Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет ___інформаційно-аналітичних технологій та менеджменту_____
(повна назва)
Кафедра _ _економічної кібернетики та управління економічною безпекою__
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____

_____Управління ризиками для забезпечення безпеки ІТ-підприємства____
_____
(тема)

Виконав:
студент _2_ курсу, групи __УФЕБм-18-1__
_____Лотвінова В.В_____
(прізвище, ініціали)

Спеціальність __073 Менеджмент_____
_____
(код і повна назва спеціальності)
Тип програми _ _освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)
Освітня програма ___Управління фінансово-економічною безпекою_____
(повна назва освітньої програми)

Керівник _____к.е.н. Кирій В.В._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ ____Полозова Т.В.__
(підпис) (прізвище, ініціали)

2019 р.

Харківський національний університет радіоелектроніки

Факультет__інформаційно-аналітичних технологій та менеджменту_
(повна назва)

Кафедра_економічної кібернетики та управління економічною безпекою___
(повна назва)

Рівень вищої освіти _____другий (магістерський)_____

Спеціальність _____073 Менеджмент_____
(код і повна назва)

Тип програми _____освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)

Освітня програма _____Управління фінансово-економічною безпекою_____
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«_____»_____ 20 ___ р.

ЗАВДАННЯ

НА АТЕСТАЦІЙНУ РОБОТУ

студентові_____Лотвіновій Вікторії Василівні_____
(прізвище, ім'я, по батькові)

1. Тема роботи _Управління ризиками для забезпечення безпеки ІТ-підприємства_____
_____
_____
затверджена наказом університету від _31_ ___жовтня_____2019 р. № _1599 Ст_
2. Термін подання студентом роботи до екзаменаційної комісії _13_ __грудня____ 2019 р.
3. Вихідні дані до роботи _Наукові літературні джерела, періодичні видання, фінансова звітність підприємства, електронні джерела_____
_____
_____
_____
_____
_____
4. Перелік питань, що потрібно опрацювати в роботі _____
Вступ. 1 Методичні аспекти управління ризиками для забезпечення безпеки високотехнологічних підприємств. 2 Техніко-економічний аналіз діяльності ІТ-компанії Appus Software та оцінка системи ризик-менеджменту на підприємстві . 3 Удосконалення системи управління ризиками ІТ-підприємства. Висновки. Перелік джерел посилання. Додаток А. Додаток Б. Додаток В. Додаток Г. Додаток Д. Додаток Е._____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій

1. Структура змісту ризиків.
2. Структура зовнішніх та внутрішніх ризиків.
3. Функціональні складові економічної безпеки.
4. Етапи загального плану управління ризиками.
5. Організаційна структура IT-підприємства Appus Software.
6. Концептуальні поняття JIRA.
7. Матриця SWOT аналізу для IT-підприємства Appus Software.
8. Загальна схема керування ризиками проекту.
9. Зовнішні ризики IT-компанії.
10. Комерційні ризики IT-компанії.
11. Управлінські ризики IT-компанії.
12. Ризики технічного характеру для IT-компанії.
13. Категорії ризиків, ідентифікованих на проекті.

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів роботи	Примітка
1	Методичні аспекти управління ризиками для забезпечення безпеки високотехнологічних підприємств	04.11.19-10.11.19	виконано
2	Техніко-економічний аналіз діяльності IT-компанії Appus Software та оцінка системи ризик-менеджменту на підприємстві	11.11.19-17.11.19	виконано
3	Удосконалення системи управління ризиками IT-підприємства	18.11.19-25.11.19	виконано
4	Оформлення атестаційної роботи	26.11.19-30.11.19	виконано
5	Перевірка атестаційної роботи на плагіат	01.12.19-03.12.19	виконано
6	Підготовка доповіді та ілюстративного матеріалу	04.12.19-08.12.19	виконано
7	Рецензування атестаційної роботи	09.12.19-12.12.19	виконано

Дата видачі завдання 04 листопада 2019 р.

Студент _____
(підпис)

Керівник роботи _____ к.е.н Кирій В.В
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Атестаційна робота: 95 с., 9 табл., 14 рис., 65 джерел, 6 додатків.

ФІНАНСОВО-ЕКОНОМІЧНА БЕЗПЕКА, РИЗИК, РИЗИК-МЕНЕДЖМЕНТ, ІТ-КОМПАНІЯ, ПРОЕКТ.

Об’єктом дослідження є процес організації забезпечення безпеки на основі ризик-менеджменту в ІТ-підприємстві.

Метою роботи є розвиток теоретичних положень ризик-менеджменту ІТ-підприємств та розробка практичних рекомендацій з організації забезпечення безпеки на основі управління ризиками.

В роботі надано визначення сутності ризику, проведена їх класифікація, наведена оцінки впливу ризиків на діяльність підприємства в цілому та на його безпеку. Розглянуто та проаналізовано визначення економічної безпеки підприємства, що наведено в наукові й та учбовій літературі провідними фахівцями. Визначено, що ризик-менеджмент є одним з найкращих інструментів забезпечення безпеки підприємства. Надано етапи, які використовуються для формування загального процесу управління ризиками.

Розглянута загальна характеристика підприємства, проаналізовано основний перелік робіт та послуг компанії, описана організаційна структура ІТ-підприємства, надано опис системи управління. Проведено техніко-економічний аналіз фінансово-економічного стану підприємства, проаналізовано динаміку показників використання трудових ресурсів, їх вікова та освітня характеристика, описано ризики діяльності ІТ-компанії Appus Software. Надано загальні рекомендації щодо створення системи управління ризиками.

Надано типові категорії ризиків для ІТ-підприємства, побудовано RBS типову для ІТ-компанії, надано кроки для складання плану управління ризиками ІТ-проекту та розроблена практична реалізація плану керування ризиками для ІТ- компанії Appus Software.

ABSTRACT

Master thesis: 95 p., 9 tables, 14 fig., 65 sources, 6 exhibits.

FINANCIAL AND ECONOMIC SECURITY, RISK, RISK MANAGEMENT, IT COMPANY, PROJECT.

The object of the study is the process of risk-based security management in an IT enterprise.

The purpose of the work is to develop the theoretical positions of risk management of IT enterprises and to develop practical recommendations for security management based on risk management.

The paper defines the nature of risk, their classification, assesses the impact of risk on the enterprise as a whole and on its safety. The definition of economic security of the enterprise, which is presented in the scientific and educational literature by leading experts, is considered and analyzed. It has been determined that risk management is one of the best tools for ensuring the security of an enterprise. The steps that are used to shape the overall risk management process are presented.

The general characteristic of the enterprise is considered, the main list of works and services of the company is analyzed, the organizational structure of the IT enterprise is described, the management system is described. A technical and economic analysis of the financial and economic state of the enterprise is conducted, the dynamics of indicators of the use of labor resources, their age and educational characteristics are analyzed, the risks of the activity of the IT company Appus Software are described. General guidance is provided on setting up a risk management system.

Typical IT enterprise risk categories were provided, an RBS typical IT company was built, steps were taken to develop an IT project risk management plan, and a practical implementation of the risk management plan for the IT company Appus Software.

ЗМІСТ

ВСТУП

У сучасних умовах питання управління безпекою ІТ-підприємства є актуальними, оскільки означені підприємства працюють в умовах високої інтенсивності змін зовнішнього середовища, прямої та опосередкованої дії зовнішніх і внутрішніх ризиків, конкурентне середовище приховує багаточисленні загрози. Перманентна новизна виробничої діяльності, переважно інноваційний її характер у сфері ІТ призводять значною мірою до зростання незахищеності підприємництва та підприємницьких ризиків. Підприємницький ризик оцінюється ймовірністю виникнення непередбачених проектами та рівнем втрат економічних ресурсів у випадку його настання.

ІТ-компанії в процесі діяльності щоденно стикаються з різними ризиками. Проте управління ризиками поки не займає в більшості ІТ-підприємств чільне місце.

Управління ризиками давно вже стало однією з ключових дисциплін менеджменту. У ряді галузей розвитку культури управління ризиками сприяють вимоги вітчизняних і міжнародних регуляторів. Однак у багатьох інших галузях підприємства приходять до необхідності системно управляти своїми ризиками, у міру того як досягають певного рівня організаційної зрілості. Схоже, щось подібне відбувається і з українськими ІТ-підприємствами: в більшості з них управлінню ризиками сьогодні приділяється явно недостатня увага.

Теоретичні засади економічної безпеки вивчалися такими вченими як Н. Подлужна, Н. Капустін, Д. Пілова, В.Пономарьова, О.Васюк, С.Ілляшенко. Незважаючи на важливість наукових досліджень в них не знайшли відображення деякі теоретичні та методичні питання, пов'язані із безпекою та ризиками ІТ-підприємства. Саме це і визначило актуальність роботи.

Метою роботи є розвиток теоретичних положень ризик-менеджменту ІТ-підприємств та розробка практичних рекомендацій з організації забезпечення безпеки на основі управління ризиками.

Мета дослідження визначила наступні завдання:

– дослідити теоретичні основи безпеки підприємства, ризиків, ризик-менеджменту;

– провести техніко-економічний аналіз ІТ-підприємства Appus Software;

– надати характеристику існуючої в ІТ-підприємства Appus Software систему управління ризиками;

– визначити та класифікувати існуючи ризики ІТ-компанії

– розробити план управління ризиками проектів.

Об’єкт дослідження – процес організації забезпечення безпеки на основі ризик-менеджменту в ІТ-підприємстві.

Предмет дослідження – методи та засоби ідентифікації та управління ризиками для забезпечення безпеки в ІТ-підприємствах.

Під час дослідження були використані методи аналізу та синтезу інформації, яка характеризує управління безпекою ІТ-компаній; порівняння та узагальнення категорій ризиків для ІТ-компаній; інтерпретація висновків, що випливають з результатів аналізу ситуації, яка складається у забезпеченні безпеки ІТ-компаній.

Для досягнення поставленої мети використовувались наступні методи дослідження – табличний, графічний, SWOT аналіз.

Методологічну та теоретичну основу роботи складають існуючі праці українських та зарубіжних науковців, законодавчі та нормативні акти. Інформаційну основу складають звітні та поточні матеріали суб’єкта господарської діяльності, дані періодичних видань, спеціальна наукова література, Інтернет.

Практичне використання розроблених підходів, обґрунтованість і достовірність отриманих результатів полягає в розробці організації забезпечення безпеки за допомогою введення ризик-менеджменту.

Практична значущість отриманих результатів полягає у тому, що запропоновані практичні рекомендації можуть бути використані IT-підприємствами для введення у свою діяльність ризик-менеджмент.

1 МЕТОДИЧНІ АСПЕКТИ УПРАВЛІННЯ РИЗИКАМИ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ВИСОКОТЕХНОЛОГІЧНИХ ПІДПРИЄМСТВ

1.1 Теоретичні засади управління ризиками

Ведення бізнесу супроводжується різними видами ризиків та небезпек. Деякі з цих потенційних небезпек можуть зруйнувати бізнес, а інші можуть завдати серйозної шкоди, усунення якої може бути дорогим та трудомістким процесом. Незважаючи на ризики, пов'язані з веденням бізнесу, керівники та менеджери з управління ризиками можуть передбачати та готуватися до потенційних ризиків незалежно від розміру бізнесу.

Бізнес-ризики – це фактори, які впливають на компанію, та можуть призвести до зниження прибутку компанії або її банкрутству.

Все, що загрожує можливості компанії досягти своєї мети або досягти своїх фінансових цілей, називається бізнес-ризиком. Ці ризики походять з різних джерел, тому не завжди винен керівник компанії чи менеджер. Натомість ризики можуть надходити з інших джерел фірми або можуть бути зовнішніми - від законодавства до загальної економіки.

Багато дослідників підприємницької діяльності особливо виділяють найбільшу його особливість - наявність ризику як на стадії створення нового підприємства, так і на стадії його подальшого функціонування. Вперше дві такі категорії, як «ризик» і «підприємець», пов'язав Річард Кантильон, який писав, що підприємець - це людина, яка діє в умовах ризику. Адам Сміт у своїй роботі «Дослідження про природу і причини багатства народів» підкреслював, що підприємець як власник йде на економічний ризик заради реалізації якоїсь комерційної ідеї та отримання прибутку.

Основні види ризику.

Стартегічний ризик. Оскільки бізнес намагається досягти стратегічних цілей, внутрішні та зовнішні події можуть стримувати або заважати їх виконувати. Це відомо як стратегічний ризик.

Стратегічні ризики можна визначити як:

– потенційний вплив стратегічних рішень або невідповідна стратегія;

– відсутність чутливості до змін у галузі;

– ризики, пов'язані з майбутніми планами, наприклад, вихід на нові ринки, розширення існуючих послуг тощо.

Управління стратегічними ризиками має бути зосереджено не лише на викликах, які можуть спричинити збій конкретної стратегії, а на будь-яких основних ризиках, які можуть вплинути на довгострокове позиціонування та результативність компанії.

Стратегічний ризик може виникати з будь-якої з наступних дій:

– злиття, поглинання та інша конкуренція;

– зміни ринку або галузі;

– зміни серед клієнтів або попиту;

– управління змінами;

– кадрові питання, такі як персонал;

– фінансові проблеми з грошовим потоком, тиском капіталу чи витратами;

– IT-катастрофи та несправність обладнання;

– питання стосунків, наприклад, з постачальниками;

– пошкодження репутації.

Наприклад, можливість американської компанії придбати одного з європейських конкурентів становитиме стратегічний ризик. Таке придбання дало б американській компанії дистрибуцію у Великобританії, зробивши їх безпосереднім конкурентом. У цій ситуації можна врахувати:

– будь-які американські компанії, які мають готівку / ціну акцій, щоб зробити це;

– будь-які європейські конкуренти, які, ймовірно, цілі поглинання - наприклад, через фінансові проблеми;

– перспектива американської компанії знизити ціни або запустити нові продукти, щоб конкурувати проти вас.

Ризики відповідності та регуляторні ризики випливають із законів та нормативних актів, які регулюють діяльність бізнесу. Регуляторний ризик це вплив зміни законів та нормативно-правових актів, які потенційно можуть спричинити збитки для вашого бізнесу, сектора чи ринку.

Регуляторні ризики можуть, наприклад:

– збільшити витрати на ведення бізнесу – наприклад, витрати на досягнення відповідності новим законам;

– змінити конкурентний ландшафт – наприклад, можливо, недійсна модель вашого бізнесу;

– зробити ділову практику незаконною – наприклад, нові правила зміни закону щодо маркетингу;

– зменшити привабливість інвестицій.

Наприклад, товари чи послуги можуть стати менш відповідними для продажу, якщо ввести нові закони чи податки. Так було у минулому з тютюном. Введення жорстких норм щодо маркування харчових продуктів аналогічно порушило харчову промисловість, підвищивши витрати і зменшивши привабливість певних видів продуктів харчування.

Нові правила можуть мати широкий вплив на стратегічний напрямок та бізнес-модель. Тому важливо враховувати нормативні вимоги, під час оцінки бізнес-ризиків.

Ризик відповідності пов'язаний з можливістю вашого бізнесу порушити закон чи положення. Часто ризик відповідності зумовлений такими діями:

– недостатня кількість систем управління;

– відсутність підготовки;

– відсутність належної ретельності;

– людська помилка.

Ризики дотримання вимог можуть потенційно піддавати бізнес ряду наслідків, включаючи:

– юридичні покарання;
– недійсні договори;
– фінансові конфіскації;
– матеріальні втрати;
– втрати можливостей для бізнесу;
– пошкоджена репутація.

Хоча ризики дотримання в основному пов'язані з необхідністю дотримання законів та правил, вони також можуть стосуватися необхідності діяти так, як очікують інвестори та клієнти. Наприклад, шляхом забезпечення належного корпоративного управління.

Фінансовий ризик – це здатність вашого бізнесу управляти своїм боргом та виконувати свої фінансові зобов'язання. Цей тип ризику, як правило, виникає через нестабільність, втрати на фінансовому ринку або рух цін на акції, валюти, процентні ставки тощо.

Фінансовий ризик пов'язаний з основною життєздатністю бізнесу. Це стосується здатності отримувати прибуток і покривати свої операційні витрати, такі як зарплата, оренда, виробничі витрати та офісні витрати.

З іншого боку, фінансовий ризик пов'язаний з витратами на фінансування та сумою боргу, який ви несете для фінансування своїх операцій.

До загальних категорій фінансового ризику належать:

– ринковий ризик;
– кредитний ризик;
– ризик ліквідності;
– операційний ризик.

Ринковий ризик пов'язаний з ймовірністю понести збитки через такі зміни, як волатильність ринку, підвищення процентних ставок або витрат на сировину, коливання цінностей в іноземній валюті тощо. Наприклад, зміни курсу валюти вплинуть на погашення боргу та конкурентоспроможність ваших товарів і послуг порівняно з товарами, що виробляються за кордоном.

Кредитний ризик - це ймовірність несплати грошей кредиторові (наприклад, банку або позикодавцю) або іншій стороні (наприклад, постачальнику). Також можна нести кредитний ризик, надаючи клієнтам кредит через можливість їх дефолту в оплаті.

Ризик ліквідності впливає на здатність відповідати короткостроковим фінансовим вимогам для здійснення бізнес-операцій. Основними джерелами ризику є потенційні проблеми грошового потоку через такі причини, як сезонне падіння доходів, відсутність покупців активів або неефективний ринок.

Операційний ризик – це ймовірність понести збитки через негативний вплив процедур, систем чи політик, які є у бізнесі. Поширені джерела включають технічні збої, шахрайські дії, помилки працівників тощо. Операційний ризик зосереджений на функціонуванні бізнесу. Зазвичай це пов'язано з тим, як бізнес функціонує та охоплює такі категорії:

– шахрайство – наприклад, хабарництво, нецільове використання активів та ухилення від сплати податків;

– інша злочинна діяльність – наприклад, крадіжка даних, злом тощо;

– політики та безпека на робочому місці – наприклад, дискримінація, здоров'я та безпека персоналу;

– продукти та ділова практика – наприклад, дефекти товару або маніпулювання ринком;

– фізичні цінності – наприклад, вандалізм, стихійні лиха, обслуговування обладнання тощо;

– бізнес-зриви – наприклад, простої комунальних послуг, збої в роботі ІТ-систем тощо;

– управління процесами – наприклад, помилки бухгалтерського обліку, помилки введення даних, неподання звітності.

Ці ризики становлять різний рівень загрози для бізнесу – від незначних незручностей до потенційного, що може поставити під загрозу саме його існування. Не варто недооцінювати потенційний вплив операційного ризику.

Якщо операційні ризики реалізуються, вони можуть завдати значної шкоди вашому бізнесу, включаючи:

– великі витрати – наприклад, витрати на усунення несправності системи або помилку обробки;

– регуляторні накладні витрати –наприклад, витрати на аудит або мандатні розслідування;

– збиток репутації – наприклад, як наслідок шахрайської діяльності чи недобросовісної практики.

На відміну від інших видів ділових ризиків, операційні ризики, як правило, не залежать від прибутків або збитків. Деякі організації сприймають їх як неминучу вартість ведення бізнесу.

На рисунку 1.1 наведена структура змісту ризиків.

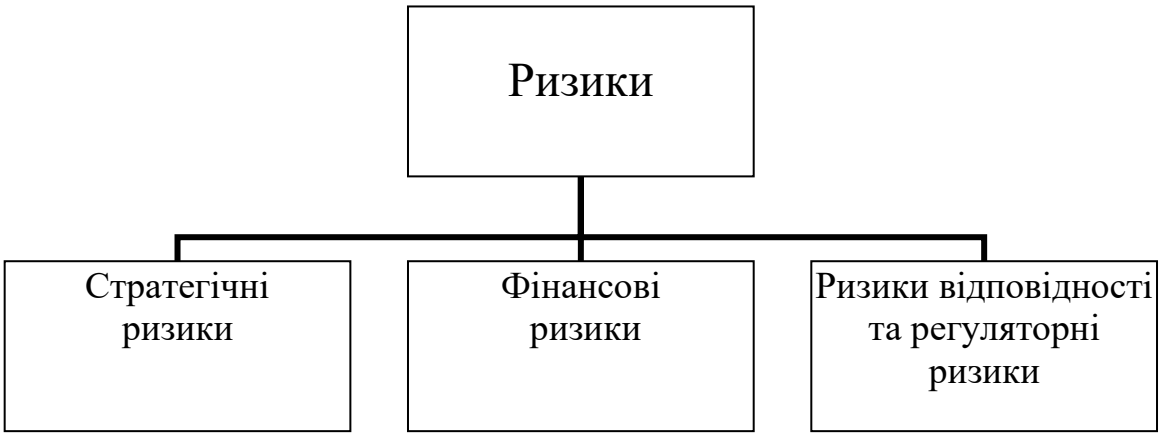

Рисунок 1.1 – Структура змісту ризиків

Також ризики бувають систематичні та несистематичні.

Несистематичний ризик пов'язаний зі специфікою діяльності фірми, складнощами її функціонування, а також з проблемами галузі, в якій вона діє. Він може бути подоланий за допомогою диверсифікації. Для підприємця найбільш складною проблемою є оцінка недиверсифікованого ризику, так як важко передбачити можливість виникнення даного типу ризику і його наслідки.

Систематичний ризик характерний для всієї економічної системи або окремого ринку і не піддається диверсифікації. Даний тип ризику визначається факторами, що впливають на всі галузі і підприємства: можливі політичні зміни в країні і світі, рівень інфляції, економічні коливання і т.д.

Ризики, за природою виникнення, можна поділити на зовнішні та внутрішні. Внутрішні ризики виникають зсередини організації та виявляються під час звичайних операцій компанії. Ці ризики можна прогнозувати з певною надійністю, а отже, компанія має можливість зменшити внутрішній бізнес-ризик.

Існує три типи внутрішніх факторів ризику – це людські фактори, технологічні та фізичні фактори.

Ризик людського фактору може включати:

– союзні страйки;
– нечесність працівників;
– неефективне управління або керівництво;
– невдача з боку зовнішніх виробників чи постачальників;
– злочинність або відверта несплата з боку клієнтів та замовників.

Проблеми з персоналом можуть становити операційні проблеми. Персонал, який захворів або травмується і, як наслідок, не може працювати, може зменшити виробництво. Для успіху компанії, можливо, компанії знадобиться найняти або замінити персонал. Страйки можуть змусити бізнес закритись;

Технологічний ризик включає непередбачені зміни у виробництві, доставці чи розповсюдженні товару чи послуги компанії.

Наприклад, технологічний ризик, з яким може зіткнутися бізнес, включає застарілі операційні системи, що знижують виробничу здатність або перебої в постачанні чи запасах;

Фізичний ризик - це втрата або пошкодження активів компанії.

Компанія може знизити внутрішні ризики шляхом хеджування впливу цих трьох типів ризику. Наприклад, компанії можуть отримати страхування кредитів за їхньою дебіторською заборгованістю через комерційних страховиків, забезпечуючи захист клієнтів, які не сплачують свої рахунки. Кредитне страхування, як правило, дуже всебічне і забезпечує захист від несплати боргу з широкого кола причин, охоплюючи практично кожну можливу комерційну або політичну причину невиплати.

Зовнішні ризики виникають через економічні події, що виникають поза корпоративної структури. Зовнішні події, що призводять до зовнішнього ризику, не може контролювати жодна компанія та вони не можуть бути прогнозовані з високим рівнем надійності. Тому важко зменшити супутні ризики.

До трьох типів зовнішніх ризиків належать економічні фактори, природні фактори та політичні фактори.

Економічний ризик включає зміни ринкових умов. Наприклад, загальний економічний спад може призвести до раптової, несподіваної втрати доходу.

До природних факторів ризику належать стихійні лиха, які впливають на звичайні господарські операції. Наприклад, землетрус може вплинути на здатність роздрібного бізнесу залишатися відкритим протягом декількох днів або тижнів, що призведе до різкого зниження загальних продажів за місяць. Це також може завдати шкоди будівлі та товарам, які продаються.

Політичний ризик складається із змін у політичному середовищі чи урядовій політиці, які стосуються фінансових справ.

Підвищення процентних ставок, зміни законів про імпорт / експорт, тарифи, податки та інші нормативні акти можуть негативно впливати на бізнес.

Оскільки зовнішні ризики неможливо передбачити з точністю, компанії важко зменшити ці три фактори ризику. Деякі види кредитного страхування можуть захистити компанію від політичних подій в інших країнах, таких як війна, страйки, конфіскація, торговельні ембарго та зміни в імпортному / експортному законодавстві. Структура зовнішніх та внутрішніх ризиків наведена на рисунку 1.2.

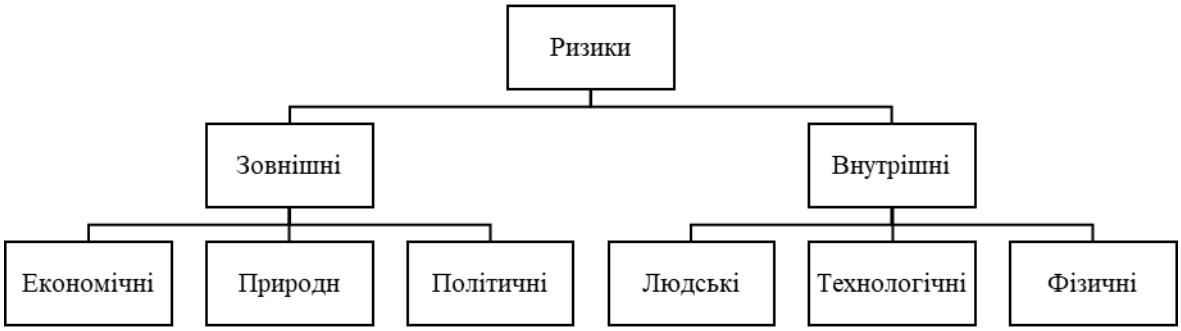

Рисунок 1.2 – Структура зовнішніх та внутрішніх ризиків

Ризик завжди пов’язаний із поняттям безпеки. Забезпечення безпеки підприємства є одним з головних завдань менеджменту.

1.2 Економічна сутність безпеки підприємств

Аналіз розуміння сутності економічної безпеки підприємства показав, що у своєму становленні ця категорія значно еволюціонувала - первісне поняття економічної безпеки розглядалося як гарантування умов збереження

комерційної таємниці й інших секретів підприємства (такому трактуванню економічної безпеки присвячені публікації початку 90-х років минулого сторіччя) до сучасних трактувань - як забезпечення стійкого і динамічного розвитку підприємства в умовах негативного впливу зовнішнього середовища.

Проведений аналіз свідчить: ставлення вітчизняних економістів до сутності економічної безпеки було неоднорідне. Існувало декілька основних підходів, які, з певною часткою умовності, можна назвати як «інформаційний», «зовнішній» та «ресурсно-функціональний». У рамках інформаційного підходу пропонувалося досліджувати виходячи з постулату, що ступінь надійності всієї системи зберігання інформації визначається рівнем безпеки найслабшої її ланки, яким вважається персонал організації. Вадою цього підходу є зведення проблеми економічної безпеки тільки до захисту інформації та комерційної таємниці, що не враховує всього спектру впливу зовнішнього середовища як основного джерела небезпек для діяльності підприємства та внутрішніх загроз його діяльності.

З позицій впливу зовнішнього середовища, захисту підприємств від його негативного впливу розглядається зміст категорії економічної безпеки підприємства у контексті «зовнішнього» підходу. Так Т. Ковальов і Т. Сухорукова тлумачать економічну безпеку як «…захищеність його діяльності від негативного впливу зовнішнього оточення, а також здатність своєчасно усунути різноманітні загрози або пристосуватись до існуючих умов, що не відбиваються негативно на їх діяльності»[26]. М. Бендиків зауважує, що під економічною безпекою слід розуміти «…захищеність його науково-технічного, технологічного, виробничого та кадрового потенціалу від прямих (активних) або непрямих (пасивних) загроз» [5]. Н.О. Подлужна наголошує, що «…економічна безпека підприємства є характеристикою системи, що самоорганізується і саморозвивається, – це стан, при якому

економічні параметри дозволяють зберегти головні її властивості: рівновагу і стійкість при мінімізації загроз» [45].

Цієї позиції дотримувалася переважна більшість вітчизняних економістів: Н. Капустін пропонує розглядати економічну безпеку суб'єкта господарювання як «…сукупність чинників, які забезпечують його незалежність, стійкість, здатність до прогресу в умовах дестабілізуючих факторів» [23]. Д.П. Пілова - «…як здатність підприємства чинити опір сукупному впливу загроз макро- та мікросередовищ з метою досягнення своєї стратегічної мети в результаті усіх видів діяльності» [43] . Цікавою в цьому аспекті є аргументація В.П. Пономарьова, який пропонує досліджувати проблему економічної безпеки через призму гармонізації його інтересів з інтересами суб'єктів зовнішнього середовища, економічну безпеку підприємства запропоновано розглядати «..як міру гармонізації в часі і просторі економічних інтересів підприємства з інтересами пов'язаних із ним суб'єктів зовнішнього середовища, що діють поза межами підприємства» [46]. Як зазначає О.С. Власюк, «генеза категорії «економічна безпека» базується на таких поняттях, як інтереси, потреби, цінності, цілі, загрози. Реалізація інтересів проявляється у досягненні певних цілей, а реалізації інтересів можуть протидіяти і заважати загрози. Необхідно мати на увазі, що в економічній сфері формування інтересів, виникнення загроз цим інтересам, їхня взаємодія відбувається в певному середовищі, яке внаслідок цього також слід розглядати як частину системи економічної безпеки» [8].

О.І. Судакова також пропонує розглядати організаційно-економічні основи та змістовне наповнення категорії «безпека» як задоволення потреб існування, цілісності, незалежності та розвитку, причому спроможність забезпечення мети суб’єкта задля його самореалізації, розширеного самовідтворення і розвитку, розцінюється як індикатор безпеки [52]. Дана теза підтверджується фактом того, що категорія безпеки одночасно

залишається також потребою за власною сутністю відповідно до відомої пірамідальної ієрархії потреб А. Маслоу.

Беззаперечно, що від змістовного наповнення понять «інтереси», «загрози», «захист» значною мірою залежать форми, методи і засоби забезпечення безпеки. Як вже зазначалося, саме протиріччя в конкретному змісті інтересів є джерелом внутрішніх і зовнішніх загроз безпеці.

Взагалі, при дослідженні сутності економічної безпеки підприємства необхідно враховувати поліструктурність даної економічної категорії, яка може розглядатися на міжнародному (глобальна та регіональна) рівні; національному (державна та недержавна) та корпоративному рівні (підприємства, фірми, корпорації тощо) .

З формуванням у країні основ ринкових відносин змінюються й наукові парадигми, виникають і розвиваються суто ринкові підходи до методів і принципів здійснення господарської діяльності. Як наслідок даного процесу можна відзначити ряд наукових робіт з проблем теоретичного осмислення категорії «економічна безпека» у рамках «ресурсно-функціонального» підходу. С.М. Ілляшенко визначає економічну безпеку як «…стан ефективного використання ресурсів підприємства та існуючих ринкових можливостей, що дозволяє попереджати зовнішні та внутрішні загрози, та забезпечує життєздатність та стабільний розвиток на ринку відповідно до обраної місії» [22]. У цьому визначенні, на погляд автора, найчіткіше виявлено сутнісну характеристику категорії «економічна безпека», що розглядається у діяльнісному аспекті (безпека як діяльність) на відміну від більш вузького статичного (безпека як стан), що не враховує динамічні процеси розвитку промислових об’єктів.

В основу сучасного уявлення про категорію економічної безпеки закладено діяльністний підхід, тобто дослідження безпеки як об’єктивної дійсності суб’єкта у певних умовах, що базується на активній взаємодії цього суб’єкта та умов його існування, якими він опанував у процесі власної

самореалізації і здатен контролювати. В.К. Сенчагов наголошує на тому, що базовим підґрунтям економічної безпеки підприємств і головним елементом активізації процесу її формування є механізм забезпечення збалансованого та безупинного розвитку, що досягається за допомогою використання усіх видів ресурсів і підприємницьких можливостей, за якими гарантується найбільш ефективне їх використання для стабільного функціонування та динамічного науково-технічного й соціального розвитку, а також запобігання внутрішнім і зовнішнім негативним впливам (загрозам) [49].

О.В. Ареф'єва, Т.Б. Кузенко дотримуються цієї ж позиції. Економічна безпека фірми (підприємства, організації) - це такий стан корпоративних ресурсів (ресурсів капіталу, персоналу, інформації і технологій, техніки та устаткування, прав) і підприємницьких можливостей, за якого гарантується найбільш ефективне їхнє використання для стабільного функціонування та динамічного науково- технічного й соціального розвитку, запобігання внутрішнім і зовнішнім негативним впливам (загрозам) [3].

У рамках ресурсно-функціонального підходу С. Олейніков виділяє фінансову, інтелектуальну, кадрову, технологічну, правову, екологічну, інформаційну та силову складові економічної безпеки підприємства [42].

Слід зазначити, що система функціональних складових оцінки економічної безпеки та їх граничні значення повинні обґрунтовуватися, виходячи з поточного стану конкретної економічної системи, з урахуванням головних тенденцій та можливостей її розвитку. Так І.Г. Аберніхіна зазначає, що «для виробничих підприємств… пріоритетними складовими економічної безпеки є техніко-технологічна й фінансова, оскільки вони безпосередньо пов'язані з формуванням конкурентоспроможності продукції і характеризують технологічний і фінансовий потенціал підприємства та ступінь його захищеності» [1]. С. Ілляшенко пропонує включати до складу функціональних складових економічної безпеки також ринкову та інтерфейсну, що характеризують надійність взаємодії з економічними

контрагентами підприємства [22]. Це дозволяє, беззаперечно, більш повно враховувати вплив зовнішнього середовища на стан підприємства в аспекті економічної безпеки.

Функціональні складові економічної безпеки наведені на рисунку 1.3.

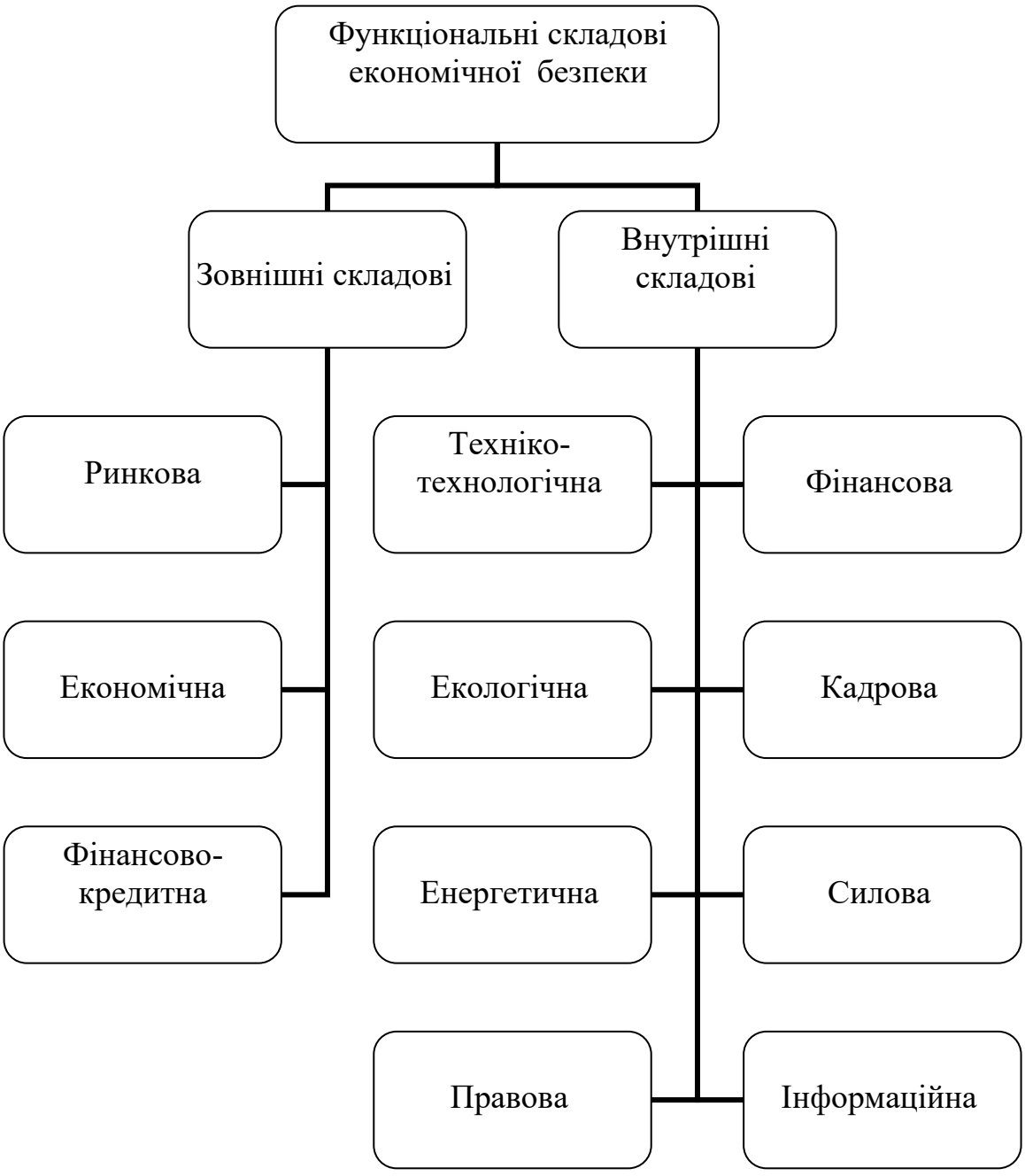

Рисунок 1.3 – Функціональні складові економічної безпеки

Мінливість зовнішнього середовища функціонування підприємств викликають необхідність використання принципів системного підходу у дослідженні процесів забезпечення економічної безпеки підприємств в сучасних економічних умовах, який є конкретизацією діалектичного методу і його застосування до вивчення об'єктів різного рівня складності.

Крім того, як зазначає І.Г. Мішина, сприйняття економічної безпеки як цілісної системи дозволяє виділити її суб'єкти і об'єкти і проводити дослідження з позиції суперечливості в процесі реалізації інтересів [36]. Складність, нестабільність і невизначеність зовнішнього середовища функціонування підприємства викликають необхідність використання принципів системного підходу у дослідженні процесів забезпечення економічної безпеки в сучасних економічних умовах і визначення підприємства як виробничо-економічної системи, під якою розуміють підсистему суспільства, що здійснює виробництво, розподіл і споживання матеріальних благ.

Використання системного підходу дозволить досліджувати особливості забезпечення економічної безпеки виробничо-збутової підсистеми (підприємство, постачальники сировини, матеріалів, споживачі готової продукції, система транспорту та складського господарства), а також особливості забезпечення економічної безпеки фінансової підсистеми (підприємство, кредитори, дебітори, фінансово-кредитні інститути).

Застосування принципів системного підходу і методів економіко-математичного моделювання, які, незважаючи на величезний потенціал, не в повній мірі використовуються для дослідження категорії економічної безпеки, дозволить досліджувати вплив превентивних заходів щодо забезпечення її певного рівня на ефективність функціонування, як у статиці, так і у динаміці.

Безумовним кроком уперед слід вважати публікації в економічній літературі щодо трактування економічної безпеки підприємства з позицій системного підходу. Так Л.П. Гончаренко і Е.С. Куценко визначають поняття

«системи економічної безпеки підприємства», що у рамках ресурсно-функціонального підходу базується на ефективному використанні його ресурсів, що забезпечувало б стабільне функціонування підприємства на теперішньому етапі та стійкий розвиток у майбутньому [13].

К.С. Горячева визначає сутність економічної безпеки як стан його економічної системи, котрий можна характеризувати «…збалансованістю і стійкістю до негативного впливу будь-яких загроз, її здатністю забезпечувати на основі власних економічних інтересів свій сталий і ефективний розвиток» [14]. При цьому до складу економічної безпеки підприємства включено такі підсистеми: фінансова, внутрішньоекономічна, зовнішньоекономічна (економіка зв'язків підприємства з зарубіжними підприємствами) і соціальноекономічна.

З позицій системного підходу, але, нажаль, у статичному аспекті, досліджує категорію економічної безпеки І.І. Нагорна: «Під економічною безпекою промислового підприємства пропонується розуміти такий стан збалансованої економічної системи внутрішнього середовища підприємства, що здатний адекватно реагувати на динаміку зовнішнього середовища» [38].

1.3 Роль ризик-менеджменту в системі управління безпекою підприємства

Одним із найкращих інструментів забезпечення безпеки підприємства є ризик менеджмент.

Управління ризиками - це систематичний процес виявлення та оцінки ризиків компанії та вжиття заходів щодо захисту компанії від них. Деякі менеджери з ризику визначають ризик як можливість того, що майбутня подія може спричинити шкоду чи збитки, зазначаючи, що ризик також може

надавати можливі можливості. Взявши на себе ризики, компанії іноді можуть досягти значних вигід. Однак компаніям потрібно керувати ризиками для аналізу можливих ризиків, щоб збалансувати потенційний прибуток від потенційних втрат та уникнути дорогих помилок. Управління ризиками найкраще використовувати як запобіжний захід, а не як реактивний захід. Компанії отримують найбільшу користь від врахування своїх ризиків, коли вони успішно працюють і коли ринки ростуть, щоб підтримувати зростання та прибутковість.

Завдання менеджера з ризиків - передбачити та прийняти заходи щодо контролю або запобігання збитків у межах компанії. Процес управління ризиками включає визначення ризику можливих втрат, вимірювання цих ризиків та вирішення способів захисту компанії від шкоди, враховуючи характер ризиків та цілі та ресурси компанії. Хоча компанії стикаються з різними ризиками, деякі важливіші, ніж інші. Менеджери ризиків визначають їх важливість та здатність впливати під час визначення та вимірювання впливу. Наприклад, ризик затоплення в Арізоні матиме низький пріоритет щодо інших ризиків, з якими може зіткнутися компанія, розташована там. Менеджери ризиків розглядають різні методи контролю або запобігання ризикам, а потім вибирають найкращий метод, враховуючи цілі та ресурси компанії. Після того, як метод буде обраний та впроваджений, його слід контролювати, щоб гарантувати, що він дає поставлені результати.

Сфера управління ризиками з'явилася в середині 1970-х років, розвинувшись із старої галузі управління страхуванням. Термін управління ризиками був прийнятий тому, що нове поле має набагато ширший фокус, ніж просто управління страхуванням. Управління ризиками включає діяльність та обов'язки поза межами загальної сфери страхування, хоча страхування є важливою його частиною, і страхові агенти часто виконують функції менеджерів з ризику. Управління страховою діяльністю було зосереджене на захисті компаній від стихійних лих та основних видів впливу,

таких як пожежа, крадіжки та травми працівників, тоді як управління ризиками зосереджено на таких видах ризиків, а також інших видах дорогих втрат, включаючи ті, що пов'язані з відповідальністю за продукцію, практики зайнятості, деградація навколишнього середовища, відповідність бухгалтерському обліку, офшорний аутсорсинг, коливання валюти та електронна комерція. У 1980-х та 90-х роках управління ризиками переросло у життєво важливу частину планування та стратегії компанії, а управління ризиками стало інтегруватися з дедалі більшою кількістю функцій компанії в міру розвитку галузі. Оскільки роль управління ризиками зросла, щоб охопити масштабні загальнодержавні програми, ця галузь отримала назву управління ризиками підприємства.

Оскільки управління ризиками стало важливою частиною страхового посередництва, багато страхових агентів працюють за плату замість комісій. Щоб вибрати найкращий тип менеджера ризику для своїх компаній, менеджерам слід враховувати цілі, розміри та ресурси компанії.

Керівники також повинні знати про типи ризиків, з якими стикаються. Загальні типи ризиків включають автомобільні аварії, травми працівників, пожежу, повені та смерчі, хоча існують і більш складні види, такі як відповідальність та деградація навколишнього середовища. Крім того, компанії стикаються з низкою ризиків, які випливають насамперед із характеру ведення бізнесу.

Один із способів менеджерів оцінити ризики ведення бізнесу - це за допомогою калькулятора ризиків, розробленого Робертом Сімонсом, професором Гарвардської бізнес-школи. Хоча калькулятор ризику не є точним інструментом, він вказує на сфери, де існують ризики та потенційні втрати, такі як швидкість розширення та рівень внутрішньої конкуренції. Використовуючи калькулятор ризиків, менеджери можуть визначити, чи є в їхній компанії безпечний чи небезпечний обсяг ризику. Калькулятор ризиків вимірює три види внутрішнього тиску: ризик, що виникає внаслідок

зростання, корпоративної культури та управління інформацією. Наприклад, швидке зростання може становити ризик і призвести до втрат, адже якщо компанія зростає занадто швидко, у неї може не вистачити часу на адекватне навчання нових працівників. Отже, некерований ріст може призвести до втрати продажів і зниження якості.

Менеджери можуть оцінити підвищений ризик, пов'язаний із зростанням, визначивши, чи встановлені цілі продажів вищим керівництвом без участі працівників. Якщо компанія встановлює цілі продажів таким чином, то вона має високий рівень ризику, оскільки ці цілі можуть бути занадто важкими для працівників. У випадках, коли працівники відчувають надзвичайний тиск, намагаючись досягти цілей, вони можуть ризикувати. Аналогічно, компанії, які в значній мірі покладаються на оплату на основі результатів діяльності, також мають більш високий рівень ризику.

Для оцінки ризику, що виникає внаслідок корпоративної культури, менеджери повинні визначити, який відсоток продажів припадає на нові продукти чи послуги, розроблені працівниками, які беруть на себе ризик. Якщо відсоток високий, то величина ризику також велика, оскільки така компанія значно залежить від нових товарів і пов'язаних з цим ризиків. Крім того, корпоративна культура, яка дозволяє або заохочує працівників працювати самостійно над розробкою нових продуктів, збільшує ризик компанії, як і високий рівень відмов нового продукту чи послуги.

Нарешті, менеджери можуть визначити бізнес-ризики, що виникають в результаті управління інформацією, визначивши, чи витрачають вони та їх підлеглі багато часу на збір інформації, яка вже повинна бути доступною. Інший спосіб оцінювання цих ризиків - менеджери розглядають, чи часто вони переглядають дані про результати діяльності та чи помічають вони, якщо звіти відсутні чи написані невчасно.

Менеджери ризиків покладаються на різноманітні методи, щоб допомогти компаніям уникнути та зменшити ризики, намагаючись

позиціонувати їх на виграш. Чотири основні методи включають уникнення впливу чи уникнення ризику, запобігання втратам, зменшення збитків та фінансування ризику. Простий метод управління ризиками - це уникнення впливу, яке стосується уникнення продуктів, послуг чи ділової діяльності з потенційними збитками, наприклад, виготовлення сигарет. Запобігання втратам намагається викорінити потенційні збитки, застосовуючи такі програми, як навчання працівників та програми безпеки, спрямовані на викорінення ризиків. Скорочення втрат прагне мінімізувати наслідки ризиків за допомогою систем реагування, які нейтралізують наслідки стихійного лиха чи іншої ситуації.

Остаточний варіант менеджерів з ризикових ризиків - це фінансування ризиків, оплата їх або шляхом утримання, або перенесення їхніх витрат. Компанії працюють з менеджерами ризику настільки, наскільки це можливо, щоб уникнути утримання ризиків. Однак якщо немає іншого способу управління певним ризиком, компанія повинна бути готова покрити збитки, тобто утримувати збитки. Вирахування страхового полісу є прикладом нерозподіленого збитку. Компанії також можуть зберігати збитки, створюючи спеціальні фонди для покриття будь-яких втрат.

Передача ризику відбувається, коли компанія ділиться своїм ризиком з іншою стороною, наприклад страховим постачальником, отримуючи страхові поліси, що покривають різні види ризику, які можуть бути застраховані. Фактично страхування є провідним методом управління ризиками.

Менеджери великих корпорацій можуть вирішити управляти своїми ризиками, придбавши страхову компанію для покриття частини або всіх своїх ризиків. Такі страхові компанії називають страховиками, що перебувають у полоні.

Менеджери ризиків також розрізняють фінансування ризиків перед вирахуванням та після втрати. Фінансування ризику перед втратою включає фінансування, отримане під час підготовки до можливих втрат, наприклад,

страхові поліси. За допомогою страхових полісів компанії сплачують премії до нанесення збитків. З іншого боку, фінансування після втрати стосується отримання коштів після виникнення збитків (тобто, коли компанії отримують фінансування у відповідь на збитки). Отримання позики та видача акцій - це методи фінансування після втрати.

На етапі впровадження менеджери компанії працюють з менеджерами ризику, щоб визначити цілі компанії та найкращі методи управління ризиками. Як правило, компанії застосовують комбінацію методів ефективного контролю та запобігання ризикам, оскільки ці методи не є взаємовиключними, а є взаємодоповнюючими. Після впровадження методів управління ризиками керівники ризиків повинні вивчити програму управління ризиками, щоб переконатися, що вона продовжує бути адекватною та ефективною.

Усі плани управління ризиками дотримуються таких кроків, які використовуються для формування загального процесу управління ризиками (рисунок 1.4):

– встановлення контексту. Зрозумійте обставини, в яких відбуватиметься решта процесу. Критерії, які будуть використані для оцінки ризику, також повинні бути встановлені та визначена структура аналізу;

– ідентифікація ризику. Компанія визначає та визначає потенційні ризики, які можуть негативно вплинути на конкретний процес чи проект компанії;

– аналіз ризиків. Після виявлення конкретних видів ризику компанія визначає шанси виникнення, а також їх наслідки. Метою аналізу ризиків є подальше розуміння кожного конкретного випадку ризику та як це може впливати на проекти та завдання компанії;

– оцінка ризиків. Потім ризик додатково оцінюється після визначення загальної ймовірності виникнення ризику в поєднанні з його загальним

наслідком. Тоді компанія може приймати рішення щодо того, чи є ризик прийнятним і чи бажає компанія прийняти його;

– пом'якшення ризиків. Під час цього кроку компанії оцінюють свої ризики з найвищим рейтингом та розробляють план їх полегшення за допомогою конкретного контролю за ризиками. Ці плани включають процеси зменшення ризику, тактику запобігання ризикам та плани на випадок надзвичайних ситуацій у разі, якщо ризик буде реалізований;

– моніторинг ризиків. Частина плану пом'якшення наслідків включає спостереження як за ризиками, так і за загальним планом постійного моніторингу та відстеження нових та існуючих ризиків. Загальний процес управління ризиками також слід переглядати та оновляти;

– спілкування та консультації. Внутрішні та зовнішні акціонери повинні включатись у спілкування та консультації на кожному відповідному етапі процесу управління ризиками та стосовно процесу в цілому.

Стратегії управління ризиками також повинні намагатися відповісти на наступні питання:

– що може піти не так? Розглянемо як компанію в цілому, так і індивідуальну роботу;

– як це вплине на організацію? Розглянемо ймовірність події та чи матиме вона великий чи малий вплив;

– що можна зробити? Які заходи можна вжити для запобігання втрат? Що можна зробити відновити, якщо збитки сталися;

– якщо щось станеться, як організація заплатить за це.

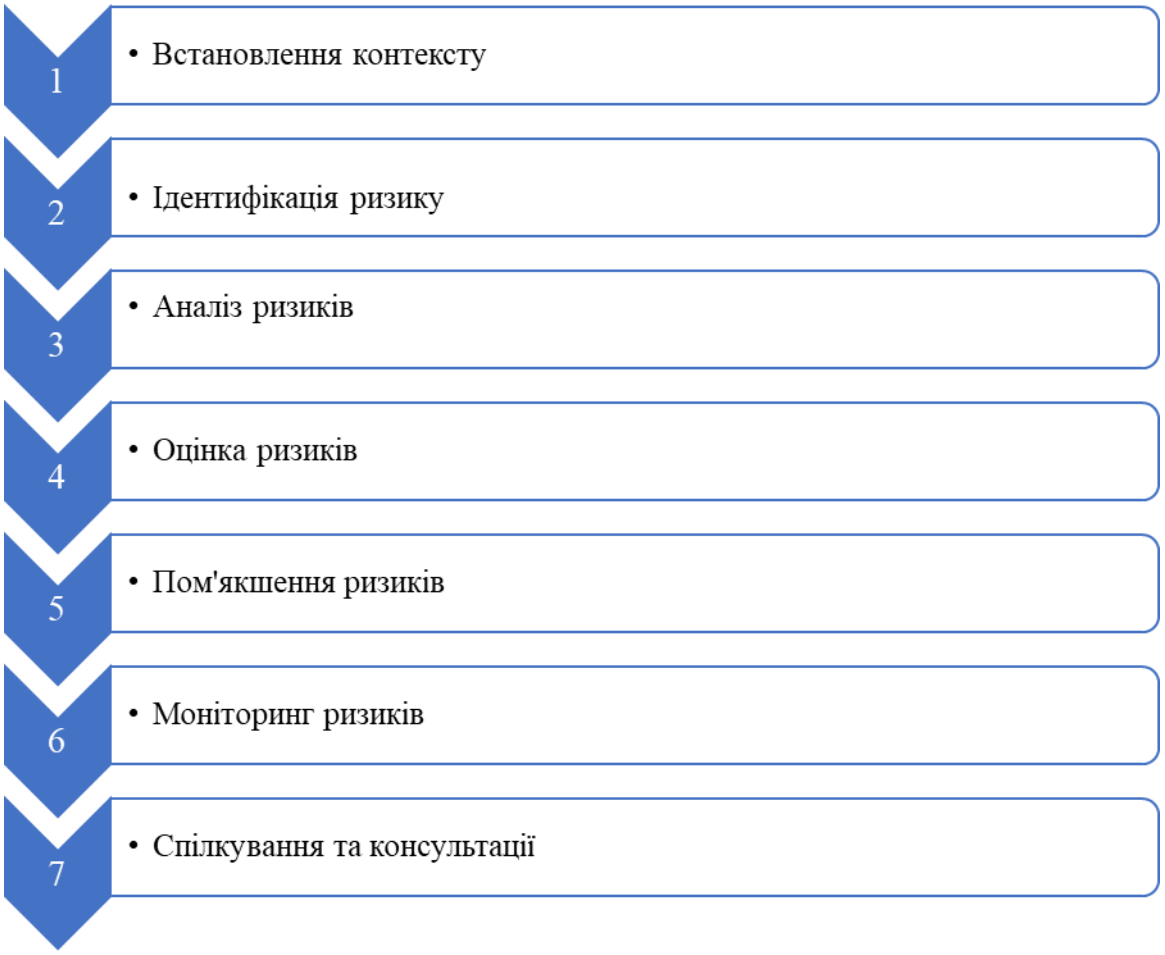

Рисунок 1.4 – Етапи загального плану управління ризиками

Висновки для першого розділу:

Таким чином в роботі надано визначення сутності ризику, проведена їх класифікація, наведена оцінки впливу ризиків на діяльність підприємства в цілому та на його безпеку. Розглянуто та проаналізовано визначення економічної безпеки підприємства, що наведено в наукові й та учбовій літературі провідними фахівцями. Визначено, що ризик-менеджмент є одним з найкращих інструментів забезпечення безпеки підприємства. Надано етапи, які використовуються для формування загального процесу управління ризиками.

2. ТЕХНІКО-ЕКОНОМІЧНИЙ АНАЛІЗ ДІЯЛЬНОСТІ ІТ-КОМПАНІЇ APPUS SOFTWARE ТА ОЦІНКА СИСТЕМИ РИЗИК-МЕНЕДЖМЕНТУ НА ПІДПРИЄМСТВІ

2.1 Загальна характеристика діяльності ІТ-компанії Appus Software

Приватне підприємтсво ІТ-компанія Appus Software засновано в 2009 році Дмитром Міхеєвим. Підприємство займається розробкою мобільних додатків. Розробка мобільних додатків на даний момент перейшла з придаткової технологічної сфери в самостійний ринок.

На нинішньому етапі розвитку індустрії мобільних технологій додатки є найбільш потужним і ефективним інструментом забезпечення зв'язку між людьми, що обумовлюється їх доступністю і поширеністю.

Компанія App Annie, яка займається виробництвом сервісів аналітики мобільного ринку, опублікувала звіт про перспективи ринку мобільних додатків. Один з основних висновків, до якого прийшли аналітики Rusbase: потенційне зростання прибутків ринку мобільних додатків до 101 мільярдів до 2020 року.

При підготовці звіту фахівці компанії App Annie використовували дані з 10 тисяч різних джерел, а також власну аналітику. Найбільш багатообіцяючими категоріями можна вважати соціальні мережі, продуктивність, рекламні сервіси, а також корисні додатки для різних цілей.

Якщо говорити про територіальні ринки, то найбільш швидкозростаючими визнані Латинська Америка і південно-східна Азія.

Розробка мобільних додатків вже не є чимось-то вузько направленим, тому кожен восьмий з усіх інтерактивних розробників в світі створює мобільні додатки, а всього число розробників мобільних додатків становить приблизно 2, 3 мільйони на людину. Компанія Apple в 2016 році під час конференції World Wide Developer Conference оголосила такі статистичні

дані по AppStore : було опубліковано більше 1,25 мільйонів додатків, які користувачі скачали 50 мільярдів разів, а розробники отримали дохід в 5 мільярдів доларів. Ринок мобільних пристроїв і додатків є одним з найбільш швидкорозвиваючихся на сьогоднішній день. Це обумовлено не тільки технологічними факторами, але і соціальними. Розвиток технологій відбувається також в силу підвищується попиту на них.

Перелік робіт, які виконує IT-компанія Appus Software:

а) мобільна розробка:

1) iOS. Крім переваг в нативної розробці під IOS варто виділити і деякі її особливості. В першу чергу варто виділити максимальну продуктивність розроблених мобільних додатків на Swift. Apple, при випуску власної мови програмування постаралася оптимізувати все, що можливо - в тому числі швидкість обробки написаних на Swift додатківЗручність розроблених інтерфейсів і звичні ефекти анімації - незаперечна перевага створення мобільних додатків на рідному для пристрою мовою;

2) Android. Крім явних переваг, які дає нативна розробка для Android платформи необхідно згадати ще й важливі особливості. Однією з них є максимальна продуктивність додатків під Android, написаних на Java. Нативні розробки дозволяють використовувати повний спектр можливостей пристрою: від доступу до камери до оптимізації внутрішньої пам'яті і завантаження процесорів;

3) кросплатформна розробка. Android, Windows, iOS - це тільки основні і найпопулярніші операційні системи мобільних пристроїв, але створювати нативні додатки навіть тільки під кожну з них далеко не завжди є доцільним. Найчастіше істотно простіше і дешевше створити універсальний продукт, який зможе показувати відмінну працездатність на всіх платформах, навіть маловідомих. Кросплатформна здійснюється подібно до звичайних web-сайтів на мові розмітки і стилів, тоді як нативні додатки розробляють під

певну платформу і не можуть використовуватися на пристроях з іншими операційними системами;

б) Веб розробка:

1) WEB. Процес створення веб сайту або веб додатку;

2) API (програмний інтерфейс програми, інтерфейс прикладного програмування) - опис способів (набір класів, процедур, функцій, структур або констант), якими одна комп'ютерна програма може взаємодіяти з іншою програмою;

3) Front-end розробка - це створення клієнтської частини сайту. Front-end розробник займається верстkою шаблону сайту і створенням користувальницького інтерфейсу;

4) Backend - це програмний код, який відповідає за роботу з сервером (базою даних), даними (для їх подальшого запису в БД або відправки клієнтові) і т. П. Як правило, саме Backend займається архітектурою;

5) Amazon cloud distribution. Amazon пропонує чудову безпеку і є досить гнучким і масштабованим у випадку, якщо потрібно оновити сервер для підтримки більшої кількості користувачів або придбання більше вільного місця. На додаток до вже захищеного AWS Cloud використовуються провідні рішення в галузі безпеки, для допомоги захиту данних;

в) графічний дизайн:

1) дизайн іконок. Кожному додатку потрібна приваблива та пам’ятна іконка, яка привертає увагу користувачів та виділяється на домашньому екрані будь-якого пристрою. Іконка о додатка - це перша можливість спілкуватися з користувачем, і насправді це відображає мету програми. Крім того, він відображатиметься у всій системі, наприклад в налаштуваннях та результатах пошуку;

2) дизайн логотипів. Логотип - найважливіший елемент корпоративного стилю компанії. Він служить, в першу чергу, для

ідентифікації компанії на ринку, складаючи візуальний образ бренду до ознайомлення з послугою або продуктом;

3) дизайн мобільних додатків. Дизайн мобільних додатків - це не тільки картинки, дизайн мобільних додатків складається з як мінімум двох основних речей - user experience і user interface (UI / UX). Тобто коли спочатку проектується взаємодія користувача і як такого сервісу, то потрібно зрозуміти, скільки і якої інформації повинно з'являтися, яким чином буде відбуватися навігація всередині - це такий великий блок, який називається user experience, той досвід, який користувач отримує від продукту, а user interface - це якраз річ набагато більш візуальна, і безумовно, вони між собою пов'язані. User interface в звичайному житті називається дизайном;

4) дизайн сайтів. Це не просто його зовнішнє оформлення, він також вирішує такі важливі завдання, як функціональність, зручність у використанні, то що на мові веб-майстрів називається юзабіліті. Відвідувач сайту повинен легко орієнтуватися на його сторінках, знаходити потрібну інформацію, мати можливість швидко повернутися на головну сторінку;

5) прототипування. Прототипування сайту - це, відповідно, процес створення прототипу. Робиться це для того, щоб:

– грамотно продумати розташування потрібних блоків і елементів дизайну;

– побачити наочно концепцію майбутнього сайту;

– правильно організувати систему навігації на сайті;

– продумати можливості взаємодії відвідувача з сайтом. Крім того, розробка прототипу сайту істотно допомагає заощадити час розробки проекту і скоротити число доробок, які виникають при невідповідності функціоналу сайту очікуванням замовника. Після представлення прототипу клієнт знає чого очікувати в результаті, а розробник упевнений в цілях і вимогах;

6) варфрейми. Варфрейм - це візуальне керівництво, яке представляє структуру сторінки, а також її ієрархію і основні елементи;

г) QA. QA послуги допомагають забезпечити якість процесу тестування, перевірити, чи виконується воно відповідно до світовими стандартами тестування. Перевірки поділяються на різні види.

Вони обов'язково проводяться під час розробки програмного додатка. Деякі з них описані нижче.

Типи тестування:

1) тестування білого ящика. Тестувальник розуміє внутрішні коди програми. Процес включає не тільки тестування певних результатів, але і їх обробку, а також управління даними в різних модулях;

2) тестування чорного ящика. Виконується згідно функціоналу і очікуванням. Воно називається саме так, оскільки тестувальник не має уявлення про внутрішні функції коду;

3) модульне тестування. Це процес, під час якого найменші тестовані частини програмного додатка перевіряються окремо, як певні функції,процедури, інтерфейси, класи;

4) інкременте тестування. Проводиться для безперервного тестування програми відразу після додавання нових функцій і модулів;

5) інтеграційне тестування. Це форма тестування, мета якого - перевірити функціонал модулів і функції, які повинні працювати разом (мається на увазі, що вони будуть обмінюватися інформацією). Таке тестування особливо стане в нагоді для серверних / клієнтських систем;

6) QA консалтинг корисний для тих, хто робить перші кроки в світі IT і тестуванні програмного забезпечення. Також, кваліфіковані фахівці користуються ним, коли потрібно забезпечити найвищу якість продуктів чи проектів;

7) функціональне тестування. Це не що інше, як техніка тестування чорного ящика, яка має справу з функціоналом. Це

найпоширеніший вид тестування, і зазвичай тільки тестувальники справляються з ним, але в деяких випадках програмісти також беруть участь в перевірці коду до його релізу;

8) Системне тестування. Інша форма тестування чорного ящика. Виконується, щоб перевірити загальні вимоги і покрити всі частини системи, які були об'єднані;

9) End to End тестування. Даний вид тестування - один з найбільших. Він розроблений для перевірки поведінки кожного компонента додатка через весь цикл запиту з симуляцією реальних умов;

10) санітарне або димове тестування. Ці тести використовуються для перевірки стабільності системної версії щоб дізнатися, чи можна її піддавати подальшого тестування;

д) розробка для Apple TV. Варто зазначити, що процес створення програми для Apple TV дуже нагадує аналогічний процес створення додатків для iOS. Тут можна розробляти гри, утиліти, медіа-додатки, і багато іншого, використовуючи ту ж техніку і фреймворки, що для iOS. Нові та вже існуючі програми можуть бути використані як на iOS, так і на новому Apple TV, причому в розрахованому на багато користувачів форматі. У Apple TV немає миші, як в комп'ютері, але передбачені пульт Siri Remote або ігровий контролер для переміщення по екрану. В цілому, тепер користувач буде керувати Apple TV абсолютно по-новому. Якщо Mac і iOS-гаджети є більш індивідуальними пристроями, то новим Apple TV легко можуть одночасно керувати кілька людей, що знаходяться в кімнаті;

е) розробка для Smart Watch. З одного боку, написання додатків для розумних годин дуже схоже на створення програм для планшетів і смартфонів. З іншого боку, компанія Apple опублікувала креативну концепцію і принципи дизайну, створені спеціально для тих, хто розробляє «носяться» додатка. У цих документах розкриваються основні відмінності між «мобільними» і «ношеними» технологіями. При розробці додатків

потрібно враховувати маленький розмір екрану розумних годин і особливий характер взаємодії користувача з пристроєм. На додаток до цього потрібно брати до уваги структуру програми, залежність поведінки програм від контексту, особливості призначеного для користувача інтерфейсу, стиль і можливість створення циферблатів;

ж) надання консалтингових послуг. Консультаційні послуги в сфері інформаційних технологій для всіх сфер діяльності (приватних або державних). IT Консалтинг включає в себе:

1) підвищення ефективності роботи компанії шляхом автоматизації всіх наявних бізнес процесів;

2) налагодження та підтримка внутрішньокорпоративної мережі, а також створення захисту внутрішньокорпоративної мережі від витоку персональних даних;

3) перевірка, побудова і управління IT інфраструктурою;

4) перевірка і модернізація, професійний підбір IT команди або цілого відділу;

5) впровадження облікових систем і систем аналізу;

з) навчання студентів. Залежно від конкретної обраної програми навчання,курси веб-програмування допоможуть вам освоїти нову спеціальність з високим рівнем доходу. З огляду на той факт, що на кваліфікованих програмістів завжди дуже високий попит, наші курси IT дозволять вам швидко знайти високооплачувану роботу. Крім того, деякі курси припускають можливість отримання працевлаштування в нашій компанії.

Основний напрямок діяльності підприємства – розробка мобільних додатків для обох операційних систем : iOS та Android.

Приватне підприємство Appus Software представляє свою продукцію на міжнародному ринку. Підприємство має замовників з таких країн: Сполучені Штати Америки, Англія, Франція, Німеччина, ОАЄ.

Організаційна структура IT-підприємства Appus Software – лінійна (рисунок 2.1).

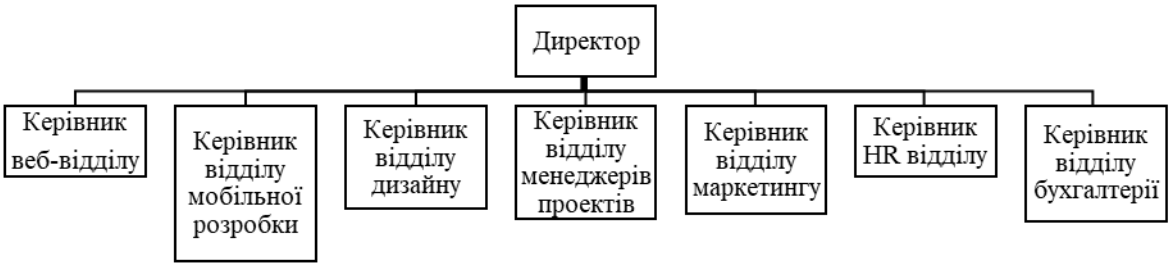

Рисунок 2.1 – Організаційна структура IT-підприємства Appus Software

Для контролю усіх виробничих процесів на підприємстві використовується JIRA.

JIRA це засіб відстеження завдань або управління проектами. Зазвичай вона використовується для відслідковування статусу розробки або багів.

Концептуальні поняття JIRA - Завдання, Проект і Процес. Це може бути проілюстровано наступним чином (рисунок 2.2):

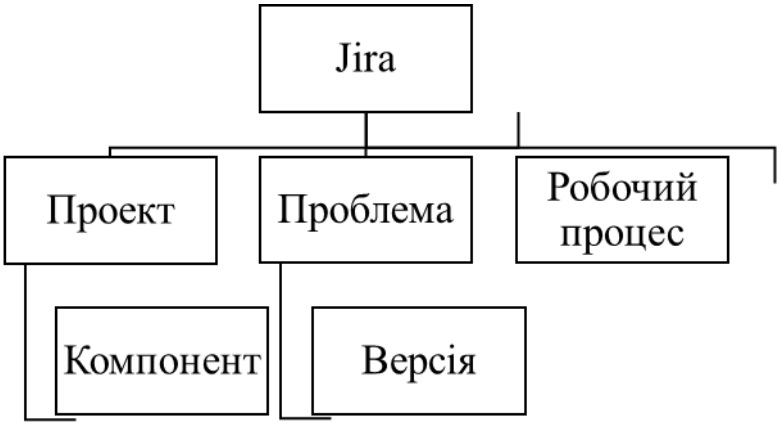

Рисунок 2.2 - Концептуальні поняття JIRA

2.2 Аналіз фінансово-економічного стану IT-компанії Appus Software

Аналіз і оцінка рівня фінансово - економічної безпеки є основою для пошуку шляхів забезпечення фінансово-економічної безпеки підприємства. Аналіз здійснюють за допомогою груп показників, до яких належать показники оцінки фінансового стану підприємства, а також показник рівня фінансової безпеки.

Фінансовий стан підприємства - це економічна категорія, яка відображає стан капіталу в процесі його кругообігу й здатність суб'єкта господарювання до саморозвитку на фіксований момент часу.

Матеріально-технічна база підприємства – сукупність усіх матеріальних умов здійснення процесу виробництва в поєднанні з його технологією в галузях і підрозділах цього підприємства.

Основні засоби – це вартість матеріально-речовинних цінностей, що використовуються підприємствами у виробничій та невиробничій сферах діяльності тривалий час (понад рік).

Відповідно до діючої типової класифікації основні засоби групуються залежно від функціонального призначення, галузевої належності, речовинно-натурального складу тощо.

Залежно від функціонального призначення основні засоби поділяються на виробничі та невиробничі.

Виробничі основні засоби – це засоби, які безпосередньо беруть участь у виробничому процесі або сприяють його здійсненню. До них належать будівлі, споруди, силові машини та устаткування, передавальні пристрої, транспортні засоби, робоча худоба, багаторічні насадження, інші основні засоби, що діють у сфері матеріального виробництва.

Невиробничі основні засоби – це засоби, що не беруть безпосередньої або побічної участі у процесі виробництва та передбачені для

обслуговування потреб житлово-комунального господарства, охорони здоров'я, освіти, культури. До них належать споруди, будівлі, машини, обладнання, апарати та інші засоби, що використовуються в невиробничій сфері.

У таблиці 2.1 показаний склад основних засобів та його зміни впродовж 2016–2018 рр. в IT-компанії Appus Software.

Таблиця 2.1 – Склад основних засобів IT-компанії Appus Software за 2016-2018 рр. (тис. грн.)

№	Показники	Значення за роками			Абсолютне відхилення		Темп росту, %	
		2016	2017	2018	2016/2017	2017/2018	2016/2017	2017/2018
1	Будинки, споруди	521,50	587,00	547,00	65,50	-40,00	112,56	93,19
2	Машини та обладнання	428,60	602,20	602,20	173,60	0,00	140,50	100,0
4	Інструменти, прилади, інвентар	249,30	528,00	560,20	278,70	32,20	211,79	106,1
5	Всього	1199,4	1717,2	1709	517,8	-7,80	464,85	299,

Як видно з таблиці 2.1 впродовж періоду 2016–2018 рр. відбулися такі зміни: найбільш зросла вартість інструментів, приладів та інвентарю (меблів) на 310,9 тис. грн., в 2017 р. вартість транспортних засобів зросла на 60,1 тис. грн. і залишилась незмінною на 2016 р., вартість машин та обладнання на протязі періоду 2016-2017 рр. по зросла на 173,6 тис. грн. та теж залишалась незмінною, на кінець 2016 р. вартість будинків та споруд зросла на 25,5 тис. грн. порівняно з 2016 р., та зменшилась на 40 тис. грн. у порівнянні з 2017р. Загальна вартість основних засобів протягом вказаного періоду зросла на 509,6 тис. грн., що свідчить про покращення стану технічного забезпечення виробництва.

Активи – це ресурси, контрольовані підприємством у результаті минулих подій, використання яких, як очікується, призведе до отримання економічних вигід у майбутньому. Активи класифікують за складом і розміщенням та функціональною участю у процесі діяльності.

У балансі активи поділяють на необоротні, оборотні та витрати майбутніх періодів.

Оборотні активи – це грошові кошти та їх еквіваленти, що не обмежені у використанні, а також інші активи, призначені для реалізації чи споживання протягом операційного циклу чи протягом 12 місяців із дати балансу. Виділяють такі оборотні активи: грошові кошти в касі і на рахунках у банках; виробничі запаси; короткострокові фінансові інвестиції; дебіторська заборгованість – поточна заборгованість із терміном погашення протягом одного року (заборгованість підзвітних осіб, заборгованість покупців); витрати майбутніх періодів – витрати, які мали місце протягом поточного або попередніх періодів, але належать до наступних звітних періодів.

Необоротні активи – термін їх корисного використання більше одного року або одного операційного циклу, який перевищує рік. Вони діляться на: основні засоби; нематеріальні активи; довгострокові фінансові інвестиції; інші необоротні активи [40].

Склад активів та їх зміни згідно з балансом підприємства представлені в таблиці 2.2.

Згідно представленим даним в таблиці 2.2 загальна вартість активів зросла на 2137,2 тис. грн. порівняно з 2016 р., але зменшилась на 1108,5 тис. грн. у порівнянні з 2017р.

Таблиця 2.2 – Склад активів підприємства ІТ-компанії Appus Software за 2016–2018 рр. (тис. грн.)

№	Показники	Значення по рокам			Абсолютне відхилення		Темп росту, %	
		2016	2017	2018	2017 / 2016	2018 / 2017	2017 / 2016	2018 / 2017
1	2	3	4	5	6	7	8	9
1	Необоротні активи, в тому числі:							
2	Незавершене виробництво	53,30	852,00	1236,0	798,70	384,00	1598,50	145,1
3	Основні засоби	2760,80	3164,40	1860,6	403,60	-1303,80	114,62	58,80
4	Довгостроко-ві фінансові інвестиції	96,80	219,20	149,50	122,40	-69,70	226,45	68,20
5	Довгостроко-ва дебіторсь-ка заборгова-ність	13,70	146,80	52,50	133,10	-94,30	1071,53	35,76
6	Оборотні активи, в тому числі:							
7	Виробничі запаси	73,00	118,80	106,30	45,80	-12,50	162,74	89,48
8	Товари	243,40	129,90	161,80	-113,5	31,90	53,37	124,6
9	Дебіторська заборгованість	3879,30	6141,30	5632,7	2262,0	-508,60	158,31	91,72
10	Грошові кошти та їх еквіваленти	853,50	730,90	470,20	-122,60	-260,70	85,64	64,33
11	Всього	6773,60	10009,3	8900,8	3235,7	-1108,50	147,77	88,93

Сьогодні підприємства дістали певну самостійність у формуванні власних фондів. Якщо раніше існували нормативи відрахувань по фондах, то тепер підприємства можуть розпоряджатися прибутком на власний розсуд, вилучати з нього такі суми по різних фондах, які вони вважають за потрібне.

Визначення основних видів прибутку підприємства ІТ-компанії Appus Software наведено в таблиці 2.3.

Таблиця 2.3 – Визначення основних видів прибутку підприємства IT-компанії Appus Software за 2016-2018рр.

(тис. грн.)

№	Показники	Значення за роками			Абсолютне відхилення		Темп росту, %	
		2016	2017	2018	2016/2017	2017/2018	2016/2017	2017/2018
1	2	3	4	5	6	7	8	9
1	Дохід (виручка) від реалізації (товарів, робіт, послуг)	57806	32 312,70	21 627,20	-25 493,30	-10 685,50	55,90	66,93
2	Податок на додану вартість	9521,7	5 047,00	3 317,20	-4 474,70	-1 729,80	53,01	65,73
3	Чистий дохід (виручка) від реалізації продукції (товарів, робіт, послуг)	48284	27 265,70	18 310,00	-21 018,60	-8 955,70	56,47	67,15
4	Собівартість реалізованої продукції (товарів, робіт, послуг)	45402	25 006,10	16 450,10	-20 395,50	-8 556,00	55,08	65,78
5	Валовий прибуток	2882,7	2 259,60	1 859,90	-623,1	-399,7	78,38	82,31
6	Інші операційні доходи	902,2	2 180,10	1 385,40	1 277,90	-794,7	241,64	63,55
7	Адміністративні витрати	1362,4	1 342,20	976,1	-20,2	-366,1	98,52	72,72
8	Витрати на збут	461,8	529,8	425,2	68	-104,6	114,72	80,26
9	Інші операційні витрати	1155,3	2 166,70	1 582,50	1 011,40	-584,2	187,54	73,04
10	Фінансові результати від операційної діяльності, прибуток	805,4	401	261,5	-404,4	-139,5	49,79	65,21
11	Інші доходи	15,6	40,9	306,2	25,3	265,3	262,18	1137,26
12	Фінансові витрати	171	43,1	108,6	-127,9	65,5	25,20	32,36
13	Інші витрати	72,6	31,4	357,1	-41,2	325,7	43,25	117,26
14	Фінансові результати від звичайної діяльності	316,6	225,8	102	-90,8	-123,8	71,32	45,17
15	Чистий прибуток	316,6	225,8	102	-90,8	-123,8	49,79	65,21

На прибуток як економічний показник впливає багато факторів. їх можна поділити на зовнішні та внутрішні.

До зовнішніх належать фактори, що не залежать від розвитку підприємства:

– інфляційні процеси;
– законодавство;
– політика;
– науково-технічний та соціальний розвиток регіону;
– політика оподаткування та ін.

До внутрішніх факторів належать ті, що залежать від діяльності окремо взятого підприємства. Вони можуть впливати на формування прибутку як безпосередньо, так і опосередковано. Ступінь впливу безпосередніх факторів обчислюється простим арифметичним способом. До них належать такі:

– обсяги продукції, що випускається;
– собівартість виробництва;
– ціна продукції, що реалізується;
– найменування (асортимент) продукції, що випускається.

Як видно з даних, представлених в таблиці 2.3 чистий прибуток підприємства зменшується у 2017 р. порівняно з 2016 р. на 90,8 тис. грн., в 2018 р. порівняно з 2016 р. – на 123,8 тис. грн., а в 2018 р. порівняно з 2016 р. прибуток зменшився на 214,6 тис. грн. Це викликано збільшенням витрат на виробництво та зменшеннями об’ємів виробництва.

Прибуток показує абсолютний ефект діяльності підприємства без урахування використаних при цьому ресурсів, тому його слід доповнювати показником рентабельності. Ступень прибутковості підприємства і характеризує рентабельність.

Фінансовий стан підприємства – це здатність, спроможність підприємства фінансувати свою діяльність. Він характеризується забезпеченням фінансовими ресурсами, які необхідні для нормального функціонування підприємства, доцільністю їх розміщення та ефективність

використання, фінансовими взаємовідносинами з іншими юридичними та фізичними особами, платоспроможністю та фінансовою стійкістю.

Основними факторами, що визначають фінансовий стан є: виконання фінансового плану і поповнення в міру потреби власного оборотного капіталу за рахунок прибутку, а також швидкість оборотності оборотних котів. Сигналом в якому проявляється фінансовий стан є платоспроможність підприємства, тобто його здатність своєчасно задовольнити платіжні вимоги постачальників сировини, техніки згідно з угодами, повертати банківські кредити проводити оплату праці персоналу, вносити платежі в бюджет.

Під фінансовими ресурсами слід розуміти загальну суму власного, позиченого й залученого капіталу, що використовується підприємствами для формування своїх активів і здійснення виробничо-господарської діяльності з метою одержання прибутку.

2.3 Аналіз трудових ресурсів підприємства

Найважливішим елементом продуктивних сил і основним джерелом розвитку економіки країни в цілому та кожного підприємства зокрема є люди, їх майстерність, освіта й фахова підготовка. Розрізняють поняття «трудові ресурси», «персонал» і «кадри» підприємства.

Трудові ресурси – це частина працездатного населення, яка за віковими, фізичними та освітніми даними відповідає тій чи іншій сфері діяльності. Серед трудових ресурсів виокремлюють реальні (люди, які працюють) і потенційні (особи, які мають бути залучені до певної праці в майбутньому).

Персонал – це сукупність постійних або тимчасових працівників, що отримали необхідну професійну підготовку або мають досвід практичної роботи.

Під поняттям «кадри» розуміється постійний кваліфікований склад працівників підприємства.

На рівні підприємства найчастіше використовують категорію «кадри» або «персонал».

Склад та кількість працюючих IT-компанії Appus Software представлено у таблиці 2.4.

Таблиця 2.4 – Кількість працівників за якісним складом підприємства IT-компанії Appus Software за 2016-2018рр.

Показники	Значення за роками			Абсолютне відхилення		Темп росту, %	
	2016	2017	2018	2016/2017	2017/2018	2016/2017	2017/2018
2	3	4	5	6	7	8	9
Кількість працюючих у віці (років):							
від 21 до 30	30	27	20	3	7	90	74,07
від 31 до 50	3	3	2	0	1	0	66,66
від 51 до 65	0	0	0	0	0	0	0
Кількість працівників, що мають вищу освіту за освітніми рівнями:							
- неповна та базова вища освіта	0	7	15	7	8	112,5	94,44
- повна вища освіта	30	20	5	-10	-15	110	96,97
Кількість працівників, які отримують пенсію, всього у тому числі:	0	0	0	0	0	0	0
за віком	0	0	0	0	0	0	0
по інвалідності	0	0	0	0	0	0	0
Кількість працівників, що працюють в умовах, що не відповідають санітарно - гігієнічним нормам	0	0	0	0	0	0	0

За принципом участі у виробничій діяльності персонал поділяється на дві категорії:

– промислово-виробничий (ПВП), який займається виробництвом та його обслуговуванням;

– непромисловий (працівники житлово-комунального господарства, лікувально-санітарних, дитячих закладів тощо).

За характером виконуваних функцій персонал підприємства поділяється на такі категорії: керівники, спеціалісти, службовці та робітники.

Виходячи з табл. 2.4 можна прослідкувати за змінами, які відбулися в якісному складі працівників. На кінець 2018 р. зменшилася облікова кількість працівників: на 8 осіб порівняно з 2017 р. і на 11 осіб порівняно з 2016 р. Це свідчить непостійність штату працівників, що не дає можливості якісно та вчасно виконувати роботу.

2.4 Ризики діяльності IT-компанії Appus Software та існуюча система їх запобігання

Існує багато методів стратегічного оцінювання підприємств. Основними методами оцінювання є:

а) SWOT-аналіз дозволяє визначити причини ефективної або неефективної діяльності підприємства, це стислий аналіз маркетингової інформації на підставі якого робиться висновок про те, в якому напрямку організація повинна розвивати свій бізнес і в кінцевому підсумку визначається розподіл ресурсів по сегментах. Результатом аналізу є розробка стратегії або гіпотези для подальшої перевірки. Класичний SWOT-аналіз передбачає визначення сильних і слабких сторін у діяльності фірми, потенційних зовнішніх загроз і сприятливих можливостей і їх оцінку щодо стратегічно важливих конкурентів;

б) конкурентний аналіз - це глибоке всебічне дослідження конкурентного положення підприємства і доступних ринків з метою формування ефективної стратегії розвитку. Конкурентний аналіз галузі включає в себе кілька розділів (етапів):

1) визначення основних економічних показників галузі;

2) визначення рушійних сил розвитку галузі;

3) оцінка сил конкуренції;

4) оцінка конкурентних позицій конкуруючих підприємств в галузі;

5) аналіз найближчих конкурентів, їх можливих дій;

6) визначення ключових факторів успіху;

7) оцінка перспектив розвитку галузі;

в) аналіз ресурсів - це аналіз внутрішнього середовища підприємства. Такий аналіз рекомендується проводити в три етапи:

1) створення профілю ресурсів - потрібно описати і оцінити наявні фінансові (наприклад, виручка), організаційні (наприклад, інформаційні системи), технологічні ресурси. Можна також порівняти свої ресурси і ресурси найближчого конкурента;

2) визначення сильних і слабких сторін - створений профіль ресурсів зіставляється з вимогами ринку. Тим самим підприємство визначає свої сильні сторони, виходячи з яких і можна розробити успішну стратегію. Крім того, ідентифікуються слабкі сторони, які повинні бути уважно опрацьовані і по можливості елімінувати;

3) ідентифікація специфічних компетенцій - сильні і слабкі сторони підприємства порівнюються з сильними і слабкими сторонами основного конкурента. Таким чином виділяються ті області діяльності, в яких дане підприємство має безсумнівні конкурентними перевагами;

г) аналіз рівня конкуренції в галузі за моделлю «5 сил конкуренції» Майкла Портера проводився шляхом аналізу п'яти зовнішніх сил:

1) ринковою владою постачальників;

2) ринковою владою покупців:

3) владою існуючих конкурентів;

4) загрозою появи нових конкурентів;

5) загрозою появи товарів-субститутів.

д) аналіз складових елементів (детермінант) цих сил дозволяє визначити «вузькі місця» проекту, з тим щоб максимально ефективно докласти зусиль до зміцнення його стійкості і ослаблення позицій конкурентів. Аналіз проводився в два етапи:

1) привласнення кількісних показників детермінантам п'яти сил методом експертної оцінки;

2) аналіз сильних і слабких сторін поточної конкурентної ситуації, а також можливих компенсаційних заходів.

Для аналізу IT-компанії Appus Software було вирішено використовувати SWOT аналіз.

Зазвичай SWOT-аналіз проводять в чотири етапи.

Перший етап - збір аналітичної інформації. Відзначимо, що інформація, необхідна для проведення аналізу, має бути присутня на підприємстві завжди. Адже управлінець повинен мати щоденні відомості про тенденції ринку, рухах товару, роботи конкурентів, постачальників і т.д. Це необхідно для ефективного управління бізнесом. Але недостатньо лише мати інформацію, необхідно грамотно і ефективно її використовувати. Саме таке використання інформації і проявляється при проведенні аналізу (за допомогою чіткого визначення подальшої стратегії).

Аналітичними даними для проведення SWOT аналізу були використані фінансова звітність підприємства, звітність про кадровий зміст підприємства, статистичні дані про стан ринку та інсайдерська інформація про конкурентів.

Другий етап - аналіз внутрішнього і зовнішнього середовища, виявлення сильних і слабких сторін підприємства. SWOT-аналіз необхідно проводити окремо для кожного продукту, ринку, конкурента. На практиці SWOT-аналіз часто складається для кожного ведучого конкурента і для

окремих ринків. Це розкриває відносні сили і слабкості компанії, її здатності в боротьбі з погрозами і використанні можливостей.

Для аналізу внутрішнього середовища підприємства було проведено такі заходи:

– опитування працівників;
– аналіз поточної інформації;
– аналіз статистичних дошок в JIRA.

Для зовнішнього аналізу було проведено такі заходи:

– аналіз ринку;
– проведення опитувань клієнтів;
– статистичні дані про конкурентів.

Третій етап - зіставлення сильних і слабких сторін підприємства і факторів зовнішнього середовища. Цей етап передбачає побудову матриці на основі стандартної методики. Було побудовано наступну матрицю (рисунок 2.3):

S Гнучка цінова політика; Широкий ранг пропонованих послуг.	W Слабке керування ризиками; Недостатність кваліфікованих кадрів; Відсутність мотивації для розвитку.
O Обслуговування нових груп клієнтів завдяки пропозиції кросплатформної розробки.	T Загроза виходу на ринок більш сильних конкурентів Загострення конкуренції.

Рисунок 2.3 – Матриця SWOT аналізу для IT-підприємства Appus Software

Виходячи з стовбців матриці W та T бачимо, що найбільшими ризиками для IT-компанії Appus Software є:

– слабке керування ризиками;
– недостатність кваліфікованих кадрів;
– відсутність мотивації для розвитку;
– загроза виходу на ринок більш сильних конкурентів;
– загострення конкуренції.

Для запобігання ризиків будь-якої природи у компанії необхідна існувати система запобігання ризиків.

IT-компанія Appus Software не має належної системи збору, аналізу, моніторингу та менеджменту ризиків. У зв’язку з цим ризики виявляються на тій стадії, коли їх запобігання вже неможливе. Це призводить до великих збитків компанії, втраті часу та репутації перед клієнтами. Через це у третьому розділі даної атестаційної роботи наведено план керування ризиками для IT-компанії Appus Software.

2.5 Система створення плану управління ризиками

Виходячи з пункту 2.4, на сьогоднішній день в IT-компанії Appus Software усталеної системи управління ризиками немає, проте запропонована така система створення плану управління ризиками.

Управління ризиками проекту включає в себе процеси, пов'язані із здійсненням планування управління ризиками, ідентифікацією, аналізом, плануванням реагування, здійсненням реагування, а також з моніторингом ризиків в проекті.

Цілями управління ризиками проекту є підвищення ймовірності виникнення і / або посилення впливу позитивних ризиків і зниження ймовірності виникнення і / або ослаблення впливу негативних ризиків з

метою максимального підвищення ймовірності успішного завершення проекту.

Управління ризиками проекту включає в себе наступні процеси:

– планування управління ризиками - це процес, який визначає, яким чином слід здійснювати заходи з управління ризиками проекту;

– ідентифікація ризиків - це процес виявлення індивідуальних ризиків проекту, а також джерел сукупного ризику проекту та документування їх характеристик;

– якісний аналіз ризиків - це процес розстановки пріоритетів щодо індивідуальних ризиків проекту для подальшого аналізу або дії, що виконується шляхом оцінки ймовірності виникнення та впливу ризиків, а також інших характеристик;

– кількісний аналіз ризиків - це процес чисельного аналізу сукупного впливу ідентифікованих індивідуальних ризиків проекту та інших джерел невизначеності на цілі проекту в цілому;

– планування реагування на ризики - це процес розробки варіантів, вибору стратегій і узгодження дій щодо схильності сукупного ризику проекту, а також щодо індивідуальних ризиків проекту;

– здійснення реагування на ризики - це процес виконання узгоджених планів реагування на ризики;

– моніторинг ризиків - це процес моніторингу виконання узгоджених планів реагування на ризики, відстеження ідентифікованих ризиків, виявлення та аналізу нових ризиків і оцінки результативності процесу управління ризиками на протязі всього проекту.

На рисунку 2.4 представлена загальна схема процесів управління ризиками проекту. Процеси ризиків в управлінні проектом представлені у вигляді дискретних процесів з визначеними межами, хоча на практиці вони накладаються один на одного і взаємодіють такими способами, які не можуть бути в повній мірі деталізовані в сьогоденні.

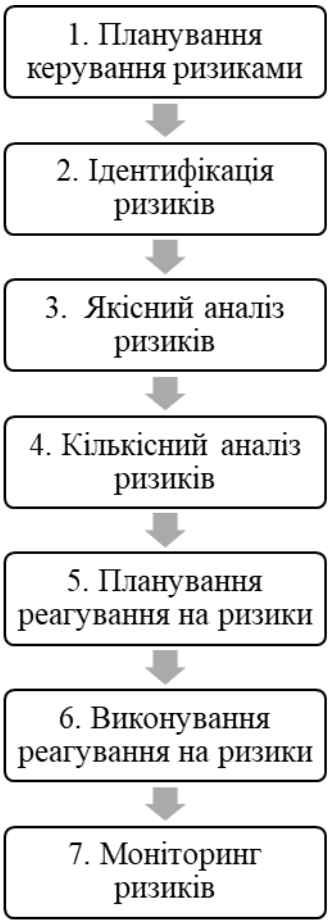

Рисунок 2.4 – Загальна схема керування ризиками проекту

Всі проекти схильні до ризику, оскільки вони є унікальними підприємствами з різним рівнем складності, які здійснюються з метою отримання вигод. Вони здійснюються в контексті обмежень і припущень, а також очікувань зацікавлених сторін, які можуть суперечити один одному і змінюватися. Організації повинні брати на себе свідомий і контрольований ризик щодо виконання проекту з метою створення цінності, зважуючи при цьому ризики і вигоди.

Мета управління ризиками проекту полягає в ідентифікації ризиків та управлінні ризиками, які не є предметом інших процесів управління проектом. Якщо не управляти ризиками, вони мають потенціал викликати відхилення проекту від плану і приводити до того, що проект не досягає поставлених цілей. В кінцевому рахунку від результативності управління ризиками проекту прямо залежить успішне завершення проекту.

Ризик всередині кожного проекту існує на двох рівнях, а саме: кожен проект має індивідуальні ризики, які можуть вплинути на досягнення цілей проекту. Важливо також враховувати ризикованість проекту в цілому, яка випливає з поєднання індивідуальних ризиків проекту та інших джерел невизначеності.

Управління ризиками проекту вирішує питання обох рівнів ризиків проекту, і їх можна визначити в такий спосіб:

– індивідуальний ризик проекту - це невизначена подія або умова, настання якого позитивно або негативно позначається на одній або декількох цілях проекту;

– сукупний ризик проекту - це вплив невизначеності на проект в цілому, виникає з будь-яких джерел невизначеності, включаючи індивідуальні ризики, що представляють собою вплив наслідків варіацій результатів проекту, як позитивних, так і негативних, на зацікавлені сторони.

Індивідуальні ризики проекту в разі їх реалізації можуть зробити позитивний або негативний вплив на цілі проекту. Управління ризиками проекту направлено на використання або посилення впливу позитивних ризиків (сприятливих можливостей) і, в той же час, щоб уникнути або пом'якшити наслідки негативних ризиків (загроз). Результатом некерованих загроз можуть стати такі проблеми, як затримки, перевищення вартості, зниження показників виконання або втрата репутації. Сприятливі можливості, за умови їх використання, можуть дати вигоди, наприклад скоротити час і вартість, підвищити показники виконання або зміцнити репутацію.

Сукупний ризик проекту також може мати позитивний або негативний характер. Метою управління сукупним ризиком проекту є збереження схильності проекту ризику в прийнятних межах за рахунок протидії рушійним силам негативних варіацій, сприяння рушійним силам позитивних варіацій і максимального підвищення ймовірності досягнення цілей проекту в цілому.

Ризики продовжують виникати на всьому протязі реалізації проекту, тому процеси управління ризиками проекту повинні здійснюватися ітеративно. Спочатку питання ризиків розглядаються в ході планування проекту при формуванні його стратегії. Моніторинг та управління ризиками повинні також здійснюватися в міру прогресу проекту, щоб виконання проекту йшло за встановленим планом, а проти несподівано виникаючих ризиків приймалися необхідні заходи. З метою результативного управління ризиками конкретного проекту його команді необхідно знати, який рівень схильності до ризику при вирішенні завдань досягнення цілей проекту є допустимим. Це визначається за допомогою піддаються вимірюванню порогів ризику, які показують схильність організації та зацікавлених сторін до ризику. Пороги ризику є вираженням ступеня допустимих варіацій в рамках мети проекту. Вони прямо заявляються і доводяться до відома команди проекту і відображаються в визначеннях рівнів впливу ризиків на проект.

Фокус управління ризиками проекту розширюється з метою охоплення всіх типів ризиків, а також для розширення контексту розуміння ризиків проекту. Тенденції і формуються практики в галузі управління ризиками проекту включають в себе, серед іншого:

Неподійні ризики. Більшість проектів фокусує свою увагу виключно на ризики, які є невизначеними подіями в майбутньому, які можуть відбутися або не відбутися. Як приклади подієвих ризиків можна навести такі ситуації: основний продавець може припинити діяльність в період здійснення проекту; замовник може змінити свої вимоги вже після завершення проектування; субпідрядник може запропонувати поліпшення стандартних процесів експлуатації. В даний час зростає розуміння того, що потрібно ідентифікувати неподійні ризики і управляти ними. Існує два основних типи неподійних ризиків:

– ризик варіативності. Існує невизначеність щодо деяких ключових характеристик передбаченого планом події, операції або рішення.

Прикладами ризиків варіативності можуть бути такі ситуації: продуктивність може бути вище або нижче цільової; кількість помилок, виявлених в ході випробувань, може бути вище або нижче очікуваних показників; в період фази будівництва можуть виникнути не властиві для даного сезону погодні умови;

– ризик неоднозначності. Існує невизначеність щодо того, що може статися в майбутньому. Області проекту, в яких неповне знання може вплинути на здатність досягти цілей проекту включають в себе: елементи вимог або технічного рішення; майбутній розвиток нормативно-правового регулювання; системна складність, притаманна проекту.

Ризики варіативності можна розглядати за допомогою аналізу за методом Монте-Карло з відображенням варіацій в певних межах розподілу ймовірностей і прийняттям на цій основі заходів для скорочення розкиду можливих наслідків. Управління ризиками неоднозначності здійснюється шляхом визначення областей, в яких спостерігається брак знання або розуміння, з подальшою ліквідацією прогалин за рахунок отримання експертних оцінок або бенчмаркінгу в зіставленні з передовими практиками. Проблему неоднозначності можна також вирішувати шляхом інкреметной поетапної розробки, створення прототипів або моделювання.

Існування несподівано виникаючих ризиків стає відомим в міру набуття знань про «невідомих невідомих». Це ризики, які можна виявити тільки після того, як вони вже настали. Справитися з несподівано виникаючими ризиками можна шляхом зміцнення стійкості проекту до впливів. Для цього необхідно, щоб кожен проект передбачав:

– правильний рівень резерву на можливі втрати в бюджеті і розкладі для несподівано виникаючих ризиків на додаток до певного резерву для відомих ризиків;

– гнучкі процеси проекту, які дозволяють протидіяти несподівано виникають ризикам, зберігаючи при цьому загальний напрямок руху до досягнення цілей проекту, включаючи надійне управління змінами;

– наявність володіє необхідними повноваженнями команди проекту, яка має чіткі цілі і якій доручено виконувати роботу в межах узгоджених обмежень;

– частий аналіз ранніх попереджувальних сигналів з метою ідентифікації несподівано виникаючих ризиків якомога раніше;

– чіткі дані від зацікавлених сторін для визначення областей, в яких вміст або стратегія проекту можуть бути скориговані у відповідь на несподівані ризики.

Інтегроване управління ризиками. Проекти існують в контексті організації та можуть входити до складу програми або портфеля. Ризики існують на кожному із зазначених рівнів і повинні мати власника і управлятися на відповідному рівні. Управління деякими ризиками, ідентифікованими на більш високих рівнях, передається команді проекту, а інші ризики можуть передаватися в порядку ескалації на більш високі рівні, якщо управління ними краще здійснювати поза проектом. Скоординований підхід до управління ризиками в масштабах всієї організації забезпечує узгодженість і послідовність порядку управління ризиками на всіх рівнях. Це робить результативне управління ризиками частиною структури програм і портфелів, забезпечуючи найвищу сукупну цінність для даного рівня схильності до ризику.

Оскільки кожен проект є унікальним, порядок застосування процесів управління ризиками проекту необхідно адаптувати. Міркування щодо адаптації містять у собі, серед іншого:

– масштаб проекту. Чи потребує проект більш детального підходу до управління ризиками з урахуванням його масштабу з точки зору бюджету, тривалості, змісту або чисельного складу команди? Або проект настільки невеликий, що це дає підстави для використання спрощеного процесу управління ризиками?

– складність проекту. Чи потрібен ретельно пророблений підхід до управління ризиками з урахуванням високих рівнів інновацій, використання

нових технологій, комерційних умов, інтерфейсів або зовнішніх залежностей, які збільшують складність проекту? Або проект є настільки простим, що потрібно використовувати спрощений процес управління ризиками?

– важливість проекту. Наскільки важливий проект зі стратегічної точки зору? Чи зростає ступінь ризику даного проекту в зв'язку з тим, що його метою є створення проривних можливостей, рішення істотних комплексних питань роботи організації, або з тим, що він передбачає значну інновацію продукту?

– підхід до розробки. Чи виконується даний проект за методом «водоспаду», коли процеси управління ризиками протікають послідовно і ітеративно, або на основі гнучкого підходу, коли з ризиками працюють на початку кожної ітерації, а також по ходу її виконання?

Адаптація процесів управління ризиками проекту з метою врахування зазначених міркувань є частиною процесу планування управління ризиками, а кінцеві результати рішень по адаптації реєструються в плані управління ризиками.

Середовища з високою варіативністю за визначенням відрізняються більш високим рівнем невизначеності і ризику. З урахуванням цієї обставини, в управлінні проектами з використанням адаптивних підходів застосовуються метод частого розгляду інкрементних продуктів роботи, а також крос-функціональні команди проекту для прискорення процесу обміну знаннями та забезпечення розуміння ризиків та управління ними. Ризики розглядаються щоразу при виборі змісту кожної ітерації; аналіз, ідентифікація ризиків і управління ними здійснюються також в ході кожної ітерації. Крім цього, облік вимог ведеться на основі документа, що безперервно уточнюється, який оновлюється регулярно, а пріоритетизація робіт може змінюватися в міру прогресу проекту на основі більш повного розуміння поточної схильності до ризиків.

Існує багато методів ідентифікації ризиків. Розглянемо кожен із них.

Першим із методів ідентифікації ризиків є експертна оцінка. Слід враховувати експертні висновки, отримані від осіб або груп осіб, що володіють спеціальними знаннями аналогічних проектів або сфер бізнесу. Таких експертів для розгляду всіх аспектів індивідуальних ризиків проекту, а також джерел сукупного ризику проекту, виходячи з їх попереднього досвіду і областей компетенції, повинен визначати і запрошувати керівник проекту. Під час даного процесу необхідно враховувати суб'єктивність оцінок експертів.

У другому розділі була розглянута загальна характеристика підприємства, проаналізовано основний перелік робіт та послуг компанії, описана організаційна структура IT-підприємства, надано опис системи управління. Проведено техніко-економічний аналіз фінансово-економічного стану підприємства, проаналізовано динаміку показників використання трудових ресурсів, їх вікова та освітня характеристика, описано ризики діяльності IT-компанії Appus Software. Надано загальні рекомендації щодо створення системи управління ризиками.

3 УДОСКОНАЛЕННЯ СИСТЕМИ УПРАВЛІННЯ РИЗИКАМИ IT-ПІДПРИЄМСТВА

3.1 Дослідження ризиків IT-підприємства

У процесі діяльності IT-підприємства виникають певні ризики. Усі ризики функціонування IT підприємства можна розподілити по категоріям. Загальноприйнятим способом структурування категорій ризиків IT компанії є використання ієрархічної структури ризиків (breakdown structure, RBS), яка є ієрархічним уявленням потенційних джерел ризику. RBS є інструментом команди проекту, який допомагає враховувати в повному обсязі джерела, з яких можуть виникати індивідуальні ризики проекту. Це може бути корисним при ідентифікації ризиків та в процесі розподілу за категоріями ідентифікованих ризиків. В організації може використовуватися:

– типова ієрархічна структура ризиків, яка застосовується у всіх проектах;

– кілька рамкових RBS для різних типів проектів;

– команда проекту може розробити адаптовану RBS.

У тих випадках, коли RBS не використовується, організація може застосувати звичайне структурування ризиків, яке може приймати форму простого переліку ризиків, заснованих на цілях проекту.

До першої категорії ризиків IT підприємства відносять зовнішні ризики.

Під зовнішніми ризиками зазвичай розуміються ті ризики, які не пов'язані безпосередньо з діяльністю компанії або її партнерів - контактних осіб, які проявляють інтерес до діяльності конкретної компанії. Перелік факторів, які впливають на зовнішні ризики компанії, дуже великий - до них відносять політичні, економічні, демографічні, соціальні та інші фактори макросередовища організації. Облік зовнішніх ризиків залежить від ступеня їх передбачуваності. Виділяють передбачувані зовнішні ризики, пов'язані,

наприклад, з коливаннями ринкової кон'юнктури, зміною цін, зміною рівня конкуренції або курсу валют. Існують також непередбачувані ризики - природні катаклізми, несподівані соціальні ефекти. Ризики зовнішнього середовища можна умовно розділити на макроризики, галузеві ризики і ризики аури. Найбільш близькими організації, а значить найбільш контрольованими і передбачуваними, є ризики аури. Наступною за ступенем передбачуваності та контролю є галузева серед компаній, яка представлена її конкурентами, споживачами, постачальниками та іншими партнерами. Макросередовище є найбільш непередбачуваною частиною зовнішнього середовища, так як залежить від безлічі різних факторів, які важко піддаються обліку і контролю.

До зовнішніх ризиків IT-компанії відносять такі ризики (рисунок 3.1):

– законодавство;
– курси обміну валют;
– майданчик / виробничі об'єкти;
– екологія / погода;
– конкуренція;
– нормативно-правове регулювання.

Рисунок 3.1 – Зовнішні ризики IT-компанії

Законодавчими ризиками ІТ компаній є:

– регуляторні ризики. Ризики, що виникають внаслідок зміни законів та правил, що суттєво впливають на бізнес чи ринок. Наприклад, будь-які зміни, внесені у відповідність оподаткування, що застосовуються до конкретної компанії, можуть спричинити штрафні санкції, накладені органами з питань оподаткування податками на прибуток або відповідними органами;

– ризик відповідності. Ризик відповідності охоплює ризик, який виникає через недотримання статутів, внутрішньої політики та найкращих практик, застосованих до будь-якої організації бізнесу. Це може призвести до фінансових втрат та судових санкцій;

– договірний ризик. Договірний ризик виникає, коли є певне невиконання договірних зобов'язань. Невиконання умов договору, ненадання послуг відповідно до договору, не включення у договір застережень щодо зменшення ризику тощо. Все це призводить до ризику контракту;

– позадоговірне зобов'язання. Ці ризики включають певні збитки, заподіяні конкурентові внаслідок порушення авторських прав або товарних знаків, здійснених вашим суб'єктом господарювання в ході ділових процесів. Інші збитки, такі як сумнівні вимоги, що виникають через недбалість, хибність подання та вимоги про несправедливе збагачення під час здійснення транскордонної ділової діяльності, також призводять до позадоговірного зобов'язання;

– суперечний ризик. Результати суперечливого ризику, коли виникають зриви, викликані зацікавленими сторонами, клієнтами та партнерами в бізнесі. Ці суперечки часто призводять до судових процесів і перекладають бізнес на тернину. Рекомендується вирішити суперечки до того, як вони перетворяться на судові спори, оскільки це спричинить величезні витрати;

– репутаційний ризик – це втрата доброго імені або статусу організації, що виникає внаслідок будь-яких зловживань чи будь-яких злочинних подій.

До курсових ризиків відносять:

– ризик транзакцій: Це ризик, з яким стикається компанія, надаючи послуги компанії, яка розташована в іншій країні. Ціна послуги буде виражена у валюті компанії-продавця.

– ризик перекладу: у наслідок здійснення закордонних операцій головна компанія, яка володіє дочірньою компанією в іншій країні, може зіткнутися з втратами, коли фінансова звітність дочірніх на голову компанію повинна здійснюватися в одній валюті;

– економічний ризик – це ризик зміни через вплив валютних коливань.

Конкурентний ризик - це потенціал дії конкурента негативно впливати на ваш бізнес. На здоровому конкурентному ринку конкурентоспроможний ризик призводить до покращення, таких як зниження витрат та підвищення якості. Нижче наведені загальні приклади конкурентного ризику:

– ціноутворення. Різкі зниження ціни конкурента можуть становити значну загрозу для бізнесу, особливо для бізнесу, який має більшу вартість, ніж конкурент. Знижки можуть бути обумовлені надмірним запасом через проблеми попиту / пропозиції або як агресивна цінова стратегія, яка спричинює цінову війну;

– інновації. Інновації конкурента можуть загрожувати всій бізнес-моделі фірми;

– місцеположення. Учасник, який відкриє місце розташування поруч із вашим або забезпечить краще місце розташування. У деяких випадках близька конкуренція не є поганою справою, оскільки може залучати більше клієнтського трафіку;

– ресурси. Конкурент, який розглядається як більш привабливий роботодавець, може призвести до втрати кваліфікованих ресурсів;

– акція. Акція конкурента може залучати ваших клієнтів. У деяких випадках просування конкурента може прямо чи опосередковано виставити вашу марку чи продукцію в негативному світлі;

– поширення. Конкурент може досягти бажаної позиції зі своїми партнерами з дистрибуції, такими як торгові мережі;

– інтелектуальна власність. Конкурент може захистити ключову інтелектуальну власність, важливу для поточних та майбутніх продуктів.

До другої категорії ризиків ІТ підприємства відносять комерційні ризики (рисунок 3.2).

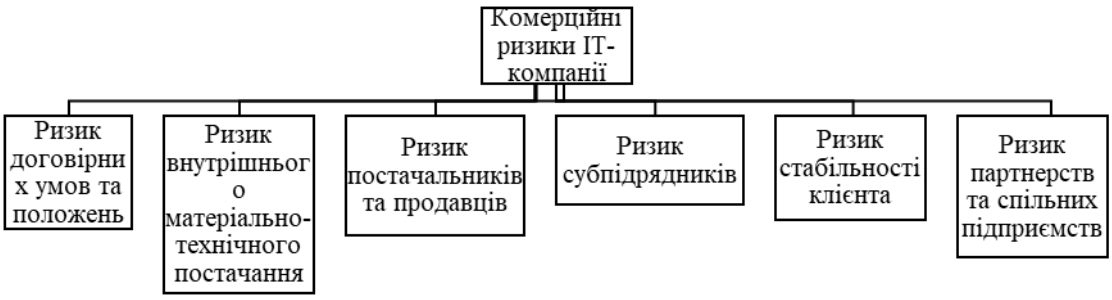

Рисунок 3.2 – Комерційні ризики ІТ-компанії

Комерційна діяльність неминуче пов'язана з ризиком. Домагаючись найбільшої ефективності організації та здійснення актів купівлі-продажу, комерсант постійно стикається з можливістю не тільки не отримати очікуваний прибуток, але і втратити те, що він уже має. Причини для цього можуть бути самі різні. Це і несприятливі природні умови, і діяльність конкурентів, і невмілі дії самого підприємця і багато іншого. Отже, виникає необхідність оцінити ризик, постаратися його передбачити і знизити до мінімуму можливі негативні наслідки.

Під ризиком в загальному розумінні цього слова розуміється можлива небезпека втрат, що випливає зі специфіки тих чи інших явищ природи і

видів діяльності людського суспільства. Можна ще сказати, що ризик - це розраховується або як-небудь інакше оцінюється ймовірність того чи іншого неблагополучного результату будь-яких дій окремої особистості, групи осіб, організації, держави і т.д. Таким чином ризик - це можливість небезпеки, невдач.

Під терміном «комерційний ризик» мається на увазі ризик, пов'язаний з господарською діяльністю підприємства і її кінцевим фінансовим результатом. Іншими словами, комерційний ризик - це загроза того, що підприємець зазнає втрат у вигляді додаткових витрат або отримає доходи нижчі за ті, на які він розраховував.

Комерційний ризик виникає в силу невизначеності умов діяльності організації, яка означає неможливість повного і всебічного аналізу всіх факторів, що впливають на результат конкретних дій. У свою чергу, невизначеність викликає ситуацію, коли є кілька можливих результатів, але наявних даних недостатньо для точного визначення, яке саме подія відбудеться. Можна виділити три основні причини, що викликають невизначеність, - це неповнота знань, випадковість і протидія.

Неповнота знань очевидна. Неможливо знати точно абсолютно все, багато явищ і процеси залишаються невідомими, не вся інформація є доступною. Отже, всі рішення комерсант приймає в умовах недостатності інформації.

Крім того, однакові події навіть в схожих умовах відбуваються по-різному, причому не можна передбачити заздалегідь, як це буде в конкретній ситуації, тобто має місце випадковість. Неможливо заздалегідь точно знати, яка кількість покупців прийде до нас за покупками, які товари їм будуть необхідні, як поведуть себе конкуренти, що буде з курсом рубля, не кажучи вже про можливі стихійні лиха та багато іншого. Спланувати кожен такий випадок неможливо, а раз невідомо, до чого може привести випадковість, з'являється ризик. До комерційних ризиків відносять:

– договірні умови та положення;

– внутрішнє матеріально-технічне постачання;

– постачальники та продавці;

– субпідрядники;

– стабільність клієнта / замовника;

– партнерства та спільні підприємства.

До ризиків договірних умов та положень в ІТ компаніях відносять:

– помилки в договорі, що може привести до зловживань клієнту;

– невизначені строки оплати рахунків;

– відсутність права власності на розроблений продукт;

– обмеженість відповідальності за продукт, або надзвичайно велика відповідальність.

До ризиків внутрішнього матеріально-технічного постачання відносять:

– відсутність можливості досягнення цілей в аналоговій схемі;

– неможливість досягнення вимог щодо розмірів у даному дизайні;

– відсутність можливості реалізації програмного алгоритму на цільовій машині;

– неможливість створення відповідності вимогам відповіді в системі реального часу;

– неможливість розміщення програмного забезпечення у доступну пам'ять.

До ризиків партнерства відносять:

– втрата самостійності: проблема процесів прийняття спільних рішень; необхідність досягнення консенсусу з партнерами перед вжиттям заходів та наслідків більшої підзвітності (перед іншими партнерами та більшими бенефіціарами);

– конфлікт інтересів: рішення або дія, що відповідає інтересам партнерства можуть суперечити індивідуальним інтересами організації;

– витрата на ресурси: докладання часу та енергії ключового персоналу для створення партнерства та розробки проектів на додаток до будь-яких додаткових фінансових чи інших вкладів у ресурси;

– виклики щодо впровадження: повсякденні вимоги щодо реалізації програми партнерства як спільної діяльності, з усіма додатковими вимогами до управління, відстеження, звітності та оцінки, що спричиняє утворення нового прихильства;

– негативний вплив на репутацію: коли партнерські стосунки виходять з ладу, завдаючи шкоди репутації чи послугам окремих партнерів асоціативно.

До третьої категорії ризиків ІТ підприємства можна віднести управлінські ризики, а саме (рисунок 3.3):

– ризик управління проектом;
– ризик управління програмою / портфелем;
– ризик управління операційною діяльністю;
– ризик організації;
– ризик забезпечення ресурсами;
– ризик комунікації.

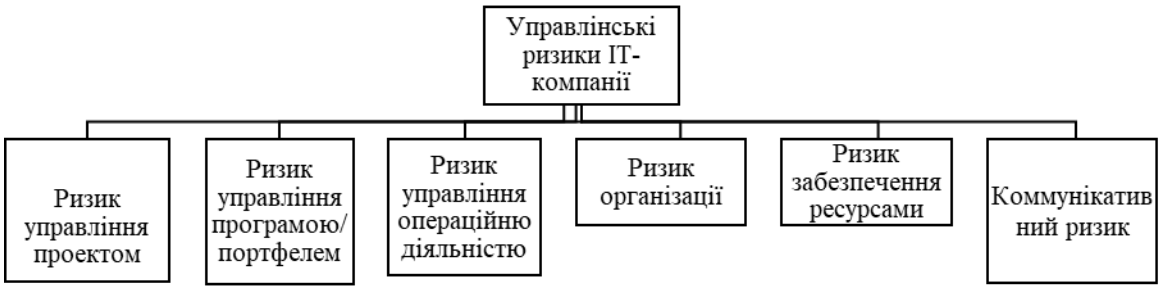

Рисунок 3.3 – Управлінські ризики ІТ-компанії

Ризики управління проектом містять в собі:

– неорганізованість процесів. Через неорганізованості процесів можуть актуалізуватися усі інші ризики. Наприклад: неорганізовано процес затвердження дизайну з менеджером проекту та зацікавленими особами, як наслідок – повторна розробка частини ПО з дизайном, який не підходить замовнику;

– неправильна оцінка часу або вартості проекту. Внаслідок неправильної оцінки часу замовник буде чекати проект раніше, ніж команда може його розробити. Через це компанія може зазнати збитків;

– недостатня комунікація з клієнтом. Через недостатню комунікацію з клієнтом можуть виникнути затримки з прийомом продукту або з підтвердженням або висуванням вимог до ПЗ.

Ризики управління програмою/портфелем складаються з таких ризиків:

– структурні ризики. Ризики, пов'язані зі змістом портфеля. Можуть бути викликані потенційними взаємодіями між компонентами портфеля. Одна з найбільш очевидних категорій загроз - доступність ресурсів. Особливості структури портфеля, в цілому, можуть бути головною причиною ряду ризиків;

– компонентні ризики. Ці ризики, пов'язані з окремими компонентами, які можуть загостритися на рівні портфеля. Компонентні ризики, як правило, пов'язані з одним або більше параметрів потрійного обмеження (час, вартість, результат);

– загальні ризики. Загальні ризики проекту більше, ніж просто сума окремих проектів портфеля (ефект синергії). Загальним ризиком є також якість управління портфелем організації: застосування передового досвіду, наприклад, може забезпечити великі можливості для досягнення мети, в той час як завищені плани, а також несумісні або швидко мінливі стратегії можуть становити загрозу для успіху.

До ризиків управління операційною діяльністю відносять:

– ризик помилок платіжних операцій;

– ризик невиконання платіжного календаря;

– ризик невірного нарахування податків і зборів;

– операційний валютний ризик;

– ризик портфельного інвестування придбання цінних паперів;

– інші операційні ризики фінансово-економічних служб.

Організаційний ризик - це потенціал збитків через невизначеність усіх необхідних умов функціонування. Це термін ризику на найвищому рівні організації, який включає:

– матеріальні;

– стратегічні;

– репутаційні;

– регуляторні;

– юридичні;

– безпекові;

– операційні ризики.

Наприклад:

– небезпечні продукти та ризики відповідальності за продукт;

– регуляторні ризики, такі як сумнівна екологічна практика;

– вразливості та загрози безпеці;

– фінансові ризики, такі як нестійкий рівень боргу;

– операційні ризики, такі як процеси схильності до відмов або старіння обладнання.

Ресурсний ризик - це ризик того, що ви не зможете досягти мети через брак ресурсів. До ресурсів можуть входити фінансовий ресурс, час, кваліфіковані працівники та інше. Наприклад:

– проект, який не може забезпечити кваліфікованого фахівця у встановлені терміни;

– проект, який зупиняється через затримання в процесах затвердження бюджету.

До ризиків комунікації можна віднести ризики:

– неопрацьований план комунікації із стейкхолдерами;

– недостатня комунікація команди та стейкхолдерів;

– недостатнє розуміння особливостей бізнесу замовника.

До четвертої категорії ризиків ІТ-підприємства можна віднести ризики технічного змісту, а саме:

– ризик визначення змісту;

– ризик визначення вимог;

– ризик оцінки, допущень і обмежень;

– ризик технічних процесів;

– ризик технології;

– ризик технічних інтерфейсів (рисунок 3.4).

Рисунок 3.4 – Ризики технічного характеру для ІТ-компанії

Розглянемо детально перераховані категорії ризиків:

– зацікавлені особи можуть додавати функції до продукту, які не були затверджені;

– команда проекту може не визначити всі результати розробки, які можуть потребувати змін пізніше;

– зміни змісту можуть не оброблятися в процесі управління змінами;

– вимоги можуть бути неправильно проаналізовані та не зрозумілі;

– вимоги можуть бути не визначені належним чином;

– структура простежуваності не може бути розроблена, що призводить до того, що вимоги не керовані процесами проектування, розробки та тестування, за рахунок неузгодженості або відсутності матриці зв’язків робіт та функіоналу;

– команда проекту може не визначити всіх дій, необхідних для створення результатів.

До ризику визначення вимог відносять такі ризики:

– пропуск зацікавлених сторін. У процесі управління вимогами не вдається виявити або залучити усі зацікавлені сторони. Наприклад, маркетинговий відділ реалізує новий продукт, але вони не беруть участь у проекті;

– помилково визначені зацікавлені сторони. Залучення зацікавлених сторін, які не володіють необхідними знаннями, вміннями чи повноваженнями для подання, валідації або відмови від вимог. Наприклад, збір вимог може бути призначений молодшим працівникам, які не мають достатнього доступу до експертних знань в організації;

– неоднозначні вимоги. Вимоги, визначені таким чином, що можливе її невірне тлумачення. У деяких випадках зацікавлені сторони можуть навмисно визначати вимоги відкритого типу, щоб уникнути прийняття рішення чи захистити себе політично. В інших випадках вимоги просто погано сформульовані. Наприклад: для покращення продуктивності користувальницький інтерфейс повинен бути упорядкований;

– неповні вимоги. Вимоги, які є неповними, призводять до результатів, які нестабільні, непридатні для використання або, як правило, неприйнятні. Наприклад, вимоги до системи, в якій не згадується користувальницький інтерфейс;

– суперечливі вимоги. Вимоги часто різними особами, які представлено списком потреб, що може конфліктувати один з одним. Власник вимог може не вирішити подібні конфлікти. Наприклад: доступ до

системи обмежений уповноваженим персоналом відділу кадрів. Користувацький інтерфейс дозволяє всім співробітникам вводити свої години за кодом діяльності;

– нездійсненні вимоги. Вимоги, що виходять за рамки можливостей організації або системи, до якої вони застосовуються. Ці ризики можна зменшити за допомогою швидкої доцільності або оцінки витрат. Наприклад: автомобіль набирає швидкість від 0 до 100 миль / год за 0,00001 секунди;

– «big ball of mud». Вимоги, які не мають загальної узгодженості, що призводить до низької якості результатів. Це буває, коли вимоги є результатом ідей багатьох людей без відповідального, який забезпечує стабільну згуртованість високого рівня. Це також може бути результатом перевірки вимог за списком без урахування вимог у цілому;

– неперевірені вимоги. Вимоги, які мають неправильно визначені критерії перевірки. Наприклад: автомобіль зробить людей щасливими;

– незадокументовані припущення. Вимоги, які працюють лише з урахуванням набору припущень, які не є задокументованими;

– недійсні припущення. Припущення часто є основним джерелом ризику, оскільки вони можуть бути надмірно оптимістичними або дезінформованими;

– бізнес-вимоги, представлені як функціональні вимоги. Бізнес-вимога, ідентифікується як функціональна вимога, та не може обмежувати результати діяльності. Іншими словами, функціональна вимога, яку безпосередньо не виконують ті, хто здійснює проект. Наприклад: Продажі покращаться на 300%;

– неадекватна перевірка. Вимоги, які не були підтверджені відповідними експертами з напрямків. Наприклад, нефункціональні вимоги до нової фінансової системи, які не були розглянуті аналітиком з безпеки.

До ризиків оцінки, допущень і обмежень відносять:

– недооцінка або переоцінка вартості проекту;

– недооцінка або переоцінка часових меж проекту;

– невірно висунуті припущення щодо проекту;

– помилкові судження щодо проектних обмежень.

До технологічних ризиків зазвичай відносять:

– архітектурний ризик. Ризик архітектури - це ризик того, що архітектурний дизайн не може задовольнити вимоги до проекту. Він включає обмеження потужностей, неякісні конструкції, недоліки та неефективність, які або відхиляються інвестором, або перешкоджають роботі над проектом;

– ризик управління активами. Невдале управління IT-активами, такі як втрата пристроїв, інструментів;

– аудиторський ризик. Це ризик вразливості безпеки чи застарілі ризики;

– ризик доступності. Доступність - це відсоток часу, коли послуга або ресурс повністю доступні за призначенням. Це ключовий операційний показник у ряді галузей;

– ризик ємності. Збої в управлінні ємністю, такі як перевантажене мережеве з'єднання, що викликає неефективність, таку як збої в процесі виконання програм;

– поганий контроль змін. Нестача контролю над змінами в складних системах, включаючи практику, управління змінами та управління конфігурацією;

– порушення відповідності. Наявність потенціалу, що може порушувати закони чи положення;

– ризик контракту. Контрагент, який не виконує своїх договірних зобов’язань перед вами, наприклад, порушення договору про рівень технічного обслуговування;

– втрата даних. Втрата даних, яку неможливо відновити;

– якість даних. Дані низької якості, що спричиняють збитки через такі фактори, як збої в процесі, проблеми з дотриманням вимог або зниження задоволеності клієнтів;

– якість рішення. Неоптимальна автоматизація рішень або неточна інформація для прийняття рішень, наприклад, аналітика;

– дизайнерське рішення. Низька якість дизайну, що призводить до майбутніх витрат;

– ризик інфраструктури. Збої основних сервісів, таких як мережі, електроживлення та обчислювальні ресурси;

– інноваційний ризик. Особлива категорія ризику, пов'язана з експериментами та агресивними темпами змін. Як правило, потрібні нові підходи до управління ризиками, такі як проектування діяльності;

– інтеграційний ризик. Прогнозована інтеграція організацій, департаментів, процесів, технологій чи даних не може бути завершена;

– спадкові технології. Використання технології, яка застаріла в тій мірі, в якій її важко підтримувати і вона загрожує збоями;

– операційний ризик. Потенціал ризику, що технологічні збої можуть порушити основні бізнес-процеси;

– ризик партнера. Ризики, пов'язані з технологічними партнерами, такими як постачальники послуг;

– фізична безпека. Фізична безпека, пов'язана з IT, наприклад, безпека в центрах обробки даних;

– загрози безпеці та вразливості безпеки. Загрози безпеці, такі як зловмисне програмне забезпечення та хакери та вразливості безпеки, такі як слабкі паролі та неякісне програмне забезпечення;

– технічний борг. Слабкі впровадження технологій, які, ймовірно, можуть спричинити майбутні витрати, такі як big ball of mud.

Отже, виходячи з вищеперерахованих факторів, можна побудувати ієрархічну структуру ризиків RBS типову для IT підприємства (таблиця 3.1).

Таблиця 3.1 – Типова ієрархічна структура ризиків ІТ підприємства

Усі джерела ризиків проекту	Рівень 1	Рівень 2
	1. Зовнішній ризик	Нормативно-правове регулювання
		Конкуренція
		Екологія/погода
		Майданчик/виробничі об’єкти
		Курси обміну валют
	2. Комерційний ризик	Внутрішнє матеріально-технічне постачання
		Договірні умови та положення
		Постачальники та продавці
		Субпідрядники
		Партнерства та сумісні підприємства
		Законодавство
	3. Управлінський ризик	Управління проектом
		Керування програмою/портфелем
		Керування операційною діяльністю
		Організація
		Забезпечення ресурсами
		Комунікація
	4.Технічний ризик	Визначення змісту
		Визначення вимог
		Оцінки, допущення, обмеження
		Технічні процеси
		Технологія
		Технічні інтерфейси

3.2 Формування методики оцінки та управління ризиками для забезпечення безпеки діяльності IT-підприємства

Проведене ґрунтовне дослідження для виявлення ризиків діяльності IT-компанії може стати основою для розробки плану реалізації стратегії управління ризиками для забезпечення безпеки діяльності IT-підприємства. Першим етапом розробки методики управління ризиками IT-підприємтсва є формування набору методів збору даних для ідентифікації ризиків в процесі діяльності конкретного підприємства

Методи збору даних, які можуть використовуватися в процесі ідентифікації ризиків, включають в себе, серед іншого:

– мозковий штурм. Метою мозкового штурму є формування вичерпного переліку індивідуальних ризиків і джерел сукупного ризику проекту. Як правило, мозковий штурм проводить команда проекту, у багатьох випадках за участю ряду експертів з різних областей, які не є членами команди. Генерація ідей відбувається під керівництвом модератора або в традиційній вільній формі мозкового штурму, або за допомогою більш структурованих методів. За основу можуть бути взяті категорії ризиків, як, наприклад, в ієрархічній структурі ризиків. Особливу увагу слід звернути на те, щоб ризики, ідентифіковані за підсумками мозкового штурму, були чітко описані, оскільки результатом даного методу можуть бути міркування, які не сформовані в повній мірі;

– контрольні списки. Контрольний список - це список питань, дій або пунктів, які потрібно розглянути. У багатьох випадках він служить пам'яткою. Контрольні списки розробляються на основі історичної інформації і знань, отриманих в ході виконання аналогічних проектів або з інших джерел інформації. Вони є результативним способом реєстрації засвоєних уроків з аналогічних завершених проектів, які перераховують індивідуальні ризики проекту, які відбулися в минулому і можуть ставитися

до даного проекту. В організації може вестися контрольний список ризиків на основі її власних завершених проектів або ж можуть використовуватися типові контрольні списки галузі. Незважаючи на те, що контрольний список може бути коротким і простим для використання, створити вичерпний список неможливо, і тому слід вжити заходів, щоб контрольний перелік не використовувався з метою уникнення трудовитрат, пов'язаних з належною ідентифікацією ризиків. Команда проекту повинна також приділяти увагу питанням, які не знайшли свого відображення в контрольному списку. Крім цього, контрольний список повинен переглядатися через певні проміжки часу з метою внесення в нього нової, а також видалення або архівування застарілої інформації;

– інтерв’ю. Індивідуальні ризики проекту і джерела сукупного ризику проекту можна ідентифікувати за допомогою інтерв'ю (опитувань) досвідчених учасників проекту, зацікавлених сторін та експертів з предметних областях. Інтерв'ю слід проводити в обстановці довіри і конфіденційності з метою створення умов для сумлінного і неупередженого обміну думками.

Методи аналізу даних, які можна використовувати в даному процесі для забезпечення безпеки ІТ-підприємства, включають в себе:

– аналіз першопричини. Аналіз першопричини зазвичай застосовується для виявлення основних причин, що призвели до виникнення проблеми, і розробки запобіжних дій. Він може використовуватися для ідентифікації загроз, починаючи з констатації проблеми (наприклад, в ході виконання проекту спостерігається затримка або перевищення бюджету) і з'ясування, результатом яких загроз може бути виникнення даної проблеми. Цей же метод може застосовуватися для пошуку сприятливих можливостей, починаючи з констатації вигод (наприклад, дострокова поставка або економія бюджетних коштів), і з'ясування, результатом яких сприятливих можливостей може стати реалізація даної вигоди;

– аналіз припущень і обмежень. Створення задуму і розробка кожного проекту і плану управління проектом здійснюється на основі ряду припущень і в рамках ряду обмежень. У багатьох випадках вони вже включені в базовий план за змістом і в оцінки проекту. Аналіз припущень і обмежень полягає в дослідженні достовірності прийнятих припущень і обмежень з метою визначення, які з них представляють ризик для проекту. Загрози можуть бути встановлені в зв'язку з неточністю, нестабільністю, непослідовністю або неповнотою припущень. Обмеження можуть стати основою для виникнення сприятливих можливостей за рахунок усунення або ослаблення обмежуючих факторів, які впливають на виконання проекту або процесу;

– SWOT-аналіз. Даний метод дозволяє провести аналіз проекту з точки зору кожного з аспектів: сильних і слабких сторін, сприятливих можливостей і загроз (strengths, weaknesses, opportunities, and threats, SWOT). Цей метод використовується при ідентифікації ризиків, щоб розширити ідентифіковані ризики за рахунок включення ризиків, що виникають всередині самого проекту. При використанні даного методу починають з визначення сильних і слабких сторін організації, приділяючи особливу увагу або проекту, або організації, або області бізнесу в цілому. Потім в процесі SWOT-аналізу ідентифікують будь-які сприятливі можливості проекту, які можуть виникати завдяки сильним сторонам організації, а також будь-які загрози, які є результатом її слабких сторін. За допомогою даного аналізу також досліджують, наскільки сильні сторони організації компенсують загрози, а також визначають, чи можуть слабкі сторони перешкодити реалізації сприятливих можливостей;

– аналіз документів. Ризики можна ідентифікувати за результатами структурованого аналізу документації по проекту, включаючи, серед іншого, плани, допущення, обмеження, архіви попередніх проектів, договори, угоди та технічну документацію. Невизначеність або неоднозначність в документації проекту, а також протиріччя в тому чи іншому документі або

між різними документами можуть служити ознаками наявності ризику в проекті;

– навички міжособистісних відносин і роботи з командою, які можна використовувати в даному процесі, включають в себе, серед іншого, фасилітації. Фасилітація підвищує результативність багатьох методів, використовуваних для ідентифікації індивідуальних ризиків проекту і джерел сукупного ризику проекту. Кваліфікований модератор може допомогти учасникам звернути належну увагу на завдання ідентифікації ризиків; точно слідувати прийомам, пов'язаним з цим методом; забезпечити чіткий опис ризиків; визначити і подолати джерела необ'єктивності; вирішити ті чи інші розбіжності, які можуть виникнути;

– довідкові списки. Довідковий список - це попередньо складений перелік категорій ризиків, які можуть служити джерелами індивідуальних ризиків проекту, а також сукупного ризику проекту. Довідковий список можна використовувати як базовий перелік як підмогу для команди в ході формування ідей в процесі застосування методів ідентифікації ризиків. Категорії ризиків самого нижнього рівня ієрархічної структури ризиків можна використовувати в якості довідкових списків для індивідуальних ризиків проекту. Деякі загальноприйняті стратегічні базові переліки більше підходять для ідентифікації джерел сукупного ризику проекту, наприклад: основа PESTLE (політичні, економічні, соціальні, технологічні, правові, екологічні ризики), основа TECOP (технічні, екологічні, комерційні, операційні, політичні ризики) або VUCA (мінливість, невизначеність, складність, неоднозначність);

– наради. Приступаючи до ідентифікації ризиків, команда проекту може провести спеціальну нараду (часто називається семінар за ризиками). У більшості випадків семінари за ризиками включають в себе мозковий штурм в тій чи іншій формі, а й інші методи ідентифікації ризиків можуть використовуватися на нараді в залежності від рівня процесу роботи з ризиками, визначеного в плані управління ризиками. Участь кваліфікованого

модератора підвищить результативність наради. Абсолютно необхідно також забезпечити належний склад учасників семінару за ризиками. У великих проектах може бути доцільно запросити спонсора проекту, експертів по предметним областям, продавців, представників замовника або інших зацікавлених сторін. Склад учасників семінарів за ризиками в разі більш дрібних проектів може бути обмежений частиною команди проекту;

– оцінка якості даних за ризиками. Оцінка якості даних за ризиками визначає ступінь, в якій дані про індивідуальні ризики проекту є точними і надійними для використання в якості основи якісного аналізу ризиків. Якщо дані за ризиками мають низьку якість, то якісний аналіз ризиків може виявитися марним для проекту. Якщо якість даних неприйнятно, можливо, буде потрібно зібрати більш якісні дані. Оцінити якість даних про ризики можна за допомогою анкети, що дозволяє отримати дані про думках зацікавлених сторін про різні характеристики, які можуть включати повноту, об'єктивність, релевантність і своєчасність. Можна отримати середньозважену оцінку за вибіркою характеристик якості даних для визначення загального балу оцінки якості;

– оцінка ймовірності та впливу ризиків. При оцінці ймовірності ризиків розглядається можливість виникнення того чи іншого ризику. При оцінці впливу ризику розглядаються потенційні наслідки, по крайней мере, для однієї з цілей проекту, наприклад розкладу, вартості, якості або виконання. Впливу будуть негативними в разі загроз і позитивними в разі сприятливих можливостей. Імовірність і вплив оцінюються для кожного ідентифікованого індивідуального ризику проекту. Ризики можуть бути оцінені в ході інтерв'ю або нарад з учасниками, яких вибирають з урахуванням їх знань про типи ризиків, зареєстрованих в реєстрі ризиків. У число опитуваних входять члени команди проекту і особи, які не беруть участі в проекті, але мають широкі пізнання в цій області. Під час інтерв'ю або наради оцінюється рівень ймовірності настання кожного ризику і його впливу на кожну з цілей проекту. Слід очікувати відмінностей в оцінках

рівня ймовірності та впливу різними зацікавленими сторонами, і ці відмінності слід уважно вивчити. Також фіксується пояснювальна інформація, в тому числі допущення, що обгрунтовують встановлені рівні. Ступеня ймовірності і впливів ризиків оцінюються з використанням визначень, передбачених в плані управління ризиками. Ризики з низьким ступенем ймовірності і впливу можуть бути включені до реєстру ризиків як частина списку спостереження для подальшого моніторингу;

– оцінка інших параметрів ризику. Команда проекту може розглянути інші характеристики ризику (крім ймовірності і впливу) при приоритизации індивідуальних ризиків проекту для аналізу і вжиття заходів у наступному.

Для вироблення ефективних рішень щодо запобігання небезпечних ризикових ситуацій слід визначити характеристики ризиків для IT-підприємства, що можуть включати в себе:

– терміновість. Період часу, протягом якого заходи реагування на ризик повинні бути здійснені, щоб вони дали очікуваний результат. Короткий період показує високу терміновість;

– близькість. Період часу до того, як ризик може вплинути на одну або кілька цілей проекту. Короткий період показує високу ступінь близькості;

– латентність. Період часу, який може пройти після настання ризику до виявлення його впливу. Короткий період свідчить низький ступінь латентності;

– керованість. Наскільки просто власник ризику (або організація-власник ризику) може керувати настанням або впливом ризику. У випадках, коли управління не представляє особливої складності, ступінь керованості є високою;

– контрольованість. Ступінь, в якій власник ризику (або організація-власник ризику) здатний контролювати наслідки ризику. У випадках, коли контроль наслідків ризику не представляє особливої складності, ступінь контрольованості є високою;

– виявлення. Наскільки просто можна виявити й пізнати ознаки настання або високої ймовірності настання ризику. У випадках, коли наступ ризику можна виявити без особливих зусиль, ступінь її виявлення вважається високою;

– спряженість. Ступінь, в якій ризик пов'язаний з іншими індивідуальними ризиками проекту. У випадку, коли ризик пов'язаний з декількома іншими ризиками, ступінь пов'язаності є високою;

– стратегічний вплив. Потенціал ризику зробити позитивний або негативний вплив на стратегічні цілі організації. У випадках, коли ризик може мати значний вплив на стратегічні цілі, ступінь стратегічного впливу є високою;

– сприйняття. Ступінь значущості ризику з точки зору сприйняття принаймні однією або декількома зацікавленими сторонами. У тому випадку, коли ризик сприймається як дуже значний, його сприйняття вважається високим.

У роботі з ризиками ІТ-підприємства пропонується використовувати п'ять альтернативних стратегій, які можна розглянути для використання, а саме:

– ескалація. Стратегія ескалації є доцільною у випадках, коли команда або спонсор проекту згодні, що загроза виходить за рамки проекту або що запропоновані заходи реагування виходять за рамки повноважень керівника проекту. Управління ескалацією ризиків здійснюється на рівні програми, портфеля або іншій відповідній частині організації, але не на рівні проекту. Керівник проекту визначає, кого слід повідомити про загрозу і доводить інформацію про неї до відома цієї особи або частини організації. Важливо, щоб володіння екскальованими погрозами було прийнято відповідною особою або частиною організації. В порядку ескалації загрози зазвичай передаються на рівень, відповідний цілям проекту, на які вплине загроза, якщо вона реалізується. Після здійснення ескалації команда проекту

не веде моніторинг загрози, переданої в порядку ескалації, хоча ця загроза може бути внесена до реєстру ризиків для інформації;

– ухилення. Ухилення від ризику - це стратегія, коли команда проекту вживає заходів з метою усунути загрозу або захистити проект від її впливу. Вона може бути доцільною в разі високо пріоритетних загроз з великою ймовірністю виникнення і серйозним негативним впливом. Ухилення може бути пов'язано з внесенням змін до той чи інший аспект плану управління проектом або зі зміною мети, яка опинилася під загрозою, щоб усунути загрозу повністю, знизивши ймовірність її виникнення до нуля. Власник ризику може також вжити заходів для огородження цілей проекту від впливу ризику в разі його настання. Як заходи ухилення можна назвати: ліквідацію причини загрози, збільшення термінів розкладу, зміна стратегії проекту або скорочення його змісту. Від деяких ризиків можна ухилитися шляхом уточнення вимог, отримання інформації, поліпшення комунікацій або придбання експертизи;

– передача. Передача складається в переході володіння загрозою до третьої сторони, яка бере на себе управління ризиком і несе наслідки в разі реалізації загрози. Передача ризику в багатьох випадках спричиняє виплату премії за ризик стороні, що приймає на себе наслідки загрози. Передача може здійснюватися шляхом ряду заходів, в числі яких, серед іншого, можна назвати наступні: використання страхування, гарантія виконання, гарантійні терміни, гарантійні зобов'язання і т. п. Певні ризики можуть передаватися за угодами про передачу власності і відповідальності;

– зниження. Стратегія зниження рівня ризику передбачає заходи щодо зниження ймовірності настання і / або впливу загрози. Ранні заходи щодо зниження ризику в багатьох випадках виявляються більш результативними, ніж спроби ліквідації збитку від незаконного продажу загрози. Як приклади дій щодо зниження ризиків можна привести впровадження менш складних процесів, проведення більшого числа випробувань або вибір більш надійного продавця. Зниження може бути

пов'язано з розробкою прототипу для зменшення ризику розростання масштабів процесу або продукту в порівнянні з стендової моделлю. Якщо зменшити ймовірність не представляється можливим, дії реагування щодо зниження ризику можуть бути спрямовані на зниження наслідків впливу ризику за рахунок впливу на фактори, які визначають тяжкість впливу. Наприклад, проектування резервування системи може зменшити важкість наслідків відмови вихідного елемента;

– ухвалення. Прийняття ризику означає усвідомлення існування загрози без прийняття проактивних заходів. Така стратегія може бути доцільною щодо фонових загроз; вона також може бути прийнята в тих випадках, коли ніякі інші заходи проти загрози не представляються можливими або економічно виправданими. Ухвалення може бути або активним, або пасивним. Найбільш поширеною стратегією активного прийняття є встановлення резерву на можливі втрати, включаючи певні величини часу, грошей або ресурсів, необхідні щоб управляти погрозами в разі їх реалізації. Пасивне прийняття не передбачає проактивних дій, крім періодичного розгляду загрози з метою переконатися у відсутності істотних змін в її стані.

3.3 Практична реалізація плану керування ризиками

У ході проведення досліджень в рамках магістерської атестаційної роботи розроблено план керування ризиками для IT-компанії Appus Software.

Практичні вказівки відноситься до проекту "ORION", який реалізується організацією "Appus Software".

План управління ризиками описує, як повинно бути організовано управління ризиками проекту, і як воно виконується в рамках проекту.

Цей план був розроблений на основі документів, які були створені в IT-компанії Appus Software, а саме: статут проекту, план управління проектом, проектні документи.

У плані керування ризиками вживаються технічні терміни та скорочення, які представлені у додатку Б.

Для впровадження плану управління ризиками проекту пропонується використовувати методології Agile (SCRUM).

Початковим етапом розробки плану керування ризиками проекту є розподіл ролей і відповідальності за ризики. Першою групою ризиків для розподілу ролей і відповідальності було обрано технічні ризики:

– зацікавлені особи можуть додавати функції до продукту, які не були затверджені – PM;

– команда проекту може не визначити всі результати розробки, які можуть потребувати змін пізніше – TL;

– вимоги можуть бути неправильно проаналізовані та зрозумілі – BA;

– команда проекту може не визначити всіх заходів, необхідних для створення результатів – TL, BA, PM;

– помилково визначені зацікавлені сторони – BA;

– неоднозначні вимоги – BA;

– неповні вимоги – BA;

– суперечливі вимоги – BA, TL;

– незадокументовані припущення – BA;

– недооцінка або переоцінка вартості проекту – PM;

– недооцінка або переоцінка часових меж проекту – PM;

– архітектурний ризик – TL;

– якість даних – TL;

– інтеграційний ризик – TL;

– ризик партнера – TL, PM;

– загрози безпеці – TL.

Таблиця із ідентифікатором ризику, розподілом ролей і відповідальності за технічні ризики надана у додатку В.

Другою групою ризиків для розподілу ролей і відповідальності було обрано управлінські ризики:

– неорганізованість процесів – CEO, PM;
– неправильна оцінка часу або вартості проекту – CEO, PM, TL;
– неналаштована комунікація з клієнтом – PM, BA;
– структурні ризики – TL, BA;
– компонентні ризики – TL, BA;
– ризик невиконання платіжного календаря – CEO;
– неможливість забезпечення кваліфікованого фахівця у встановлені терміни – CEO, PM, HR;
– не пропрацьований план комунікації із заінтересованими особами – BA;
– недостатня комунікація команди та заінтересованих осіб – PM, BA;
– недостатнє розуміння доменної області бізнесу замовника – PM, BA.

Таблиця із ідентифікатором ризику, розподілом ролей і відповідальності за управлінські ризики надана у додатку Б.

Третьою групою ризиків для розподілу ролей і відповідальності було обрано комерційні ризики:

– недостатньо прописані пункти договору – CEO, PM;
– невизначені строки оплати рахунків – CEO, PM;
– обмеженість відповідальності за продукт, або надзвичайно велика відповідальність – CEO.

Таблиця із ідентифікатором ризику, розподілом ролей і відповідальності за управлінські ризики надана у додатку Г.

Третьою групою ризиків для розподілу ролей і відповідальності було обрано зовнішні ризики:

– регуляторні ризики – CEO;

– ціноутворення – CEO;

– інновації – CEO;

– ресурси – CEO, HR;

– політичний стан – CEO.

Ідентифікатор ризику, розподіл ролей і відповідальності за зовнішні ризики представлено у додатку Д.

Для успішного впровадження плану керування ризиками необхідно ідентифікувати ризики та описати їх керування за наступними категоріями:

– протиризиковий захід;

– назва ризику;

– періодичність ризику або його прогнозована дата;

– граничний термін дії ризику;

– відповідальний за ризик.

Приклад термінів ризиків та протиризикових заходів,відсортованих по критерію періодичності(перед кожним спринтом) надано в таблиці 3.2.

Таблиця 3.2 – Терміни ризиків та протиризикові заходи

Проти ризиковий захід	Назва ризику	Періодичність або прогнозована дата	Гранічний термін	Відповідальний
Підтвердження вимог перед початком кожного спринта	Вимоги можуть бути неправильно проаналізовані та зрозумілі	Перед кожним спринтом	Кінець проекту	BA
Технічний спайк перед кожним спринтом	Команда проекту може не визначити всіх заходів, необхідних для створення результатів	Перед кожним спринтом	Кінець проекту	TL,BA,PM
Використання широкого рангу технік виявлення вимог та підтвердження їх	Неоднозначні вимоги	Перед кожним спринтом	Кінець проекту	BA
Використання широкого рангу технік виявлення вимог та підтвердження їх	Неповні вимоги	Перед кожним спринтом	Кінець проекту	BA

Продовження таблиці 3.2

Використання широкого рангу технік виявлення вимог та підтвердження їх, технічні перевіркиможливості виконання вимог	Суперечливі вимоги	Перед кожним спринтом	Кінець проекту	BA, TL
Моніторинг припущень щодо кожної вимоги	Незадокументовані припущення	Перед кожним спринтом	Кінець проекту	BA

Повний перелік термінів ризиків та протиризикові заходів надано у додатку Е.

Наступним кроком складання плану управління ризиками є створення структури категорій ризиків проекту (рисунок 3.5).

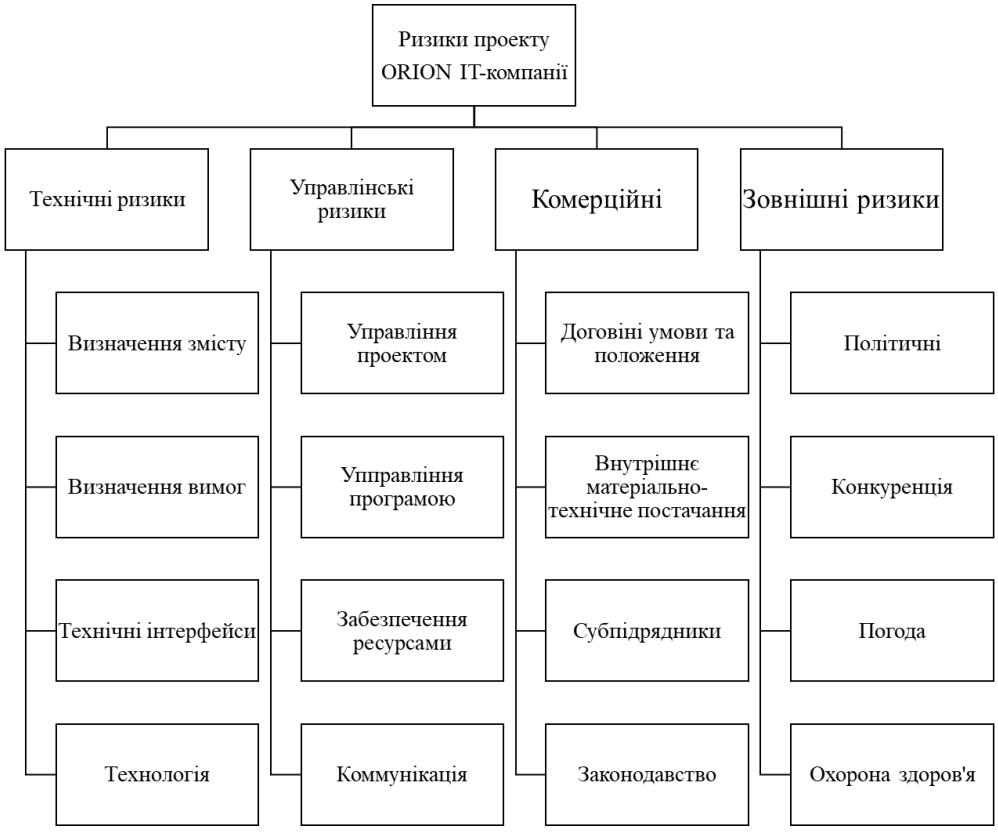

Рисунок 3.5 – Категорії ризиків, ідентифікованих на проекті

Шляхом експертного оцінювання було виявлення значущість кожного критерію для проекту (таблиця 3.3).

Таблиця 3.3 – Умови для оцінки впливу ризику на основні цілі проекту

Критерії проекту	Імовірність по відносній і числовий шкалами				
	Дуже низька 5%	Низька 10%	Помірна 20%	Висока 40%	Дуже висока 80%
Вартість	Незначне збільшення вартості	Збільшення вартості <10%	Збільшення вартості на 10-20%	Збільшення вартості на 20-40%	Збільшення вартості >40%
Строки	Незначне збільшення часу	Збільшення часу <5%	Збільшення часу на 5-10%	Збільшення часу на 10-20%	Збільшення часу >20%
Зміст	Ледь помітне зменшення змісту	Порушено другорядні області змісту	Порушено основні області змісту	Зменшення змісту неприйнятно для Замовника	Кінцевий продукт проекту фактично марний
Якість	Ледь значне зменшення якості	Порушено тільки самі трудомісткі додатки	Для зниження якості потрібне схвалення замовника	Зниження якості неприйнятно для Замовника	Кінцевий продукт проекту фактично марний

Наступним кроком було зроблено розподіл ризиків за критерієм вагомості ризику та ймовірністю його настання. Матриця ймовірності і наслідків представлена у таблиці 3.4.

Таблиця 3.4 – Матриця ймовірності і наслідків

Вагомість ризику	Ймовірність настання ризику				
	5	10	20	40	80
90					TR1 TR8 TR10 TR11 MR1 MR2 MR7 ER4
70					
50				TR9	TR3 TR4 TR6 TR7 MR4 MR5
30		TR2	MR10	MR8 MR9	TR12 TR14 TR16 MR6
10			TR15	TR5 TR13	MR3 CR1 CR2 CR3 ER1 ER2 ER5

Методом опитувань була виявлена толерантність зацікавлених сторін до ризиків, результати яких надані у таблиці 3.5.

Таблиця 3.5 – Толерантність зацікавлених сторін до ризиків

Зацікавлена сторона	Вартість	Строки	Зміст	Якість
Власник продукту	Граничне відхилення 5%	Граничне відхилення 5%	Граничне відхилення 0%	Граничне відхилення 0%
Спонсор проекту	Граничне відхилення 5%	Граничне відхилення 10%	Граничне відхилення 10%	Граничне відхилення 5%

Наступним кроком було виконано обговорення та прийняття форм звітності, які повинні бути на проекті. Форми звітності по ризикам на проекті:

– щоденне оновлення статусу розробки додатку по скайпу з власником продукту;

– щотижневий звіт по витраченому на проектування/ розробку/ дизайн/ тестування часу для власника продуку та спронсора проекту;

– демо по закінченню спринта для власника продукта та спонсора проекта;

– надання доступу до таблиці Терміни ризиків та протиризикових заходи.

Для відстеження статусів ризиків було обрано кольоровий контроль ризиків. За допомогою перефарбування слоту таблиці у відповідний колір можна зрозуміти у якому стані знаходиться ризик (рисунок 3.6).

	Ризик не активізован
	Ризик активізован
	Ризик в роботі
	Ризик закрито

Рисунок 3.6 – Таблиця значення кольорів

У третьому розділі було надано типові категорії ризиків для IT-підприємства, побудовано RBS типову для IT-компанії, надано кроки для складання плану управління ризиками IT-проекту та розроблена практична реалізація плану керування ризиками для IT- компанії Appus Software.

ВИСНОВКИ

Таким чином в роботі надано визначення сутності ризику, проведена їх класифікація, наведена оцінки впливу ризиків на діяльність підприємства в цілому та на його безпеку. Розглянуто та проаналізовано визначення економічної безпеки підприємства, що наведено в наукові й та учбовій літературі провідними фахівцями. Визначено, що ризик-менеджмент є одним з найкращих інструментів забезпечення безпеки підприємства. Надано етапи, які використовуються для формування загального процесу управління ризиками.

У другому розділі була розглянута загальна характеристика підприємства, проаналізовано основний перелік робіт та послуг компанії, описана організаційна структура IT-підприємства, надано опис системи управління. Проведено техніко-економічний аналіз фінансово-економічного стану підприємства, проаналізовано динаміку показників використання трудових ресурсів, їх вікова та освітня характеристика, описано ризики діяльності IT-компанії Appus Software. Надано загальні рекомендації щодо створення системи управління ризиками.

У третьому розділі було надано типові категорії ризиків для IT-підприємства, побудовано RBS типову для IT-компанії, надано кроки для складання плану управління ризиками IT-проекту та розроблена практична реалізація плану керування ризиками для IT- компанії Appus Software.

План управління ризиками описує, як повинно бути організовано управління ризиками проекту, і як воно виконується в рамках проекту.

Цей план був розроблений на основі документів, які були створені в IT-компанії Appus Software, а саме: статут проекту, план управління проектом, проектні документи.

У плані керування ризиками вживаються технічні терміни та скорочення, які представлені у додатку Б.

Для впровадження плану управління ризиками проекту пропонується використовувати методології Agile (SCRUM).

В ході виконання атестаційної роботи було виконано усі поставлені завдання:

- описано теоретичні дані з безпеки підприємтсва, ризиків, ризик-менеджменту;
- проведено техніко-економічний аналіз IT-компанії Appus Software;
- описано існуючу в IT-компанії Appus Software систему керування ризиками;
- розроблено план керування ризиками для проектів IT-компанії Appus Software.

ПЕРЕЛІК ДЖЕРЕЛ ПОСИЛАННЯ

1. Аберніхіна І.Г. Аналіз сучасних підходів до визначення економічної безпеки підприємства: навч. посібник. Київ, 2008. 113с.

2. Авдошин С.М. Информатизация бизнеса. Управление рисками: уч.пособ. Москва: ДМК Пресс, 2011. 176 с.

3. Ареф'єва О.В., Кузенко Т.Б. Економічні основи формування фінансової складової економічної безпеки. *Актуальні проблеми економіки*.2009. №1(91). С. 98-103.

4. Балдин К.В. Управление рисками в инновационно-инвестиционной деяльности предприятия: уч. пособие. Москва: Дашков и К, 2013. 420 с.

5. Бендиків М. Економічна безпека промислового підприємства. *Консультант директора.*2000. № 2.7. С .13.

6. Бендиків М.А. Економічна безпека промислового підприємства в умовах кризового розвитку: навч. посібник. Київ, 2000. 23с.

7. Васильців Т.Г. Економічна безпека підприємництва України: стратегія та механізми зміцнення: монографія. Львів: Арал, 2008. 386 с.

8. Власюк О.С. Теорія і практика економічної безпеки в системі науки про економіку: монографія. Київ, 2008. 48с.

9. Воробьев С.Н. Управление рисками в предпринимательстве: уч. пособие. Москва: Дашков и К, 2013. 482 с.

10. Геєць В.М. Моделювання економічної безпеки: держава, регіон, підприємство: монографія. Харків, 2006. 240 с.

11. Геєць В.М., Кизим М.О., Клебанова Т.С., Черняк О.І . Моделювання економічної безпеки: держава, регіон, підприємство: монографія. Харків: ІНЖЕК, 2006. 240 с.

12. Говтань О.Дж. Системний ризик у фінансовому середовищі: теоретичний аналіз і підходи до оцінювання: навч. посібник. Київ, 2011. 236 с.

13. Гончаренко Л.П., Куценко Е.С. Управление безопасностью: уч.пособие. Москва: КНОРУС, 2005. 272 с.

14. Горячева К.С. Фінансова безпека підприємства. Сутність та місце в системі економічної безпеки. *Економіст.* 2003. С. 65-67.

15. Гринькова В.М. Фінанси підприємств: навч. посібник. Київ: Знання-Прес, 2004. 424 с.

16. Дикань В.Л. Економічна безпека підприємств: навч. посібник. Харків: УкрДАЗТ, 2011. 266с.

17. Домащенко Д.В. Управление рисками в условиях финансовой нестабильности: уч. пособие. Москва: Магистр, ИНФРА-М, 2010. 238 с.

18. Драчов С.С. Основы корпоративной безопасности: уч. пособие. Санкт-Петербург: «Издательство Полигон», 2000. 240 с.

19. Єрмошенко М.М., Горячева К.С., Ашуєв А.М. Економічні та організаційні засади забезпечення фінансової безпеки підприємства: навч. посібник. Київ: Національна академія управління, 2005. 78 с.

20. Зубик В.Б. Економічна безпека підприємства: навч. посібник. Київ, 1998. 391 с.

21. Ільяшенко С.Н. Складові економічної безпеки підприємства та новітні підходи до їх оцінки. *Актуальні проблеми економіки.* 2009.№3. С.11-20.

22. Ільяшенко С.Н. Складові економічної безпеки підприємства та підходи до їх оцінювання. *Актуальні проблеми економіки.*2003.№1. С.21-24.

23. Капустин Н. Економічна безпека галузі та фірми. *Бізнес-інформ.* Київ,1999. № 11-12. С.45-47.

24. Кирій В.В. Обґрунтування розробки системи економічного моніторингу на основі використання інформаційних технологій. Харків: ХНУРЭ, 2015. С.161-172.

25. Кирій В.В. Формування інформаційної складової забезпечення безпеки підприємств. Харків: ХНУРЭ, 2014. 58с.

26. Ковалев Д., Сухорукова Т. Економічна безпека підприємства. *Економіка україни.* Київ, 1998. №10.С.48-52.

27. Ковалев П.П. Банковский риск-менеджмент: уч.пособие. Москва: ИНФРА-М, 2014. 320 с.

28. Козаченко Г.В. Економічна безпека підприємства:сутність та механізм забезпечення: монографія. Київ: Либра, 2003. 280 с.

29. Крисін А.В. Безпека підприємницької діяльності: навч. посібник. Москва,1996. 384 с.

30. Крушельницька О.В. Управління персоналом: навч. посібник. Київ: Кондор, 2003. 296 с.

31. Кудрявцев А.А. Інтегрований Ризик-менеджмент: навч. посібник. Москва: Економика, 2010. 656 с.

32. Лапченко Д.А. Методи оцінки ризику інвестиційних проектів. *Планово-економічний відділ*. 2013. № 3. С. 23-36.

33. Леонович Т.І. Управління ризиками в банківській діяльності: навч. посібник. Мінськ: Дикта, Місанта, 2012. 136 с.

34. Лященко В.П. Торгівля зброєю: проведення НДДКР, операції зі стратегічними матеріалами і сировиною, ризики та управління ризиками: навч. посібник. Москва: Економіка, 2008. 351 с.

35. Мамаєва Л.Н. Управління ризиками: навч. посібник. Москва: Дашков і К, 2013. 256 с.

36. Мішина І.Г. Сутність та елементи економічної безпеки, їх значимість в процесі реалізації національної безпеки країни: навч. посібник. Хмельницький: ТУП, 2003. 269с.

37. Мунтіян В.І. Економічна безпека України: навч. посібник. Київ: КВІЦ, 1999. 464 с.

38. Нагорна І.І. Організаційно-економічний механізм у забезпеченні стійкої економічної безпеки промислових підприємств: автореф. дис. на здобуття наук, ступеня канд. екон. наук: спец. 08.00.04. Одеса, 2008. 22 с.

39. Нагорна І.І Оцінка стійкої економічної безпеки промислового підприємства: навч. посібник. Одеса, 2008. 255 с.

40. Новіков А.І. Теорія прийняття рішень та управління ризиками у фінансовій і податковій сферах: навч. посібник. Москва: Дашков і К, 2012. 88 с.

41. Новікова О.Ф., Покотиленко Р.В. Економічна безпека: концептуальне визначення та механізм забезпечення: монографія. Донецьк: НАН України, 2006. 408 с.

42. Олейників Е.А. Основи економічної безпеки: навч. посібник. Москва:«Бизнес-школа «Интел-Синтез», 1997. 288 с.

43. Пілова Д.П. Обґрунтування рівня економічної безпеки підприємства як критерію оцінки результатів його господарської діяльності. *Економіка: проблеми теорії та практики.* Київ, 2007. № 224. С. 900-910.

44. Плошкіна В.В. Оцінка і управління ризиками на підприємствах: навч. посібник. Оскол: ТНТ, 2013. 448 с.

45. Подлужна Н.А. Вибір критерію економічної безпеки підприємства. *Наукові праці Донецького державного технічного університету.* 2002. № 47. С. 10-16.

46. Пономарев В.П. Економічна безпека підприємства: сутність та крітерії оцінки. *Вісник Східноукраїнського державного університету.* 1998. № 5. С. 90-96.

47. Рижикова О.Н. Управління ризиками інноваційних проектів. *Аудит і фінансовий аналіз.* 2011. № 6. С.4-8.

48. Рихтікова Н.А. Аналіз і управління ризиками організації: навч. посібник. Москва: Форум, 2012. 240 с.

49. Сенчагов В.К. Економічна безпека: геополітика, глобалізація, самозбереження і розвиток: навч. посібник. Москва, 2002.127с.

50. Склярова В.В. Особливості оцінки та управління інноваційними ризиками. *Фінанси і кредит.* 2011. № 13. С. 72-79.

51. Стребел П. Грамотні ходи. Як розумні стратегія, психологія та управління ризиками забезпечують успіх бізнесу: навч. посібник. Москва: Олімп-Бізнес, 2013. 208 с.

52. Судакова О.І. Формування системи управління економічною безпекою підприємництва: наукова праця. Дніпропетровськ: ДНУ, 2007. 1661с.

53. Титович А.А. Менеджмент ризику і страхування: навч. посібник. Мінськ: Вишейшая школа, 2011. 287 с.

54. Тімофеев В.О., Кирій В В. Використання методів моніторингу як інструменту оцінки стану соціально-еколого-економічної системи / *Міжнародна науково-практична конференція «Математичне моделювання процесів в економіці та управлінні проектами і програмами (ММП-2017)*. Харків: ХНУРЕ, 2017. С. 178-179.

55. Трофимчук О.М. Трансформація життєпридатності в небезпеку - головний тренд еволюції міського середовища України 21 століття. *Екологічна безпека та природокористування.* 2009 № 1. С. 5-27.

56. Уємов А.И. Ситемний підхід та загальна теорія систем: навч. посібник. Москва, 1978. 178с.

57. Уродовскіх В.Н. Управління ризиками підприємства: навч. посібник. Москва: ИНФРА-М, 2012. 168 с.

58. Федотова Г.В. Особливості оцінки інноваційних ризиків. *Фінанси і кредит.* 2011. № 10. С. 52-62.

59. Федотова Г.В. Управління ризиками в інноваційній діяльності підприємств . *Фінанси і кредит.* 2012. № 41. С. 27-34.

60. Філін С.О. Ризик як елемент стратегічного управління в інноваційній сфері. *Управління ризиком.* 2012. № 3.С. 38-51.

61. Фірсова О.А. Управління ризиками організацій: навч. посібник. Москва: МГО, 2014. 226 с.

62. Фомічов А.Н. Ризик-менеджмент: навч. посібник. Москва: Дашков і К, 2011. 376 с.

63. Хайлова Т.В. Основи комплексного підходу до управління економічною безпекою підприємництва: навч. посібник. Донецьк: ДонДАУ, 2003.240с.

64. Швиданенко Г.О. Бізнес-діагностика підприємства: навч. посібник. Київ: КНЕУ, 2008.344 с.

65. Шкарлет С.М. Еволюція категорії “безпека” в науковому та економічному середовищі. *Формування ринкових відносин в Україні*. 2007. №6. С. 6-12.