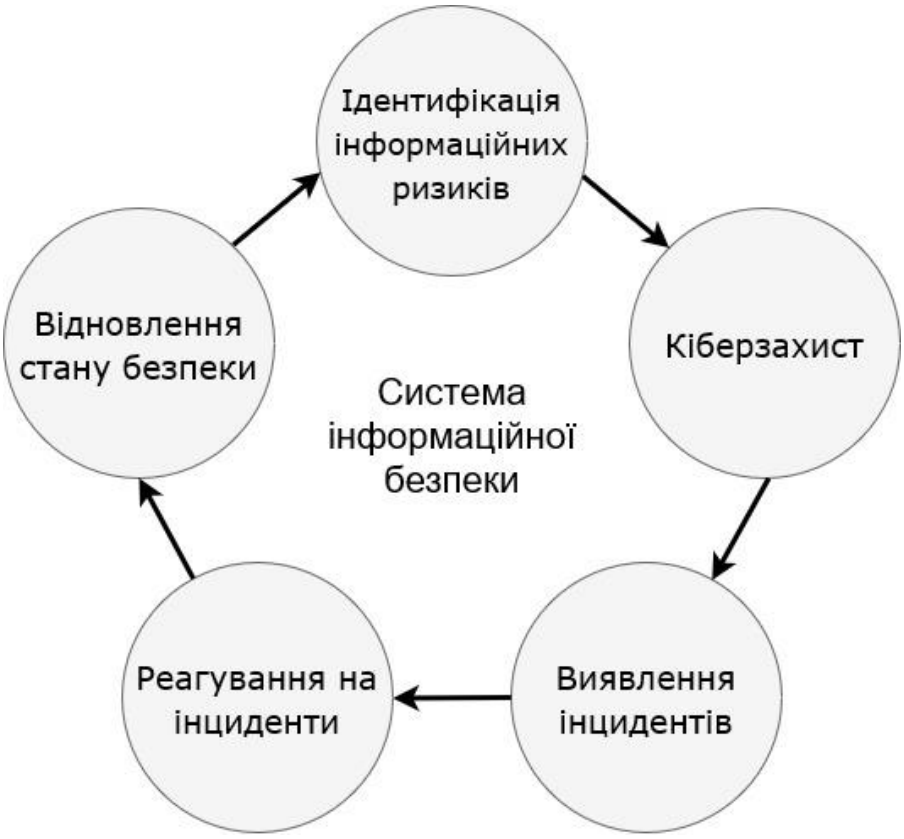

Рис. 3.1 Цикл управління кібербезпекою

Процес «Ідентифікація інформаційних ризиків» включає заходи, реалізація яких спрямована на ідентифікацію та вивчення наявних ризиків, а також способи управління ризиками для інформаційних систем та даних.

«Кіберзахист» реалізовує діяльність з розробки та впровадження методів та засобів, які допоможуть обмежити або стримати вплив небажаних ситуацій.

«Виявлення інцидентів» – своєчасне виявлення потенційних небажаних ситуацій.

«Реагування на інциденти» – процес, який реалізовує заплановані заходи реагування на небажані ситуації та кібератаки, знижуючи або унеможливлюючи потенційний негативний вплив цих ситуацій.

«Відновлення стану безпеки» – відновлення процесів, які були порушені та зменшення негативного впливу інциденту (кібератаки).

Наведена процедура інтеграції ризик-орієнтованого підходу в діяльність приватного підприємства «IT МАСТЕР СЕРВІС» дає можливість позначити конкретні кроки з впровадження даного підходу. Концепція, яка

наведена у даній процедурі, передбачає охоплення не тільки ризиків в IT-сфері підприємства, а й ризиків в усіх видах його діяльності, що окреслює ключові кроки цього підходу.

3.2 Ідентифікація та оцінка інформаційних ризиків діяльності

Першим кроком для впровадження системи ризик-орієнтованого підходу був аналіз потенційних небезпек для IT-інфраструктури та їх вплив на діяльність підприємства. Ідентифікація інформаційних ризиків – це процес виявлення потенційних загроз, які можуть призвести до порушення цілісності, конфіденційності або доступності інформації, що використовується підприємством. Процес ідентифікації інформаційних ризиків є першим кроком у процесі управління інформаційними ризиками. Він дозволяє зрозуміти підприємству, які ризики загрожують нормальній діяльності та розробити заходи для зниження впливу їх наслідків.

Одним з відомих методів ідентифікації ризиків є аналіз загроз і вразливостей. Цей метод полягає в аналізі потенційних загроз для інформаційної діяльності підприємства і вразливостей, які можуть зробити інформацію вразливою до цих загроз.

Нами була зібрана нарада, до якої входило вище керівництво та керівники підрозділів. На цій нараді, використовуючи один з популярних методів висування та обговорення ідей – «Мозковий штурм», було виділені та систематизовані основні загрози для IT діяльності приватного підприємства «IT МАСТЕР СЕРВІС». Результати діяльності представлені у вигляді діаграми Ісікави (рис 3.2).

Наступним етапом розробки процедури було ранжування загроз. Для того, щоб виділити найвпливовіші загрози інформаційній безпеці підприємства нами було проведено оцінку та оброблено результати оцінювання небезпечних факторів (табл. 3.1) співробітниками підприємства. Оцінку проводили: керівник підрозділу закупівлі, обраний на виробничій нараді керівником системи з управління ризиками; керівник сервісного центру; системний адміністратор та відповідальний за інтернет-магазин.

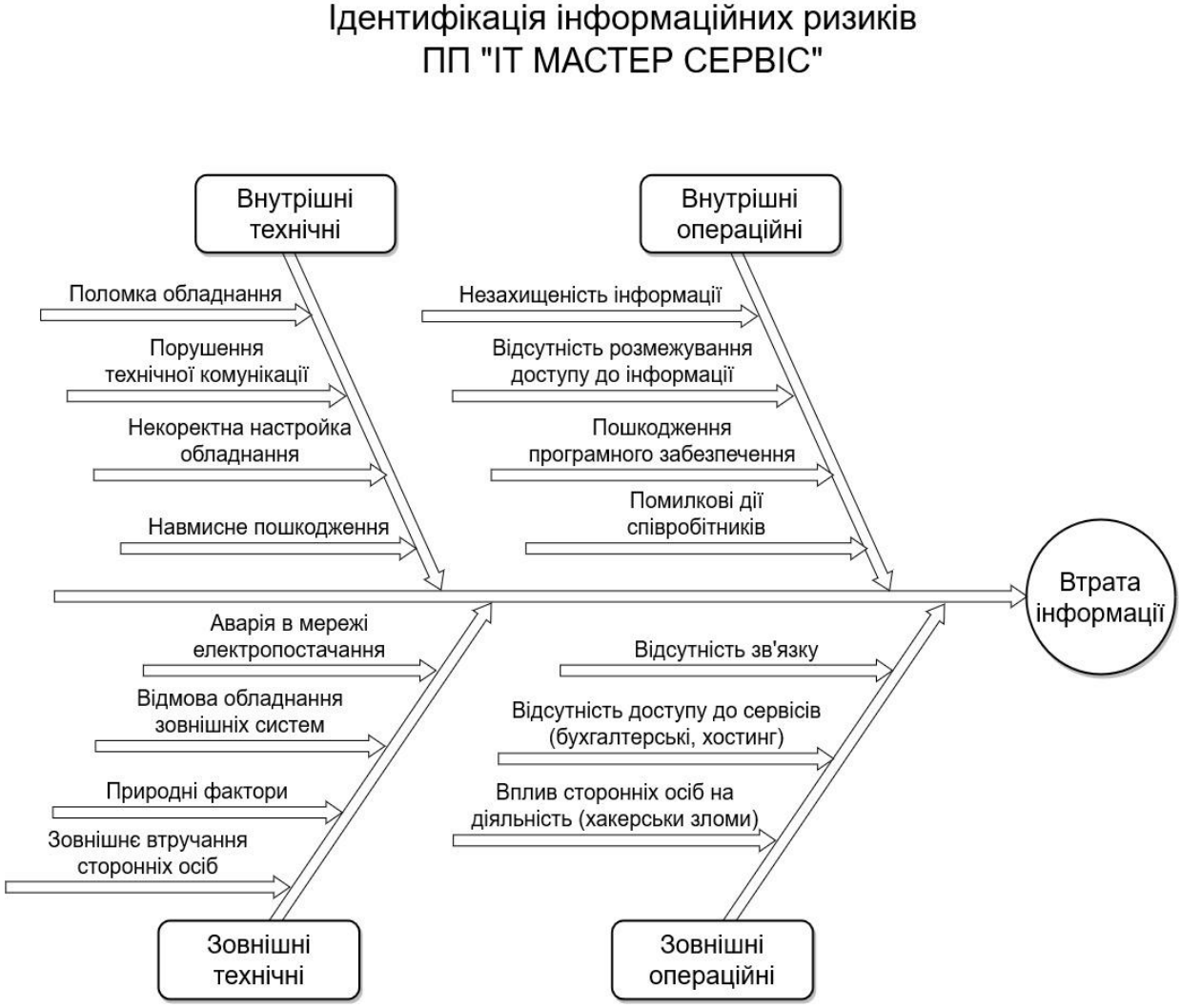

Рис. 3.2 Діаграма Ісікави. Ідентифікація інформаційних ризиків

Обраним співробітникам треба було оцінити небезпечні фактори за такими параметрами як: Тяжкість наслідків; Ймовірність виникнення; Ймовірність виявлення використовуючи десятибальну шкалу. Результати оцінки та шкали наведені у Додатку А.

Після обробки результатів нами було визначено пріоритетне число ризиків (ПЧР), яке було прийняте за основу побудови діаграми Парето (рис. 3.3), яка відображає ранжування ризиків приватного підприємства «ІТ МАСТЕР СЕРВІС» за впливом на його діяльність.

За результатами ранжування маємо визнати, що для нашого підприємства найкритичнішим ризиком є «помилкові дії співробітників», тому в першу чергу працювати ми будемо саме над зменшенням можливості його виникнення.

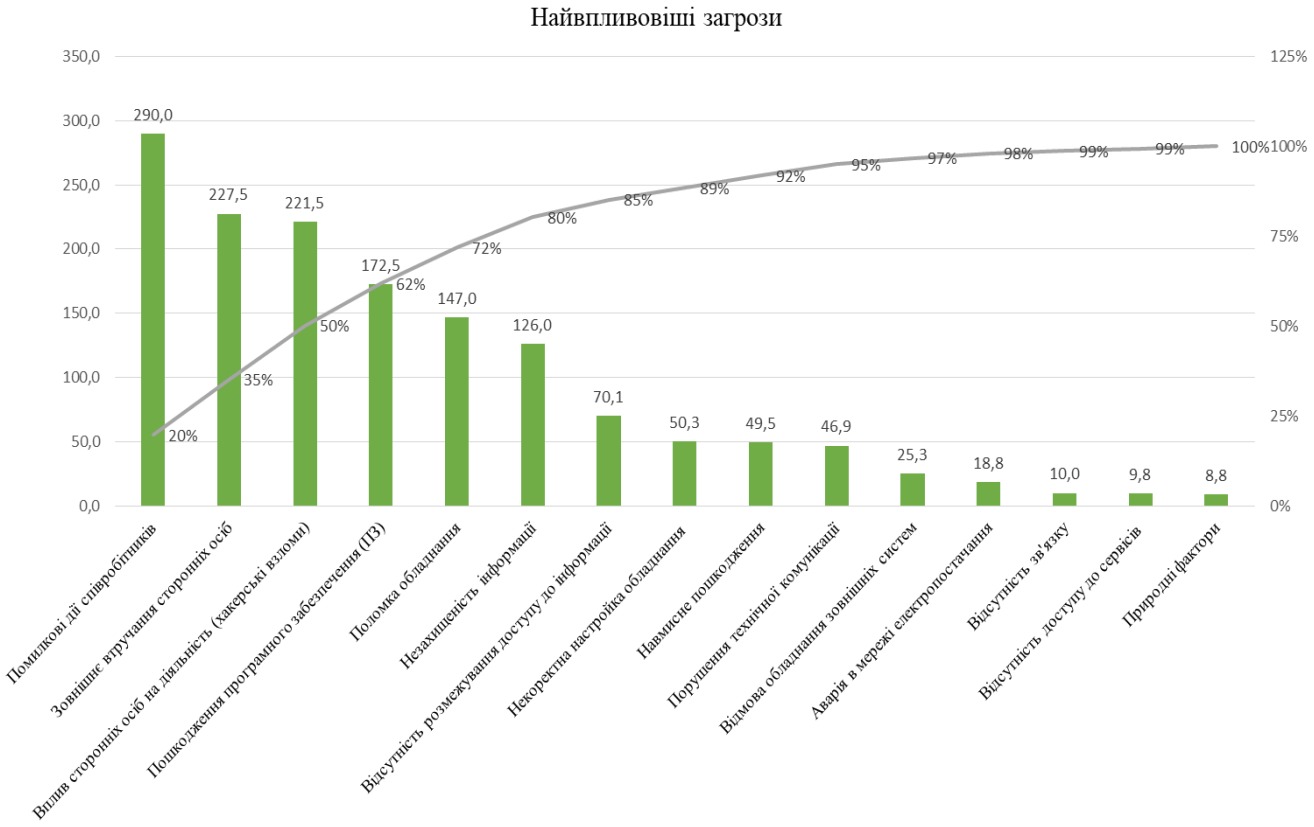

Рис. 3.3 Визначення найвпливовіших загроз

Наступним кроком було призначення особи, відповідальної за діяльність процесів системи управління ризиками – керівника з управління ризиками. В обов'язковому порядку було проінформовано усіх співробітників з даним призначенням. Керівником з управління ризиками було призначено співробітника з керівного складу підприємства з розвинутими лідерськими якостями, а саме керівника відділу постачання. Ця особа своїм прикладом повинна буде спрямовувати персонал на реалізацію основних цілей системи управління ризиками. Основні вимоги, яким повинен відповідати керівник з управління ризиками є:

– високий рівень професійної підготовки та досвіду в галузі інформаційних технологій;
– керівні та організаційні навички;
– навички критичного мислення;
– аналітичний склад розуму;
– гарні комунікаційні здібності;

Побудова матриці відповідальності, у свою чергу, допомогла розподілити відповідальність окремих співробітників щодо здійснення заходів запобігання виникненню небажаних ситуацій (табл.3.2).

Таблиця 3.2

Матриця відповідальності за напрямками впровадження кібербезпеки

	Керівник з управління ризиками	Керівник сервісного центру	Системний адміністратор	Бухгалтерія	Менеджерський склад	Відповідальний за інтернет магазин
Робота з даними на серверному обладнанні	Контр.	Відп.	Вик.			Вик.
Налаштування мережевого обладнання	Відп.	Контр.	Вик.			Вик.
Технічне обслуговування обладнання	Відп.	Вик.				
Резервування живлення	Контр.	Вик.				
Налаштування програмного забезпечення	Контр.	Відп.	Вик.			
Використання ПЗ	Контр.	Вик.	Відп.	Вик.	Вик.	Вик.
Планування та проведення аудитів	Відп.		Вик.			Вик.
Планування та проведення навчання	Відп.				Вик.	Вик.
Заходи безпеки	Контр.	Відп.	Вик.	Вик.	Вик.	Вик.
Взаємодія з сервісними операторами	Контр.	Вик.	Вик.	Вик.	Вик.	Вик.

Вик. – виконавець, Відп. – відповідальний, Контр. – контролер

Наступним кроком впровадження системи було корегування посадових інструкцій співробітників, яких було призначено відповідальними по реагуванню на небажані ситуації. Посадові інструкції передбачали використання відповідальним персоналом підприємства наявних ресурсів задля мінімізації загроз. Також було розроблено навчальний план та заходи щодо періодичної оцінки компетентності персоналу, що сприятиме виявленню прогалин у знаннях та вміннях у запобіганні небажаних ситуації.

Прикладом змін до посадової інструкції начальника підрозділу постачань (Додаток Б) можна побачити додавання наступних:

До загальних положень:

– Керівник з управління ризиками є посадовою особою організації, яка відповідає за розробку, впровадження та моніторинг системи управління ризиками в організації.

– Повинен пройти підготовку або підвищення кваліфікації в сфері управління інформацією.

– Повинен володіти знаннями щодо управління інформаційними ризиками та зміст стандартів ISO 31000 та ISO 27001

До завдань та обов'язків:

– Розробляє та впроваджує систему управління ризиками на підприємстві відповідно до рекомендації стандарту ISO 31000:2018 та ДСТУ ISO 27001:2023

– Забезпечує ефективну діяльність системи управління ризиками підприємства.

– Організовує розробку та впровадження процесів і процедур управління ризиками на підприємстві.

– Організовує розробку та впровадження методів і інструментів управління ризиками підприємства.

– Проводить аналіз ризиків підприємства.

– Визначає заходи щодо зниження ризиків підприємства та здійснює контроль за виконанням цих заходів.

– Готує звіти про стан управління ризиками на підприємстві.

До прав:

– Вносити пропозиції щодо вдосконалення системи управління інформаційними ризиками на підприємстві.

– Здійснювати контроль за діяльністю підрозділів підприємства, відповідальних за управління інформаційними ризиками.

– Використовувати ресурси підприємства для усунення причин або наслідків небажаних ситуацій.

До відповідальності:

– Несе повну відповідальність за ефективну діяльність системи управління інформаційними ризиками.

– Несе повну відповідальність за своєчасне та якісне виконання своїх посадових обов'язків.

Враховуючи дуже великий влив на кібербезпеку людського фактору, а саме ризик прийняття помилкових рішень співробітниками, нами була розроблена внутрішня інструкція щодо дій співробітників підприємства у разі виникнення, або підозри виникнення небажаної ситуації. Основними пунктами цієї інструкції є:

Виявлення. Співробітники повинні бути пильними до потенційних ознак кіберзагроз, та обов’язково повідомити керівника системи управління ризиками, або IT-адміністратора у разі виявлення чогось незвичайного, а саме:

– Незвичайні електронні листи або посилання.

– Незвичайна поведінка комп'ютера.

– Раптові зміни у продуктивності комп'ютера.

Ідентифікація. Після отримання інформації про потенційну кіберзагрозу, керівник системи управління ризиками або IT-адміністратор проведе аналіз, щоб визначити, чи є це справжньою загрозою. Вони можуть

використовувати такі інструменти, як антивірусне програмне забезпечення, різні утиліти, щоб допомогти в ідентифікації кіберзагрози.

Реагування. Якщо кіберзагроза є справжньою, IT-адміністратор повинен вжити заходів для її усунення, а саме:

– Закриття уразливості, яка була використана для здійснення кіберзагрози.

– Видалення шкідливого програмного забезпечення.

Звітування. Після усунення кіберзагрози IT-адміністратор звітує до керівника системи управління ризиками про причини виникнення та прийняті заходи запобігання цієї загрозі. Це допоможе запобігти повторенню кіберзагрози в майбутньому.

Не менш важливим заходом у запобіганню людського фактору є навчання співробітників з питань IT безпеки. Під час навчання співробітники отримують інформацію щодо потенційних загроз IT безпеки, як їх уникнути або самостійно запобігти виникненню цих загроз.

Для підвищення ефективності системи управління IT-ризиками нами було сформовано команду IT-моніторингу. До неї увійшли по одному співробітнику з кожного підрозділу підприємства, до їх обов’язків входить моніторинг антивірусних програм на комп’ютерах співробітників, перевірка оновлень систем безпеки, вибірковий аналіз вхідної пошти на скриньках, адреси яких розміщені на публічних ресурсах. Ці поштові скриньки становлять дуже високий рівень загрози IT діяльності підприємства, оскільки будь хто може надіслати на них будь яку інформацію, включаючи потенційно небезпечні файли.

Діяльність команди допоможе завчасно виявити деякі загрози, та прийняти заходи із запобігання, що зменшить можливість появи цих загроз, та підвищить раціональність використання ресурсів щодо нейтралізації наслідків потенційно небажаних ситуацій.

Подальшим кроком було визначення плану дій персоналу щодо запобігання небажаним ситуаціям. Цей план прописує заходи, які повинні

бути реалізовані персоналом під час настання небажаної події. Розроблений план заходів наведено у зведеній таблиці 3.3. Розширенням цього плану може бути зазначення кількості ресурсів, які можуть бути використані відповідальними особами для ліквідації цієї загрози у вигляді інструкцій.

Таблиця 3.3

Зведена таблиця заходів запобігання ризикам

ПП «ІТ МАСТЕР СЕРВІС»

Небажана подія	**Заходи запобігання виникненню небажаних подій**
Поломка обладнання	– Створення резервних копій даних. – Періодичний технічний огляд стану обладнання. – Навчання персоналу щодо протидії позаштатним ситуаціям.
Порушення технічної комунікації	– Перевірка внутрішніх каналів зв'язку. – Перевірка мережевого обладнання. – Перевірка відгуків серверного обладнання.
Некоректне налаштування обладнання	– Розмежування програмного доступу до обладнання. – Проведення аудитів ключових налаштувань обладнання. – Резервування ключових налаштувань в файл конфігурації. Забезпечення надійного зберігання цього файлу.
Навмисне пошкодження	– Обмеження фізичного доступу до обладнання як співробітниками, так й сторонніми особами. – Розробка політики безпеки підприємства.
Незахищеність інформації	– Розробка правил зберігання та доступу до інформації. – Розмежування доступу до інформації. – Використання алгоритмів шифрування даних.
Відсутність розмежування доступу до інформації	– Проведення аудиту безпеки.
Пошкодження програмного забезпечення (ПЗ)	– Обмеження доступу до налаштувань ПЗ. – Використання антивірусного ПЗ. – Регулярне оновлення ПЗ.
Помилкові дії співробітників	– Навчання персоналу щодо протидії позаштатним ситуаціям. – Проведення аудиту безпеки. – Розмежування доступу дообладнання та інформації.

Продовження табл. 3.3

Аварія в мережі електропостачання	– Забезпечення короткочасного резервування живлення шляхом використання ДБЖ. – Забезпечення довготривалого резервування живлення за допомогою бензинового генератора.
Відмова обладнання зовнішніх систем	– Негайне інформування відповідних служб, які використовують дане обладнання.
Природні фактори	– Організація фізичного захисту обладнання. – Навчання персоналу щодо протидії позаштатним ситуаціям. – Використання хмарних сховищ для резервного зберігання даних.
Зовнішнє втручання сторонніх осіб	– Розробка заходів фізичного захисту зовнішніх мереж та обладнання.
Відсутність зв'язку	– Негайне інформування операторів зв’язку. – Використання резервних каналів. – Перенаправлення потоків даних.
Відсутність доступу до сервісів (бухгалтерські, хостинг)	– Негайне інформування операторів сервісу.
Вплив сторонніх осіб на діяльність (хакерські злами)	– Використання антивірусного ПЗ. – Застосування заходів безпеки, таких як аутентифікація, авторизація та облік доступу.

Для спрощення подальшої роботи з ризиками, заходи запобігання були об’єднані в групи за напрямками (табл 3.4). Систематизація та об’єднання небажаних подій та заходів, спрямованих на запобігання цим подіям, допомогло побудувати матрицю відповідальності.

Отже, для ідентифікації та оцінки інформаційних ризиків приватного підприємства «IT МАСТЕР СЕРВІС» нами було розроблено декілька кроків.

По-перше, на нараді керівників відділу методом мозкового штурму було визначено потенційні ризики, які в подальшому були систематизовані та представлені за допомогою діаграми Ісікави.

Таблиця 3.4

Групи ризиків за напрямками.

Група небажаних подій	**Заходи запобіганню НС**
Робота з даними на серверному обладнанні	– Створення резервних копій даних. – Резервування ключових налаштувань в файл конфігурації. Забезпечення надійного зберігання цього файлу. – Використання алгоритмів шифрування даних.
Налаштування мережевого обладнання	– Використання резервних каналів. – Використання хмарних сховищ для резервного зберігання даних. – Перенаправлення потоків даних. – Застосування заходів безпеки, таких як аутентифікація, авторизація та облік доступу.
Технічне обслуговування обладнання	– Періодичний технічний огляд стану обладнання. – Перевірка мережевого обладнання. – Перевірка відгуків серверного обладнання. – Перевірка внутрішніх каналів зв’язку.
Резервування живлення	– Забезпечення короткочасного резервування живлення шляхом використання ДБЖ. – Забезпечення довготривалого резервування живлення за допомогою бензинового генератора.
Налаштування програмного забезпечення	– Розмежування програмного доступу до обладнання. – Розмежування доступу до інформації. – Обмеження доступу до налаштувань ПЗ. – Регулярне оновлення ПЗ.
Використання ПЗ	– Використання антивірусного ПЗ.
Планування та проведення навчання	– Розробка правил зберігання та доступу до інформації. – Навчання персоналу щодо протидії небажаним ситуаціям – Розробка політики безпеки підприємства.
Планування та проведення аудитів	– Проведення аудиту безпеки. – Проведення аудитів ключових налаштувань обладнання.
Заходи безпеки	– Розробка заходів фізичного захисту зовнішніх мереж та обладнання. – Обмеження фізичного доступу до обладнання як співробітниками, так й сторонніми особами.
Взаємодія з сервісними операторами	– Негайне інформування відповідних служб, які використовують дане обладнання. – Негайне інформування операторів зв’язку. – Негайне інформування операторів сервісу.

Наступним кроком було обрання особи з керівного складу, на яку покладено відповідальність за функціонування системи ризик-менеджменту. Останнім кроком в ідентифікації ризиків була побудова плану дій персоналу щодо запобігання небажаної ситуації (НС). Також відбулося корегування посадових інструкцій частини персоналу, задіяних в системі ризик-менеджменту, яким було надано право використання певних ресурсів підприємства для мінімізації наслідків, або повного усунення небажаної ситуації. Для запобіганню виникнення небажаної ситуації при отриманні підозрілого листа, або потенційно небезпечного файлу співробітниками, нами було розроблено внутрішню інструкцію підприємства щодо реагування цей тип кіберзагроз.

3.3 Розробка та аналіз ефективності заходів із запобігання інформаційним ризикам діяльності

Нами пропонується узагальнений алгоритм реагування на всі небажанні події (рис.3.4). Цей алгоритм дає можливість розробити інструкції для кожного конкретного типу загрози та прописати дії співробітників. Прикладом внутрішньої інструкції для співробітників, а саме для запобігання найпоширенішого ризику – помилкових дій персоналу, нами розроблено алгоритм з поясненнями щодо дій співробітників у разі відкриття підозрілого файлу у електронному листі, або підозри на зараження комп'ютера шкідливим програмним забезпеченням:

1. Не вимикати комп'ютер.
2. Закрити всі робочі програми без збереження поточної інформації.
3. Не від'єднувати підключені зовнішні носії інформації.
4. Якщо можливо, від'єднати комп'ютер від внутрішньої мережі підприємства.
5. Повідомити про інцидент системного адміністратора, або керівника системи управління ризиками.

Подальші дії щодо ліквідації загрози здійснюються фахівцем (системним адміністратором), у відповідності до узагальненого алгоритму реагування на загрози.

Слідування цієї простої інструкції не допустить втрати даних при перезавантаженні комп'ютера у разі пошкодження системних розділів жорсткого диску. Зменшить ризик збереження заражених файлів та копій шкідливого програмного забезпечення (ПЗ), а також обмежить використання потенційно небезпечних зовнішніх носіїв інформації до їх перевірки на наявність шкідливого ПЗ. Від'єднання від мережі унеможливіть розповсюдження шкідливого ПЗ внутрішньою мережею підприємства, у разі звернення інших співробітників до комп'ютера з потенційною загрозою.

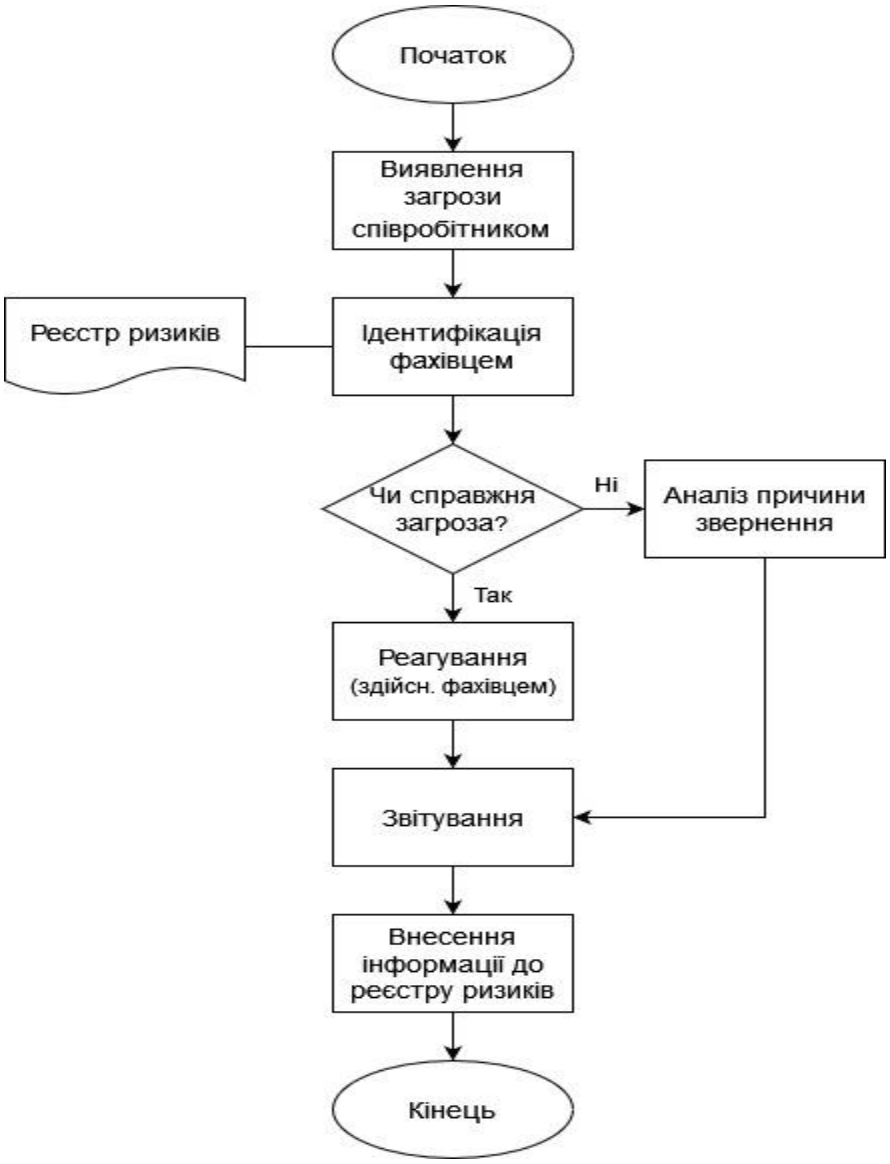

Рис. 3.4 Узагальнений алгоритм реагування на небажанні події

Для аналізу ефективності розробленої процедури управління ризиками нами було проведено повторний аналіз найвпливовіших загроз ІТ діяльності підприємства співробітниками, відповідальними за діяльність системи управління ризиками. Ця оцінка проводилась за складовими: «Ймовірність виникнення» та «Ймовірність виявлення» після впровадження заходів із запобігання ризикам (табл. 3.5). Повторну оцінку за складовою «Тяжкість наслідків» не проводили, а використали результати попередньої оцінки, оскільки прийняли її незмінною у рази виникнення небажаної ситуації. Результати оцінки до та після впровадження заходів представлені на порівняльній діаграмі (рис. 3.5).

Таблиця 3.5

Оцінка небезпечних факторів після впровадження процедури управління інформаційними ризиками.

Небезпечний фактор	**Перша оцінка**							**Повторна оцінка**				
	Тяжкість наслідків		**Ймовірність виникнення**		**Ймовірність виявлення**		**ПЧР І**	**Ймовірність виникнення**		**Ймовірність виявлення**		**ПЧР ІІ**
	Оцінка	**Середнє**	**Оцінка**	**Середнє**	**Оцінка**	**Середнє**		**Оцінка**	**Середнє**	**Оцінка**	**Середнє**	
Помилкові дії співробітників	9	9,25	5	4,75	6	6,5	285,6	4	3,75	7	6,75	234,1
	10		5		7			4		7		
	9		4		7			4		7		
	9		5		6			3		6		
Зовнішнє втручання сторонніх осіб	9	8,75	4	4	6	6,5	227,5	4	3,5	6	6,5	199,1
	10		3		7			3		6		
	8		5		6			4		7		
	8		4		7			3		7		
Вплив сторонніх осіб на діяльність (хакерські взломи)	8	8,75	4	3,75	7	6,75	221,5	2	2,75	7	7	168,4
	9		4		6			4		6		
	9		3		7			3		8		
	9		4		7			2		7		

Продовження табл. 3.5

Пошкодження програмного забезпечення (ПЗ)	7	8	4	3,75	6	5,75	172,5	3	3	6	5,5	132,0
	8		4		5					5		
	9		3		6					5		
	8		4		6					6		
Поломка обладнання	8	8	3	3,5	5	5,25	147,0	2	2,25	3	3,25	58,5
	9		4		5			2		3		
	7		4		6			3		4		
	8		3		5			2		3		
Незахищеність інформації	8	7	3	3,25	5	5,5	125,8	2	2,75	5	5,5	105,9
	6		3		6			3		5		
	7		4		6			3		6		
	7		3		5			3		6		

За основу побудови порівняльної діаграми було взято розрахований коефіцієнт пріоритетного числа ризиків (ПЧР), який обчислювався як добуток середніх оцінок співробітників за такими параметрами як «Тяжкість наслідків», «Ймовірність виникнення» та «Ймовірність виявлення».

Рис. 3.5 Порівняльна діаграма найвпливовіших загроз

На діаграми ми бачимо зменшення пріоритетного числа ризиків, що вказує на позитивний вплив наших запобіжних заходів та, як слідство, ефективність розробленої нами системи в цілому.

Зниження основних ризиків діяльності дозволить уникнути економічних втрат і збитків для репутації підприємства. Результати наших досліджень допоможуть підвищити відповідальність та ІТ-обізнаність і компетентність наших співробітників, стандартизувати та контролювати інформаційні процеси, що є першочерговим завданням з точки зору системи управління ризиками.

Висновки до розділу 3

Отже, в ході проведених нами досліджень було розроблено процедуру управління ризиками в ІТ діяльності приватного підприємства «ІТ МАСТЕР СЕРВІС». В основу процедури покладено вимоги стандарту ДСТУ ISO 27001:2023 та рекомендації стандарту ISO 31000:2018. В процесі розробки процедури нами було вивчено діяльність підприємства, та проаналізовано причини виникнення ІТ ризиків.

Результатом розробки було запропоновано заходи запобіганню небажаних ситуацій та зменшення їх негативного впливу на діяльність підприємства, а також зміни до посадових інструкцій задіяного в системі персоналу. Додатково була розроблена внутрішня інструкція щодо запобігання виникненню найвпливовішого ризику – людського фактору, у разі підозри співробітників наявність втручання в комп’ютер або його зараження.

Проаналізувавши результати інтеграції процедури управління ризиками в діяльність підприємства, можемо сказати, що розроблена процедура ефективна, оскільки коефіцієнт пріоритетного числа ризиків знизився у порівнянні цього ж коефіцієнта до розробки та впровадження системи.

ЗАГАЛЬНІ ВИСНОВКИ

Використання інтегрованої системи управління на підприємстві ПП «ІТ МАСТЕР СЕРВІС» надає йому ряд конкурентних переваг. За результатами кваліфікаційної роботи можна зробити наступні висновки:

1. Нами було проведено дослідження щодо сучасних підходів до інформаційної безпеки. Постійна модернізація ІТ інфраструктури підприємства вимагає переглядати методи протидії виникаючим загрозам, розробляти новітні та сучасні алгоритми цих методів, вивчати самі загрози. Самі загрози можна поділити на два типи – це можуть бути інциденти, спричинені як внутрішніми, так і зовнішніми сторонами. Найбільшою зовнішньою загрозою для підприємств становлять кібератаки, спрямовані на крадіжку даних. Проте, найвпливовішу внутрішню загрозу становлять ненавмисні, або навмисні дії співробітників, які призводять до порушень кібербезпеки.

2. Вивчаючи стандарт ISO 31000:2018, ми прийшли висновку, що для боротьби з ІТ загрозами дуже важливу роль відіграє лідерство керівників. ISO 31000:2018 надає загальне керівництво, він використовується як допоміжний стандарт для побудови системи управління ризиками, щоб гарантувати досягнення організацією виробничих цілей з ощадливим використанням ресурсів. У свою чергу, стандарт ДСТУ ISO 27001:2023 встановлює саме вимоги до системи управління інформаційною безпекою, структуруючи підхід до захисту інформаційних активів організації. Розглядаючи детально стандарт ДСТУ ISO 27001:2023 ми бачимо, що основними цілями його є забезпечення конфіденційності, цілісності та доступності інформації, зниження ризиків ІБ, підвищення довіри до організації з боку зацікавлених сторін.

3. В ході роботи була вивчена та досліджена діяльність вітчизняного комерційного підприємства «ІТ МАСТЕР-СЕРВІС». Нами було проведено SWOT-аналіз підприємства, завдяки якому ми змогли виявити загрози його діяльності, та виділити загрози саме ІТ діяльності. Подальший розгляд загроз

інформаційної безпеки допоміг структурувати їх за впливом та наслідками, а також виділити й проаналізувати найвпливовіші з них. Аналіз загроз допоміг нам розробити заходи запобігання їм, або мінімізації їх руйнівного впливу. При розгляді діяльності приватного підприємства «ІТ МАСТЕР СЕРВІС» стало зрозумілим, що причиною основної небажаної ситуації може бути людський фактор. Він криється у діяльності або бездіяльності співробітників, а також цілеспрямованих дій сторонніх осіб. Другою за впливовістю є загроза поломки обладнання. Обидві ці загрози можуть призвести до розвитку критичної ситуації, а саме – втрати або розголошенню комерційної інформації.

4. Для запобіганню виникнення, розвитку або наслідків кризової ситуації нами було розроблено низку заходів реагування до кожної потенційної небезпеки. Реалізацію цих заходів покладено на відповідальних осіб, яких призначено на нарадах підприємства. Права та обов’язки відповідальних осіб були зафіксовані, в корегованих у відповідності до розробленої процедури, посадових інструкціях. Останнім кроком було розроблено механізм оцінки ефективності впроваджених заходів реагування на кризові ситуації. Цей механізм передбачає періодичне проведення аналізу після змін в системі управління ризиками, або після поліпшення самої системи. Проведення аналізу ефективності довело ефективність розроблених нами заходів та в цілому процедури управління інформаційними ризиками на підприємстві.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Дослідження IBM X-Force Threat Intelligence Index, 2022. Електронний ресурс. https://www.ibm.com/security/assets/pdf/xforce-threat-intelligence-index-2022.pdf

2. Дослідження PwC про кібербезпеку, 2022. Електронний ресурс. https://www.pwc.com/us/en/cybersecurity/publications/2022-state-of-information-security-survey.html

3. Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. Communications of the ACM, 46 (3), стор. 81–85.

4. Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security (TISSEC), 5 (4), стор. 438-457.

5. ESET THREAT REPORT T1 2022. Електронний ресурс. https://web-assets.esetstatic.com/wls/2022/06/eset_threat_report_t12022.pdf#page=4

6. ДСТУ ISO 9000:2015(ISO 9001:2015, IDT) Основні положення та словник термінів. Видання офіційне. Київ : ДП «Укр-НДНЦ », 2016.

7. Матеріали I науково-практичної internet-конференції з міжнародною участю «Актуальні проблеми якості, менеджменту і економіки у фармації і охороні здоров'я» Облог С. В., Зборовська Т. В. Національний фармацевтичний університет, м. Харків. Оцінка інформаційних ризиків як запорука конкурентоспроможності та якісного управління с. 194-197.

8. IBM Ponemon. Cost of a data breach report 2020. Електронний ресурс. https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pdf. 2020.

9. Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Електронний ресурс https://doi.org/10.1016/j.cose.2013.04.004

10. Hurst, W., Merabti, M., & Fergus, P. (2014, May). Big data analysis techniques for cyber-threat detection incritical infrastructures. InProceedings of the

2014 28th International Conference on Advanced Information Networking and Applications Workshops стор. 916–921.

11. Marotta, A., & McShane, M. (2018). Integrating a proactive technique into a holistic cyber risk management approach. Risk Management and Insurance Review,21(3), стор. 435–452.

12. Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. Financial Review,53(2), стор. 413–455

13. Kamiya, S., Kang, J. K., Kim, J., Milidonis, A., & Stulz, R. M. (2020). Risk management, firm reputation, and theimpact of successful cyberattacks on target firms. Journal of Financial Economics.

14. Higgs, J. L., Pinsker, R. E., Smith, T. J., & Young, G. R. (2016). The relationship between board-level technology committees and reported security breaches. Journal of Information Systems,30(3), стор. 79–98.

15. Boasiako, K. A., & Keefe, M. O. C. (2020). Data breaches and corporate liquidity management. European Financial Management.

16. Ettredge, M., & Richardson, V. (2002). Assessing the risk in e-commerce. In R.H. Sprague, Jr. (ed.), Proceedingsof the 35th Annual Hawaii International Conference on System Sciences. Computer Society Press: LosAlamitos, CA (USA)

17. Eling, M., & Wirfs, J. (2019). What are the actual costs of cyber risk events? European Journal of Operational Research, 272(3).

18. Amir, E., Levy, S., & Livne, T. (2018). Do companies underestimate information about cyber attacks? Evidence from capital markets. Review of Accounting Studies, 23 (3), стор. 1177–1206.

19. Cavusoglu, H., Mishra, B., & Raghunathan, S. The effect of internet security breach announcements onmarket value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, 9 (1), стор. 70–104.

20. Garg, P. Cybersecurity breaches and cash holdings: Spillover effect. Financial Management, 49 (2), стор. 503–519.

21. Gartner. Gartner Forecasts Worldwide IT Spending to Grow 8% in 2024. Електронний ресурс. https://www.gartner.com/en/newsroom/press-releases/2023-10-18-gartner-forecasts-worldwide-it-spending-to-grow-8-percent-in-2024

22. Ekwere, N. (2016). Framework Of Effective Risk Management In Small And Medium Enterprises (SMEs): A Literature Review. Bina Ekonomi, 20 (1), стор. 23–46.

23. Md. Sum, R., & Hamir, H. (2019). Sole Proprietor Micro Enterprise Risks and Risk Mitigation Techniques. In K. Mohd Noor, N. H. Ab Aziz, & M. Jober (Eds.), National Conference on the Humanities and Social Sciences (NACOSS) Proceeding. стор. 17.

24. ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови. (ISO 31000:2018, IDT).

25. ДСТУ ISO/IEC 27001:2023 Інформаційна безпека, кібербезпека та захист конфіденційності. Системи керування інформаційною безпекою. Вимоги (ISO/IEC 27001:2022, IDT)

26. G. Joyce, (2009). ISO Risk Management, Guidelines and Principles.

27. Хімічева, Г. І., & Горецька, Н. Б. (2018). Вибір і обґрунтування механізмів та інструментів оцінки ризиків за вимогами стандартів ISO 31000. In Science, Research, Development. Technics and Technology. # 4. Wydawca: Sp. z oo" Diamond trading tour".

28. The new ISO 31000 keeps risk management simple. Електронний ресурс. https://www.iso.org/news/ref2263.html

29. Lam, J. (2014). Enterprise risk management: from incentives to controls. John Wiley & Sons.

30. Olechowski, A., Oehmen, J., Seering, W., and. Ben-Daya, M. 2016. The Professionalization of Risk Management: What Role Can the ISO 31000 Risk Management Principles Play?, Int. J. Proj. Manag. vol. 34, no. 8, стор. 1568–1578.

31. Kothari CR. Quantitative Techniques, 2nd ed., New Delhi: Vikas Publishing House Pvt. Ltd., 2009.

32. Звітність українських підприємств. Електронний ресурс. https://zvitnist.com/

33. О.Є. Кузьмін, Н.Ю. Подольчак, Н.І. Подольчак, Л.Г. Вербицька. Управління ризиками в інноваційній діяльності: навч. посіб. Львів: Видавництво Львівської політехніки, 2012. 240 с.

ДОДАТКИ

ДОДАТОК А

Таблиця 3.1

Оцінка небезпечних факторів ПП «ІТ МАСТЕР СЕРВІС»

Небезпечний фактор	Тяжкість наслідків		Ймовірність виникнення		Ймовірність виявлення		ПЧР
	Оцінка	Середнє	Оцінка	Середнє	Оцінка	Середнє	
Поломка обладнання	8	8	3	3,5	5	5,25	147,0
	9		4		5		
	7		4		6		
	8		3		5		
Порушення технічної комунікації	5	5,25	3	2,75	4	3,25	46,9
	6		3		4		
	4		2		2		
	6		3		3		
Некоректна настройка обладнання	6	5,75	2	2,5	4	3,5	50,3
	7		3		3		
	5		3		3		
	5		2		4		
Навмисне пошкодження	8	8,25	2	2	3	3	49,5
	9		2		3		
	7		1		2		
	9		3		4		
Відсутність розмежування доступу до інформації	7	5,75	3	3,25	3	3,75	70,1
	5		2		4		
	6		4		5		
	5		4		3		
Незахищеність інформації	8	7	3	3,25	5	5,5	125,8
	6		3		6		
	7		4		6		
	7		3		5		
Пошкодження програмного забезпечення (ПЗ)	7	8	4	3,75	6	5,75	172,5
	8		4		5		
	9		3		6		
	8		4		6		
Помилкові дії співробітників	9	9,25	5	4,75	6	6,5	285,6
	10		5		7		
	9		4		7		
	9		5		6		
Аварія в мережі електропостачання	4	5	3	2,5	1	1,5	18,8
	6		3		2		
	5		2		2		
	5		2		1		

Продовження табл. 3.1

Відмова обладнання зовнішніх систем	5	5,25	2	2,75	2	1,75	25,3
	6		3		2		
	5		3		1		
	5		3		2		
Природні фактори	4	4	2	1,75	2	1,25	8,8
	4		2		1		
	5		1		1		
	3		2		1		
Зовнішнє втручання сторонніх осіб	9	8,75	4	4	6	6,5	227,5
	10		3		7		
	8		5		6		
	8		4		7		
Відсутність зв'язку	4	4	2	2	1	1,25	10,0
	3		1		1		
	4		2		2		
	5		3		1		
Відсутність доступу до сервісів	5	5,25	1	1,25	2	1,5	9,8
	5		1		1		
	6		2		1		
	5		1		2		
Вплив сторонніх осіб на діяльність (хакерські взломи)	8	8,75	4	3,75	7	6,75	221,5
	9		4		6		
	9		3		7		
	9		4		7		

Шкали оцінювання ризиків

Шкала оцінки тяжкості наслідків

Тяжкість наслідків небажаної ситуації	**Бал**
Вплив, близький до нуля. Наслідки невідчутні. Без збитків.	1
Незначний вплив. Наслідки ледь відчутні. Без збитків.	2-3
Помірний вплив. Наслідки відчутні. Незначні, нематеріальних збитки.	4-6
Істотний вплив. Наслідки дуже відчутні. Значні матеріальні збитки.	7-9
Критичний вплив. Важкі наслідки. Завдано значних збитків.	10

Шкала для оцінки ймовірності виникнення

Ймовірність виникнення небажаної ситуації	**Бал**
Імовірність близька до нуля. 1 раз за декілька років.	1
Незначна ймовірність. 1 раз на рік.	2-3
Середня ймовірність. 2-3 рази на рік.	4-6
Висока ймовірність. 4-5 разів на рік	7-9
Дуже висока ймовірність. 6 та більше разів на рік	10

Шкала для оцінки ймовірності виявлення

Ймовірність виявлення небажаної ситуації	**Бал**
Дуже висока ймовірність. Контроль факторів не проводиться	1
Помірна ймовірність. Проводяться періодичний контроль	2-3
Невелика ймовірність. Постійний контроль факторів.	4-6
Дуже маленька ймовірність. Постійний моніторинг факторів.	7-9
Імовірність близька до нуля. Причини відмов виявити неможливо	10

ДОДАТОК Б

ЗАТВЕРДЖУЮ

_____
(назва установи, організації)

_____
(уповноважена особа)

_____
(ПІБ, підпис)

"___" _____ 202_ р.

ПОСАДОВА ІНСТРУКЦІЯ НАЧАЛЬНИКА ПІДРОЗДІЛУ ПОСТАЧАННЯ ТА КЕРІВНИКА СИСТЕМОЮ З УПРАВЛІННЯ РИЗИКАМИ

І. Загальні положення

1. Дана посадова інструкція визначає функціональні обов'язки, права і відповідальність Начальника підрозділу постачання.
2. Начальник підрозділу постачання є основним організатором стратегії Підприємства в області закупівель.
3. Керівник з управління ризиками є посадовою особою організації, яка відповідає за розробку, впровадження та моніторинг системи управління ризиками в організації.
4. Підбирається з числа кваліфікованих фахівців, що володіють високим рівнем організаторських здібностей і мають стаж роботи на аналогічній посаді не менше 3-х років.
5. Призначається на посаду та звільняється з посади в установленому чинним трудовим законодавством порядку, наказом директора підприємства.
6. Основним завданням начальника підрозділу постачання є забезпечення підприємства усіма необхідними для його діяльності матеріальними ресурсами.
7. Підпорядковується безпосередньо директору підприємства.
8. В роботі керується:
   - даною посадовою інструкцією;
   - положеннями, що регламентують внутрішньофірмові відносини;
   - потребами підрозділу продажів, та власними потребами підприємства.
9. Основними показниками ефективності роботи є;

- Організація безперебійного постачання;
- Зменшення собівартості закуповуваного товарів та послуг;
- Дотримання затвердженого кошторису витрат;
- Вдосконалення роботи відділу, розробка і впровадження нових систем, спрямованих на підвищення ефективності використання коштів;
- Підвищення рентабельності.

10. Повинен пройти підготовку або підвищення кваліфікації в сфері управління інформацією.
11. Повинен володіти знаннями щодо управління інформаційними ризиками та зміст стандартів ISO 31000 та ISO 27001

II. Завдання та обов'язки

1. Здійснює організацію процесу закупівлі товарів та послуг.
2. Контролює правильність і своєчасність виконання поставлених завдань співробітниками відділу.
3. Керує розробкою проектів перспективних і річних планів матеріально-технічного забезпечення.
4. Стежить за станом власних запасів підприємства, вживає заходів для мінімізації затрат на закупівлю цих запасів.
5. Виконує роботи, пов'язані з підготовкою претензій до постачальників.
6. Бере участь в узгодженні умов і укладанні договорів поставок з матеріально-технічного забезпечення підприємства, вживає заходів з розширення прямих зв'язків з постачальниками.
7. Здійснює організацію оперативного обліку постачальницьких операцій.
8. Своєчасно складає і подає на погодження кошторис витрат по закупівлях у відповідності до чинного «Положення про планування».
9. Контролює дотримання норм розрахунків по відділу, відповідно до затвердженого кошторису.
10. Своєчасно і в повному обсязі складає і передає до бухгалтерії необхідні звіти.
11. Контролює своєчасність здачі звітів в бухгалтерію співробітниками відділу.
12. Розробляє та впроваджує систему управління ризиками на підприємстві відповідно до рекомендації стандарту ISO 31000 та ISO 27001.
13. Забезпечує ефективну діяльність системи управління ризиками підприємства.
14. Організовує розробку та впровадження процесів і процедур управління ризиками на підприємстві.
15. Організовує розробку та впровадження методів і інструментів управління ризиками підприємства.
16. Проводить аналіз ризиків підприємства.

17. Визначає заходи щодо зниження ризиків підприємства та здійснює контроль за виконанням цих заходів.
18. Готує звіти про стан управління ризиками на підприємстві.

III. Права

Начальник підрозділу постачання має право:

1. Давати підлеглим йому співробітникам і службам доручення, завдання по колу питань, що входять в його функціональні обов'язки.
2. Вимагати від керівників усіх підрозділів надання необхідних матеріалів, звітів, інформації для планування та організації планової роботи підрозділу постачання.
3. Запитувати й одержувати необхідні матеріали і документи, пов'язані з питаннями його діяльності.
4. Виступати від імені Підприємства в інших організаціях та установах з питань, що відносяться до компетенції відділу.
5. Вносити пропозиції щодо вибору та розстановки персоналу, відповідального за закупівлі.
6. Проводити наради з обговорення питань, що входять у компетенцію підрозділу.
7. Видавати розпорядження по відділу про заохочення працівників, які відзначилися в роботі, і про накладення стягнень на працівників підрозділу, які порушили трудову дисципліну і посадові обов'язки.
8. Рекомендувати до прийняття на роботу і звільнення персонал Підприємства.
9. Подавати пропозиції з удосконалення своєї роботи.
10. Приймати участь в розробці стратегії та цінової політики Підприємства у галузі постачань.
11. Координувати взаємодію відділу з іншими підрозділами Підприємства відповідно до розроблених та затверджених норм.
12. Вносити пропозиції щодо вдосконалення системи управління інформаційними ризиками на підприємстві.
13. Здійснювати контроль за діяльністю підрозділів підприємства, відповідальних за управління інформаційними ризиками.
14. Використовувати ресурси підприємства для усунення причин або наслідків небажаних ситуацій.

IV. Відповідальність

Начальник відділу постачання несе відповідальність за:

1. Результати і ефективність підрозділу закупівлі підприємства.

2. Незабезпечення виконання своїх функціональних обов'язків з питань забезпечення.
3. Недостовірну інформацію про стан виконання завдань підлеглими.
4. Невиконання наказів, розпоряджень і доручень директора підприємства.
5. Невжиття заходів по припиненню виявлених порушень правил техніки безпеки, протипожежних та інших правил, що створюють загрозу нормальній (безпечній) діяльності підприємства, його працівникам.
6. Незабезпечення дотримання трудової і виконавської дисципліни працівниками, що знаходиться в його підпорядкуванні.
7. Порушення внутрішнього розпорядку підприємства.
8. Несе повну відповідальність за ефективну діяльність системи управління інформаційними ризиками.
9. Несе повну відповідальність за своєчасне та якісне виконання своїх посадових обов'язків.

УЗГОДЖЕНО

Керівник підприємства: _____ (підпис) _____ (ПІБ) "__" _____ 202_ р.

З інструкцією ознайомлений: _____ (підпис) _____ (ПІБ) "__" _____ 202_ р.

Національний фармацевтичний університет

Кафедра управління та забезпечення якості у фармації

СЕРТИФІКАТ № 81

Облог Сергій

учасника І Науково-практичної internet-конференції з міжнародною участю «Актуальні проблеми якості, менеджменту і економіки у фармації і охороні здоров'я»

19 травня 2023 року, м. Харків

Оргкомітет засвідчує, що отримувач (ка) прийняв (ла) активну участь в обговоренні актуальних питань за темою конференції (обсяг 15 годин – 0,5 кредита ECTS) і набув (ла) відповідних компетентностей:

- **здатність опанувати сучасні підходи управління якістю та соціально-економічними процесами в закладах охорони здоров'я та фармацевтичних організаціях;**
- **здатність діяти на основі етичних міркувань та мотивів;**
- **здатність до саморозвитку, навчання впродовж життя та ефективного самоменеджменту.**

В.о. Ректора Національного фармацевтичного університету **Алла КОТВІЦЬКА**

Міністерство охорони здоров'я України
Міністерство освіти і науки України
Національний фармацевтичний університет
Кафедра управління та забезпечення якості у фармації

МАТЕРІАЛИ

І науково-практичної internet-конференції з міжнародною участю

«АКТУАЛЬНІ ПРОБЛЕМИ ЯКОСТІ, МЕНЕДЖМЕНТУ І ЕКОНОМІКИ У ФАРМАЦІЇ І ОХОРОНІ ЗДОРОВ'Я»

(19 травня 2023 р.)

MATERIALS

of I scientific and practical internet-conference
with international participation

«ACTUAL PROBLEMS OF QUALITY, MANAGEMENT, AND ECONOMY IN PHARMACY AND HEALTH CARE»

(19 May 2023)

Харків

2023

УДК 330.101:615.1

Реєстр з'їздів, конгресів, симпозіумів та науково-практичних конференцій: реєстраційне свідоцтво № 552 від 19.12.2022 р.

Актуальні проблеми якості, менеджменту і економіки у фармації і охороні здоров'я: матер. І міжнарод. наук.-практ. internet-конференції з міжнар. участю, Харків, 19 травня 2023 / ред. кол.: Т.В. Крутських, О.В. Літвінова, Ю.С. Братішко**.**– Харків : НФаУ, 2023. – 250 с.

Actual problems of quality, management, and economy in pharmacy and health care: materials of I scientific and practical internet-conference with international participation. May 19, 2023 / ed. board. : T.V. Krutskikh, O.V. Litvinova, Yu.S. Bratishko. Kharkiv : NUPh, 2023. – 250 p.

Збірник містить матеріали І науково-практичної конференції, які присвячені обговоренню наукових та практичних проблем управління якістю і менеджменту в фармації і охороні здоров'я; визначенню напрямів удосконалення господарської й інноваційної діяльності підприємств (організацій, закладів) у ринковій економіці, підготовки сучасних кадрів із залученням вчених, фахівців-практиків, викладачів навчальних закладів та дослідників, докторантів, аспірантів, підприємців з України та зарубіжжя.

Матеріали подаються мовою оригіналу
За достовірність матеріалів відповідальність несуть автори

Облог С. В., Зборовська Т. В.

Національний фармацевтичний університет, м. Харків

Оцінка інформаційних ризиків як запорука конкурентоспроможності та якісного управління

34444@i.ua

Вступ. Інформація – це дуже вагоме та змістовне слово. «Хто володіє інформацією, той володіє світом» – відомий вислів Натана Ротшильда, пізніше процитований і поширений Вінстоном Черчиллем, сьогодні актуальний як ніколи.

У сучасному світі інформаційних технологій ставлення до інформації дуже різноманітне, та суперечливе. Інформація може бути загальнодоступною, та закритою, вона може бути захищеною, та, у той же час, відкритою для загалу, змінною або недостовірною, тощо. Кожна компанія, від маленького підприємства до великих корпорацій має власне ставлення до інформації. Всі хочуть отримати якомога більше інформації стосовно ринків збуту продукції, виробництва, фінансової інформації, даних про конкурентів та партнерів, у той же час зберегти в таємниці свою комерційну інформацію, втрата, або розповсюдження якої може фатально вплинути на діяльність компанії та її позицій на ринку.

Основні ризики, які можуть бути розглянуті щодо інформації підприємства, пов’язані з неправильним підходом до керування інцидентами інформаційної безпеки; незахищеністю активів IT-інфраструктури; неналежним захистом інформації у мережах та на носіях з використанням технічних уразливостей цих самих носіїв, тощо.

Аналіз стандартів з інформаційної безпеки дозволяє виявити основні елементи ризиків, які описуються інформаційною структурою та визначають вплив на діяльність інформаційних систем. Під ризиком розуміють можливість або ймовірність настання подій з негативними або позитивними наслідками в результаті певних рішень або дій. Тому потрібно проводити оцінку ризику –

процес ідентифікації інформаційних ресурсів системи і загроз цих ресурсів, а також можливих втрат, заснований на оцінці частоти виникнення подій та розміру збитку від них.

Мета дослідження. Виходячи з цього ми ставимо за мету нашої роботи провести дослідження щодо встановлення методичних підходів з оцінки різного роду впливів, наприклад таких ризиків як втрата або несанкціоноване розповсюдження комерційної інформації, та їх наслідків і заходів з протидії на успішність функціонування підприємства.

Матеріали та методи. В наших дослідженнях в якості матеріалів ми використовували аналіз джерел літератури, вимог стандарту ISO/IEC 27001:2022 «Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги» та досвіду провідних підприємств різних галузей, які впровадили інформаційний захист у вигляді сертифікації системи управління інформаційної безпеки.

Результати дослідження.

Проаналізувавши вимоги стандарту можемо встановити етапи управління інформаційною безпекою підприємства наведені на Рис.1:

Рис.1. Сценарій управління інформаційною безпекою підприємства.

Які найчастіше виникають ризики щодо втрати або розповсюдження комерційної або закритої інформації? Наприклад, втрата інформації найчастіше виникає при поломці або відмові обладнання, при втраті живлення, або при

помилкових діях персоналу та користувачів обладнання. Також ризик втрати даних буває мнеш передбачуваним – це, наприклад, може бути навмисне або випадкове зараження комп'ютерних систем шкідливими програмами. Іншими ризиками для компаній може бути витік або розповсюдження комерційної інформації. Цей тип ризиків також є менш передбачуваним, але дуже впливовим. Ризики, пов'язані з розповсюдженням інформації можуть зашкодити розвитку компанії, або діяльності в цілому, що у свою чергу може привести до втрати конкурентних позицій та відтоку клієнтів.

Ризики інформаційної безпеки є складовою частиною операційних ризиків підприємства. Одним із шляхів вирішення проблеми оцінки ризиків та вибору оптимального варіанта їх обробки є визначення методики з отриманням необхідної інформації для проведення оцінки з метою прийняття обґрунтованих рішень стосовно того, яким чином краще забезпечувати захист активів підприємства від певних загроз інформаційної безпеки. Оцінка ризиків інформаційної безпеки може здійснюватися у розрізі підприємства або його інформаційних систем.

Оцінка ризиків інформаційної безпеки складається з етапів припустимого та існуючого ризику здійснення загрози, значення ймовірності кожного із загроз допомагає співвіднести оцінку можливих збитків із витратами на захист.

Таблиця 1.

Етапи ризик-орієнтованого підходу в інформаційній безпеці підприємства

Етап роботи з інформаційними ризиками	Необхідні дії з боку підприємства
Ідентифікація загроз відповідно до специфіки діяльності	Формування повної множини загроз для інформаційних потоків
Ідентифікація джерел та каналів інформаційної діяльності	Визначення переліку об'єктів інформації, що потребують захисту
Ідентифікація джерел загроз	Виявлення можливих джерел впливу (ризиків) на інформаційні потоки
Ранжування інформаційних ризиків за ступенем впливу та ймовірністю настання	Аналіз і вибір переліку ризиків, з огляду на особливості функціонування підприємства та оцінка наслідків їх впливу, визначення імовірності здійснення потенційних загроз
Оцінка наслідків	Обрахунок можливого рівня фінансових, технологічних та іміджевих втрат
Корегування інформаційного захисту	Розробка заходів з попередження та коригування наслідків інформаційних загроз

Отже ризики ми можемо класифікувати за властивостями інформаційних ресурсів, які порушуються при розвитку кризової ситуації (цілісність, доступність, конфіденційність), а також ризики за втратами, в наслідок настання кризової ситуації. Втрати можуть бути по-перше фінансовими, далі – репутаційними, (порушення контрактів), порушення законодавства. З наведених типів втрат, фінансові втрати найбільше піддаються кількісній оцінці. Репутаційні втрати частково можливо оцінити з фінансової точки зору – це, наприклад, втрата контрактів, яка призведе до фінансових втрат компанії, та до втрати її конкурентоспроможності.

При визначені ступеню потенційної загрози, підприємства повинні проводити оцінку ризиків, за впровадженою програмою ризик-менеджменту. Оцінка ризиків, в свою чергу, допоможе впровадити відповідні заходи для зниження або усунення ризиків.

Висновки. Для визначення та передбачення несприятливих подій, загрози треба проаналізувати заздалегідь в поєднанні з потенційними вразливостями. Також повинні бути проаналізовані потенційні місця прояву цих несприятливих подій. Рівень впливу тієї чи іншої ризикової ситуації визначається величиною збитку, який може бути заподіяний відповідними загрозами. Такий підхід дає можливість, у подальшому, сформувати рекомендації щодо формування програми ризик-менеджменту ІТ-інфраструктури підприємства.

Національний фармацевтичний університет

Факультет фармацевтичних технологій та менеджменту
Кафедра управління та забезпечення якості у фармації
Рівень вищої освіти другий магістерський
Спеціальність 073 Менеджмент
Освітня програма Якість, стандартизація та сертифікація

ЗАТВЕРДЖУЮ
Завідувачка кафедри
управління та забезпечення
якості у фармації
Тетяна КРУТСЬКИХ
“17” жовтня 2023 року

ЗАВДАННЯ
НА КВАЛІФІКАЦІЙНУ РОБОТУ
ЗДОБУВАЧА ВИЩОЇ ОСВІТИ

Сергія ОБЛОГА

1. Тема кваліфікаційної роботи: **«Розробка процедури Управління інформаційними ризиками в організації»**, керівник кваліфікаційної роботи: Тетяна ЗБОРОВСЬКА, канд. фармац. наук, доцент,

затверджений наказом НФаУ від “16”жовтня 2023 року № 229

2. Строк подання здобувачем вищої освіти кваліфікаційної роботи: 05.02.2024 р.

3. Вихідні дані до кваліфікаційної роботи: наукова та навчально-методична література, законодавчі й нормативні акти України, інформаційна діяльність організації на основі ризик-орієнтованого підходу; стандарт ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови.

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):
Актуальність роботи. Мінімізація можливості виникнення інформаційних ризиків, підприємства потребує впровадження ефективних системи управління інформаційною безпекою. Ці системи повинні включати в себе заходи щодо запобігання, виявлення та реагування на інформаційні ризики.
Розділ І. Впровадження ризик-орінтованого підходу в інформаційну діяльність організацій. Досвід побудови інформаційної діяльності організації на основі ризик-орієнтованого підходу. Вимоги стандарту ДСТУ ISO 31000:2018 Менеджмент ризиків. Принципи та настанови. Процес реалізації управління інформаційними ризиками.
Розділ ІІ. Аналіз діяльності ПП "ІТ МАСТЕР СЕРВІС". Аналіз економічної діяльності підприємства. SWOT аналіз поточного стану підприємства Підходи та оцінка ймовірності настання кризових ситуацій на ПП "ІТ МАСТЕР СЕРВІС". Причини виникнення інформаційних ризиків діяльності. Наслідки впливу інформаційних ризиків на бізнес-процеси ПП "ІТ МАСТЕР СЕРВІС".
Розділ ІІІ. Практичні аспекти формування ризик-орієнтованого підходу в ПП "ІТ МАСТЕР СЕРВІС". Формування процедури ризик-орієнтованого підходу в інформаційну діяльність

компанії. Ідентифікація інформаційних ризиків діяльності. Розробка та аналіз ефективності заходів із запобігання інформаційним ризикам діяльності.
Висновки. У роботі здійснено детальний огляд підходів до виконання процесу Управління інформаційними ризиками в організації. Запропоновані практичні рекомендації щодо побудови такого процесу та запропоновано документовану процедуру його виконання.

5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень):
1. Організаційна структура приватного підприємства «ІТ МАСТЕР СЕРВІС».
2. Динаміка активів «ПП «ІТ МАСТЕР СЕРВІС» у 2019-2020 рр., тис. грн..
3. Співставлення рентабельності активів «ПП «ІТ МАСТЕР СЕРВІС» з інфляцією в Україні у 2020 р., %
4. Діаграма Ісікави. Втрата Інформації.
5. Цикл управління кібербезпекою.
6. Діаграма Ісікави. Ідентифікація інформаційних ризиків.
7. Визначення найвпливовіших загроз.
8. Узагальнений алгоритм реагування на небажанні події.
9. Порівняльна діаграма найвпливовіших загроз.

6. Консультанти розділів кваліфікаційної роботи

Розділ	**Ім'я, ПРІЗВИЩЕ, посада консультанта**	**Підпис, дата**	
		завдання видав	**завдання прийняв**
Вступ	Тетяна ЗБОРОВСЬКА, доцент закладу вищої освіти кафедри управління та забезпечення якості у фармації		
Розділ І	Тетяна ЗБОРОВСЬКА, доцент закладу вищої освіти кафедри управління та забезпечення якості у фармації		
Розділ ІІ	Тетяна ЗБОРОВСЬКА, доцент закладу вищої освіти кафедри управління та забезпечення якості у фармації		
Розділ ІІІ	Тетяна ЗБОРОВСЬКА, доцент закладу вищої освіти кафедри управління та забезпечення якості у фармації		
Висновки	Тетяна ЗБОРОВСЬКА, доцент закладу вищої освіти кафедри управління та забезпечення якості у фармації		

7. Дата видачі завдання: 17.10.2023 р.

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів кваліфікаційної роботи	Термін виконання етапів кваліфікаційної роботи	Примітка
1.	Формулювання мети, задач, об'єкту та предмету досліджень в рамках кваліфікаційної роботи	17.10.2023 р.	**виконано**
2.	Складання розширеного плану та опрацювання етапів виконання кваліфікаційної роботи	18.10.2023 р.	**виконано**
3.	Збір літературних джерел та проведення загального літературного огляду за напрямком теми	19.10.2023 р.	**виконано**
4.	Обґрунтування актуальності обраного напрямку досліджень, зведення статистичних даних	24.10.2023 р.	**виконано**
5.	Складання та оформлення вступу до кваліфікаційної роботи	26.10.2023 р.	**виконано**
6.	Складання та оформлення І-го розділу роботи (літературний огляд, теоретичні засади)	31.10.2023 р.	**виконано**
7.	Проведення аналізу об'єкту та предмету досліджень, аналіз ситуації на базі стажування	07.11.2023 р.	**виконано**
8.	Оформлення ІІ-го розділу роботи (аналітична частина) з формулюванням проблематики	21.11.2023 р.	**виконано**
9.	Розробка прикладних пропозицій для розв'язання визначених у ІІ-му розділі проблем	28.11.2023 р.	**виконано**
10.	Оформлення ІІІ-го розділу роботи з обґрунтуванням раціональності висунутих пропозицій	15.12.2023 р.	**виконано**
11.	Оформлення додатків до роботи (розроблених документів та форм, запропонованих заходів)	21.12.2023 р.	**виконано**
12.	Остаточне оформлення кваліфікаційної роботи та пред'явлення її для перевірки керівником	08.01.2024 р.	**виконано**
13.	Розробка мультимедійних слайдів та складання плану доповіді. Робота з рецензентами.	15.01.2024 р.	**виконано**
14.	Проходження попереднього захисту, коригування роботи, підготовка до офіційного захисту	22.01.2024 р.	**виконано**

Здобувач вищої освіти _____ Сергій ОБЛОГ

Керівник кваліфікаційної роботи _____ Тетяна ЗБОРОВСЬКА

ВИТЯГ З НАКАЗУ № 229
по Національному фармацевтичному університету
від 16 жовтня 2023 року

Про затвердження тем кваліфікаційних робіт

Затвердити теми кваліфікаційних робіт, керівників-консультантів та рецензентів здобувачам вищої освіти **2 курсу,** спеціальність – **073 Менеджмент**, освітня програма – **Якість, стандартизація та сертифікація**, ступінь вищої освіти – **магістр**, термін навчання – **1 р. 6 міс.**, очна (**денна**) та **заочна** форми здобуття освіти.

Прізвище, ім'я по батькові здобувача вищої освіти	**Тема кваліфікаційної роботи** (українською мовою)	**Тема кваліфікаційної роботи** (англійською мовою)	**Керівник кваліфікаційної роботи**	**Рецензент кваліфікаційної роботи**
Облог Сергій Володимирович	Розробка процедури Управління інформаційними ризиками в організації	Development of the information risk management procedure in the organization	к.фарм.н., доцент, доцент ЗВО кафедри управління та забезпечення якості у фармації, Зборовська Т. В.	д.фарм.н., професор, професор ЗВО кафедри фармацевтичного менеджменту та маркетингу НФаУ Ткачова О. В.

В.о. ректора **Алла КОТВІЦЬКА**

Вірно:
Декан факультету фармацевтичних технологій та менеджменту **Наталія ЖИВОРА**

Ф А2.8-47-110

ВИСНОВОК

Комісії з академічної доброчесності про проведену експертизу

щодо академічного плагіату у кваліфікаційній роботі

здобувача вищої освіти

№ 125768 від «29» січня 2024 р.

Проаналізувавши випускну кваліфікаційну роботу за магістерським рівнем здобувача вищої освіти денної форми навчання Облог Сергія Володимировича, 2 курсу, _____ групи, спеціальності 073 Менеджмент , на тему: «Розробка процедури Управління інформаційними ризиками в організації / Development of the information risk management procedure in the organization», Комісія з академічної доброчесності дійшла висновку, що робота, представлена до Екзаменаційної комісії для захисту, виконана самостійно і не містить елементів академічного плагіату (компіляції).

Голова комісії,
професор **Інна ВЛАДИМИРОВА**

1%

6%

ВІДГУК

наукового керівника на кваліфікаційну роботу другого (магістерського) ступеня вищої освіти спеціальності 073 Менеджмент освітньої програми Якість, стандартизація та сертифікація

Сергія ОБЛОГА

на тему "Розробка процедури Управління інформаційними ризиками в організації"

Актуальність теми. В умовах сьогодення, а саме фінансової, політичної нестабільності в Україні, підвищеної конкуренції між підприємствами, актуальним постає питання вивчення сучасних підходів до управління та розвитку, які б допомогли оперативно реагувати на непередбачувані зміни та впливи зовнішнього та внутрішнього середовища. Актуальним питанням для будь-яких організацій є і буде приділення достатньої уваги до забезпечення захисту комерційної інформації. Грамотна побудова системи безпеки з урахуванням потенційних ризиків є одним з важливих етапів збереження комерційної таємниці, втрата або розповсюдження якої може, а іноді навіть і фатально, вплинути на діяльність компанії та її позицію на ринку.

Практична цінність висновків, рекомендацій та їх обґрунтованість. Проаналізовані у роботі дані літературних джерел і досвід Європейських країн щодо цього питання дали автору підставу проведення аналізу діяльності ПП «ІТ МАСТЕР СЕРВІС» щодо підходів до формування процедури управління інформаційними ризиками, а також алгоритму розробки рекомендацій щодо побудови системи управління інформаційною безпекою для оцінки ризиків даного підприємства. Результати дослідження будуть практично використовуватися в діяльності ПП «ІТ МАСТЕР СЕРВІС».

Оцінка роботи. У процесі виконання кваліфікаційної роботи здобувач опанував навички роботи з науковою літературою, навчився збирати, систематизувати, аналізувати, узагальнювати інформацію, закріпив набуті протягом навчання теоретичні знання та практичні навички. Кваліфікаційна робота належно оформлена і написана лаконічною науковою мовою, містить необхідні структурні елементи та посилання на актуальні джерела літератури.

Загальний висновок та рекомендації про допуск до захисту. Враховуючи вищенаведене, вважаю, що робота здобувача 2-го курсу спеціальності 073 Менеджмент освітньої програми Якість, стандартизація та сертифікація Сергія ОБЛОГА на тему "Розробка процедури Управління інформаційними ризиками в організації" за обсягом та змістом відповідає вимогам, що висуваються до кваліфікаційних робіт вищих навчальних закладів IV рівня акредитації і може бути представлена до захисту в Екзаменаційну комісію Національного фармацевтичного університету.

Науковий керівник
доцент закладу вищої освіти кафедри управління
та забезпечення якості у фармації
канд. фармац. наук, доц. _____ Тетяна ЗБОРОВСЬКА
“16” січня 2024 року

РЕЦЕНЗІЯ

на кваліфікаційну роботу здобувача другого (магістерського) ступеня вищої освіти спеціальності 073 Менеджмент освітньої програми Якість, стандартизація та сертифікація

Сергія ОБЛОГА

на тему "Розробка процедури Управління інформаційними ризиками в організації".

Актуальність теми. У складних умовах фінансової і політичної нестабільності в Україні та існуючої конкуренції між підприємствами, актуальним є питання оцінки ризиків у процесі їх професійної діяльності. Багато комерційних підприємств намагаються використати різні інноваційні рішення та впровадити новітні інформаційні технології для забезпечення своєї конкурентоспроможності у певному сегменті ринку, але при цьому не повинні забувати про те, що будь-які нововведення вимагають особливих підходів до системи управління інформаційною безпекою, яка базується на управлінні ризиками.

Теоретичний рівень роботи. Аналіз літературних джерел дав розуміння ситуації щодо питання інформаційних загроз та сучасних шляхів їх вирішення, аналіз проведений автором, довів важливість та необхідність розробки схеми впровадження заходів кіберзахисту в загальну систему управління підприємства для подальшої їх імплементації в діяльність.

Пропозиції автора з теми дослідження. Виходячи з актуальності питання, основною метою роботи Сергія ОБЛОГА стала розробка процедури управління інформаційними ризиками, що виникають в діяльності комерційних підприємств. Автор кваліфікаційної роботи пропонує певні рекомендації для побудови системи управління інформаційною безпекою на ПП «ІТ МАСТЕР СЕРВІС».

Практична цінність висновків, рекомендацій та їх обґрунтованість. Результатами даної роботи є проведення аналізу діяльності ПП «ІТ МАСТЕР СЕРВІС» щодо підходів до формування процедури управління інформаційними ризиками, а також розробка рекомендацій щодо побудови системи управління інформаційною безпекою для оцінки ризиків даного підприємства.

Недоліки роботи. У роботі присутні стилістичні та орфографічні помилки, є зауваження до оформлення окремих літературних посилань, але це не впливає на зміст та значущість, а також на загальне позитивне враження від роботи.

Загальний висновок і оцінка роботи. Кваліфікаційна робота належно оформлена і написана лаконічною науковою мовою, містить необхідні структурні елементи та посилання на джерела літератури.

Враховуючи вищенаведене, вважаю, що робота здобувача 2-го курсу спеціальності 073 Менеджмент освітньої програми Якість, стандартизація та сертифікація Сергія ОБЛОГА на тему "Розробка процедури Управління інформаційними ризиками в організації" за обсягом та змістом відповідає вимогам, що висуваються до випускових робіт вищих навчальних закладів IV рівня акредитації і може бути представлена до захисту в Екзаменаційну комісію Національного фармацевтичного університету.

Рецензент
професор закладу вищої освіти кафедри
фармацевтичного менеджменту і маркетингу,
д-р.фармац.наук, професор _____ Оксана ТКАЧОВА
“25” січня 2024 року

ВИТЯГ З ПРОТОКОЛУ № 6
засідання кафедри управління за забезпечення якості у фармації НФаУ

від «19» січня 2024 р.

ГОЛОВУЮЧИЙ: д.фарм.н., проф. Крутських Т.В.
СЕКРЕТАР: к.фарм.н., доц. Лісна А.Г.
ПРИСУТНІ: зав. каф., проф. Крутських Т.В., проф. Коваленко С.М., проф. Посилкіна О.В., проф. Літвінова О.В., проф. Братішко Ю.С., доц. Баєва О.І., доц. Гладкова О.В., доц. Глєбова Н.В., доц. Деренська Я.М., доц. Зборовська Т.В., доц. Коляда Т.А., доц. Ковальова В.І., доц. Лісна А.Г., доц. Ткаченко О.В., доц. Мороз С.Г., здобувач вищої освіти Облог С.В.

ПОРЯДОК ДЕННИЙ:

1. Попередній захист кваліфікаційної роботи здобувача вищої освіти спеціальності 073 Менеджмент, освітньої програми Якість, стандартизація та сертифікація другого (магістерського) рівня Сергія ОБЛОГА на тему «Розробка процедури Управління інформаційними ризиками в організації».

СЛУХАЛИ: доповідь до кваліфікаційної роботи здобувача вищої освіти спеціальності 073 Менеджмент, освітньої програми Якість, стандартизація та сертифікація другого (магістерського) рівня Сергія ОБЛОГА на тему «Розробка процедури Управління інформаційними ризиками в організації».

УХВАЛИЛИ: допустити Сергія ОБЛОГА до захисту кваліфікаційної роботи на засіданні Екзаменаційної комісії.

Зав. кафедри управління та забезпечення якості у фармації, професор _____ **Тетяна КРУТСЬКИХ**

Секретар кафедри _____ **Анастасія ЛІСНА**

НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ

ПОДАННЯ
ГОЛОВІ ЕКЗАМЕНАЦІЙНОЇ КОМІСІЇ
ЩОДО ЗАХИСТУ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Направляється здобувач вищої освіти Сергій ОБЛОГ до захисту кваліфікаційної роботи
за галуззю знань 07 Управління та адміністрування
спеціальністю 073 Менеджмент
освітньою програмою Якість, стандартизація та сертифікація
на тему: "Розробка процедури Управління інформаційними ризиками в організації"

Кваліфікаційна робота і рецензія додаються.

Декан факультету _____ / Наталія ЖИВОРА

Висновок керівника кваліфікаційної роботи

Здобувач вищої освіти Сергій ОБЛОГ підготував кваліфікаційну роботу, яка відповідає всім вимогам, виконана у встановлені строки, має наукову новизну та може бути рекомендована до захисту.

Керівник кваліфікаційної роботи Тетяна ЗБОРОВСЬКА

_____

“18” січня 2024 року

Висновок кафедри про кваліфікаційну роботу

Кваліфікаційну роботу розглянуто. Здобувач вищої освіти Сергій ОБЛОГ допускається до захисту даної кваліфікаційної роботи в Екзаменаційній комісії.

Завідувачка закладу вищої освіти кафедри
Управління та забезпечення якості у фармації

_____ Тетяна ЗБОРОВСЬКА

“19” січня 2024 року

Кваліфікаційну роботу захищено

у Екзаменаційній комісії

13 лютого 2024 року

З оцінкою _____

Голова Екзаменаційної комісії:

доктор наук з державного управління, кандидат економічних наук, професор, заслужений діяч науки і техніки України
професор кафедри публічного управління та підприємництва Національний аерокосмічний університет імені М.Є. Жуковського "Харківський авіаційний інститут"
Андрій ДЄГТЯР

_____
(підпис)