МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Безпека комп'ютерних систем і мереж»

Група: 4КБ-01

Дипломний проект

здобувача освіти денної форми навчання
КБ.01.17.000.ДП

СТРИЖАК
ЯРОСЛАВ ВЛАДИСЛАВОВИЧ

м. Одеса
2024 р.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Спеціальність: **123 «Комп'ютерна інженерія»**

Освітня програма: «**Безпека комп'ютерних систем і мереж»**

Група: **4КБ-01**

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту на тему:

Розробка рішення щодо оцінки стану рівня захищеності сучасного підприємства.

Проектний матеріал складається з пояснювальної записки на 67 сторінках та графічного (презентаційного) матеріалу на 6 аркушах (слайдах).

Дипломник _____ (Стрижак Я.В.)

Керівник _____ (Стайкуца С.В.)

Консультанти:

з економічного розділу_____ (Іванченков В.С.)

з розділу охорони праці та техніки безпеки_____ (Чорновол Н.І.)

з нормоконтролю _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Голова циклової комісії _____ (Кривченко Ю.В.)

Завідувач відділення _____ (Скорнякова О.В.)

Захист «21» 06 2024 р. Протокол ЕК № 5

Оцінка ЕК 4 (добре) 75 б.

Секретар ЕК _____

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *комп'ютерних систем* Комісія *КТ та ПІ*

Спеціальність *123 «Комп'ютерна інженерія»*

Освітня програма *«Безпека комп'ютерних систем і мереж»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР Беркань І.В.

"15" 01 2024 р.

ЗАВДАННЯ

на дипломний проект

Здобувачеві (здобувачці) освіти Стрижак Ярославу Владиславовичу

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи)) Розробка рішення щодо оцінки стану рівня захищеності сучасного підприємства

затверджена наказом по коледжу від "02" листопада 2023 р. № 244-А2-09

2. Термін здачі закінченого проекту (роботи) 10.06.2024 р.

3. Вихідні данні до проекту (роботи):

Екосистема ризиків - внутрішні та зовнішні

Ключові етапи роботи з ризиками - ідентифікація, оцінювання, вимірювання

Показник, відповідальний за ризик - карта ризиків (радар ризиків)

Елементи реалізації - JavaScript, Vue.js, ApexCharts.js, Vuetify

4. Зміст розрахунково-пояснювальної записки (перелік питань, які необхідно розробити)

Провести аналіз діяльності компанії з позиції ризик-менеджменту. Дослідити технології аналізу корпоративних ризиків. Розробити опитувальні анкети та механізми захисту. складність опитувальних листків для анкетування – базова. Реалізувати програмно рішення Щодо оцінки захищеностів підприємства. Навести економічну частину та охорону праці.

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

Базові поняття щодо ризиків та роботи з ними; Основні процеси життєвого циклу управління ризиками; Інструменти кількісного аналізу ризиків; Технології роботи з корпоративними ризиками; Побудова системи управління ризиками сучасного підприємства; Методики і рекомендації з управління ризиками; Розробка рішення щодо проведення перевірки стану захищеності підприємства; Модель оцінки рівня інформаційної безпеки підприємства; Побудова радару загроз; Засоби розробки ПЗ; Порівняння станів захищеності.

6. Консультанти по проекту, із зазначенням розділів проекту, що їх стосується

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
Основний розділ	*Стайкуца С.В.*		
Економічний розділ	*Іванченков В.С.*		
Розділ охорони праці	*Чорновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання 15 січня 2024 р.

Керівник *Стайкуца С.В.* _____
(підпис)

Завдання прийняв до виконання *Стрижак Я.В.* _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів дипломного проекту (роботи)	Термін виконання етапів дипломного проекту (роботи)	Відмітка про виконання
1.	*Вступ. Постановка задачі проектування*	*29.04.24-2.05.24*	Виконав
2.	*Аналіз технічного завдання та пошук літератури*	*2.05.24-4.05.24*	Виконав
3.	*Аналіз загроз та вразливостей сучасних підприємств*	*4.05.24-10.05.24*	Виконав
4.	*Вивчення методик аналізу та управління ризиками компанії*	*10.05.24-15.05.24*	Виконав
5.	*Дослідження методики і рекомендації з управління ризиками*	*15.05.24-19.05.24*	Виконав
6.	*Вибір моделі оцінки та складання базових питань*	*19.05.24-23.05.24*	Виконав
7.	*Аналіз механізмів захисту систем відеоспостереження*	*19.05.22-25.05.24*	Виконав
8.	*Вибір засобів розробки*		Виконав
9.	*Програмна реалізація інтерфейсу рішення*	*25.05.24-29.05.24*	Виконав
10.	*Виконання економічних розрахунків*	*29.05.24-2.06.24*	Виконав
11.	*Розробка питань з охорони праці та техніки безпеки*	*2.06.24-6.06.24*	Виконав
12.	*Підготовка мультимедійної презентації проекту*	*06.06.24-09.06.24*	Виконав

Дипломник _____
(підпис)

Керівник _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			КБ 01. 17 000. 00 ДП	Дипломний проект		
А4			КБ 01. 17 000. 00 ДП ПЗ	Пояснювальна записка	1	

Зм.	Арк.	№ докум.	Підпис	Дата	КБ 01. 17 000. 00 ДП		
Розробив		Стрижак Я.В.		10.06	Розробка рішення щодо оцінки стану захищеності сучасного підприємства	Літ.	Аркуш 4 / Аркушів 67
Перевірив		Стайкуца С.В.		10.06		Н Д П	
Н. Контр.		Петрашова Р.І.		10.06		ВСП "ОТФК ОНТУ" гр.4КБ-01	
Затверд.		Кривченко Ю.В.		10.06			

ЗМІСТ

ВСТУП

Ризик - одна з найважливіших складових підприємницької діяльності. У такому документі, як статут підприємства, чітко визначено, що підприємець веде свою господарську діяльність на свій страх і ризик. Від ризику не можна позбутися на 100%, але знаючи правила, методи і інструменти, їх можна істотно знизити.

Ряд керівників, які відповідальні за організацію режиму інформаційної безпеки, задаються питанням щодо оцінки рівня безпеки інформаційної системи підприємства. Які обрати механізми і алгоритми, з чого почати, як використовувати внутрішні корпоративні програми і методики кількісного аналізу інформаційних ризиків в сукупності з оцінками економічної ефективності інвестицій в забезпечення безпеки і захист інформації.

В цілому, розуміння методів роботи з корпоративними ризиками дає можливість більш ефективно вести роботу підприємства, оптимізувати бізнес-процеси та приймати правильніше рішення на основі ймовірностей і обґрунтувань.

Проблема в тому, що у більшості українські підприємці сприймають безпеку як додаткову опцію. Відповідно, опція часто стає не обов'язковою, а додатковою. при цьому в країнах Європи та Північної Америки вкладення у безпеку – давно не витрати, а інвестиції у безперервність. Розробка програмного рішення, яке дозволить оперативно провести перевірку поточного рівня безпеки та у вигляді радара загроз дати розуміння широкої аудиторії у різних сферах господарської діяльності стану безпеки - актуальне та необхідне рішення.

1 ОСНОВНА ЧАСТИНА

1.1 Аналіз загроз та вразливостей сучасних підприємств

1.1.1 Роль ризиків в діяльності сучасного підприємства

Внаслідок сучасної економічної кризи визначено, що включення управління ризиками в стандартні функції корпоративного управління стає дедалі важливішим аспектом.

Ризик розглядається як можливість завдання шкоди підприємству через реалізацію конкретної загрози його стабільності, використовуючи вразливості активів чи групи активів підприємства. Основна мета управління ризиками в процесі управлінських рішень на підприємстві – це підвищення ймовірності успішного функціонування на ринку за рахунок зниження впливу ризиків до прийнятного рівня та добуття конкурентних переваг.

Основні ризики підприємств спостерігаються у сфері реалізації продукції / надання послуг, у сфері постачання, в системі управління підприємством і персоналом. До найбільш значущих внутрішніх факторів ризику відносяться: збої в сфері реалізації продукції / надання послуг (розірвання договорів, повернення продукції, відмова від оплати продукції клієнтами тощо), перебої у сфері постачання (зрив поставок сировини, комплектуючих, матеріалів і т. п.), помилки персоналу і порушення виробничої дисципліни, порушення основного виду діяльності підприємства.

Ризик – це взаємодія двох ключових факторів: ймовірності виникнення інциденту та величини його потенційного впливу. Важливо розуміти, що ризик ніколи не може бути повністю усунутий. Визнання та прийняття залишкового ризику є невід'ємною частиною визначення того, що рівень безпеки відповідає вимогам підприємства. Керівництво компанії має бути обізнаним про всі ризики, їхні потенційні негативні наслідки та ймовірність інцидентів.

Фундаментальні компоненти управління ризиками на підприємстві охоплюють ідентифікацію та аналіз ризиків, оцінку виявлених ризиків та розробку захисних заходів. Такий комплексний підхід забезпечує системне розуміння потенційних загроз, що дозволяє приймати обґрунтовані рішення та розробляти стратегії для зменшення ризиків та ефективного управління ними.

Оцінка ризиків визначає ймовірність, наслідки та допустимі межі можливих інцидентів. "Оцінка ризиків є невід'ємною частиною ширшої стратегії управління ризиками, спрямованої на впровадження заходів контролю для усунення або зменшення будь-яких потенційних наслідків, пов'язаних з ризиком". Основна мета оцінки ризиків - уникнути негативних наслідків, пов'язаних з ризиком, або оцінити можливі можливості.

В рамках підходу до оцінки ризиків аналізуються взаємозв'язки між активами, процесами, загрозами, вразливостями та іншими факторами. Існує багато методів, але кількісний та якісний аналіз є найбільш відомими та використовуваними класифікаціями. Загалом, методологія, обрана на початку процесу прийняття рішень, повинна бути здатною надати кількісне пояснення впливу ризиків та питань безпеки, а також ідентифікувати ризики та сформувати реєстр ризиків. Також повинні бути якісні твердження, які пояснюють важливість і придатність заходів контролю та безпеки для мінімізації цих областей ризику.

Загалом, життєвий цикл управління ризиками включає сім основних процесів, які підтримують і доповнюють один одного (рис. 1.1):

Для оцінки та визначення пріоритетності ризику можна використовувати різні методи. Залежно від того, наскільки добре відомий ризик і чи можна його своєчасно оцінити та визначити пріоритетність, можна зменшити можливі негативні наслідки або збільшити можливі позитивні наслідки та скористатися можливостями. "Кількісний аналіз ризику намагається визначити об'єктивні числові або вимірювані значення" незалежно від компонентів оцінки ризику та оцінки потенційних втрат. І навпаки, "якісний аналіз ризиків базується на сценаріях".

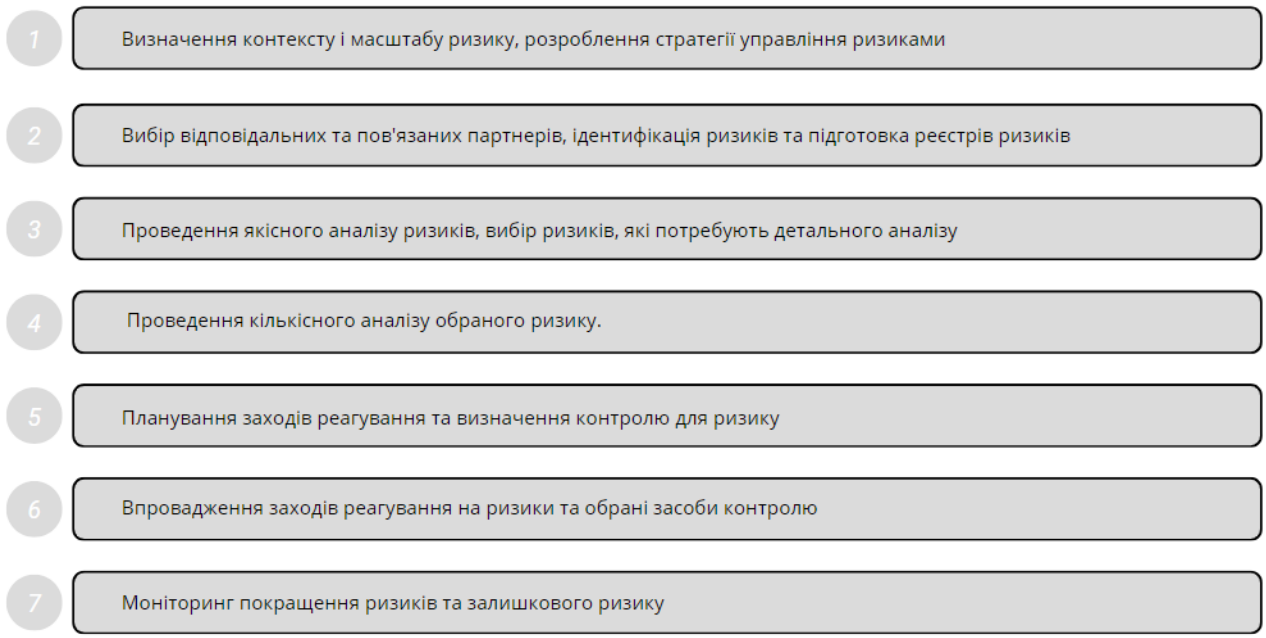


Рисунок 1.1. Основні процеси життєвого циклу управління ризиками

Метою якісного аналізу ризиків є визначення ризиків, які потребують детального аналізу, а також необхідних заходів контролю та дій на основі впливу ризику та його впливу на цілі. У якісному аналізі ризиків добре відомі два прості методи, які легко застосовуються до ризиків:

Keep It Super Simple (KISS) - цей метод можна використовувати у вузькоспеціалізованих або невеликих проектах, де слід уникати зайвої складності, а оцінка може бути легко здійснена командами, яким бракує зрілості в оцінці ризиків. Ця одновимірна методика передбачає оцінювання ризику за базовою шкалою, наприклад, дуже високий/високий/середній/низький/дуже високий.

Ймовірність/вплив - цей метод можна використовувати для більших і складніших питань у багатосторонніх командах, які мають досвід оцінки ризиків. Цей двовимірний метод використовується для оцінки ймовірності та впливу. Ймовірність - це ймовірність того, що ризик відбудеться. Вплив - це наслідок або ефект ризику, зазвичай пов'язаний з впливом на графік, вартість,

обсяг і якість. Оцініть ймовірність і вплив, використовуючи шкалу від 1 до 10 або від 1 до 5, де оцінка ризику дорівнює ймовірності, помноженій на вплив.

Якісний аналіз ризиків зазвичай можна проводити для всіх бізнес-ризиків. Якісний підхід використовується для швидкого виявлення зон ризику, пов'язаних зі звичайними бізнес-функціями. Оцінка може визначити, чи пов'язані занепокоєння людей щодо їхньої роботи з цими сферами ризику. Потім кількісний підхід допомагає розробити відповідні сценарії ризиків, щоб запропонувати більш детальну інформацію для прийняття рішень. Перед прийняттям важливих рішень або виконанням складних завдань кількісний аналіз ризиків надає більш об'єктивну інформацію і точні дані, ніж якісний аналіз. Хоча кількісний аналіз є більш об'єктивним, слід зазначити, що в ньому все одно присутня оцінка або висновок. Мудрі ризик-менеджери враховують інші фактори в процесі прийняття рішень. Після якісного аналізу також може бути застосований кількісний аналіз. Однак, якщо результати якісного аналізу є достатніми, немає необхідності проводити кількісний аналіз кожного ризику.

Кількісний аналіз ризиків - це ще один вид аналізу високопріоритетних та/або ризиків з високим рівнем впливу, де надається числовий або кількісний рейтинг для розробки ймовірнісної оцінки питань, пов'язаних з бізнесом. Крім того, кількісний аналіз ризиків для всіх проектів або питань/процесів, що управляються за допомогою проектного підходу, має більш обмежене застосування, залежно від типу проекту, проектного ризику та наявності даних, які можна використовувати для кількісного аналізу. Метою кількісного аналізу ризиків є переведення ймовірності та впливу ризику у вимірювану величину. На рис. _ представлено До основних задач кількісного аналізу відносяться:

– визначення можливих наслідків для бізнес-проблем та оцінка ймовірністі досягнення конкретних бізнес-цілей"

– забезпечення кількісного підходу до прийняття рішень в умовах невизначеності

– створення реалістичних та досяжних цілей щодо вартості, графіку або обсягу робіт

Переваги використання кількісного аналізу ризиків представлено на рис. 1.2

Рисунок 1.2. Переваги використання кількісного аналізу ризиків

Найпоширенішою проблемою кількісного оцінювання є недостатня кількість даних для аналізу.

Для проведення кількісного аналізу ризиків бізнес-процесу або проекту необхідні якісні дані, чіткий бізнес-план, добре розроблена модель проекту та перелік пріоритетних ризиків бізнесу/проекту. Кількісна оцінка ризику ґрунтується на реалістичних і вимірюваних даних для розрахунку значень впливу, які ризик створить з ймовірністю настання. Така оцінка спирається на математичні та статистичні основи і може "виразити значення ризику в грошовому еквіваленті, що робить її результати корисними поза контекстом оцінки (втрата грошей зрозуміла для будь-якої бізнес-одиниці)". Найпоширенішою проблемою кількісної оцінки є відсутність достатньої кількості даних, що підлягають аналізу. Також можуть виникнути труднощі з розкриттям предмета оцінки за допомогою числових значень, або кількість відповідних змінних є занадто великою. Це робить аналіз ризиків технічно складним.

Існує кілька інструментів і методів, які можна використовувати в кількісному аналізі ризиків. Ці інструменти та методи включають:

Рисунок 1.3. Інструменти кількісного аналізу ризиків

Існують також деякі базові (цільові, оціночні або розрахункові) значення, що використовуються при кількісній оцінці ризику. Очікуваний разовий збиток (SLE) - це гроші або цінності, які, як очікується, будуть втрачені, якщо інцидент станеться один раз, а річна частота виникнення (ARO) - це те, скільки разів протягом одного року очікується, що інцидент станеться. Очікуваний річний рівень втрат (ALE) може бути використаний для обґрунтування вартості застосування контрзаходів для захисту активу або процесу. Очікується, що ці гроші/цінності будуть втрачені протягом одного року з урахуванням SLE та ARO. Цю величину можна розрахувати, помноживши SLE на ARO. Для кількісної оцінки ризику - це величина ризику.

Використання обох підходів може підвищити ефективність процесу та допомогти досягти бажаного рівня безпеки.

Щодо репутаційних ризиків. За визначенням, репутаційний ризик - це ймовірність того, що негативна реклама, громадська думка або неконтрольовані події можуть негативно вплинути на репутацію компанії, тим самим зменшуючи її доходи.

Репутаційний ризик настає без попередження і змінює ваш корпоративний ландшафт. Навіть гірше, він вносить несприятливий наратив у результати пошуку, що впливає на думку клієнтів і знижує доходи. Існує незліченна кількість статистичних даних про репутацію в Інтернеті, які підтверджують цей висновок.

На жаль, репутаційним ризиком часто нехтують або плутають з іншими видами корпоративних ризиків. Розглянемо, як вони пов'язані між собою.

Стратегічний ризик є конкретним, вимірюваним і передбачуваним. Тому його можна контролювати. Репутаційний ризик, з іншого боку, значною мірою непередбачуваний. Насправді, він може бути пов'язаний навіть з подіями, в яких ваша компанія не винна. Тим не менш, думки клієнтів, інвесторів, ділових партнерів і широкої громадськості можуть мати значний вплив на доходи вашої фірми. Тому дуже важливо знати про небезпеки, які можуть призвести до репутаційної шкоди для бізнесу.

Репутація вашого бізнесу - це ваш найцінніший актив. Негативна корпоративна репутація шкодить довірі клієнтів та інвесторів, підриває вашу клієнтську базу та перешкоджає продажам. Погана репутація також корелює зі збільшенням витрат на найм та утримання персоналу, що знижує операційну рентабельність і перешкоджає підвищенню прибутковості.

Крім того, репутаційна шкода збільшує ризик ліквідності, що впливає на ціну акцій і, зрештою, знижує ринкову капіталізацію.

1.1.2 Базовий склад ризиків

Компанії стикаються з бізнес-ризиками, коли існує потенційна невизначеність щодо стратегії, прибутків, дотримання законодавства, навколишнього середовища, охорони здоров'я та безпеки. Бізнес-ризики можуть вплинути на фінансовий результат компанії та її репутацію серед споживачів, а плани управління ризиками можуть допомогти їх пом'якшити.

Бізнес-ризик загрожує фінансовим цілям компанії. Бізнес-ризики можна класифікувати як внутрішні та зовнішні, і вони можуть включати в себе політичні зміни, загрози кібербезпеці, загрози репутації, злиття та поглинання, кризи у сфері охорони здоров'я та небезпеки, пов'язані з місцезнаходженням.

Розглянемо декілька типів бізнес-ризиків, на які слід звертати увагу при оцінці стану компанії:

1. Комплаєнс-ризик

Комплаєнс-ризик - це ризик для репутації або фінансів компанії, який виникає через порушення компанією зовнішніх законів і нормативних актів або внутрішніх стандартів. Комплаєнс-ризик може призвести до сплати штрафних санкцій або втрати клієнтів.

2. Юридичний ризик

Юридичний ризик - це особливий вид комплаєнс-ризику, який виникає, коли компанія не дотримується встановлених урядом правил для компаній. Юридичні ризики можуть призвести до дорогих судових позовів та негативної репутації компанії. Ось кілька типів юридичних ризиків для компаній:

Договірні ризики: Договірні ризики виникають, коли компанія не виконує зобов'язання або зобов'язання за бізнес-контрактом.

Судові ризики: Судові ризики виникають, коли юридичний конфлікт із клієнтом, зацікавленою стороною або членом громади перериває бізнес-процеси.

Регуляторні ризики: Регуляторний ризик може виникнути, якщо державний регулятор відкликає ліцензію на діяльність компанії.

3. Стратегічний ризик

Стратегічний ризик виникає, коли бізнес-стратегія компанії є хибною або її керівники не дотримуються бізнес-стратегії взагалі. Через стратегічні ризики компанія може не досягти своїх цілей.

4. Репутаційний ризик

Репутаційний ризик загрожує становищу компанії або громадській думці. Репутаційні ризики можуть призвести до зменшення прибутку та втрати довіри серед акціонерів компанії.

5. Операційний ризик

Операційний ризик виникає, коли повсякденна діяльність бізнесу загрожує зменшенню його прибутку. Внутрішні системи або зовнішні фактори можуть спричинити операційні ризики для компаній. Ось кілька конкретних видів операційних ризиків:

Помилки персоналу: Бізнес може зіткнутися із загрозою для своєї діяльності, якщо працівники припускаються значних помилок у роботі.

Пошкодження активів: Стихійне лихо може пошкодити фізичні активи компанії, що також є операційним ризиком.

Зовнішнє шахрайство: Коли компанія стикається із зовнішнім шахрайством, наприклад, крадіжкою третьою стороною, крадіжка становить операційний ризик для компанії.

6. Людський ризик

Людські ризики в бізнесі можуть виникати через невиконання працівниками своїх основних обов'язків на робочому місці. Людські ризики можуть виникати через фактори, які працівники не можуть контролювати, наприклад, проблеми зі здоров'ям, або через навмисні дії, такі як крадіжка чи шахрайство. Коли бізнес стикається з людськими ризиками, він може зазнати втрати прибутку.

7. Ризик безпеки

Бізнес може зіткнутися з ризиком безпеки, якщо він не створить або не дотримуватиметься стратегії кібербезпеки. Неефективне навчання працівників, відсутність тестування програмного забезпечення та недостатня політика щодо

оновлень безпеки - все це може поставити під загрозу фінанси та репутацію компанії.

8. Фінансовий ризик

Фінансові ризики можуть виникати, коли компанія не виконує завдання з управління боргом або фінансового планування. Зміни на ринку або збитки можуть загрожувати фінансовому стану компанії. Ось кілька типів фінансових ризиків для бізнесу:

Валютний ризик: Бізнес може зазнати валютних ризиків у міжнародних ділових операціях, оскільки вартість іноземної валюти може несподівано знецінитися.

Ризик дефолту: Отримання бізнес-кредиту під більший відсоток, ніж компанія може собі дозволити, може поставити компанію під загрозу дефолту або несплати кредиту.

Ризик ліквідності: Компанія стикається з ризиком ліквідності, коли вона не може швидко конвертувати свої активи в готівку.

9. Ризик конкуренції

Ризик конкуренції може виникнути, коли конкурент завойовує все більшу частку ринку для продукту або послуги. Іноді його називають ризиком комфорту, оскільки він може бути наслідком того, що керівники компанії настільки задоволені результатами діяльності компанії, що не здатні постійно вдосконалювати продукти чи послуги компанії.

10. Фізичний ризик

Фізичні ризики - це загрози фізичним активам компанії, таким як обладнання, будівлі та працівники. Причинами фізичних ризиків можуть бути пошкодження будівель внаслідок пожежі або стихійного лиха, а також недостатнє навчання щодо належного використання обладнання. Через фізичні ризики бізнесу може знадобитися оплатити ремонт матеріальних активів.

Нижче наведено перелік кроків, які ви можете зробити для виявлення ризиків для вашого бізнесу:

1. Проаналізуйте бізнес-процеси

Першим кроком до виявлення бізнес-ризиків є аналіз процесів. Ви можете провести SWOT-аналіз, щоб оцінити діяльність компанії в наступних сферах:

Сильні сторони: Визначення сильних сторін вашої компанії може допомогти вам дізнатися, що компанія робить добре. Ви також можете розширити сильні сторони, щоб захиститися від бізнес-ризиків.

Слабкі сторони: Визначивши слабкі сторони вашої компанії, ви можете розробити стратегії для зміцнення компанії в цих сферах.

Можливості: Ви можете провести дослідження ринку, щоб дізнатися про потенціал зростання вашої компанії або інші можливості для вдосконалення

2. Дослідження ризиків на всіх рівнях

Після того, як ви проаналізуєте робочі процеси, ви можете шукати ризики на кожному рівні бізнесу. Анонімне опитування працівників, від керівництва до працівників початкового рівня, може допомогти вам виявити загрози для кожної сфери бізнесу.

Рисунок 1.4. Класифікація ризиків підприємства

3. Визначте загальні ризики у вашій галузі

Ви можете провести дослідження ринку, щоб визначити сильні, слабкі сторони та ризики ваших конкурентів у вашій галузі чи регіоні. Пошук спільних

ризиків для подібних бізнесів може дати вам ідеї щодо політик та процесів, які зменшують ці ризики.

4. Записуйте ризики

Ви можете створити запис для кожного ризику, щоб дізнатися про повторювані загрози для репутації або прибутку бізнесу. Якщо бізнес стикається з тими самими ризиками неодноразово, ви можете розробити політику, яка допоможе захистити бізнес від загрози.

1.1.3 Інтеграфія ризик-менеджменту в аспекті стратегії неперервного управління

Процес забезпечення безпеки на підприємстві передбачає низку періодичних дій і повинен бути впроваджений у виробничі та комерційні операції. Безперервне управління ризиками має вирішальне значення, і воно повинно здійснюватися в будь-який відповідний момент. Впровадження інтегрованого підходу до управління ризиками складається з ланки етапів :

Ідентифікація важливих ризиків (передбачає складання переліків і карт значущих ризиків та їх оцінку для розуміння їхнього впливу).

Вимірювання ризиків (включає такі заходи, як стрес-тестування для кількісної оцінки виявлених ризиків).

Комплексний підхід до аналізу ризиків:

Використання комплексного підходу до аналізу ризиків дозволяє застосовувати методи раннього попередження для виявлення потенційних проблем та KPI ключових ризиків підприємства.

Необхідність щодо внесення змін з боку підприємства у сфері безпеки мають бути враховані під час планування та прийняття рішень щодо його господарської діяльності. Варто зазначити, що деяким підприємствам бракує усвідомлення власних бізнес-процесів. Ці організації не визначили ключові процеси або ті, що є невід'ємною частиною основних процесів.

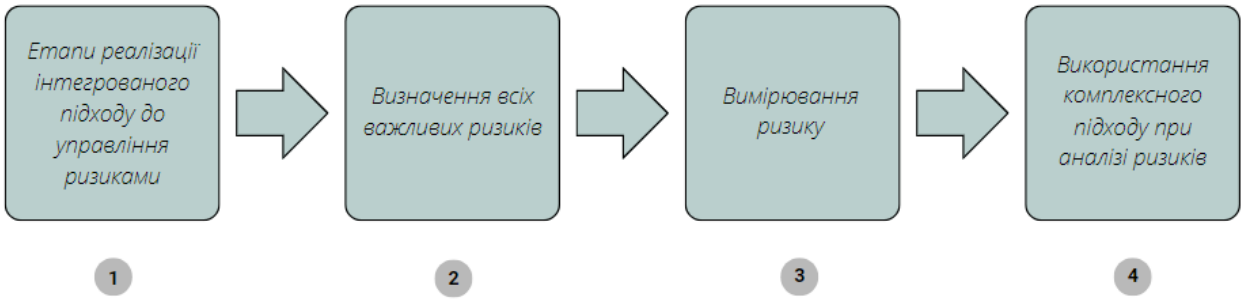


Рисунок 1.5. Етапи реалізації інтегрованого підходу до управління ризиками

Загальноприйнятого каталогу бізнес-процесів не існує, оскільки кожна компанія формує свою бізнес-структуру таким чином, щоб сприяти ефективному управлінню ризиками в організації. На будь-якому підприємстві бізнес-процеси можна розділити на основні та допоміжні. Основні процеси є невід'ємною частиною повсякденної діяльності компанії, генеруючи результати, спрямовані на задоволення потреб зовнішніх клієнтів. У той же час, допоміжні процеси покликані підтримувати та сприяти безперебійному функціонуванню основних процесів.

До основних бізнес-процесів на підприємстві зазвичай відносять маркетинг, закупівлі, виробництво/надання послуг, логістику, продажі та сервіс. Такі процеси, в основному, є в більшості видів бізнесу. З іншого боку, допоміжні процеси охоплюють такі види діяльності, як навчання, фінансова та бухгалтерська підтримка, адміністративно-господарська підтримка, безпека, IT-підтримка та інші. На рис. 1.6 представлено класифікацію бізнес-процесів підприємства.

Допоміжні бізнес-процеси не є другорядними, вони мають фундаментальне значення для загальної операційної ефективності підприємства. Кількість бізнес-процесів варіюється від підприємства до підприємства і часто залежить від специфіки його діяльності. Як правило, компанії мають близько 3-4 основних процесів і до 10-ти допоміжних бізнес-процесів.

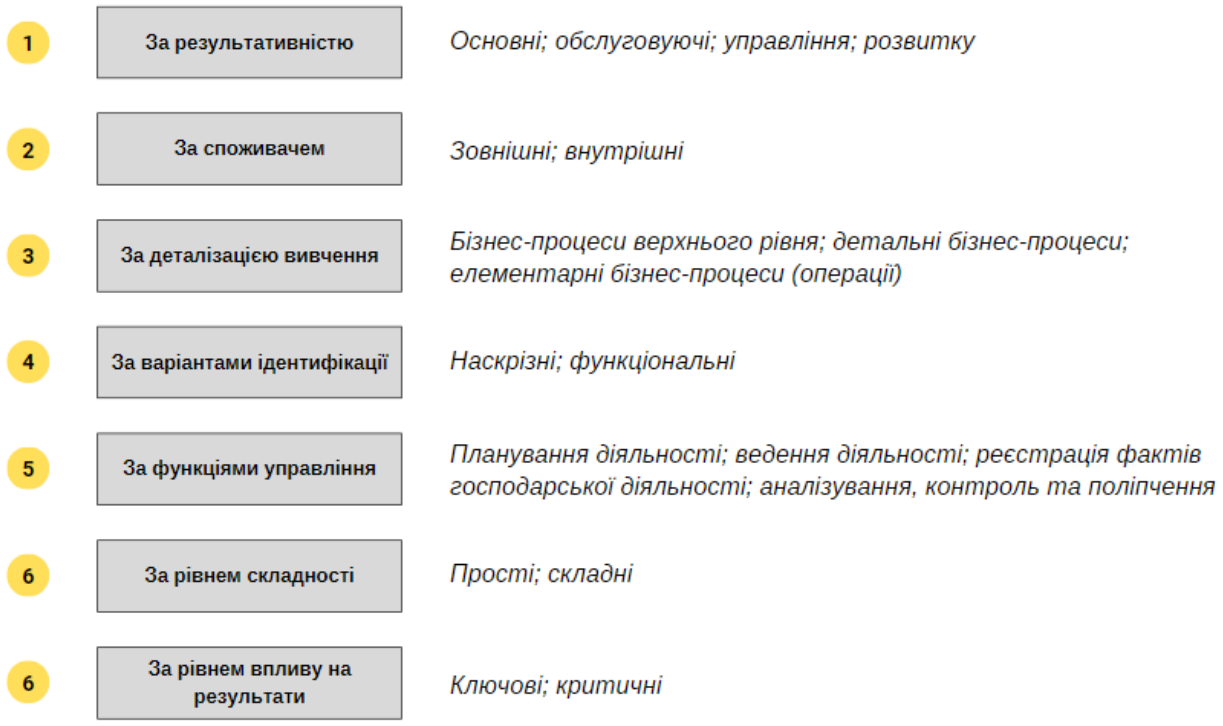


Рисунок 1.6. Класифікація бізнес-процесів підприємства

1.2 Технології роботи з корпоративними ризиками

1.2.1 Щодо аналізу та управління ризиками

Ідентифікація ризиків.

У будь-якій методиці необхідно ідентифікувати ризики, як варіант - їх складові (загрози і вразливості). Природною вимогою до списку є його повнота. Складність завдання складання списку і доказ його повноти залежить від того, які вимоги пред'являються до деталізації списку. На базовому рівні безпеки (третій рівень зрілості організації) спеціальних вимог до деталізації класів, як правило, не пред'являється і досить використовувати будь-якої відповідний в даному випадку стандартний список класів ризиків. Оцінка величини ризиків не розглядається, що прийнятно для деяких різновидів методик базового рівня. Списки класів ризиків містяться в деяких посібниках, в спеціалізованому ПО аналізу ризиків. Прикладом є стандарт BSI, в якому є каталог загроз стосовно до

різних елементів інформаційної технології. Перевагою подібних списків є їх повнота: класів, як правило, трохи (десятки), вони досить широкі і свідомо покривають все існуюче безліч ризиків. Недолік - складність оцінки рівня ризику та ефективності контрзаходів для широкого класу, оскільки подібні розрахунки зручніше проводити по більш вузьким (конкретним) класів ризиків. Наприклад, клас ризиків «несправність маршрутизатора» може бути розбитий на безліч підкласів, що включають можливі види несправності (уразливості) ПЗ конкретного маршрутизатора і несправності обладнання.

Оцінювання ризиків. Оцінка ризику - це систематичний процес, що виконується компетентною особою, який включає виявлення, аналіз і контроль небезпек і ризиків, присутніх у ситуації або місці. Цей інструмент прийняття рішень спрямований на визначення того, яких заходів слід вжити для усунення або контролю цих ризиків, а також на визначення того, які з них мають бути пріоритетними відповідно до рівня ймовірності та впливу, який вони чинять на бізнес. Оцінка ризику є одним з основних компонентів аналізу ризику. Аналіз ризиків - це процес, що складається з декількох етапів, метою якого є виявлення та аналіз усіх потенційних ризиків і проблем, що завдають шкоди бізнесу або підприємству. Це безперервний процес, який оновлюється в міру необхідності. Ці поняття взаємопов'язані і можуть використовуватися окремо.

Комунікація про ризики - це процес обміну інформацією та думками про ризики із зацікавленими сторонами. Управління ризиками - це попереджувальний контроль та оцінка загроз і ризиків для запобігання нещасним випадкам, невизначеностям і помилкам. Разом з оцінкою ризиків усе це життєво важливі елементи, які допомагають ухвалювати обґрунтовані рішення, наприклад, щодо зниження ризиків..

Процес отримання суб'єктивної ймовірності зазвичай поділяють три етапи: підготовчий етап, отримання оцінок, етап аналізу отриманих оцінок.

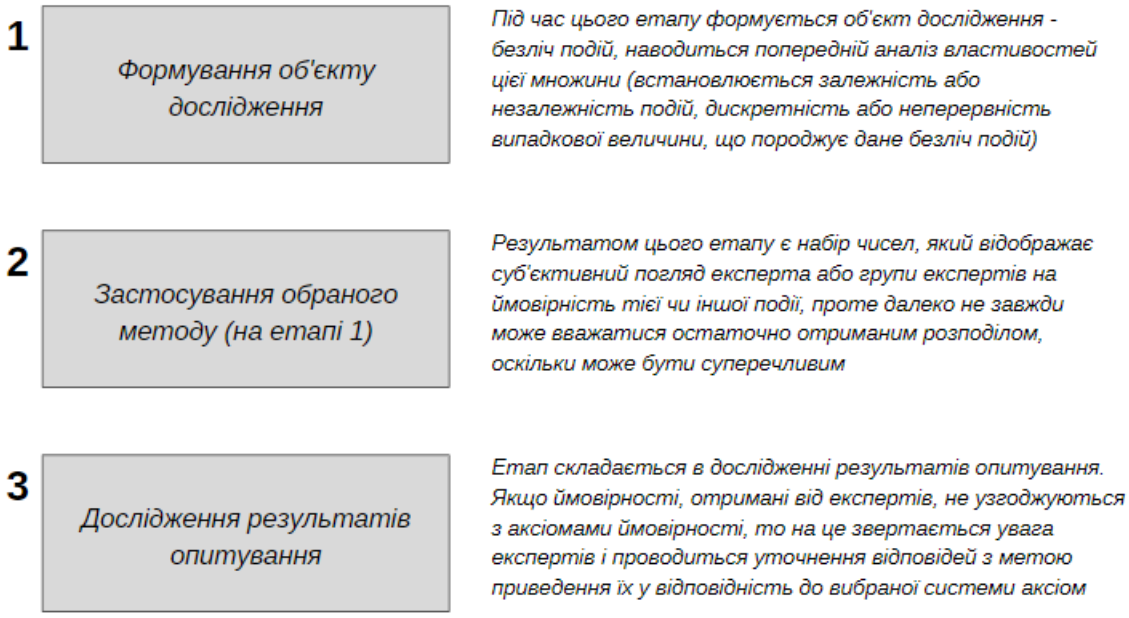


Рисунок 1.7. Етапи процесу отримання суб'єктивної ймовірності

Вимірювання ризиків. Вимірювання ризиків (також кількісна оцінка ризиків) - це широкий термін, що позначає будь-яку діяльність, спрямовану на кількісну оцінку (отримання числових показників) ризиків для організації. Зазвичай вважається, що ризики, які підлягають вимірюванню, були ізольовані в процесі ідентифікації ризиків, який логічно передує вимірюванню ризиків.

Залежно від типу ризику, що вимірюється, існує велика різноманітність методологій та інструментів кількісної оцінки. У більш вузькому контексті кількісного управління ризиками вимірювання ризиків значною мірою делегується застосуванню кількісної моделі ризику. Кількісна модель ризику - це будь-який кількісний (математичний) інструмент, спрямований на систематичну оцінку/прогнозування ризиків з метою управління ризиками. Кількісна модель ризику є повністю реалізованим результатом, коли - як мінімум - наявні наступні компоненти/результати

1. Точна специфікація моделі з усіма математичними / концептуальними елементами, які дозволяють зрозуміти і відтворити (реалізувати) модель компетентними фахівцями

2. Програмна реалізація (Model Implementation) (вихідний код або інша цифрова реалізація моделі), яка реалізує концепцію, сформульовану в специфікації моделі

3. Виробничий екземпляр реалізації, який використовується в реальних процесах прийняття рішень / управління ризиками.

На практиці може бути більше компонентів (документація джерел даних, тестові реалізації, сімейства моделей, різні типи екземплярів тощо).

Різні ризики за своєю природою можуть бути занадто складними для надійної кількісної оцінки. Для регульованих фірм наглядові органи можуть вимагати, щоб їх оцінювали в інший спосіб (наприклад, на основі експертних оцінок) та управляли ними за допомогою лімітів, засобів контролю та нагляду з боку керівництва.

Як правило, для оцінки загроз та вразливостей використовуються різні методи, в основі яких можуть лежати:

– експертні оцінки;

– статистичні дані;

– облік чинників, що впливають на рівні загроз і вразливостей.

Для оцінки загроз обрано певну ланку непрямих факторів, які представлено на рис.1.9:

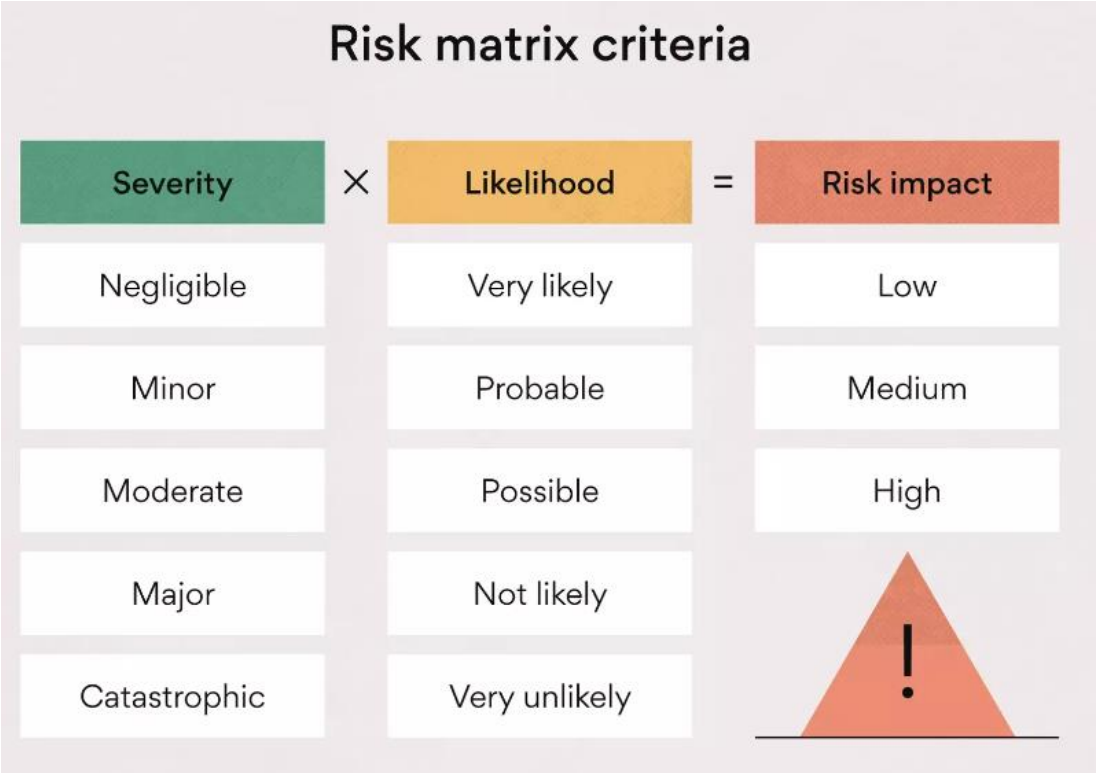


Рисунок 1.8. Матриця критеріїв ризиків

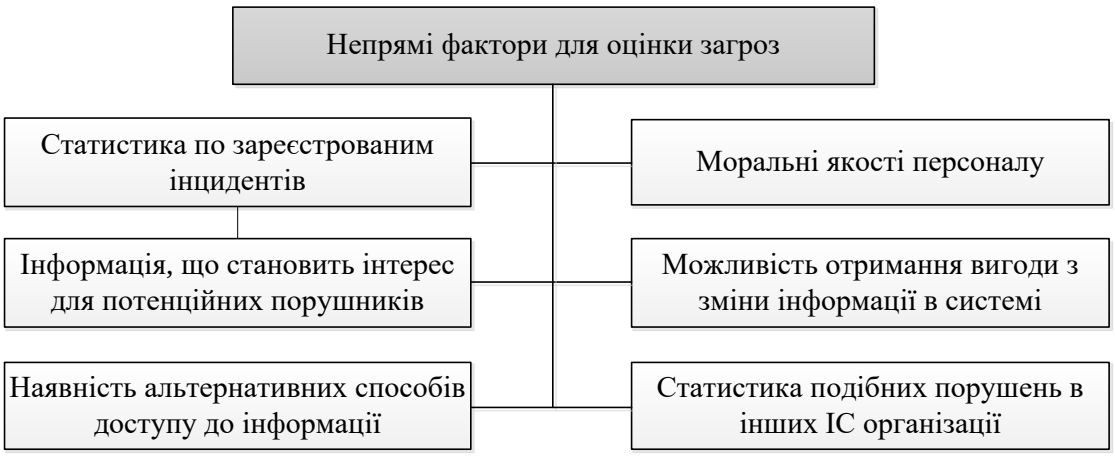


Рисунок 1.9. Непрямі фактори для оцінки загроз

1.2.2 Методики аналізу та управління ризиками компанії

Оскільки компанія являє собою єдиний складний взаємопов'язаний комплекс, то управління ризиками не може бути відокремлено. Механізм

управління ризиками повинен бути інтегрований в загальну систему менеджменту підприємства.

Визначальною сучасною концепцією управління є підхід на основі KPI (Key Performance Indicators), або ключових показників результативності. Суть це підходу досить проста. Спочатку на вербальному рівні формулюються цілі, які повинні бути досягнуті компанією на різних рівнях її структури, а потім цим цілям ставляться у відповідність певні кількісні метрики. Надалі будемо використовувати наступне робоче визначення: «KPI - це оцифрована мета». Видається очевидним, що ступінь досягнення мети можна оцінити тільки в тому випадку, якщо вона оцифрована.

Логічним продовженням цієї концепції стала запропонована Р. Капланом і Д. Нортоном збалансована система показників, Balanced Scorecard (BSC), яка завоювала визнання серед багатьох компаній і їх керівників. Стратегічні карти (як інструмент, що зв'язує взаємно узгоджені цілі і KPI) є ефективним інструментом контролю досягнення цілей, що дозволяє представити основні ризики недосягнення цілей. Більш того, в сучасних умовах система вибору цілей компанії повинна включати фактори ризику як адекватне відображення сучасної турбулентного середовища.

Корисним є розгляд наступних п'яти KPI, які описують цілі, пов'язані з управлінням ризиками:

– середньоквадратичне відхилення показника, що відповідає за ризик, або його коефіцієнт варіації;

– ймовірність небажаної події;

– імовірнісна вартість, імовірнісні втрати;

– економічна додана вартість;

– карта ризиків.

Останній інструмент виходить за межі типового визначення KPI, так як містить цілий набір показників, об'єднаних в загальну карту. Розглянемо деякі методи управління ризиками детальніше.

Середньоквадратичне відхилення, коефіцієнт варіації

Відхилення характеризує розкид випадкової величини щодо її середнього значення і вимірюється в абсолютних одиницях. Коефіцієнт варіації (відношення середнього квадратичного відхилення до математичного сподівання) дозволяє співвідносити розкид кількох випадкових величин, які мають різні значення математичного очікування, і виражається у відносних одиницях.

Інтерпретація середнього квадратичного відхилення і коефіцієнта варіації в розрізі ризик-менеджменту полягає в наступному: чим вище розкид параметра невизначеності (ризику), тим вище ризик компанії, пов'язаний з цим параметром.

Наприклад, менеджер має десятимісячну статистику продажів за двома філіям однієї дистриб'юторської компанії (табл. 1.1). Необхідно визначити, в якому з філій більше ризик, пов'язаний з об'ємом продажів.

Таблиця 1.1 - Десятимісячна статистика продажів по філіях (в тис. у.о.)

Місяць	1	2	3	4	5	6	7	8	9	10
Одеса	469	567	594	507	685	496	459	585	52	456
Дніпро	440	432	489	481	527	548	511	520	471	389

Для вирішення поставленого завдання необхідно розрахувати середньоквадратичне відхилення і коефіцієнт варіації і на їх підставі прийняти рішення про ступінь ризику діяльності того чи іншого філії (табл. 1.2).

Таблиця 1.2 - Статистичні оцінки обсягу продажів по філіях

Оцінки	Математичне сподівання	Середнє квадратичне відхилення	Коефіцієнт варіації
Одеса	533,9	73,3	0,137
Дніпро	480,8	49,1	0,102

Розраховані статистичні оцінки дозволяють зробити висновок про те, що виходячи з волатильності обсягу продажів діяльність філії в Одесі більш ризикована, ніж в Дніпрі. У той же час в середньому одеська філія заробляє на продажах більше. Керівнику компанії належить визначитися в критеріях оцінки діяльності цих двох філій і віддати перевагу або більш надійний (менш ризиковий) дніпровський філія, або в середньому більш результативний і менш

надійний одеський. Волатильність - це ступінь схильності вартості фінансового інструменту коливань ринку. Чим сильніше відхилення ціни активу від середнього значення, тим вище рівень його ризику.

Концепція і показник VAR

Концепція Value-at-Risk є основним положенням сучасного фінансового ризик-менеджменту. Цей показник був розроблений фахівцями відомого банку J. P. Morgan і завоював визнання багатьох найбільших компаній. Його успіх обумовлюється простотою розуміння співробітниками на всіх рівнях управління компанією. Тепер VaR є одним з індикаторів ризику для менеджерів компанії, інвесторів і регулюючих органів.

Value-at-Risk дослівно перекладається з англійської як «Вартість, піддана ризику». З практичної точки зору VaR відображає максимально можливі збитки від зміни вартості фінансового інструменту, портфеля активів, наявних запасів товару компанії і т. д., Яке може статися за певний період часу із заданою ймовірністю.

Коли говорять, що ризикова вартість на один день становить 500000 дол, з довірчою ймовірністю 95% (т. Е. Ймовірністю втрат 5%), це означає, що втрати протягом цього дня, які перевищують 500 000 дол., Можуть відбутися не більше ніж в 5% випадків. Таким чином, ризикова вартість - це розмір збитку по відношенню до математичного сподівання параметра вартості, який не може бути перевищений з імовірністю. Зазвичай ймовірність втрат встановлюється на рівні 1%, 2,5% або 5%, і відповідний довірчий інтервал становить 99%, 97,5% і 95%.

Практична інтерпретація корисності VaR полягає в наступному: ми приймаємо, що якщо подія має ймовірність 5%, то воно практично незначимо, т. Е. Очікувати його появи не варто ніколи. Тому ми не будемо «закладатися на такі ймовірності» (адже це не стрибки з парашутом) при аналізі фінансових показників. Таким чином, VaR в практичному сенсі виступає як максимально можливі втрати вартості.

Для оцінки VaR необхідно знати щільність розподілу ймовірностей. У

практичних розрахунках найчастіше використовується нормальне (гауссових) розподіл.

Дамо розподіл усіх визначення VaR. Якщо від математичного очікування параметра вартості відняти VaR, то це буде довірчої кордоном параметра вартості, що відповідає заданій довірчій ймовірності (1 а) відсотків.

Розрахункове співвідношення для нормального розподілу ймовірностей виглядає наступним чином:

$$VAR = z_{\alpha} \times \sigma \tag{1.1}$$

де σ - середньоквадратичне відхилення результуючого параметра;

z_{α} - квантиль нормального розподілу ймовірності α (табл. 1.3).

Таблиця 1.3 - Квантиль нормального розподілу ймовірності

a	5%	2,5%	1%
Z	1.64	1.96	2,33

Таким чином, основним принципом VaR є встановлення можливих імовірнісних втрат, пов'язаних з ризиком. Розрізняють такі види імовірнісних втрат:

- втрати вартості активів - Value-at-Risk, VaR;
- втрати доходу (виручки) - Revenue-at-Risk, RaR;
- втрати прибутку - Earnings-at-Risk, EaR;
- втрати грошового потоку - Cash-Flow-at-Risk, CFaR.

Вибір кожного з показників визначається типом бізнесу і завданням, яке вирішує аналітик по ризиках. Якщо на конкретному етапі бізнесу головна мета полягає в тому, щоб забезпечити максимальний обсяг продажів, то його буде цікавити показник RaR. Традиційно власника цікавить отримання заданого значення прибутку. У цьому випадку може бути рекомендований показник EBIT-at-Risk. Якщо завдання видається більш утилітарною з точки зору

генерування грошей, то більше доречний показник EBITDA-at-Risk.

Для розрахунку показника ризикової вартості використовуються трьома різними способами:

- аналітичний;
- метод історичного моделювання;
- метод статистичних випробувань Монте-Карло.

Перший з них є параметричних і дозволяє отримувати оцінки в замкнутому вигляді, а два інших уявляють свого роду математичний експеримент. Початковим етапом і необхідною умовою реалізації згаданих методів є визначення так званих факторів ризику, до яких відносять ціни, процентні ставки, валютні курси і т. п. Величина результуючого показника є функцією набору цих ризикових факторів. Їх кількість визначає точність математичної моделі.

При використанні нормального розподілу спочатку оцінюються або вважаються заданими числові характеристики факторів ризику, такі як математичне очікування, середньоквадратичне відхилення і коефіцієнт варіації. Потім, використовуючи модель залежності визначального параметра від факторів ризику, розраховується математичне сподівання і середнє квадратичне відхилення результуючого показника. Після цього, застосовуючи базову співвідношення (1.3), розраховується VaR для обраного результуючого показника.

Карта ризиків (ризик-профіль)

Карта ризиків (risk тар) - це метод аналізу портфеля ризиків компанії, що дозволяє виявити їх взаємний зв'язок і взаємовплив. Ця технологія дає можливість виміряти всі виявлені ризики в двох координатах: ймовірність виникнення і серйозність наслідків. Числа на поле карти ризиків відповідають порядковим номерам в реєстрі ризиків компанії.

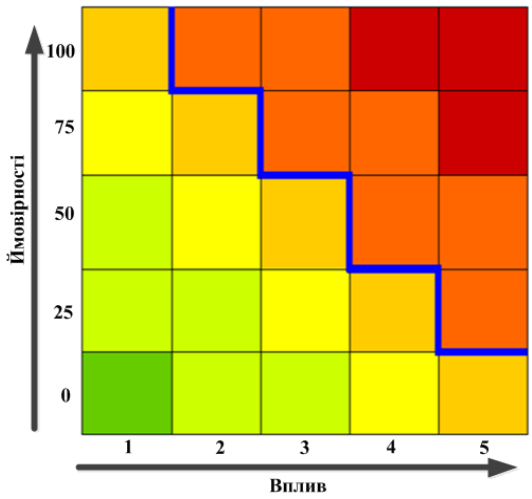


Рисунок 1.10. Карта ризиків

Сьогодні Існує декілька способів вимірювання ризиків: категорійний та кількісний. Категорійний використовує вербальні (словесні) вимірювачі типу «сильний» - «слабкий». В рамках категорійного підходу «ймовірність» описується так:

майже неможливо - може бути - ймовірно - майже напевно.

А «серйозність наслідків»:

незначна - помірна - значна - висока.

Як приклад розглянемо ризик-профіль компанії UGI (рис. 1.11).

Менеджери компанії UGI обрали для вимірювання ризиків категорійний підхід, сформувавши карту, яка складається з 16 квадрантів.

Рисунок 1.11. Риск-профиль компании UGI

Для зручності кожному виявленому ризику присвоюється своя буква:
D - стихійне лихо;
E - екологічна проблема;
F - неполадки обладнання;
L - трудовий спір;
M - пошкодження критичного запасу на складі;
R - порушення законодавчо-регулятивних актів;
V - неполадки засобів пересування.

Найбільш небезпечними ризиками є ті, які розташовані ближче до правого верхнього кута. Для компанії UGI такими є стихійне лихо (D) і неполадки засобів пересування (V).

Для побудови карти ризиків використовується два підходи: «зверху вниз» і «знизу вгору». Процедура «зверху вниз» має на увазі виявлення і аналіз ризиків, що існують в кожному підрозділі компанії, на рівні топ-менеджерів, і визначення ступеня їх взаємовпливу і впливу на організацію в цілому (рис. 1.12). При використанні підходу «знизу вгору» використовується серія інтенсивних дискусій, проведених в цільових «виробничих» групах, в ході яких відбувається виявлення, обговорення і аналіз ризиків.

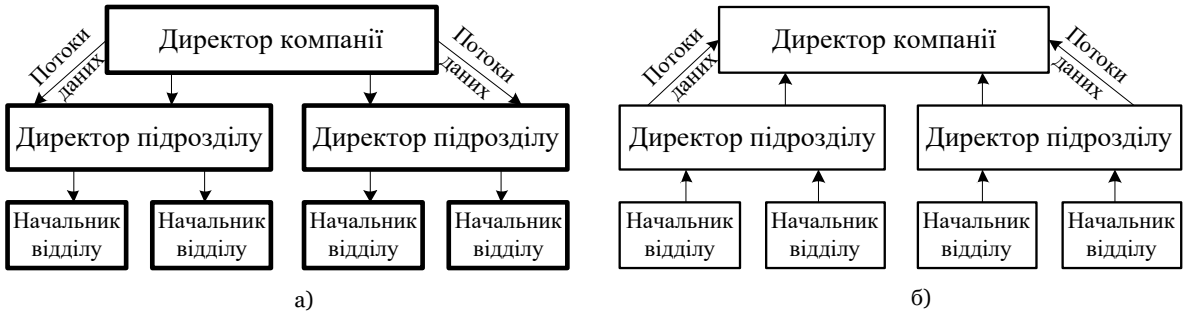


Рисунок 1.12. Підходи до побудови карти ризиків

Побудова ризик-профілю за допомогою підходу «зверху вниз» включає наступні етапи:

1. Ідентифікація ризиків. Виявлення ризиків відбувається за умови погляду на компанію як на єдине ціле. На цьому етапі використовується інформація, що знаходиться в широкому доступі, на основі якої проводяться сесії мозкового штурму за участю ключових осіб компанії, в ході чого виявляються загрозливі організації ризики і виробляється попередня інформація для аналізу портфеля.

2. Оцінка ризиків і побудова ризик-профілю. Виявлені ризики аналізуються з точки зору ймовірності і серйозності. Ця інформація часто зображується у вигляді різних матриць або осей координат, що відображають частоту (ймовірність) і серйозність наслідків кожного ризику. Отримані результати зображуються у вигляді ризик-профілю: можливі ризики утворюють сімейства - від високій ймовірності, але незначних випадків до малоймовірних катастроф. Потім на основі цього профілю визначаються пріоритети стратегії пом'якшення ризиків.

3. Кількісне вимірювання ризиків. Проводиться повна оцінка ризик-сімейств параметрів, відібраних для побудови моделі оцінки інтегральних характеристик ризику EAR, VAR і ін. Оцінюються інтервали невизначеності параметрів ризику і закони імовірнісних розподілів. Ці розрахунки зазвичай ґрунтуються на думках кількох експертів в поєднанні з будь-якими доступними фактичними даними.

4. Консолідація ризиків. Ризики, аналіз яких здійснювався на рівні підрозділів або дочірніх підприємств, необхідно звести воєдино на корпоративному рівні. Існує два способи консолідації: 1) суб'єктивний аналіз ризик-профілю, здійснюваний групою кваліфікованих співробітників, і 2) математичні розрахунки у випадках, де можливі кількісні вимірювання.

Побудова ризик-профілю «знизу вгору» включає в себе наступні етапи:

1. Декомпозиція організації з точки зору ризиків. На цьому етапі вивчається структура компанії з точки зору впливу її підрозділів на окремі види ризиків, виділяються центри відповідальності за ризик - групи підрозділів, схожі з точки зору їх впливу на окремі види ризиків: служби продажів, служби постачання, виробничі підрозділи тощо.

2. Семінари по обговоренню ризиків. Організовуються семінари під керівництвом фахівців з ризиків за участю обраних працівників підрозділів компанії. Провідними семінарів можуть бути працівники компанії або консультанти. Вони ставлять перед групою приватні цілі, керують процесом обговорення і роблять необхідні висновки.

3. Побудова ризик-профілю. Отримані результати зображуються у вигляді ризик-профілю. Висновки щодо пріоритетів важливості ризиків роблять експерти в області ризик-менеджменту. Потім на основі цього профілю визначаються пріоритети стратегії пом'якшення ризиків.

4. Консолідація ризиків. Цей крок аналогічний тому, який використовується в підході «зверху вниз».

Практика професіоналів в області ризик-менеджменту підтверджує ефективність як підходу «зверху вниз», так і «знизу вгору». Готова карта ризиків дозволяє визначити можливі напрями розробки заходів щодо зменшення можливості виникнення ризиків.

1.3 Застосування нормативних документів та стандартів управління інформаційною безпекою

Ряд організацій і відомств запропонував свої специфікації для базового рівня ІБ. Нижче розглядається деякі з них: специфікація сервісів базового рівня XBSS, стандарт NASA «Безпека інформаційних технологій» та ін.

XBSS - специфікації сервісів безпеки X / Open.

Консорціум X / Open випустив документ під назвою «Специфікації сервісів базового рівня ІБ». Специфікація може бути застосована до інформаційних систем, побудованим на базі типових проектних рішень. Передбачається, що концепція забезпечення ІБ організації відповідає стандарту BS 7799 (ISO 17799). При розробці специфікації використовувалося поняття профілю захисту з компонентами, що задовольняють вимогам «Good Practice», формалізованим у вигляді чітких критеріїв.

У специфікації визначені:

- вимоги в області ІБ до сервісів інформаційної системи;
- налаштування для за замовчуванням, що відповідають вимогам ІБ.

Стандарт NASA «Безпека інформаційних технологій»

Мінімальні вимоги до базового рівня захищеності відповідає документу «Керівництво по політиці безпеки для автоматизованих інформаційних систем» і конкретизує його положення. Використовується диференційований підхід: вводиться 4 рівня критичності технології, для яких по 30 позиціям специфікуються вимоги. Слід зазначити, що подібний підхід: визначення декількох варіантів базових вимог для різних типів технологій, безумовно, виправданий і дозволяє врахувати їх специфіку. Цей документ доступний в інтернет і є вельми корисним при розробці специфікацій на підсистему інформаційної безпеки з урахуванням її специфіки.

Концепція управління ризиками MITRE.

Організацією MITRE була запропонована концепція управління ризиками при побудові різних систем (не тільки інформаційних). В цілому ця концепція близька до рекомендацій розглянутого стандарту США NIST 800-30. Організація MITRE безкоштовно розповсюджує найпростіший інструментарій на базі електронної таблиці, призначений для використання на етапі ідентифікації та оцінки ризиків, вибору можливих контрзаходів відповідно до цієї концепції - «Risk Matrix». У даній концепції ризик не поділяється на складові частини (загрози і вразливості), що в деяких випадках може виявитися більш зручним з точки зору власників інформаційних ресурсів.

1.3.1 Методики і рекомендації з управління ризиками

Методика оцінки і управління ризиками OCTAVE

Методика оцінки і управління ризиками OCTAVE містить матеріали, що відображають накопичений її авторами досвід в ході декількох робіт за даним профілем.

Характерне для академічних кіл прагнення до більш високого рівня абстракції і універсалізму виразилося як в зовнішньому побудові документів, так і в їх внутрішню структуру.

По-перше, сам документ розділений на три частини: OCTAVE-критерії, яка містить найбільш абстрактні вимоги і рекомендації, і два документа, що описують варіанти реалізації даних критеріїв для великих організацій (так званий OCTAVE-метод) і для невеликих компаній (OCTAVE-S -метод).

Самі OCTAVE-критерії (рис. 1.13) формулюються спочатку як десять принципів оцінки і управління ризиками, які ведуть до п'ятнадцяти основних вимог (attributes) для проведених процесів. Потім формулюються три основних етапи (фази):

– побудова профілів загроз для активів;
– ідентифікація вразливостей інформаційної структури;
– вироблення стратегії і планів забезпечення інформаційної безпеки.

В даних фазах розташовуються шістнадцять напрямків діяльності (activity), які проявляються в власне процесах оцінки і управління ризиками.

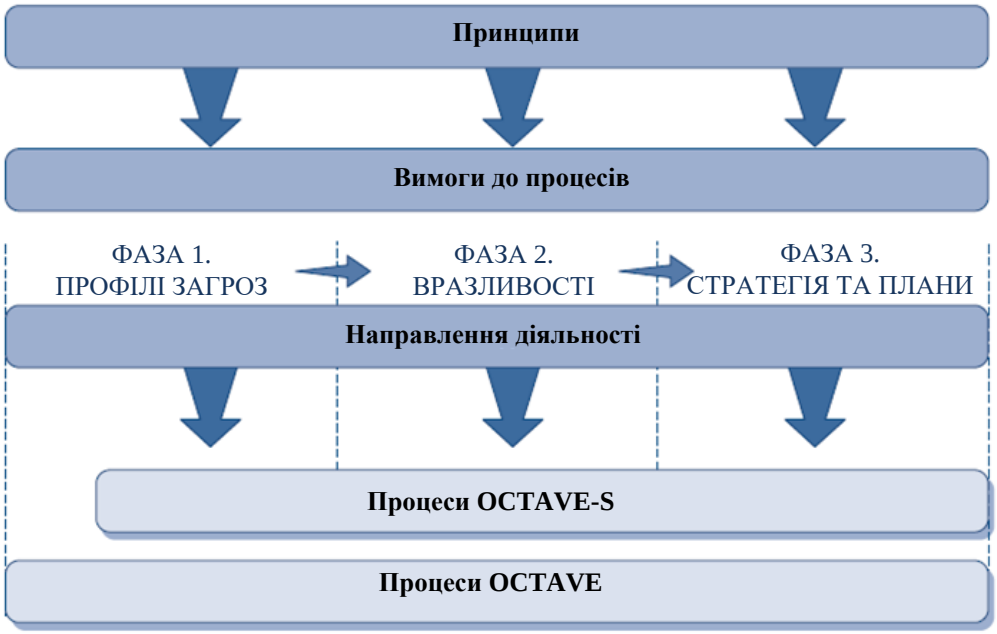


Рисунок 1.13. OCTAVE – критерії

Необхідно відзначити, що дані рекомендації проводять весь процес оцінки і управління ризиками, відштовхуючись від класифікації активів. Так, після закінчення кожної з фаз основним документом є профілі загроз / вразливостей / ризику / залишкового ризику для кожного типу активів. Рекомендації OCTAVE приділяють велику увагу вимогам до складу та змісту вихідних документів кожного з етапів діяльності.

Рекомендації з управління ризиками MG-2

Рекомендації з управління ризиками в IT-системах Канадського уряду MG-2 були вперше опубліковані в 1996 році. Рекомендації створені на основі трьох існуючих раніше урядових документів: Політики безпеки, Керівництва з оцінки та протидії ризикам, Керівництва по сертифікації та акредитації систем.

Рекомендації аналогічно всім розглянутим стандартам формулюють основні етапи управління ризиками, проте в основу їх викладу покладено життєвий цикл системи (спіраль, на кожному витку якої слід дотримуватися тих чи інших процесів з методичного набору з управління ризиками - рис. 1.14):

1. Планування:
   - збір інформації та опис системи;
   - визначення прийнятних рівнів ризику.
2. Підготовка до оцінки та аналізу ризиків:
   - виявлення активів.
   - складання «Класифікатора активів» із зазначенням вимог до їх конфіденційності, цілісності та доступності.
3. Оцінка ризику:
   - виявлення загроз, вразливостей і існуючих засобів протидії вразливостям;
   - виявлення можливої ступеня впливу загрози на актив.
4. Прийняття рішень щодо пом'якшення, ухилення, передачі або прийняття ризику.
5. Вироблення вимог до активу (в разі прийняття рішення щодо

пом'якшення ризику).

6. Вибір контрзаходів (технічних або нетехнічних).

7. Використання контрзаходів.

8. Сертифікація.

9. Акредитація.

10. Підтримка функціонування.

11. Вироблення пропозицій щодо вдосконалення.

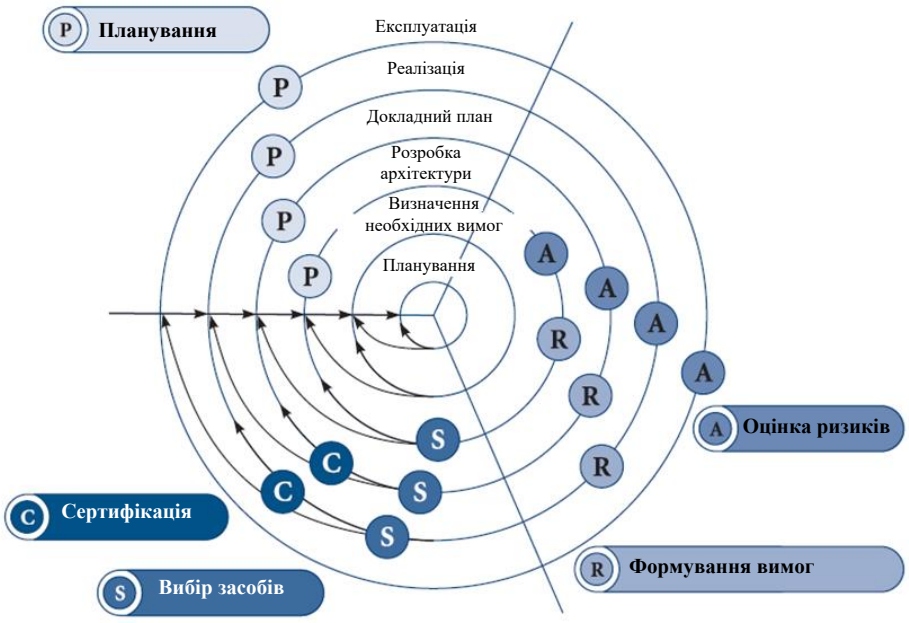


Рисунок 1.14. “Життєвий цикл” управління ризиками згідно MG-2

Особливу увагу в рекомендаціях приділено створенню «Класифікатора активів», в якому повинно бути наведено докладний опис активу, його роль у функціонуванні установи, вимоги до забезпечення його конфіденційності, цілісності та доступності.

1.3.2 Оцінка інформаційних ризиків в компанії

Сьогодні на практиці використовуються різні методи оцінки і управління інформаційними ризиками вітчизняних компаній. Оцінка інформаційних ризиків

компанії може виконуватися за таким планом (рис 2.12):

Рисунок 1.15. Складові оцінки інформаційних ризиків компанії

Логічно припустити, що у бізнес-середовищі на активи компанії спрямовано вектор загрози. Ризики описують небезпеку, на яку можуть бути піддані елементи інформаційної екосистеми компанії. Ризики, що з'являються в компанії, залежать від трьох компонентів - цінності IT, ймовірності реалізації загрози та ефективності системи безпеки, яка вже реалізована в компанії.

Основна мета оцінки ризиків полягає в оцінці атрибутів ризику, пов'язаних з корпоративною інформаційною системою та її ресурсами. Завдяки цьому процесу стає можливим вибір заходів, які гарантують рівень інформаційної безпеки компанії. Оцінка ризиків враховує такі фактори, як вартість ресурсів, серйозність загроз і вразливостей, ефективність заходів безпеки.

Оцінка передбачає комплексний аналіз, який враховує як кількісні, так і якісні методи. Кількісні методи можуть включати визначення характеристик, пов'язаних з витратами, тоді як якісні методи можуть охоплювати оцінку звичайних або надзвичайно небезпечних впливів на навколишнє середовище. Оцінюючи такі показники, як цінність ресурсів, значущість загрози, вразливість та ефективність заходів безпеки, організації можуть приймати обґрунтовані рішення щодо посилення інформаційної безпеки та вибирати відповідні стратегії зменшення ризиків.

Оцінка ймовірності реалізації загрози ґрунтується на ймовірності її настання у визначений часовий проміжок для конкретного ресурсу компанії. Визначення ймовірності реалізації загрози передбачає врахування ключових факторів, представлених на рис.1.16:

Рисунок 1.16. Фактор визначення ймовірності реалізації загрози

1.4 Розробка рішення для оцінки стану захищеності підприємства

1.4.1 Вибір моделі оцінки та складання базових питань

Для оцінки рівня інформаційної безпеки організації при виконанні дипломної роботи було використано «якісний» метод оцінки загроз як найбільш прийнятний для практичного використання у розрізі експрес-методу.

Загальна ідея полягає в тому, щоб дати можливість підприємцям, компаніям малого та середнього бізнесу оцінити поточний рівень безпеки, зробити висновки та застосувати оптимальні методи та засоби захисту. Користувач вибирає певні відповіді із заготовлених форм, за результатами яких

будується радар погроз. Радар, за принципом світлофора, розділений на 3 колірні зони: червоний – високий ризик, жовтий – допустимий ризик, зелений – безпечна зона. Таким чином, відповідаючи на запитання, користувач бачить поточний рівень безпеки компанії. Завдання далі – вивести всі загрози з червоної зони у жовту, а потім залишити у жовтій зоні не більше 25%. У зеленій зоні має бути 75%

Базові вихідні дані – ситуації, змодельовані за 5-ма напрямками у роботі гіпотетичного підприємства (об'єктивно їх може бути більше), а саме:

- кадри
- робота з контрагентами
- фізичний захист та технічні засоби охорони
- IT-сегмент
- документи та персональні дані.

Питання для програмної реалізації експрес-методу оцінки рівня інформаційної безпеки було складено на основі ланки стандартів з інформаційної безпеки та забезпечення неперервності бізнесу. Згідно з цим, питання розбито за такими групами – кадри, робота з контрагентами, фізичний захист та технічні засоби охорони, IT-сегмент, документи та персональні дані.

По кожному із напрямів сформовано 10 питань, відповіді на які показують загальний стан спрямування, при цьому мінімальний бал – 0, максимальний бал – 10. Наведемо приклад 2-х опитувальних таблиць за базовими напрямами захисту для підприємства

Табл. 1.4 – Перелік питань та відповідей для кадрового напряму

№ з/п	Запитання	Відповіді	Оцінка
Кадровий напрямок			
1	На етапі працевлаштування кандидат попередньо проходить перевірку – відгуки, рекомендаційні листи, соціальні мережі	Так	1
		Ні	0
2	У штаті компанії є спеціаліст з роботи з персоналом	Так	1
		Ні	0
3	Чи відбувається моніторинг дій співробітника під час його роботи на підприємстві, наприклад, у соціальних мережах, форумах	Так	1
		Ні	0
4	Серед працівників компанії є матеріально-відповідальні особи	Так	1
		Ні	0
5	На підприємстві розроблено та впроваджено положення про комерційну таємницю	Так	1
		Ні	0
6	У штатній структурі підприємства є посада спеціаліста з ІБ або відділу СБ	Так	1
		Ні	0
7	За останні 12 місяців у компанії були інциденти, пов'язані з кадрами	Так	1
		Ні	0
8	Головний бухгалтер (статус працевлаштування) – офіційно оформлений співробітник (а), аутсорсинг (б), трудовий договір (в), працює неофіційно (г)	а	1
		б	0,75
		в	0,5
		г	0
9	ІТ-фахівець (статус працевлаштування) – офіційно оформлений співробітник, аутсорсинг, трудовий договір, працює неофіційно	а	1
		б	0,75
		в	0,5
		г	0
10	На підприємстві відбувається навчання персоналу з питань ІБ – системно(а), періодично(б), ніколи(в)	а	1
		б	0,5
		в	0

Табл.1.5 – Перелік питань та відповідей для напряму контрагентів

№ з/п	Запитання	Відповіді	Оцінка
Контрагенти			
1	На підприємстві триває попередня перевірка контрагентів?	Так	1
		Ні	0
2	За останні 12 місяців на підприємстві було виявлено випадки лобіювання співробітниками компанії інтересів контрагентів?	Так	1
		Ні	0
3	За час роботи компанії (12 місяців) траплялися випадки порушень договірних відносин з боку контрагентів? Неодноразово (а) – 1 бал, разово (б) – 0,5 бала, ніколи (в) – 0 балів)	а	1
		б	0,5
		в	0
4	Близькі друзі чи родичі ключових співробітників працюють у компаніях-контрагентах?	Так	1
		Ні	0
5	За 12 місяців компанії були випадки, коли дебіторську заборгованість доводилося отримувати через рішення суду?	Так	1
		Ні	0
6	Чи відомі випадки, що співробітники компанії отримували відкат від контрагентів? (неодноразово (а) – 1 бал, разово (б) – 0,5 бала, ніколи (в) – 0 балів)	а	1
		б	0,5
		в	0
7	Чи відомі випадки, коли робота з контрагентом провадиться без офіційних договірних відносин? (неодноразово (а) – 1 бал, разово (б) – 0,5 бала, ніколи (в) – 0 балів)	а	1
		б	0,5
		в	0
8	На підприємстві поставлено превентивну роботу з аналізу контрагентів доступними та законними силами та засобами?	Так	1
		Ні	0
9	Чи можна стверджувати, що на підприємстві незадовільний рівень перевірки чи ігнорування фактичного ризикового стану контрагента	Так	1
		Ні	0
10	На підприємстві проводиться неефективний моніторинг договірної роботи	Так	1
		Ні	0

Додатково розглядаються напрями фізичного захисту та технічних засобів охорони, інформаційної інфраструктури та напрями документації та

персональних даних. Після відповідей на інтерактивні анкети користувач отримує радар погроз як візуалізацію вимірного стану безпеки підприємства. Приклад радара загроз із зазначенням зонування подано на рис.1.17.

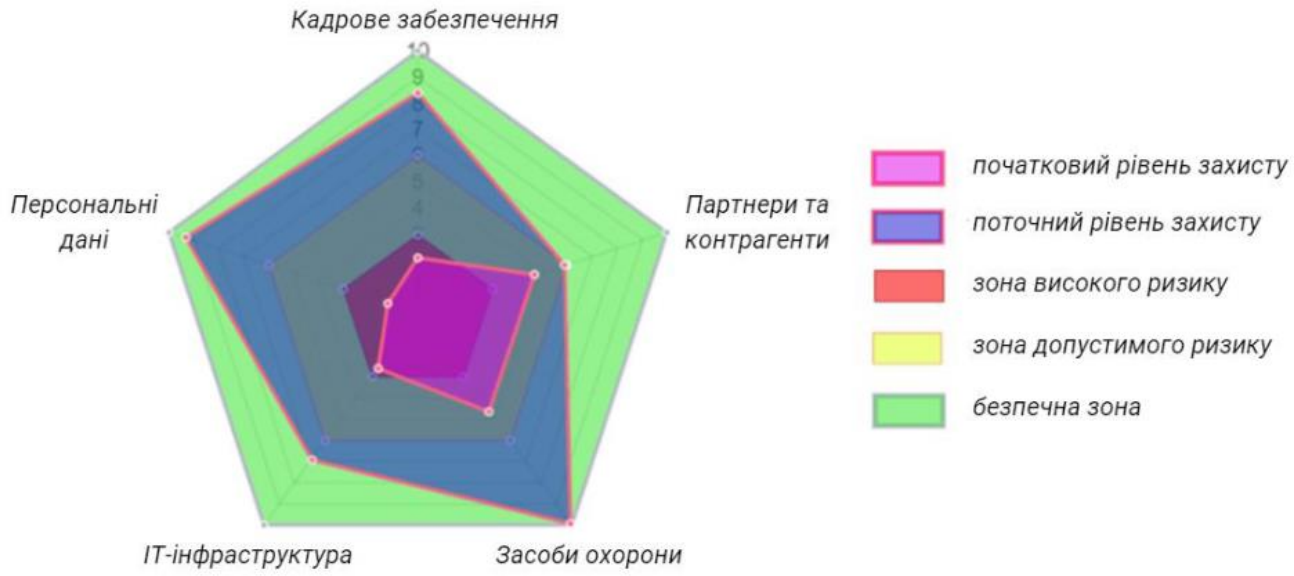


Рисунок 1.17. Візуалізація рівнів захисту та зон ризиків у вигляді радару загроз

Як видно з рисунка, на радарі загроз представлено таке зонування:

- початковий рівень захисту (початкові дані);
- поточний рівень захисту (результат роботи);
- зона високого ризику (показник ≤3);
- зона допустимого ризику (значення в діапазоні 3-7);
- безпечна зона (показник ≥7).

На рис. 1.18 представлено результати відповіді на інтерактивні анкети. Ключові напрями на радарі загроз – кадрове забезпечення, робота з контрагентами, фізичний захист та технічні засоби охорони, інформаційна інфраструктура та документообіг.

Рисунок 1.18. Результати відповіді на інтерактивні анкети у вигляді радару загроз

В програмні реалізації під радаром загроз представлено кнопку “поліпшити захист”. Після переходу пропонується заповнити інтерактивні таблиці з певними ваговими значеннями, де кожне рішення додає позитивних змін в напрямку безпеки. На рис. 1.19 представлено питання з інтерактивного блоку “Фізичний захист і технічні засоби охорони”.

Кожен з напрямків може мати свою деталізацію. Чим більше вибір методів та засобів захисту за напрямком – тим більше гнучкість в питаннях підвищення рівня захисту. Очікується, що застосування експрес-аудиту стану рівня безпеки у компанії дозволить власникам та керівникам у комплексі побачити реальний стан безпеки. У свою чергу, запропоновані методи та засоби захисту, реалізовані через інтерактивні анкети, а також візуалізація результатів вибору, дають можливість більшості користувачів, незалежно від рівня кваліфікації та виду діяльності компанії, оцінити ефективність вибору інструментів в рамках підвищення загального рівня захисту.

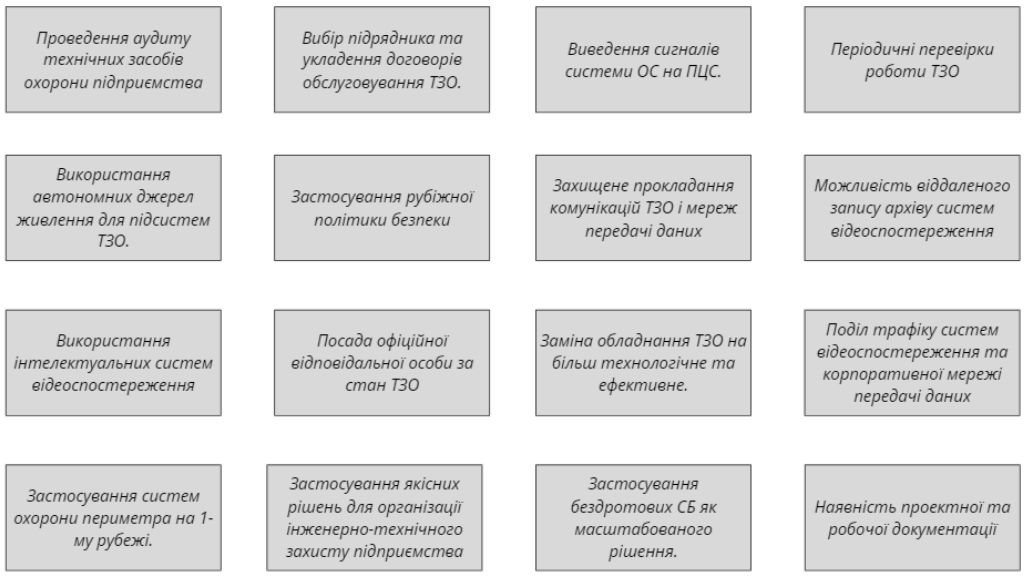


Рисунок 1.19. Питання з блоку “Фізичний захист і технічні засоби охорони”

В табл. 1.6 представлено приклад можливих методів та засобів захисту в напрямках інформаційного середовища компанії (IT) та роботи в кадровому напрямку. Перелік захисних мір може додаватися.

Таблиця 1.6 – Методи та засоби захисту в напрямках інформаційного середовища компанії (IT)

№	Дія	Бал
1	Офіційне оформлення всіх співробітників IT-відділу	0,25
2	Працюючи в IT-напрямку підприємства 3-х осіб обов'язкове укладання договірних відносин	0,25
3	Періодичне проведення пентестингу з метою перевірки рівня безпеки корпоративної мережі підприємства	0,25
4	Використання ліцензійного програмного забезпечення	0,25
5	Використання тонких клієнтів	0,25
6	Розташування сервера за межами підприємства	0,25
7	Застосування технології RAID	0,25
8	Контроль стану трафіку та роботи користувачів із застосуванням DLP-систем	0,25
9	Використання антивірусних програм	0,25
10	Застосування періодичного архівування даних (організаційні, програмно-апаратні рішення)	0,25

11	Навчання персоналу питанням комп'ютерної грамотності – загрози та ризики, можливості, правила, заборони	0,25
12	Виділення бюджету на розвиток IT-сегменту компанії	0,25
13	Використання хмарних сервісів та технологій	0,25
14	Поділ корпоративної мережі на гостьові та робочі сегменти	0,25
15	Обов'язкове застосування парольної політики	0,25
16	Безпечна утилізація комп'ютерів та жорстких дисків	0,25
17	Періодична інвентаризація IT-активів	0,25
18	Використання шифрування	0,25
19	Захист від соціальної інженерії	0,25
20	Захист бездротових точок доступу	0,25

Таблиця 1.7 – Методи та засоби захисту в кадровому напрямку

№	Действие	Балл
1	Аналіз претендента перед проведенням співбесіди (листи, дзвінки, соціальні мережі, реєстри тощо)	0,5
2	Застосування методів та засобів конкурентної розвідки	0,35
3	Лише офіційне працевлаштування співробітників	0,5
4	Моніторинг СБ підприємства дій співробітників на повному життєвому циклі – на роботі, поза роботою, соціальні мережі	0,25
5	Системне навчання персоналу підприємства з питань безпеки	0,5
6	Використання управлінських рішень, спрямованих на лояльність персоналу та оптимальні KPI	0,25
7	Наявність власного відділу кадрів (HR)	0,5
8	На підприємстві відсутні порушення КЗпП та заборгованості із ЗП	0,35
9	Застосовуються легальні засоби віддаленого контролю персоналу	0,25
10	У компанії має місце колективна робота з оптимізації процесів та побудови BCM (безперервності бізнесу)	0,5

Потенціал подальшого розвитку – вибір ключових напрямів захисту у компанії, збільшення кількості методів та засобів захисту у напрямку, деталізація інструментів, підключення фінансових показників (наприклад, розрахунок вартості обраних рішень), довідковий розділ із розширеними коментарями тощо.

1.4.2 Вибір засобів розробки

Для розробки програмного забезпечення була використана мова програмування JavaScript, фреймворк Vue.js - для спрощеної роботи з елементами сторінки і обробки подій та бібліотеку ApexCharts.js - для побудови радару ризиків.

Для візуальної побудови проекту були використана мова гіпертекстової розмітки - HTML та один з синтаксисів препроцесора SASS - SCSS. Задання дизайну сайту забезпечено за допомогою UI Component фреймворку - Vuetify. Зберігання даних реалізовано на стороні клієнта для цього використовується бібліотека - Pinia.

Опитування створюється за допомогою форми, сторінок опитування та сховища для зберігання та обробки даних. Приклад форми, сторінок опитування та сховища наведено на рис. 1.20

```
<ModalCommon id="test" persistent>
  <v-window v-model="stepTab">
    <v-window-item value="step-0">
      <Step0 />
    </v-window-item>
    <v-window-item value="step-1">
      <div class="wrap-step q-px-md">
        <Step1 />
      </div>
    </v-window-item>
    <v-window-item value="step-2">
      <div class="wrap-step q-px-md">
        <Step2 />
      </div>
    </v-window-item>
    <v-window-item value="step-3">
      <div class="wrap-step q-px-md">
        <Step3 />
      </div>
    </v-window-item>
    <v-window-item value="step-4">
      <div class="wrap-step q-px-md">
        <Step4 />
      </div>
    </v-window-item>
    <v-window-item value="step-5">
      <div class="wrap-step q-px-md">
        <Step5 />
      </div>
    </v-window-item>
  </v-window>
</ModalCommon>
```

Рисунок 1.20. – Форма опитування

```
// STORES
const storePoll = usePoll();

// STATES
const { step1, rule } = storeToRefs(storePoll);
const form = ref(null);

const prev = () => {
  storePoll.$patch({ stepTab: "step-0" });
};

const next = async () => {
  const { valid } = await form.value.validate();
  if (valid) storePoll.$patch({ stepTab: "step-2" });
};
</script>
```

```
<template>
  <div class="flex justify-center align-center">
    <v-form @submit.prevent ref="form">
      <v-card :title="$t('staff.staff')">
        <v-card-text>
          <p>
            {{ $t("staff.q1") }}
          </p>
          <v-radio-group
            v-model="step1.r1"
            :rules="rule"
            inline
            style="justify-content: space-evenly"
          >
            <v-radio :label="$t('yes')" :value="1"></v-radio>
            <v-radio :label="$t('no')" :value="0"></v-radio>
          </v-radio-group>
          <p>
            {{ $t("staff.q2") }}
          </p>
          <v-radio-group
            v-model="step1.r2"
            :rules="rule"
            inline
            style="justify-content: space-evenly"
          >
            <v-radio :label="$t('yes')" :value="1"></v-radio>
            <v-radio :label="$t('no')" :value="0"></v-radio>
          </v-radio-group>
          <p>
            {{ $t("staff.q3") }}
          </p>
          <v-radio-group
            v-model="step1.r3"
            :rules="rule"
            inline
            style="justify-content: space-evenly"
          >
            <v-radio :label="$t('yes')" :value="1"></v-radio>
            <v-radio :label="$t('no')" :value="0"></v-radio>
          </v-radio-group>
          <p>
            {{ $t("staff.q4") }}
          </p>
          <BtnContBack :prev="prev" :next="next" submit />
        </v-card>
      </v-form>
```

Рисунок 1.21. Приклад коду сторінки опитування

```
// Utilities
import { defineStore } from "pinia";
import { useLocalStorage } from "@vueuse/core";

export const usePoll = defineStore("poll", {
  state: () => ({
    stepTab: "step-0",
    step1: {
      r1: null,
      r2: null,
      r3: null,
      r4: null,
      r5: null,
      r6: null,
      r7: null,
      r8: null,
      r9: null,
      r10: null,
    },
    beforeSum1: useLocalStorage("beforeSum1", 0),
    afterSum1: useLocalStorage("afterSum1", 0),
    step2: {
      r1: null,
      r2: null,
      r3: null,
      r4: null,
      r5: null,
      r6: null,
      r7: null,
      r8: null,
      r9: null,
      r10: null,
    },
    beforeSum2: useLocalStorage("beforeSum2", 0),
    afterSum2: useLocalStorage("afterSum2", 0),
    step3: {
      r1: null,
      r2: null,
      r3: null,
      r4: null,
      r5: null,
      r6: null,
      r7: null,
      r8: null,
      r9: null,
      r10: null,
      r11: null,
      r12: null,
      r13: null,
      r14: null,
      r15: null,
    },
    beforeSum3: useLocalStorage("beforeSum3", 0),
    afterSum3: useLocalStorage("afterSum3", 0),
    step4: {
      r1: null,
      r2: null,
      r3: null,
      r4: null,
      r5: null,
      r6: null,
      r7: null,
      r8: null,
      r9: null,
      r10: null,
      r11: null,
      r12: null,
      r13: null,
      r14: null,
      r15: null,
      r16: null,
      r17: null,
      r18: null,
      r19: null,
      r20: null,
    },
    beforeSum4: useLocalStorage("beforeSum4", 0),
    afterSum4: useLocalStorage("afterSum4", 0),
    step5: {
      r1: null,
      r2: null,
      r3: null,
      r4: null,
      r5: null,
      r6: null,
      r7: null,
      r8: null,
      r9: null,
      r10: null,
    },
    beforeSum5: useLocalStorage("beforeSum5", 0),
    afterSum5: useLocalStorage("afterSum5", 0),
    showAfter: false,
    rule: [
      (value) => {
        if (value !== null) return true;
        return "Оберіть один із варіантів";
      },
    ],
  }),
```

```
actions: {
  calculatePoll(buy = false) {
    let objectsArray = [
      this.step1,
      this.step2,
      this.step3,
      this.step4,
      this.step5,
    ];

    if (buy) {
      this.afterSum1 = this.beforeSum1;
      this.afterSum2 = this.beforeSum2;
      this.afterSum3 = this.beforeSum3;
      this.afterSum4 = this.beforeSum4;
      this.afterSum5 = this.beforeSum5;
      for (let i = 0; i < objectsArray.length; i++) {
        for (let key in objectsArray[i]) {
          switch (i) {
            case 0:
              this.afterSum1 += objectsArray[i][key];
              break;
            case 1:
              this.afterSum2 += objectsArray[i][key];
              break;
            case 2:
              this.afterSum3 += objectsArray[i][key];
              break;
            case 3:
              this.afterSum4 += objectsArray[i][key];
              break;
            case 4:
              this.afterSum5 += objectsArray[i][key];
              break;
          }
        }
      }
    } else {
      for (let i = 0; i < objectsArray.length; i++) {
        for (let key in objectsArray[i]) {
          switch (i) {
            case 0:
              this.beforeSum1 += objectsArray[i][key];
              break;
            case 1:
              this.beforeSum2 += objectsArray[i][key];
              break;
            case 2:
              this.beforeSum3 += objectsArray[i][key];
              break;
            case 3:
              this.beforeSum4 += objectsArray[i][key];
              break;
            case 4:
              this.beforeSum5 += objectsArray[i][key];
              break;
          }
        }
      }
    }
  },      You, last month • Додасть радарчарт та опрос
```

Рисунок 1.22. Сховище, де зберігаються та обчислюються дані

Виведення результатів опитування здійснюється в радарі ризику. Програмний код представлено на рис. 1.23.

```
const props = defineProps({
  showAfter: PROPS_BOOLEAN_DEFAULT,
});
// HOOKS
const { xs, sm } = useDisplay();

// STORES
const storePoll = usePoll();

// STATES
const {
  beforeSum1,
  beforeSum2,
  beforeSum3,
  beforeSum4,
  beforeSum5,
  afterSum1,
  afterSum2,
  afterSum3,
  afterSum4,
  afterSum5,
} = storeToRefs(storePoll);
```

```
const series1 = [
  {
    name: "",
    data: [
      beforeSum1.value,
      beforeSum2.value,
      beforeSum3.value,
      beforeSum4.value,
      beforeSum5.value,
    ],
  },
];

const series2 = [
  {
    name: "",
    data: [
      beforeSum1.value,
      beforeSum2.value,
      beforeSum3.value,
      beforeSum4.value,
      beforeSum5.value,
    ],
  },
  {
    name: "",
    data: [
      afterSum1.value.toFixed(2),
      afterSum2.value.toFixed(2),
      afterSum3.value.toFixed(2),
      afterSum4.value.toFixed(2),
      afterSum5.value.toFixed(2),
    ],
  },
];
```

Рисунок 1.23. Радар ризиків

1.4.3 Реалізація інтерфейсу рішення

Візуальну частину програми можна розділити на три частини, перша – стартовий екран, друга – список питань та відповідей на кожну з груп питань, третя – відображення радару загроз підприємства.

При вході на сайт користувач бачить екран з текстовим коментарем та запрошенням щодо проходження аудиту стану інформаційної безпеки підприємства.

Далі на сторінці користувач послідовно дає відповіді на п’ять інтерактивних анкет. По кожному з питань пропонується обрати відповідь. При цьому кожна з відповідей має свій ваговий коефіцієнт. (рис. 1.24).

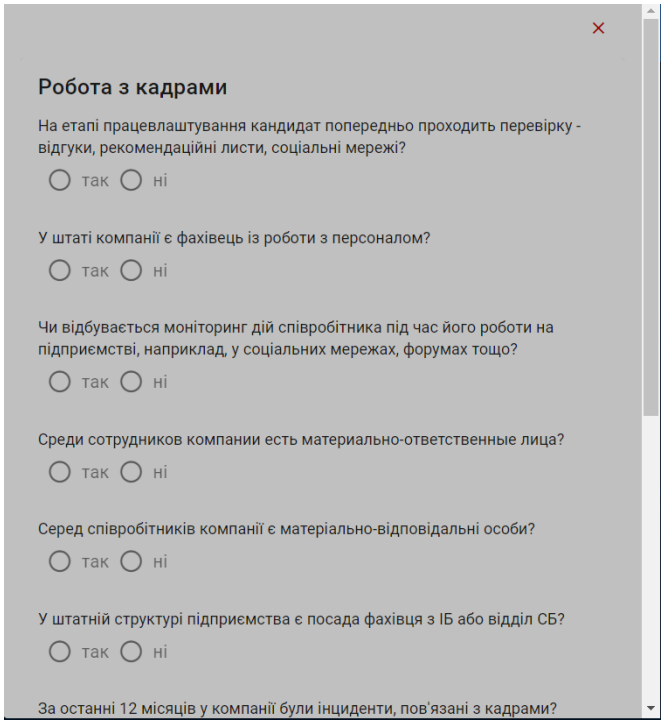


Рисунок 1.24. Частина анкети з напряму роботи з кадрами

Рисунок 1.25 – Радар загроз з відображення початкового та поточного рівня захисту, після застосування інструментів захисту

2. ЕКОНОМІЧНИЙ РОЗДІЛ

2.1 Резюме

В даному дипломному проекті розроблено рішення щодо оцінки стану рівня захищеності сучасного підприємства.

Оцінка якості програмного продукту з точки зору користувача визначається необхідним на стадії функціонування розміром оперативної пам'яті ЕОТ, витратами машинного часу, пропускною спроможністю каналів передачі даних. Оцінка якості програмного продукту включає визначення трудомісткості і вартості його створення.

2.2 Визначення трудомісткості розробки програмного забезпечення

Тривалість розробки програмного продукту залежить від його обсягу, трудомісткості розробки, кваліфікації виконавців, а також планових термінів, визначених умовами ринку. Методом структурної аналогії по відповідних каталогах аналогів програмного забезпечення визначається обсяг програмних засобів, у тисячах умовних машинних команд програми аналога

Каталог аналогів

У таблиці 2.1 представлені аналоги програмного забезпечення, функції яких, у більшому або меншому ступені, виконує розроблений програмний продукт. Для нашого варіанта виділено сірим кольором.

Таблиця 2.1. Аналоги програмного забезпечення

Найменування ПЗ	*Обсяг функції ПП = V_0, ум. машинних команд*
1. ПП СУБД	1300 – 8600
2. ПП введення інформації	1800 – 8800
3. ПП оптимізаційних розрахунків	13000 – 10200

Вибравши аналог ПП, що містить Vo в умовних машинних командах, трудомісткості визначати на основі табл.2.2

Таблиця.2.2. Трудомісткість

Обсяг ПП, тис.умов.машинних команд	Норма часу, люд/год
1.00	229
2.00	244
3.00	262

На підставі отриманого значення, по довіднику, визначається укрупнена норма часу на розробку аналога програмного забезпечення (коректується поправочним коефіцієнтом враховуючої умови розробки ПП, тобто в умовах комп'ютера, Кк=0,7÷0,8): Тар = 244 х 0,8 = 195.20 (люд/годин).

Трудомісткість програмного продукту визначається по кожному етапу розробки окремо на підставі трудомісткості аналога з урахуванням складності розробки, ступеня новизни і ступеня використання в розробці стандартних модулів на підставі формул:

$$T_{ТЗ} = T^a p \times L_1 \times K_H \quad (2.1)$$

$$T_{ТП} = T^a p \times L_2 \times K_H \quad (2.2)$$

$$T_{РП} = T^a p \times L_3 \times K_H \times K_T \quad (2.3)$$

Для розрахунку необхідні наступні коефіцієнти:

Li – питома вага і-го етапу розробки (див. табл. 2.2.);

Кн – поправочний коефіцієнт, що враховує ступінь новизни (див. табл. 2.3.); Кт – поправочний коефіцієнт, що враховує ступінь використання в розробці типових програм (див. табл. 2.4.).

Таблиця 2.3. Значення питомих коефіцієнтів трудомісткості стадії в загальній трудомісткості розробки ПП

Код стадії	Ступінь новизни		
	А	Б	В
ТЗ (L_1)	0,15	0,12	0,12
ТП (L_2)	0,16	0,15	0,11
РП (L_3)	0,55	0,58	0,61

Для нашого варіанта виділено сірим кольором.

Таблиця 2.4. Значення поправочного коефіцієнта, що враховує ступінь новизни

Код ступеня новизни	Ступінь новизни	Значення $К_н$
А	Принципово нові ПЗ	1,75 – 1,2
Б	ПЗ – розвиток визначеного параметричного ряду	1,0 – 0,8
В	ПЗ маючий аналог	0,7

Для нашого варіанта виділено сірим кольором.

Таблиця 2.5. Значення коефіцієнта ступеня використання в розробці типових програм

Ступінь охоплення реалізованих функцій розроблювального ПО типовими програмами, %	Значення $К_т$
60 і вище	0,6
40-60	0,7
20-40	0,8
До 20	0,9

Для нашого варіанта виділено сірим кольором. Тепер розраховуємо трудомісткість по кожному етапу окремо:

Трудомісткість технічного завдання

$$Т_{тз}=Та*L_1*К_н=195,2 *0,12*0,7= 16,40 \text{ (люд/годин)}$$

Трудомісткість розробки технічного проекту

$$Т_{тп}=Та*L_2*К_н =195,2 *0,11*0,7 = 15,04 \text{ (люд/годин)}$$

Трудомісткість розробки робочого проекту

$$Т_{рп}=Та*L_3*К_н*К_т=195,2 *0,61*0,7*0,7= 58,35 \text{ (люд/годин)}$$

Для подальших розрахунків визначили кількість папера, витраченого на кожен етап: технічне завдання $N_{тз}=2$ (стр), розробка ТП $N_{тп}=15$(стр), розробка робочого проекту $N_{рп}=25$ (стр), пояснювальна записка відповідно $N_{пз}=50$ (стр)

Розрахунок зведений у таблицю 2.6

Таблиця 2.6. Розрахунок трудомісткості ПП

Найменування етапів	Розрахунок, годин.		
1	2	3	4
1.ТЗ	$T_{Pтз}$=16,40	$T_{кк}=0,7*N_{тз}$= 0,7*2=1,4	$T_{нк}=0,15*N_{тз}$=0,15*2=0,30
2.Розробка ТП	$T_{Pтп}$=15,04	$T_{кк}=0,7*N_{тп}$=0,7*15=10,50	$T_{нк}=0,15*N_{тп}$=0,15*15=2,25
3.Розробка РП	$T_{Ррп}$=58,35	$T_{кк}=0,7*N_{рп}$=0,7*25=17,5	$T_{нк}=0,15*N_{рп}$=0,15*25=3,75
4.Розробка ПЗ	$T_{пз}=1,5**N_{пз}$=1,5*50 =75	$T_{кк}=0,7*N_{тз}$=0,7*50=35	$T_{нк}=0,15*N_{пз}$=0,15*50 =7.5
Усього, в т.ч.:	230,2		
- на розробку	$\Sigma T_{р}$=152		
- контроль керівника		$\Sigma T_{кк}$= 64,4	
- нормоконтроль			$\Sigma T_{нк}$=13,8

2.3 Розрахунок ціни програмного продукту

У цьому розділі для визначення ціни розраховуємо основну заробітну плату виконавців, матеріальні витрати, вартість машино – години і витрати на розробку ПЗ. Розрахунок основної заробітної плати виконавців приведений у таблиці 2.7. Відповідно до статті 8 «Закону про Державний бюджет України на 2024» встановлено мінімальну заробітну плату.

Таблиця 2.7 Розрахунок основної заробітної плати виконавців

Найменування робіт	Трудомісткість робіт, години	Погодинна тарифна ставка, грн.	Розрахунок, грн.
1.Розробка ПП	152	39.26	5958,15
2.Контроль керівника	65	38,50	2502,50
3.Нормоконт-роль	14	38,50	539,00
Усього	-	-	ΣЗо= 8999,15

Зробимо розрахунок матеріальних витрат на розробку ПП. Розрахунок зведемо в таблицю 2.8.

Таблиця 2.8. Розрахунок матеріальних витрат на розробку ПЗ

Найменування матеріальних витрат	Тип, модель	Кількість	Ціна одиниці, грн.	Вартість, грн.
Папір	Лист А4	60	2.60	160,0
Разом	-	-	-	$В_{м\ і}$ =160,0
Транспортно– заготівельні витрати (10%)				$Втр\_з = 0{,}1 \times Вм1$= 0,1х160.0=16,0
Усього				$В_м=В_{мі}+В_{тр\ з=}$ 176,0

На підставі отриманих даних по окремих статтях витрат складена калькуляція планової собівартості в цілому ПП за формою, приведеною в таблиці 2.9.

Таблиця 2.9. Розрахунок статей витрат планової собівартості

Стаття витрат	Значення, грн.	Формула розрахунку
1. Матеріали	176,0	$В_м$ (див. табл. 2.7)
2. Основна заробітна плата	8999,15	$З_о$ (див. табл. 2.6)
3.Додаткова заробітна плата	1349,87	$Зд = 0{,}15 \times Зо$ =8999,15х0,15
4.Відрахування до єдиного фонду соціального внеску	2276,78	$Вє.с.в. = 0{,}22 \times (Зо + Зд)$=0,22х (8999,15+ 1349,87)
5. Накладні витрати	2699,75	$Внак. = 0{,}3 \times Зо$ =0,3 х 8999,15
6. Повна собівартість	15501,55	$С_{пов}= В_м +З_о + З_д$ +Вє.с.в. + Внак.= 176,0+8999,15+1349,87+2276,78+ 2699,75

Розмір прибутку, що включається в ціну, визначаємо по наступній формулі:

$$П=(С_п*Р)/100= (15501,55*10)/100 = 1550,15грн \quad (2.4)$$

Де р – плановий рівень рентабельності (10-15%).

Оптова ціна (кошторисна вартість) визначається по формулі:

$$Ц_о =С_п+П =15501,55+1550,15= 17051,70 \text{ грн} \quad (2.5)$$

Податок на додану вартість визначаємо по наступній формулі:

$$ПДВ = 0.2 * Ц_о = 17051,70 *0,2 = 3410,34грн; \quad (2.6)$$

Виходячи з отриманих даних, ціна реалізації розробленого програмного продукту на основі наступної формули, становитиме:

$$Ц_р=Ц_о+ПДВ = 17051,70 + 3410,34 = 20462,04 \text{ грн} \quad (2.7)$$

3 РОЗДІЛ ОХОРОНИ ПРАЦІ ТА ТЕХНІКИ БЕЗПЕКИ

Охорона праці, як соціальний чинник, відіграє на підприємстві важливу, роль оскільки, якими б важливими не були трудові здобутки, вони не можуть компенсувати людині втраченого здоров'я, а тим більше життя. Те і інше дається лише один раз. Необхідно пам'ятати, що внаслідок нещасних випадків та аварій гинуть на виробництві не просто робітники та службовці, на підготовку яких держава вкладає значні кошти, а перш за все люди – годувальники сімей, батьки та матері дітей. Незадовільний стан охорони праці відображається на економіці держави. Служба охорони праці створюється на підприємствах незалежно від форми власності та видів діяльності для виконання правових, організаційно-технічних, санітарно-гігієнічних, соціально-економічних і лікувально-профілактичних заходів, спрямованих на запобігання нещасних випадків, професійних захворювань і аваріям в процесі праці. Основна мета всіх цих заходів – створити на підприємстві безпечні та здорові умови праці.

У розділі охорона праці дипломного проекту наведені характеристики приміщень, де експлуатуються ВДТ. До розгляду взято робоче місце програміста (оператора ЕОМ).

3.1 Аналіз небезпечних та шкідливих чинників, що впливають на працівника

Оператори ПК і програмісти зіштовхуються із впливом таких фізично небезпечних і шкідливих виробничих факторів, як підвищений рівень шуму, підвищена температура зовнішнього середовища, недостатня освітленість робочої зони, електричний струм та інші. Тому на робочому місці програміста повинні бути створені умови для високопродуктивної праці.

Перетворення і обробка інформації проводиться за допомогою ПК. Робота може кваліфікуватися як робота оператором ЕОМ.

3. 2 Розробка заходів з охорони праці

3.2.1 Виробничі приміщення

При плануванні виробничого приміщення врахована санітарна характеристика виробничих процесів, дотримуються норми корисної площі для працюючих, а також нормативи площ для розташування устаткування, що забезпечують безпечну роботу та зручне обслуговування устаткування.

Об’ємно-планувальні рішення будівель та приміщень для роботи з ВДТ мають відповідати вимогам ДСанПіН 3.3.2.007-98. Розміщення робочих місць З ВДТ ЕОМ і ПЕОМ у підвальних приміщеннях, на цокольних поверхах заборонено. Площа на одне робоче місце становить не менше ніж 6,0 $м^2$, а об’єм – не менше ніж 20,0$м^3$.

Виробничі приміщення повинні обладнуватися шафами для зберігання документів, полицями, стелажами, тумбами тощо, з урахуванням вимог до плащі приміщення.

У приміщеннях з ВДТ слід щоденно робити вологе прибирання. Приміщення повинні бути оснащені аптечками першої медичної допомоги.

3.2.2 Мікроклімат робочої зони працівників, вентиляція

У виробничих приміщеннях на робочих місцях з ВДТ мають забезпечуватись оптимальні значення параметрів мікроклімату: температури, відносної вологості й рухливості повітря (ДСанПіН 3.3.2.007-98).

Таблиця 3.1. Норми мікроклімату для приміщень з ВДТ ЕОМ та ПЕМ

Пора року	Категорія робіт	Температура повітря, С, не більше	Відносна вологість повітря %	Швидкість руху повітря, м/с
Холодна	Легка-1а	22-24	40-60	0,1
	Легка-1б	21-23	40-60	0,1
Тепла	Легка-1а	23-25	40-60	0,1
	Легка-1б	22-24	40-60	0,1

Рівні позитивних і негативних іонів у повітрі приміщень з ВДТ мають відповідати санітарно-гігієнічним нормам № 2152-80.

Таблиця 3.2. Рівні позитивних і негативних іонів

Рівні	Число іонів в 1 $см^3$ повітря	Число іонів в 1 $см^3$ повітря
	n+	n-
Мінімально необхідні	400	600
Оптимальні	1500-3000	3000-5000
Максимально допустимі	50000	50000

3.2.3 Освітлення робочого місця, шум, вібрація

Штучне освітлення в приміщеннях з робочими місцями, обладнаними ВДТ має здійснюватись системою загального рівномірного освітлення. У виробничих та адміністративних приміщеннях, у разі переважної роботи з документами, допускається застосування системи комбінованого освітлення – крім системи загального освітлення додатково встановлюються світильники місцевого освітлення.

Значення освітленості на поверхні робочого столу в зоні розміщення документів має становити 300-500лк.

Як джерела світла для штучного освітлення мають застосовуватись переважно люмінесцентні лампи типу ЛД. Допускається застосування ламп розжарювання у світильниках місцевого освітлення.

3.2.4 Організація робочого місця користувача ПК

Робочі місця слід так розташовувати відносно світових прорізів, щоб природне світло падало збоку, переважно зліва. При розміщенні робочих столів з ВДТ слід дотримуватися таких відстаней: між бічними поверхнями ВДТ -1,2м; від тильної поверхні одного ВДТ до екрану іншого – 2,5м.

Екран ВДТ має розташовуватися на оптимальній відстані від очей користувача, що становить 600…700 мм, але не ближче ніж за 600 мм з урахуванням розміру літерно-цифрових знаків і символів.

Клавіатуру розташовують на поверхні столу на відстані 100…300 мм від краю, зверненого до працюючого. У конструкції клавіатури має передбачатися опорний пристрій, який дає змогу змінювати кут нахилу поверхні клавіатури у межах $5…15^0$.

При оснащенні робочого місця лазерним принтером параметри лазерного випромінювання повинні відповідати вимогам СанПіН № 5804-91.

ЕОМ ВДТ і ПК , інше устаткування , електропроводи та кабелі за виконанням і ступенем захисту мають відповідати класу зони за НПАОП 40.1-1.01-97, мати апаратуру захисту від струму короткого замикання та інших аварійних режимів. У приміщеннях, де одночасно експлуатується понад п’ять ЕОМ встановлюється аварійний резервний вимикач, який може повністю вимкнути електричне живлення приміщення, крім освітлення. Не допускається підключати ЕОМ з ВДТ і ПК до звичайної двопровідної електромережі, в тому числі – з використанням перехідних пристроїв

3.2.5 Електробезпека

Це система організаційних і технічних заходів та засобів, що забезпечують захист людей від шкідливої і небезпечної дії електричного струму, електричної дуги, електричного поля і статичної електрики.

Основні технічні засоби і заходи забезпечення електробезпеки при нормальному режимі роботи електроустановок включають:

- ізоляцію струмовідних частин;
- недоступність струмовідних частин;
- блоківки безпеки;
- засоби орієнтації в електроустановках;
- виконання електроустановок, ізольованих від землі;
- захисне розділення електричних мереж;
- компенсацію ємнісних струмів замикання на землю;
- вирівнювання потенціалів.

Із метою підвищення рівня безпеки, залежно від призначення, умов експлуатації і конструкції, в електроустановках застосовується одночасно більшість з перерахованих технічних засобів і заходів.

Особа відповідальна за електрогосподарство призначається з числа працівників, які мають не нижче IV групи з електробезпеки та відповідний стаж роботи для обслуговування електроустановок несе персональну відповідальність за допущення працівника використовувати в роботі електричну енергію

3.3 Пожежна безпека

Пожежна небезпека – це можливість виникнення та розвитку пожежі в будь-якій речовині, процесі, стані.. Коли людина перебуває в зоні впливу пожежі, то вона може потрапити під дію наступних небезпечних та шкідливих факторів: токсичні продукти згорання, вогонь, підвищена температура середовища, дим, недостатність кисню, руйнування будівельних конструкцій, вибухи, паніка.

Усі працівники повинні вміти користуватись наявними вогнегасниками, іншими первинними засобами пожежогасіння, знати місце їх знаходження.

До первинних засобів пожежогасіння відносяться:

- вогнегасники;

- пожежний інвентар (покривала з негорючого теплоізоляційного полотна, грубововняної тканини або повсті;
- ящики з піском;
- бочки з водою, пожежні відра, совкові лопати) та пожежний інструмент (гаки, ломи, сокири тощо).

Пожежні щити (стенди) встановлюються на території об’єкта з розрахунку один щит (стенд) на площу 5000 м^2. Ящики для піску повинні мати місткість 0,5, 1,0 або 3,0 м3 та бути укомплектованими совковою лопатою.

ВИСНОВКИ

Поняття "ризик" присутнє у діяльності будь-якого підприємства, незалежно від етапу його розвитку або виду господарської діяльності. Якщо в планах керівників компаній присутні плани з розвитку, розширення і потенційному зростанню - однозначно, в стратегії компанії повинні бути присутніми механізми роботи з ризиками від їх виявлення до розробки комплексу контрзаходів. Розуміння природи ризиків, повноцінне впроваження ризик-менеджменту роботу підприємства любих масштабів – це запорука довгостроковості перебування на ринку, гарантування прибутків та виконання обов’язків перед клієнтами та партнерами. Можливість проведення базового аудиту на основі онлайн-рішення дозволить навіть мікробізнесу користуватися підходом великих компаній без експертизи в безпеці. А це - важливий крок до розуміння необхідності використання методів та засобів захисту і досягнення мети захисту.

ПЕРЕЛІК ВИКОРИСТАНИХ ІНФОРМАЦІЙНИХ ДЖЕРЕЛ

1. Управление рисками на предприятии / CIDCON CONSULTING COMPANY. - Киев, 2012. - 43 стр.

2. Савчук В. Основи ризик-менеджменту підприємств / Володимир Савчук. – Дніпро: Баланс Бізнес Букс, 2019. – 280 с.

3. Приймак В. М. Управління проектами / В. М. Приймак. – Київ: Київський національний університет імені Тараса Шевченка, 2017. – 464 с.

4. Десять основных рисков для бизнеса в ближайшие два года [електронний ресурс]. Режим доступу: http://forbes.ua/nation/1349183-10-osnovnyh-riskov-dlya-biznesa-v-blizhajshie-dva-goda

5. Стайкуца С. В. Аналіз ризиків корпоративного середовища з позиції міжнародних стандартів інформаційної безпеки / С. В. Стайкуца, С.О. Дігол, О.М. Бердніков, В.І. Верстаков // Сборник тезисов третьей всеукраинской научно-практической конференции "Перспективные направления защиты информации", ОНАС им. А.С. Попова. – 2017. – С. 68–72.

6. Стайкуца, С. (2023). Підходи до організації корпоративної безпеки у фокусі підприємств малого бізнесу. Науковий збірник «InterConf», (180), 394–397.

7. Програмна реалізація аудиту стану інформаційної безпеки підприємства малого бізнесу / М. М. Гаджиєв, С. В. Стайкуца, А. М. Хряпа, А. В. Вербецький. // InterConf. – 2024. – №181.

8. Що таке Vue.js? [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://ru.vuejs.org/v2/guide/index.html.

9. Modern & Interactive Open-source Charts. APEXCHARTS.JS [Електронний ресурс]. – 2023. – Режим доступу до ресурсу: https://apexcharts.com/.

ДОДАТОК А. Слайди мультимедійної презентації

ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ

РОЗРОБКА РІШЕННЯ ЩОДО ОЦІНКИ СТАНУ РІВНЯ ЗАХИЩЕНОСТІ СУЧАСНОГО ПІДПРИЄМСТВА

ДИПЛОМНИЙ ПРОЕКТ

Керівник:
к.ф.н., доцент каф. КБ та ТЗІ ДУІТЗ Стайкуца С.В.

Виконав:
студент групи 4КБ-01 Стрижак Я.В.

2024

БАЗОВІ ПОНЯТТЯ ЩОДО РИЗИКІВ ТА РОБОТИ З НИМИ

Ризик – це взаємодія двох ключових факторів:
ймовірності виникнення інциденту та величини його потенційного впливу.

$$РИЗИК = P_{події} \times ЦІНА\ ВТРАТИ$$

Класифікація ризиків підприємства

ОСНОВНІ ПРОЦЕСИ ЖИТТЄВОГО ЦИКЛУ УПРАВЛІННЯ РИЗИКАМИ

1. Визначення контексту і масштабу ризику, розроблення стратегії управління ризиками
2. Вибір відповідальних та пов'язаних партнерів, ідентифікація ризиків та підготовка реєстрів ризиків
3. Проведення якісного аналізу ризиків, вибір ризиків, які потребують детального аналізу
4. Проведення кількісного аналізу обраного ризику.
5. Планування заходів реагування та визначення контролю для ризику
6. Впровадження заходів реагування на ризики та обрані засоби контролю
7. Моніторинг покращення ризиків та залишкового ризику

ІНСТРУМЕНТИ КІЛЬКІСНОГО АНАЛІЗУ РИЗИКІВ

1. Експертні оцінки
2. Статистичні дані
3. Облік чинників, що впливають на рівні загроз і вразливостей

Непрямі фактори для оцінки загроз

Методи оцінки загроз та ризиків

ТЕХНОЛОГІЇ РОБОТИ З КОРПОРАТИВНИМИ РИЗИКАМИ

Об'єктивність в оцінці

Поле прогнозування витрат/вигод

Вразливість ресурсу

Гнучкість для задоволення потреб конкретних ситуацій

Гнучкість для задоволення потреб конкретних галузей

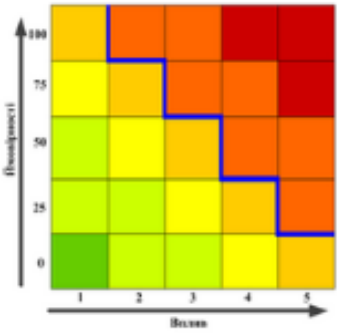
Потужний інструмент продажу керівництву

Переваги використання кількісного аналізу ризиків

1. **Евристичні методи** — Засновані на досвіді або експертні методи для оцінки непередбачених обставин
2. **Трикрапкова оцінка** — Метод, який використовує оптимістичні, найбільш вагомі та песимістичні значення для визначення найкращої оцінки
3. **Аналіз дерева рішень** — Діаграма, яка показує наслідки вибору різних альтернатив
4. **Очікувана грошова вартість (EMV)** — Метод, який використовується для створення резерву на випадок непередбачених обставин
5. **Аналіз Монте-Карло** — метод, який використовує оптимістичні, найбільш вагомі та песимістичні оцінки для визначення вартості бізнесу та терміна завершення проекту
6. **Аналіз чутливості** — Метод, що використовується для визначення ризику, який має найбільший вплив на проект або бізнес-процес
7. **Аналіз дерева несправностей (FTA)** — Аналіз структурованої діаграми, яка визначає елементи, що можуть спричинити відмову системи

Інструменти кількісного аналізу ризиків

ПОБУДОВА СИСТЕМИ УПРАВЛІННЯ РИЗИКАМИ СУЧАСНОГО ПІДПРИЄМСТВА



Координати карти ризиків:
Вплив (значимість, втрати) - ймовірність.
Для впливу (значимості, втрати):
1 - незначний ризик;
2 - допустимий ризик;
3 - підвищений ризик;
4 - критичний ризик;
5 - катастрофічний ризик.
Для ймовірності (частоти реалізації):
0 - ризик напевно не реалізується;
25 - ризик швидше за все, не реалізується;
50 - про настання події не можна сказати нічого певного;
75 - ризик, швидше за все, реалізується
100 - ризик напевно реалізується.

Арабські цифри на карті - позначення ризиків, які були класифіковані за категоріями значущості та шкалі категорій ймовірності
Жирна ламана лінія - критична межа терпимості до ризику

Ймовірність події	незначна	помірна	значна	висока
майже точно			V	
ймовірно		D	D	
Може бути		L	E,F,R	E
майже неможливо			M	R

Серйозність наслідків

Для зручності кожному виявленому ризику присвоюється своя буква:
D - стихійна лихо;
E - екологічна проблема;
F - наполадки обладнання;
L - трудовий спір;
M - пошкодження критичного запасу на склад;
R - порушення законодавчо-регулятивних актів;
V - наполадки засобів паралювання.
Найбільш небезпечними ризиками є ті, які розташовані ближче до правого верхнього кута.
Для компанії UCI такими є стихійне лихо (D) і наполадки засобів паралювання (V).

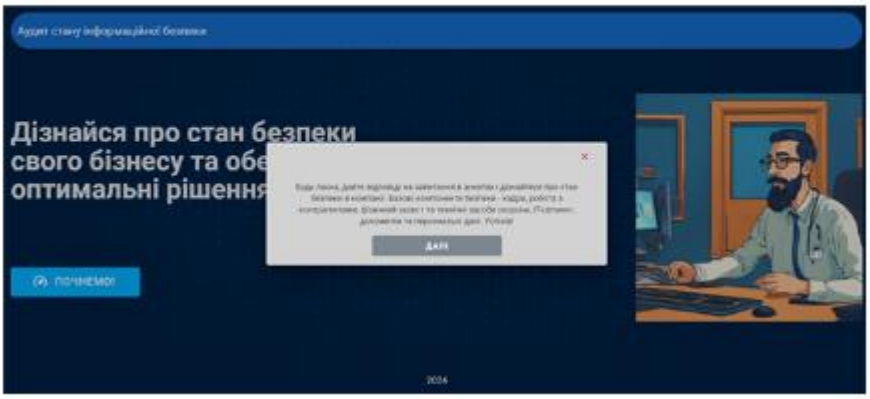
МЕТОДИКИ І РЕКОМЕНДАЦІЇ З УПРАВЛІННЯ РИЗИКАМИ

Життєвий цикл" управління ризиками згідно MG-2

Фактор визначення ймовірності реалізації загрози

РОЗРОБКА ПРОГРАМНОГО МЕТОДУ ОЦІНКИ РІВНЯ БЕЗПЕКИ ПІДПРИЄМСТВА

Програмна реалізація перевірки стану захищеності підприємства

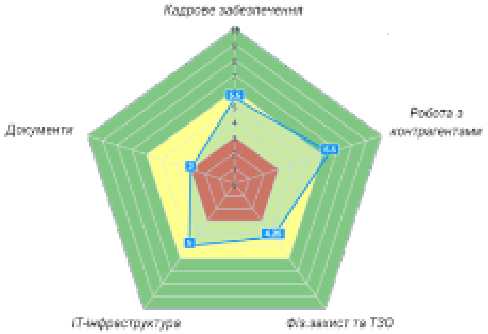


РОЗРОБКА ПРОГРАМНОГО МЕТОДУ ОЦІНКИ РІВНЯ БЕЗПЕКИ ПІДПРИЄМСТВА

Модель оцінки рівня інформаційної безпеки підприємства

Перелік питань та відповідей для напряму контрагентів

№ з/п	Запитання	Відповіді	Оцінка
	Контрагенти		
1	На підприємстві триває попередня перевірка контрагентів?	Так	1
		Ні	0
2	[illegible]	Так	1
		Ні	0
3	[illegible] (а) – 1 бал, [illegible] (б) – 0,5 бала, [illegible] (в) – 0 балів)	а	1
		б	0,5
		в	0
4	[illegible]	Так	1
		Ні	0
5	[illegible]	Так	1
		Ні	0
6	[illegible] (а) – 1 бал, [illegible] (б) – 0,5 бала, [illegible] (в) – 0 балів)	а	1
		б	0,5
		в	0
7	[illegible] (а) – 1 бал, [illegible] (б) – 0,5 бала, [illegible] (в) – 0 балів)	а	1
		б	0,5
		в	0
8	На підприємстві [illegible]	Так	1
		Ні	0
9	[illegible]	Так	1
		Ні	0
10	На підприємстві [illegible]	Так	1
		Ні	0



Представлено таке зонування:

- *початковий рівень захисту (початкові дані);*
- *поточний рівень захисту (результат роботи);*
- *зона високого ризику (показник ≤3);*
- *зона допустимого ризику (значення в діапазоні 3-7);*
- *безпечна зона (показник ≥7).*

РОЗРОБКА ПРОГРАМНОГО МЕТОДУ ОЦІНКИ РІВНЯ БЕЗПЕКИ ПІДПРИЄМСТВА

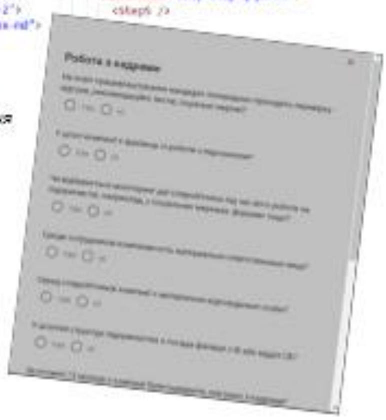
Побудова радару загроз

Методи та засоби захисту в кадровому напрямку

№	Действие	Балл
1	Аналіз претендента перед проведенням співбесіди (листи, дзвінки, соціальні мережі, реєстри тощо)	0,5
2	Застосування методів та засобів конкурентної розвідки	0,35
3	Лише офіційне працевлаштування співробітників	0,5
4	Моніторинг СБ підприємства дій співробітників на повному життєвому циклі – на роботі, поза роботою, соціальні мережі	0,25
5	Системне навчання персоналу підприємства з питань безпеки	0,5
6	Використання управлінських рішень, спрямованих на лояльність персоналу та оптимальних KPI	0,25
7	Наявність власного відділу кадрів (HR)	0,5
8	На підприємстві відсутні порушення КЗпП та заборгованості із ЗП	0,35
9	Застосовуються легальні засоби віддаленого контролю персоналу	0,25
10	У компанії має місце колективна робота з оптимізації процесів та побудови BCM (безперервності бізнесу)	0,5

```
<ModelCommon id="test" persistent>
  <v-window v-model="steptab">
    <v-window-item value="step-0">
      <Step0 />
    </v-window-item>
    <v-window-item value="step-1">
      <div class="wrap-step q-px-md">
        <Step1 />
      </div>
    </v-window-item>
    <v-window-item value="step-2">
      <div class="wrap-step q-px-md">
        <Step2 />
      </div>
    </v-window-item>
    <v-window-item value="step-3">
      <div class="wrap-step q-px-md">
        <Step3 />
      </div>
    </v-window-item>
    <v-window-item value="step-4">
      <div class="wrap-step q-px-md">
        <Step4 />
      </div>
    </v-window-item>
    <v-window-item value="step-5">
      <div class="wrap-step q-px-md">
        <Step5 />
```

Реалізація форми опитування



ЗАСОБИ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Мова програмування - ***JavaScript***

Фреймворк - ***Vue.js***

Бібліотека ***ApexCharts.js***

Візуалізація ***HTML + SCSS UI Component фреймворку - Vuetify***

РАДАР ЗАГРОЗ З ВІДОБРАЖЕННЯ ПОЧАТКОВОГО ТА ПОТОЧНОГО РІВНЯ ЗАХИСТУ, ПІСЛЯ ЗАСТОСУВАННЯ ІНСТРУМЕНТІВ ЗАХИСТУ

Візуалізація результатів після застосування методів та засобів захисту по базовим напрямам захисту

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника на дипломний проект здобувача (здобувачки) освіти

відділення комп'ютерних систем

Стрижак Ярославу Владиславовичу

(прізвище, ім`я та по батькові)

Спеціальність: *123 "Комп'ютерна інженерія"*

Освітня програма: *«Безпека комп'ютерних систем і мереж»*

Тема дипломного проекту: Розробка рішення охоронної щодо оцінки стану рівня захищеності сучасного підприємства

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ

а) обсяг і якість виконання проекту (графічного матеріалу і розрахунково-пояснювальної записки) *Дипломний проект виконано відповідно технічному завданню. Пояснювальна записка містить 67 сторінки. У пояснювальній записці розглянуто питання створення рішення для можливості перевірки станц захищеності підприємства по базовим напрямкам бізнес-процесів. Графічна частина складається з слайдів мультимедійної презентації, які також містять креслення, передбачені технічним завданням. Якість виконання пояснювальної записки та графічної частини добра, розробку виконано в повному обсязі.*

б) самостійність роботи над проектом: *Протягом всього строку дипломного проектування та переддипломної практики здобувач освіти Стрижак Я.В. виконував всі етапи розробки проекту, без порушення термінів. Роботу студент виконував в більшій мірі самостійно, з оглядом на рекомендації керівника та отримуючи зворотній зв'язок.*

в) теоретична підготовка випускника (випускниці): *Здобувач освіти Стрижак Я.В під час роботи над дипломним проектом проаналізував достатню кількість літературних джерел та матеріалів за обраною тематикою.*

Вважаю, що теоретична підготовка дипломника якісна, дипломник готовий до захисту дипломного проекту.

г) вміння розв'язувати виробничі та конструкторські питання _____

Під час дипломного проектування здобувач освіти Стрижак Я.В. приймав рішення щодо вибору методик, аналізував вимоги на етапах проектування, розробляв проектні рішення, обґрунтовував вибір платформи розробки, мови програмування та алгоритмів реалізації розробленого проекту.

Оцінка розрахункової частини *Добре*

Оцінка графічної частини *Відмінно*

Загальна оцінка *Добре*

Прізвище, ім'я, по батькові керівника дипломного проекту _____

Стайкуца Сергій Володимирович

Місце роботи і посада керівника дипломного проекту _____

"Державний університет інтелектуальних технологій і зв'язку", доцент кафедри кібербезпеки та технічного захисту інформації, помічник декана факультету інформаційних технологій та кібербезпеки

Підпис _____

«12» 06 2024 р.

Підпис посвідчую
Начальник відділу
кадрів ДУІТЗ
12.06.2024 р.

Міністерство освіти і науки України * Державний університет інтелектуальних технологій і зв'язку * 43997335 * Відділ кадрів

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на дипломний проект (роботу) здобувача (здобувачки) освіти

відділення комп'ютерних систем

Стрижак Ярославу Владиславовичу

(прізвище, ім'я та по батькові)

Спеціальність 123 "Комп'ютерна інженерія"

Освітня програма «Безпека комп'ютерних систем і мереж»

Керівник дипломного проекту (роботи) Стайкуца Сергій Володимирович

(прізвище, ім'я та по батькові)

Тема дипломного проекту (роботи) Розробка рішення щодо оцінки стану рівня захищеності сучасного підприємства

Обсяг розрахунково-пояснювальної записки _____ сторінок

Обсяг графічної (презентаційної) частини _____ аркушів (слайдів)

ХАРАКТЕРИСТИКА ДИПЛОМНОГО ПРОЕКТУ (РОБОТИ)

а) заключення про ступінь відповідності виконаного дипломного проекту (роботи) завданню

Представлений на рецензію дипломний проект повністю відповідає меті проектування та технічному завданню. Тематика дипломного проекту є актуальною та присвячена розробці рішення з оцінки стану захищеності сучасного підприємства

б) характеристика виконання кожного розділу дипломного проекту (роботи)

Дипломний проект складається зі вступу, трьох розділів, висновків, переліку використаних джерел. В основноій частині проведено аналіз загроз та вразливостей сучасних підприємств, методики і рекомендації з управління ризиками, представлено розробку рішення для оцінки стану захищеності підприємства.

в) оцінка якості виконання пояснювальної записки та графічної частини дипломного проекту (роботи) Графічна частина виконана на достатньо високому рівні у вигляді презентації із використанням офісного пакету Microsoft PowerPoint та Visio. Пояснювальна записка виконана акуратно та у відповідності до норм оформлення документів із використанням офісного пакету Microsoft Word. Загальна якість виконання – добра, академічного плагіату у роботі не виявлено.

г) перелік позитивних якостей дипломного проекту (роботи)

1. Проведено детальний аналіз загроз та вразливостей сучасних підприємств
2. Розглянуто технології роботи з корпоративними ризиками
3. Представлено цікаве програмне рішення для оцінки рівня захищеності компаній

д) основні недоліки дипломного проекту (роботи)

1. Треба було провести аналіз існуючих на ринку безпеки програмних рішень
2. Було б доцільним при виборі механізмів захисту навести критерії бюджету, щоб була змога розуміти фінансові витрати на реалізацію захисту

Оцінка розрахункової частини добре

Оцінка графічної частини відмінно

Загальна оцінка добре

Прізвище, ім'я, по батькові рецензента к.т.н. Селіванова Алла Віталіївна

Місце роботи і посада рецензента Одеський національний технологічний університет, декан факультету комп'ютерної інженерії, програмування та кіберзахисту

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ ОДЕСЬКИЙ НАЦІОНАЛЬНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ ФАКУЛЬТЕТ КОМП'ЮТЕРНОЇ ІНЖЕНЕРІЇ, ПРОГРАМУВАННЯ ТА КІБЕРЗАХИСТУ

Підпис:

« 17 » червня 2024 р.

UNICHECK
by Turnitin

Ім'я користувача:
Катерина Григоріївна Краснокутська

ID перевірки:
1016338545

Дата перевірки:
09.06.2024 17:10:26 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
09.06.2024 18:04:09 EEST

ID користувача:
100011688

Назва документа: 4КБ-01 Стрижак Ярослав

Кількість сторінок: 48 Кількість слів: 8214 Кількість символів: 61724 Розмір файлу: 1.57 MB ID файлу: 1016139641

10.2%
Схожість

Найбільша схожість: 2.53% з Інтернет-джерелом (https://card-file.ontu.edu.ua/server/api/core/bitstreams/4c0773a8-2d0..

10.2% Джерела з Інтернету **166** ..... **Сторінка** 50

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

ДОЗВІЛ
НА РОЗМІЩЕННЯ
ВИПУСКНОЇ КВАЛІФІКАЦІЙНОЇ РОБОТИ
В ЕЛЕКТРОННОМУ РЕПОЗИТАРІЇ ВСП «ОТФК ОНТУ»

Ми, що нижче підписалися,

Стрижак Ярослав Владиславович,
здобувач освіти гр. 4КБ-01, та

Стайкуца Сергій Володимирович,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до дипломного проекту фахового молодшого бакалавра на тему:

«Розробка рішення щодо оцінки стану рівня захищеності сучасного підприємства»

(автор роботи – Стрижак Я.В., керівник роботи – Стайкуца С.В.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2024 році, у повному обсязі в електронному репозитарії ВСП «ОТФК ОНТУ» для вільного доступу через мережу Інтернет.

Несемо відповідальність за ідентичність електронного та друкованого варіантів випускної кваліфікаційної роботи і даємо згоду на обробку персональних даних.

Виконавець _____ / Стрижак Я.В. /

Керівник _____ / Стайкуца С.В. /

«12» червня 2024 р.