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

Спеціальність: 123 «Комп'ютерна інженерія»

Освітня програма: «Комп'ютерна інженерія»

Група: 2БКС-27

КВАЛІФІКАЦІЙНА РОБОТА БАКАЛАВРА

здобувача освіти денної форми навчання

БКС.27.29.000.КРБ

Ускова Сергія Олександровича

м. Одеса
2023 р.

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

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

Освітня програма: **«Комп'ютерна інженерія»**

Група: **2БКС-27**

ПОЯСНЮВАЛЬНА ЗАПИСКА

До кваліфікаційної роботи бакалавра на тему: _____

«Дослідження ролі аудиту та ризик-менеджменту в системі безпеки підприємства»

_____

Проектний матеріал складається з пояснювальної записки на 67 сторінках та графічного (презентаційного) матеріалу на 17 аркушах (слайдах)

Виконавець _____ (Усков С.О.)

Керівник проекту _____ (Кільдішев В.Й.)

Консультанти:

з охорони праці _____ (Чорновол Н.І.)

з дотримання вимог ЄСКД _____ (Петрашова В.І.)

старший консультант _____ (Кривченко Ю.В.)

До захисту допущений

Завідувачка кафедри _____ (Іванова Л.В.)

Завідувач відділення _____ (Скорнякова О.В.)

Захист «20» 06 2023 р. Протокол ДКК № 1

Оцінка ДКК 4 (добре)

Секретар ДКК _____

АНОТАЦІЯ

Метою даної роботи є дослідження ролі аудиту та ризик-менеджменту в системі безпеки підприємства.

У бакалаврській роботі розглянуто базові відомості про IT-інфраструктуру сучасного підприємства, розглянуто компонентний склад, вимоги до безперебійної роботи, представлено класифікацію IT-систем за рівнем безперервності. Розглянуто загрози та ризики кіберсередовища підприємства, наведено класифікацію порушників та модель загроз інформаційної безпеки підприємства. Проведено дослідження життєвого циклу інформаційних засобів та систем, розглянуто стадії, стандарти, обрано додаткові етапи в рамках життєвого циклу – аудит та інвентаризацію.

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

Відділення *комп'ютерних систем* Кафедра *комп'ютерної інженерії*

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Спеціальність *123 «Комп'ютерна інженерія»*

ЗАТВЕРДЖУЮ:

Заст. дир. з НВР Беркань Т.В.

"_____" _____ 202___ р.

ЗАВДАННЯ

на кваліфікаційну роботу бакалавра

Здобувачеві (здобувачці) освіти Ускову Сергію Олександровичу

(прізвище, ім'я, по батькові)

1. Тема кваліфікаційної роботи Дослідження ролі аудиту та ризик-менеджменту в системі безпеки підприємства

затверджена наказом по коледжу від "17" жовтня 2022 р. № 235-А2-ОД

2. Термін здачі кваліфікаційної роботи 15 червня 2023 р.

3. Вихідні дані до роботи Об'єкт аналізу – компоненти базової IT- інфраструктури: фізична мережа, сервіси, служба каталогу, захищене з'єднання, файлові сервіси. Кількість складових ТСО - 15. Моделі життєвого циклу – каскадна, спіральна. Етапи оптимізації ЖЦ – аудит, інвентаризація, пентестінг, програмні засоби, WLAN.

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

Вступ. 1. Розглянути склад, компоненти, класифікацію щодо IT – інфраструктури підприємства. 2. Навести загрози та ризики кіберсередовища підприємства. 3. Дослідити життєвий цикл інформаційних систем та засобів. 4. Обрати та впровадити етапи оптимізації життєвого циклу інформаційної системи підприємства. 5. Охорона праці. Висновки. Перелік використаних джерел. Додаток

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

Лист 1 – Аудит, процес збору та аналізу для якісної оцінки

Лист 2 – Цілі аудиту ІБ організації

Лист 3 – Способи проведення аудиту власними та довіреними

Лист 4 – Порядок проведення аудиту

6. Консультанти по кваліфікаційній роботі, із зазначенням розділів роботи, що стосується їх

Розділ	Консультант	ПІДПИС	
		Завдання видав	Завдання прийняв
Основний	*Кільдішев В.Й.*		
Охорона праці	*Черновол Н.І.*		
Нормоконтроль	*Петрашова В.І.*		
Старший консультант	*Кривченко Ю.В.*		

7. Дата видачі завдання Кільдішев В.Й.

Керівник роботи _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/р	Назва етапів кваліфікаційної роботи	Термін виконання етапів кваліфікаційної роботи	Примітка
1	Вступ. Базові відомості про ІТ-інфраструктуру сучасного підприємства	**24.05.2023 р.**	Виконано
2	Загрози та ризики кіберсередовища підприємства	**26.05.2023 р.**	Виконано
3	Дослідження «життєвого» циклу інформаційних засобів та систем	**01.06.2023 р.**	Виконано
4	Оптимізація життєвого циклу ІТ - системи підприємства з позиції кібербезпеки	**03.06.2023 р.**	Виконано
5	Виконання розділу «Охорона праці»	**08.06.2023 р.**	Виконано
6	Виконання графічної частини роботи	**13.06.2023 р.**	Виконано
7	Чистове оформлення пояснювальної записки кваліфікаційної роботи	**15.06.2023 р.**	Виконано
8	Підготовка доповіді та презентації для захисту	**17.06.2023 р.**	Виконано
9	Отримання рецензії, відповіді на зауваження рецензента	**21.06.2023 р.**	Виконано
10	Захист роботи	**23.06.2023 р.**	Виконано

Виконавець _____
(підпис)

Керівник роботи _____
(підпис)

Формат	Зона	Поз.	Позначення	Назва	Кіл.	Примітка
				Документація		
			БКС 27.29.000.00 КРБ	*Кваліфікаційна робота*		
А4			БКС 27.29.000.00 КРБ ПЗ	*Пояснювальна*	*1*	
				записка		
			БКС 27.29.000.00 КРБ МП	*Мультимедійна*		
				презентація		

Ізм.	Арк.	№ докум.	Підпис	Дата	*БКС 27.29.000.00 КРБ ПЗ*		
Розробив		Усков С.О.			Дослідження ролі аудиту та ризик-менеджменту в системі безпеки підприємства	Літ.	Аркуш
Перевірив		Кільдішев В.Й.				*Н Д П*	*3*
						ОТФК ОНТУ гр.БКС-27	
Н. Контр.		Петрашова В.І.					
Затверд.		Іванова Л.В.					

ЗМІСТ

ВСТУП

Інформаційне середовище сучасного підприємства – це завжди багатогранне та неоднорідне середовище, різноманітність технологій, зміни парадигм загроз та ризиків. Для збереження ефективності потрібно шукати оптимальні інструменти для аналізу ризиків середовища та вибору методів та засобів захисту. До цих рішень можна віднести ризик-менеджмент та аудит.

Найбільш поширеним є визначення ризик-менеджменту як системи управління ризиком та економічними, точніше фінансовими відносинами, які виникають у процесі управління. Управління ризиком - багатоетапний процес, мета якого зменшити чи компенсувати збитки для об'єкта при настанні несприятливих подій. Це сукупність принципів, методів і форм управління організацією та її поведінкою в зовнішньому середовищі в умовах невизначеності та конфліктності.

В рамках ризик-менеджменту вирішуються три основні завдання: профілактика виникнення ризиків; мінімізація збитку, спричиненого ризиками; максимізація додаткового прибутку, який отримує підприємство внаслідок управління ризиками.

До цілей аудиту може відноситись бажання керівництва зрозуміти стан на реальний момент часу, проведення систематизації для впорядкування існуючих засобів захисту, розслідування інциденту або дії, направлені на відповідність вимогам законодавства тощо. Отримуючи певні результати на кожному із етапів (розробка регламенту, збір та аналіз інформації, розробка рекомендацій) в рамках аудиторського звіту керівництво компаній отримую можливість зі сторони побачити свій бізнес та стан його компонентів, щоб в подальшому приймати ефективні управлінські рішення.

1 ТЕХНОЛОГІЧНИЙ РОЗДІЛ

1.1 Роль аудиту в системі інформаційної безпеки компанії

Сьогодні інформаційні системи (ІС) відіграють ключову роль в забезпеченні ефективності роботи комерційних і державних підприємств. Повсюдне використання ІС для зберігання, обробки і передачі інформації робить актуальними проблеми їх захисту, особливо з огляду на глобальну тенденцію до зростання числа інформаційних атак, що приводять до значних фінансових і матеріальних втрат. Для ефективного захисту від атак компаніям необхідна об'єктивна оцінка рівня безпеки ІС - саме для цих цілей і застосовується аудит безпеки.

1.1.1 Визначення, цілі, задачі проведення аудиту ІБ

Аудит безпеки в загальному випадку ного можна описати як процес збору та аналізу інформапіі про ІБ для якісної або кількісної оцінки рівня її захищеності від атак зловмисників. Існує безліч випадків, коли доцільно проводити аудит безпеки. Це робиться, зокрема, при підготовці технічного завдання на проектування і розробку системи захисту інформації та після впровадження системи безпеки для оцінки рівня її ефективності.

Можливий аудит, спрямований на приведення діючої системи безпеки у відповідність вимогам українського або міжнародного законодавства. Аудит може також призначатися для систематизації та впорядкування існуючих заходів захисту інформації або для розслідування інциденту, що стався, пов'язаного з порушенням інформаційної безпеки [1].

Як правило, для проведення аудиту залучаються зовнішні компанії, які надають консалтингові послуги в області шформацдйної безпеки Ініціатором процедури аудиту може стати керівництво підприємства, служба автоматизації або служба ін формаційної безпеки У ряді випадків аудит також проводиться на вимогу страхових компаній або регулюючих органів. Аудит безпеки виконується групою експертів, чисельність і склад якої залежить від цілей і завдань обстеження, а також від складності об'єкта оцінки.

Аудит ІБ організації: систематичний, незалежний та документований процес отримання свідоцтв діяльності організації щодо забезпечення інформаційної безпеки та встановлення ступеня виконання в організації критеріїв інформаційної безпеки, а також допускає можливість формування професійної аудиторської думки про стан інформаційної безпеки організації.

Цілі аудиту ІБ:

Аналіз можливості здійснення загроз безпеці по відношенню до інформаційних систем.

Визначення рівня захищеності ІВ та виявлення слабких місць у системі захисту.

Формування рекомендацій щодо підвищення ефективності механізмів безпеки ІВ.

Оцінка повноти виконання законодавчих вимог, стандартів, нормативних документів.

Основні форми аудиту для ІС:

1. Первинний аудит – проводиться на етапі формування бізнес-вимог до ІС, що впроваджується. Основна мета – формування концепції ІБ у межах цієї ІВ вирішення проблем реалізації вимог нормативних документів.

2. Проектний аудит – проводиться на етапі формування функціональних та технічних вимог до впроваджуваної ІВ. Основна мета – формування конкретних вимог до ІВ щодо забезпечення безпеки, визначення необхідних засобів захисту.

3. Атестаційний аудит – проводиться після завершення робіт із побудови ІВ. Основна мета – підтвердження відповідності вжитих заходів у частині ІБ необхідним стандартам.

4. Плановий аудит – проводиться протягом усього життєвого циклу ІС. Основна мета – контроль (підтвердження) рівня ІБ ІВ, перевірка дотримання користувачами ІВ політик безпеки.

Проведення регулярного аудиту систем інформаційної безпеки дозволить:

> Запобігти витоку конфіденційної інформації з компанії;

> Виявити найвужчі місця у компанії з погляду інформаційної безпеки;

> Підвищити культуру інформаційну безпеку серед співробітників компанії.

Основними передумовами проведення аудиту ІБ є:

Отримання об'єктивної інформації про захищеність інформаційних активів, оцінка ефективності діючих систем захисту;

Оцінка відповідності систем захисту (отримання сертифікату відповідності) вимогам міжнародних та вітчизняних стандартів, галузевим нормативним документам;

Контроль функціонування ІС та діяльності персоналу (регулярна діяльність).

Рисунок 1.1 – Переваги та недоліки аудиту власними та зовнішніми силами

1.1.2 Види аудиту інформаційної безпеки

Можна виділити наступні основні види аудиту інформаційної безпеки:

• експертний аудит безпеки, в ході якого виявляються недоліки в системі заходів захисту інформації на основі досвіду експертів, що беруть участь в процедурі обстеження:

• оцінка відповідності рекомендаціям міжнародного стандарту ISO 17799. а також вимогам керівних документів:

• інстлзументальний аналіз захищеності ІС, спрямований на виявлення та усунення вразливостей програмно-апаратного забезпечення системи:

• комплексний аудит, який включає в себе всі перераховані вище форми проведення обстеження.

Будь-який з перерахованих видів аудиту може проводитися окремо або в комплексі, в залежності від тих завдань, які вирішує підприємство. Як об'єкт

аудиту може виступати як ІС компанії в цілому, так і її окремі сегменти, в яких обробляється інформація, що підлягає захисту [2].

Розглянемо ще одну точку зору щодо аудиту ІБ безпеки компанії.

Активний аудит представляє дослідження дослідження стану захищеності інформаційної системи з точки зору хакера (або якогось зловмисника зловмисника, що володіє високою кваліфікацією в галузі інформаційних технологій).

Суть активного аудиту полягає в тому, що за допомогою спеціального програмного забезпечення (у тому числі за допомогою систем аналізу захищеності захищеності) та спеціальних методів здійснюється збір інформації про стан системи мережевого захисту. При здійсненні даного виду аудиту на систему мережевий захист моделюється якомога більше таких мережевих атак атак, які може виконати хакер.

Результатом активного аудиту є інформація про всі вразливості, ступінь їх критичності та методи усунення усунення, відомості про широкодоступну інформацію (інформація інформація, доступна будь-якому потенційному порушнику порушника) мережі замовника замовника. Після закінчення активного аудиту видаються рекомендації щодо модернізації системи системи мережевого захисту, які дозволяють усунути небезпечні вразливості.

Активний аудит ділиться на зовнішній активний аудит і внутрішній активний аудит. При зовнішньому активному аудиті фахівці моделюють дії зовнішнього зловмисника. В даному випадку проводяться такі процедури:

- визначення доступних із зовнішніх мереж IP-адрес замовника;

- сканування даних адрес з метою визначення працюючих сервісів та служб, визначення призначення відсканованих хостів;

- Визначення версій сервісів і служб хостів, що скануються;

- Вивчення маршрутів проходження трафіку до хостів замовника;

- збирання інформації про ІВ замовника з відкритих джерел;

- аналіз даних з метою виявлення вразливостей.

«Внутрішній» активний аудит за складом робіт аналогічний до «Зовнішнього», проте при його проведенні за допомогою спеціальних програмних засобів моделюються дії «внутрішнього» зловмисника.

Експертний аудит, про який говорилося вище, становить порівняння стану інформаційної безпеки з «ідеальним» описом описом, який базується на наступному:

- вимоги вимоги, які були пред'явлені керівництвом у процесі аудиту;

- опис «ідеальної» системи безпеки безпеки, заснований на акумульованому в компанії компанії-аудиторі світовому та приватному досвіді.

Склад експертного аудиту:

- збір вихідних даних про інформаційну систему системи, про її функції та особливості особливості, що використовуються технології автоматизованої обробки та передачі даних (з урахуванням найближчих перспектив розвитку);

- збір інформації про наявні організаційно-розпорядчі документи щодо забезпечення інформаційної безпеки та їх аналіз;

- Визначення точок відповідальності систем систем, пристроїв та серверів ІС ІС;

- Формування переліку підсистем кожного підрозділу компанії з категоруванням критичної інформації та схемами інформаційних потоків.

Етапи експертного аудиту.

1. Аналіз проекту інформаційної системи системи, топології мережі та технології обробки інформації інформації, у ході якого виявляються, наприклад, такі недоліки існуючої топології мережі, які знижують рівень захищеності інформаційної системи.

2. Аналіз інформаційних потоків організації. На даному етапі визначаються типи інформаційних потоків ІС організації та складається їх діаграма, де для кожного інформаційного потоку вказується його цінність (у тому числі цінність інформації інформації, що передається) і використовувані методи забезпечення безпеки безпеки, що відображають рівень захищеності інформаційного потоку потоку.

3.Аналіз організаційно-розпорядчих документів документів, таких як політика безпеки, план захисту та різноманітних інструкцій. Організаційно-розпорядчі документи оцінюються на предмет достатності та несуперечності декларованим цілям та заходам інформаційної безпеки.

1.1.3 Аудит як метод збереження і підвищення ефективності IT-інфраструктури

Періодичний аудит інформаційної інфраструктури дає уявлення про відповідність її стану і розвитку конкретним приватним завданням і цілям всього бізнесу. Крім того, аудит допомагає оцінити стан окремих елементів інфраструктури та пов'язані з ними ризики, а значить, дозволяє визначити, які елементи інформаційної інфраструктури повинні удосконалюватися в першу чергу. Коротко сформулювати цілі аудиту IT-інфраструктури можна наступним чином:

– виявлення проблем функціонування IT і складання рекомендацій по їх усуненню. Надання замовникові інформації про виявлені проблеми з IT і рекомендацій щодо їх усунення.

– оцінка якості IT. Замовнику надаються дані про відповідність IT його діловим потребам, важливість справ, стандартам (міждержавним, національним, міжнародним і внутрішньокорпоративних), рекомендаціями виробників

обладнання і загальним принципам створення аналогічних систем. Може бути оцінена інтегральна вартість ІТ і сукупна вартість володіння.

– інвентаризація і документування ІТ. Замовник отримує комплект експлуатаційної документації, що полегшує вирішення завдань поточної експлуатації (додавання і видалення користувачів, впровадження нових додатків тощо).

Про необхідність аудиту корпоративної мережі змушують задуматися конкретні проблеми, що перешкоджають повсякденній діяльності персоналу. Наприклад, вкрай повільне завантаження додатків, потрібних для роботи, або файлів з даними. Часті збої в роботі ІТ створюють загрозу своєчасному виконанню будь-яких важливих поточних завдань (це може бути здача балансу бухгалтерією або проведення важливих платежів). Якщо компанія користується послугами ІТ-аутсорсингу (наприклад, укладає контракт на сервісне обслуговування мережі в сторонньої організації), то аудит, проведений перед укладенням контракту, дасть обслуговуючої організації чітке уявлення про обсяг робіт і дозволить оцінити ризики, пов'язані з обслуговуванням мережі.

Аудит допоможе оптимально сформувати умови договору, виявити критично важливі елементи корпоративної мережі, обслуговування яких має бути пріоритетним, визначити необхідні режими обслуговування (24х7, 8х5 і т. П.). При відпрацюванні сервісних запитів результати аудиту допомагають прискорити виявлення джерела проблеми і, в кінцевому підсумку, знизити час непрацездатності мережі або її елементів.

Періодичне проведення аудитів в ході виконання тривалого контракту з обслуговування складної розвивається мережі дозволить зберігати актуальність уявлень про неї як у обслуговуючої організації, так і у замовника, що також сприяє підвищенню якості обслуговування. Якщо для обслуговування мережі передбачена складна структура з поділом повноважень, то аудит може спростити

управління такою структурою, зробивши її більш прозорою, виявивши рівні відповідальності і кордони поділу повноважень. Перед глибокої модер нізації великої складної корпоративної мережі доцільно провести її аудит. Це допоможе оптимально спланувати модернізацію, зберегти інвестиції, забезпечити гладке впровадження нових технологій. Результати аудиту в цьому випадку стануть частиною вихідних даних для концепції, ескізного проекту, технічного проекту модернізації корпоративної мережі.

Аудит може бути корисний і в ситуації, коли виникає необхідність впровадити нові мережеві додатки, користуючись існуючою корпоративною мережею (без її змін або з мінімальними змінами). Прикладами таких додатків можуть служити системи управління підприємством (SAP / R3, Oracle Applications), системи передачі мультимедійної інформації (IP-телефонії, відеоконференцзв'язок) і т. П. У цьому випадку аудит забезпечить впевненість в достатності ресурсів мережі для роботи нових додатків.

Побудова і модернізація інформаційної інфраструктури є, в основному, проектну діяльність. Дійсно, створення кабельної системи, ЛВС, серверного комплексу, системи зберігання даних, системи резервного копіювання, а також розробка і впровадження прикладного програмного забезпечення майже завжди спрямовані на досягнення унікального результату. Така діяльність організовується за принципами проектного управління.

Грамотно організована експлуатація інформаційної інфраструктури, навпаки, здійснюється зазвичай за принципом конвеєра. Профілактика, сервісне обслуговування, додавання, видалення і переміщення робочих місць, а також інші роботи, пов'язані з експлуатацією, як правило, регламентуються інструкціями. Навіть в тих випадках, коли регламенти не зафіксовано у вигляді документів, фактично вказані операції завжди зводяться до невеликого набору цілком певних дій, регламентування яких не становить серйозної проблеми. Аудит, як одна з

робіт, пов'язаних з експлуатацією корпоративної мережі, також добре піддається регламентації і стандартизації.

Розглянемо складові частини IT-аудиту (рис. 1.2):

Аудит обладнання:

– обстеження стану робочих місць і оргтехніки;

– обстеження стану серверів;

Рисунок 1.2 - Складові частини IT-аудиту

– аналіз стану активного і пасивного мережевого обладнання, кабельної системи;

– аналіз функціонування серверного обладнання та відповідності вимогам;

– аналіз джерел безперебійного живлення, їх достатності.

Аудит програмного забезпечення:

– обстеження встановленого програмного забезпечення на робочих машинах і серверах компанії;

– перевірка програмного забезпечення на наявність ліцензій, прав на його використання, відповідність кількості ліцензій і встановлених програм.

Аудит каналів зв'язку і комунікації:

– обстеження каналів передачі даних;

– аналіз роботи телефонії;

– аналіз роботи і налаштувань корпоративної електронної пошти.

Аудит систем безпеки:

– обстеження систем інформаційної безпеки, що використовуються;

– перевірка роботи антивірусного захисту і антиспам захисту електронної пошти;

– обстеження систем захисту від злому інфраструктури;

– аналіз можливих шляхів доступу до інформації компанії;

– обстеження міжмережевих налаштувань безпеки;

– аналіз налаштувань мережевих політик;

– аналіз системи зберігання і бекапірованія даних.

1.1.4 Інвентаризація IT-ресурсів

Інвентаризація, як рішення для збільшення "життєвого" циклу IT-інфраструктури, дозволяє виявити програмне забезпечення з вичерпаним терміном

підтримки, морально-застаріле обладнання, несанкціоновані програмні і апаратні засоби і т.д. Завдяки інвентаризації, IT-служба підприємства отримує можливість оперативно реагувати на поточні події. Правильно проведена інвентаризація дозволяє досить ефективно управляти апаратними та програмними ресурсами, які числяться на балансі підприємства. З точки зору управління обладнанням, тут можна говорити про можливість виявлення виходу з ладу або розкрадання врахованого обладнання, а так само про виявлення стороннього (шкідливого) обладнання.

При інвентаризації IT-інфраструктури, можна використовувати:

– скрипти зі збору інформації з кожного комп'ютера в мережі. Такий спосіб застосовується, тільки у випадку з однорідною мережею;

– стікери з матричним кодом, QR-кодом. За допомогою спеціального пристрою стікерами маркується все обладнання, і при скануванні заноситься в базу даних. Такий спосіб дозволяє врахувати все обладнання, проте в разі великого обсягу даних - важко вручну обробляти і аналізувати інформацію;

– автоматизовані програмні комплекси (АПК) інвентаризації, що дозволяють накопичувати, порівнювати і аналізувати дані, отримані в різний час. АПК призначені для обліку обладнання, контролю встановленого програмного забезпечення, контролю конфігурації мережі, стану ПК, інвентаризації ПК і пристроїв. На рис. 1.3 представлений набір з різних програмних комплексів для проведення аудиту, і їх функціонал.

Варто зазначити, що використання комбінації з декількох рішень дозволяє більш ефективно проводити інвентаризацію і уникати потенційних ризиків.

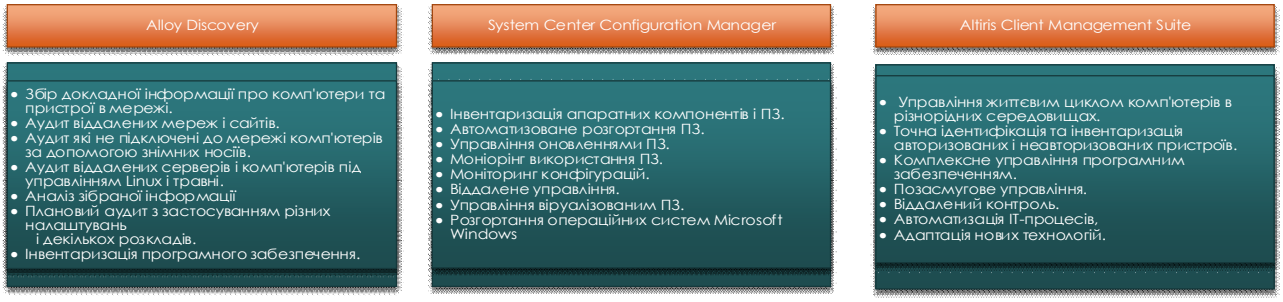


Рисунок 1.3 – Програмні рішення для проведення інвентаризації та їх основні функції

1.1.5 Дослідження етапів проведення аудиту ІБ

У загальному випадку аудит безпеки, незалежно від форми його проведення, складається з чотирьох основних етапів, на кожному з яких виконується певне коло робіт.

На першому етапі спільно з замовником розробляється регламент, який встановлює склад і порядок проведення робіт. Основне завдання регламенту - визначити межі, в рамках яких буде проводитися обстеження. Регламент дозволяє уникнути взаємних претензій по завершенні аудиту, оскільки чітко визначає обов’язки сторін. Як правило, регламент містить наступну основну інформації:

• склад робочих груп від виконавця і замовника для проведення аудиту;

• список і місце розташування об’єктів замовника, що підлягають аудиту;

• перелік інформації, яка буде надана виконавцю;

• перелік ресурсів, які розглядаються в якості об’єктів захисту (інформаційні,

програмні, фізичні ресурси і т. д.);

• модель загроз інформаційній безпеці, на основі якої проводиться аудит;

• категорії користувачів, які розглядаються в якості потенційних порушників;

• порядок і час проведення інструментального обстеження ІС замовника.

На другому етапі, відповідно до узгодженого регламенту, збирається вихідна інформація. Методи збору інформації включають інтерв'ювання співробітників замовника, заповнення опитувальних листів, аналіз наданої організаційно-розпорядчої та технічної документації, використання спеціалізованих інструментальних засобів.

Третій етап робіт передбачає аналіз зібраної інформації з метою оцінки поточного рівня захищеності ІС підприємства. За результатами проведеного аналізу на четвертому етапі розробляються рекомендації з підвищення рівня захищеності ІС від загроз інформаційної безпеки. Нижче докладніше розглянуто етапи аудиту, пов'язані зі збором інформації, її аналізом і розробкою рекомендацій щодо підвищення рівня захисту ІС.

Збір вихідних даних.

Якість аудиту безпеки багато в чому залежить від повноти і точності інформації, отриманої в процесі збору вихідних даних. Тому в неї необхідно включити наступне: організаційно-розпорядчу документацію, яка стосується питань інформаційної безпеки, відомості про програмно-апаратне забезпечення ІС, інформацію про засоби захисту, встановлених в ІС і т.д. Більш детальний перелік вихідних даних представлений далі.

Перелік вихідних даних, необхідних для аудиту безпеки	
Тип інформації	**Склад вихідних даних**
Організаційно-розпорядча документація з питань інформаційної безпеки	• Політика інформаційної безпеки ІС; • Керівні документи (накази, розпорядження, інструкції) з питань зберігання, порядку доступу і передачі інформації; • Регламенти роботи користувачів з інформаційними ресурсами ІС
Інформація про апаратне забезпечення хостів	• Перелік серверів, робочих станцій і комунікаційного устаткування, встановленого в ІС; • Апаратні конфігурації серверів і робочих станцій; • Відомості по периферійному обладнанню
Інформація про загальносистемне ПЗ	• Відомості про ОС, встановлену на робочих станціях і серверах; • Відомості про СУБД, встановлену в ІС
Інформація про прикладне ПЗ	• Перелік прикладного ПЗ загального і спеціального призначення, встановленого в ІС; • Опис функціональних завдань, що вирішуються за допомогою прикладного ПЗ
Інформація про засоби захисту, що встановлені в ІС	• Виробник засобів захисту; • Конфігураційні налаштування засобів захисту; • Схема встановлення засобів захисту
Інформація про топологію ІС	• Карта локальної обчислювальної мережі, включаючи схему розподілу серверів і робочих станцій за сегментами мережі; • Типи каналів зв'язку, що використовується в ІС • Використовувані в ІС мережеві протоколи; • Схема інформаційних потоків ІС

Рисунок 1.4 – Вихідні дані необхідні для аудиту безпеки

Розглянемо методи, які використовуються для збору вихідних даних. Одним з методів є інтерв'ювання співробітників замовника, що володіють необхідною інформацією. Інтерв'ю зазвичай проводяться як з технічними фахівцями, так і з представниками керівної ланки компанії. Перелік питань, які планується обговорити в процесі інтерв'ю, узгоджується заздалегідь.

Надання опитувальних листів з певної тематики, які співробітники замовника заповнюють самостійно. У тих випадках, коли представлені матеріали не повністю відповідають на необхідні питання, проводиться додаткове інтерв'ювання.

Аналіз організаційно-технічної документації, що використовується замовником.

Використання спеціалізованого ПЗ, яке дозволяє отримати необхідну інформацію про склад і настройках програмно-апаратного забезпечення ІС підприємства. Наприклад, за допомогою систем аналізу захищеності (security scanners) можна провести інвентаризацію мережевих ресурсів і виявити уразливості в них.

Оцінка рівня безпеки ІС.

Після збору необхідної інформації проводиться її аналіз з метою оцінки поточного рівня захищеності системи. У процесі такого аналізу визначаються ризики інформаційної безпеки, яким схильна компанія. Фактично ризик являє собою інтегральну оцінку того, наскільки ефективно існуючі засоби захисту здатні протистояти інформаційним атакам [3].

Зазвичай виділяють дві основні групи методів розрахунку ризиків безпеки. Перша група дозволяє встановити рівень ризику шляхом оцінки ступеня відповідності певним набором вимог до інформаційної безпеки. Як джерела таких вимог можуть виступати:

• нормативно-правові документи підприємства, що стосуються питань інформаційної безпеки (політика безпеки, регламенти, накази, розпорядження);

• вимоги чинного українського законодавства;

• рекомендації міжнародних стандартів – ISO 17799, OCTAVE, CoBIT, BS 7799-2 і т. д .;

• рекомендації компаній-виробників програмного і апаратного забезпечення - Microsoft. Oracle. Cisco і т. д.

Друга група методів оцінки ризиків інформаційної безпеки базується на визначенні ймовірності реалізації атак, а також рівнів їх збитку. Значення ризику обчислюється окремо для кожної атаки і в загальному випадку є як добуток імовірності проведення атаки на величину можливого збитку від цієї атаки. Значення шкоди визначається власником інформаційного ресурсу, а ймовірність атаки обчислюється групою експертів, які проводять процедуру аудиту. Імовірність в даному випадку розглядається як міра того, що в результаті проведення атаки порушники досягли своїх цілей і завдали шкоди компанії [4].

Методи обох груп можуть використовувати кількісні або якісні шкали для визначення величини ризику інформаційної безпеки. У першому випадку для ризику і всіх його параметрів беруться чисельні вираження. Наприклад, при використанні кількісних шкал ймовірність проведення атаки може виражатися числом в інтервалі [0,1], а збиток від атаки - задаватися у вигляді грошового еквівалента матеріальних втрат, які може понести організація в разі успішної атаки. При використанні якісних шкал числові значення замінюються на еквівалентні їм понятійні рівні. Кожному понятійному рівню в цьому випадку буде відповідати певний інтервал кількісної шкали оцінки.

Кількість рівнів може варіюватися в залежності від застосовуваних методик оцінки ризиків. У табл. 1.1 і 1.2 наведені приклади якісних шкал оцінки ризиків інформаційної безпеки, в яких для оцінки рівнів збитків та ймовірності атаки використовується п’ять понятійних рівнів.

Для обчислення рівня ризику за якісними шкалами застосовуються спеціальні таблиці, в яких в першому стовпці задаються понятійні рівні збитку, а в першому рядку – рівні ймовірності атаки. Осередки же таблиці, розташовані на перетині відповідних рядків і стовпців, містять рівень ризику безпеки (табл. 1.3).

Розмірність таблиці залежить від кількості концептуальних рівнів ймовірності атаки і шкоди.

Таблиця 1.1 – Якісна шкала оцінки рівня збитку

Якісна шкала оцінки рівня збитку

№	Рівень збитку	Опис
1	Малий	Незначні втрати матеріальних активів, які швидко відновлюються, або незначні наслідки для репутації компанії
2	Помірний	Помітні втрати матеріальних активів або помірних наслідків для репутації компанії
3	Середньої тяжкості	Істотні втрати матеріальних активів або значної шкоди репутації компанії
4	Великий	Великі втрати матеріальних і великих втрат репутації компанії
5	Критичний	Критичні втрати матеріальних активів або повна втрата репутації компанії на ринку, що робить неможливим її подальшу діяльність

Таблиця 1.2 – Якісна шкала оцінки ймовірності проведення атаки

Якісна шкала оцінки ймовірності проведення атаки

№	Рівень збитку	Опис
1	Малий	Атака практично ніколи не буде проведена. Відповідає числовому інтервалу ймовірності [0, 0,25)
2	Помірний	Вірогідність проведення атаки досить низька. Відповідає числовому інтервалу ймовірності [0,25 0,5)
3	Середньої тяжкості	Вірогідність проведення атаки приблизно дорівнює 0,5
4	Великий	Атака швидше за все буде проведена. Відповідає числовому інтервалу ймовірності (0,5 0,75]
5	Критичний	Атака напевне буде проведена. Відповідає числовому інтервалу ймовірності (0,75 1]

Таблиця 1.3 – Визначення рівня ризику інформаційної безпеки за якісною шкалою

Визначення рівня ризику інформаційної безпеки за якісною шкалою					
	Вірогідність атаки				
Збиток	Дуже низька	Низька	Середня	Висока	Дуже висока
Малий	Низький ризик	Низький ризик	Низький ризик	Середній ризик	Середній ризик
Помірний	Низький ризик	Низький ризик	Середній ризик	Середній ризик	Високий ризик
Середньої тяжкості	Низький ризик	Середній ризик	Середній ризик	Середній ризик	Високий ризик
Великий	Середній ризик	Середній ризик	Середній ризик	Середній ризик	Високий ризик
Критичний	Середній ризик	Високий ризик	Високий ризик	Високий ризик	Високий ризик

При розрахунку значень ймовірності атаки, а також рівня можливого збитку використовують статистичні методи, експертні оцінки або елементи теорії прийняття рішень. Статистичні методи передбачають аналіз вже накопичених даних про реально траплялися інциденти, пов'язані з порушенням інформаційної безпеки. На основі результатів такого аналізу будуються припущення про ймовірність проведення атак і рівнях збитку від них в інших ІС. Однак статистичні методи не завжди вдається застосувати через нестачу статистичних даних про раніше проведених атаках на ресурси ІС, аналогічної тій, яка виступає в якості об'єкта оцінки [5].

При використанні апарату експертних оцінок аналізуються результати роботи групи експертів, компетентних в області інформаційної безпеки, які на основі наявного у них досвіду визначають кількісні або якісні рівні ризику. Елементи теорії прийняття рішень дозволяють застосовувати для обчислення значення ризику безпеки більш складні алгоритми обробки результатів роботи групи експертів.

Існують спеціалізовані програмні комплекси, що дозволяють автоматизувати процес аналізу вихідних даних і розрахунку значень ризиків при аудиті безпеки.

Результати аудиту безпеки.

На останньому етапі аудиту інформаційної безпеки розробляються рекомендації щодо вдосконалення організаційно-технічного забезпечення захисту на підприємстві. Такі рекомендації можуть включати в себе різні типи дій, спрямованих на мінімізацію виявлених ризиків.

Зменшення ризику за рахунок додаткових організаційних і технічних засобів захисту, що дозволяють знизити ймовірність проведення атаки або зменшити можливі збитки від неї. Так, установка міжмережевих екранів в точці підключення ІС до Інтернету істотно знижує ймовірність проведення успішної атаки на загальнодоступні інформаційні ресурси ІС – такі, як веб-сервери, поштові сервери і т. д.

Ухилення від ризику шляхом зміни архітектури або схеми інформаційних потоків ІС, що дозволяє виключити проведення тієї чи іншої атаки. Наприклад, фізичне відключення від Інтернету сегмента ІС, в якому обробляється конфіденційна інформація, дозволяє уникнути зовнішніх атак на конфіденційну інформацію.

Зміна характеру ризику в результаті вживання заходів по страхуванню. Як приклади зміни характеру ризику можна привести страхування обладнання ІС від пожежі або страхування інформаційних ресурсів від можливого порушення їх конфіденційності, цілісності або доступності. В даний час ряд українських компаній вже пропонують послуги страхування інформаційних ризиків. Прийняття ризику, якщо він зменшений до того рівня, на якому вже не представляє небезпеки для ІС.

Рекомендації спрямовані не на повне усунення всіх виявлених ризиків, а лише на їх зменшення до прийнятного рівня. При виборі заходів для підвищення рівня захисту ІС враховується одне принципове обмеження - вартість реалізації цих заходів не повинна перевищувати вартості захищаються інформаційних

ресурсів, а також збитків компанії від можливого порушення конфіденційності, цілісності або доступності інформації. На завершення процедури аудиту його результати оформляються у вигляді звітного документа, який надається замовнику. У загальному випадку цей документ складається з наступних основних розділів:

– опис меж, в рамках яких проводився аудит безпеки;

– опис структури ІС замовника;

– методи і засоби, які використовувалися в процесі проведення аудиту;

– опис виявлених вразливостей і недоліків, включаючи рівень їх ризику;

– рекомендації щодо вдосконалення комплексної системи забезпечення інформаційної безпеки;

– пропозиції до плану реалізації першочергових заходів, спрямованих на мінімізацію виявлених ризиків.

Порядок проведення аудиту (рис. 1.5):

1. Постановка завдання аудиту.

2. Інтерв'ювання.

3. Збір вихідних даних.

4. Аналіз даних і оформлення результатів аудиту.

5. Представлення результатів аудиту.

В ході першого етапу виявляються елементи корпоративної мережі, що підлягають обстеженню, такі як активне мережеве обладнання, кабельні системи, системи управління мережею і інші. Фіксується їх кількість, розташування, визначається коло осіб, безпосередньо експлуатують інфраструктуру, що відповідають за її експлуатацію і використовують її в роботі. На етапі збору даних з цими співробітниками проводяться інтерв'ю. Постановка завдання завершується розробкою, узгодженням і затвердженням технічного завдання (ТЗ). У ТЗ на аудит

обов'язково фіксуються вимоги до обстежуваної системі, склад і зміст робіт по аудиту і вимоги до розроблюваних документів.

Рисунок 1.5 - Порядок проведення аудиту

На етапі збору даних цьому етапі зазвичай проводять інтерв'ювання персоналу замовника, огляд і інвентаризацію обладнання, збір конфигурационной і операційної інформації, вимірювання різних параметрів мережі.

Збір даних може включати такі типові роботи:

– інтерв'ювання персоналу замовника;
– аналіз поданих документів;
– приладові вимірювання;
– збір конфигурационной і операційної інформації;
– огляд обладнання.

План інтерв'ювання включається в ТЗ. Як додаток до ТЗ можуть виступати опитувальні листи, адаптовані під конкретного замовника. Зазвичай вони містять питання наступної тематики:

- вимоги, що пред'являються до мережі;
- порядок обслуговування мережі;
- активне мережеве обладнання;
- програмне забезпечення;
- кабельні системи;
- допоміжні і суміжні системи;
- умови встановлення та експлуатації обладнання.

Вся документація на ТІ, надана замовником, збирається для подальшого аналізу. Особлива увага звертається на журнали внесення змін до системи і журнали обслуговування заявок користувачів.

Етап аналізу даних і оформлення результатів зазвичай включає такі типові роботи:

- перевірка зібраних даних;
- аналіз структури ТИ;
- аналіз конфігураційних файлів;
- аналіз операційного стану ТИ;
- підготовка аналітичного звіту;
- підготовка експлуатаційної документації;
- презентація результатів.

Зібрані дані перевіряються на повноту (чи відображають вони ситуацію з ТИ повністю, чи всі елементи охоплені, чи всі зв'язки враховані), коректність (чи є суперечливі або свідомо невірні дані), достатність (чи приводить їх аналіз до досягнення цілей аудиту). При необхідності, збирається заново деяку інформацію або додаткова інформація.

На етапі представлення результатів аудиту мінімальний комплект експлуатаційної документації на корпоративну мережу зазвичай включає наступні документи:

– схему топології мережі;
– таблицю конфігурації мережевих пристроїв;
– таблицю конфігурації пристроїв, що підключаються до мережі.

Все що видають рекомендації, класифікується на невідкладні і довгострокові дії. Невідкладні дії слід реалізувати якомога швидше, це негайно дасть помітний результат: будуть усунені найбільш наявні проблеми, що супроводжують експлуатацію корпоративної мережі замовника. Методику класифікації рекомендацій ілюструє рис. 1.6. В результаті проведення аудиту виявляються розбіжності між потребами замовника і характеристиками використовується мережі. Рекомендації, включені до звіту, спрямовані на усунення цих розбіжностей. Реалізація всіх або частини рекомендацій може бути представлена як проект модернізації корпоративної мережі.

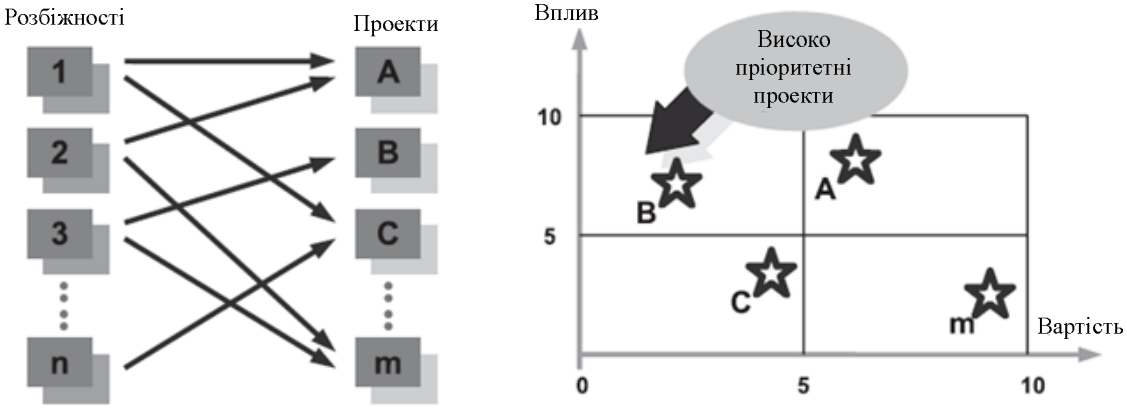


Рисунок 1.6 - Ухвалення рішення про модернізацію корпоративної мережі

На етапі аудиту оцінюється ступінь впливу на мережу тих чи інших рекомендацій, і, відповідно, ступінь відповідності мережі потребам замовника після їх виконання. Також вже на етапі аудиту може бути оцінена вартість реалізації проекту модернізації мережі і ризиків, пов'язаних з цим проектом. Модернізації, вплив яких на мережу істотно, а вартість впровадження мінімальна, і рекомендуються як невідкладні.

Заключні процедури аудиту.

За результатами аудиту розробляється звіт керівництву з областей, які потребують поліпшення, якщо такі є. Це включає зазначення недоліків і рекомендації щодо вдосконалення існуючих організаційних і технічних заходів (тобто рекомендації щодо усунення недоліків). Такі рекомендації повинні бути специфічними/конкретними та реалістичними/практичними, при цьому вартість розроблюваного рішення (час та гроші) не повинна перевищувати можливих наслідків реалізації зазначеного ризику. Відповідно, частину ризиків внаслідок незначності негативних наслідків їх реалізації можна прийняти. Однак у будь-якому випадку тільки керівництво організації може прийняти рішення про впровадження того чи іншого контролю або прийняття ризику.

План коригувальних заходів повинен включати вказівку осіб, відповідальних за реалізацію конкретної дії (впровадження конкретного контролю), а також пріоритет та реалістичні терміни для впровадження такого рішення.

В першу чергу рекомендується впроваджувати ті контролі, які не вимагають серйозних інвестицій та націлені на компенсацію критичних недоліків (наприклад, зміна налаштування системи може бути реалізована досить швидко та без серйозних інвестицій).

1.2 Принцип ризик-менеджмент в управлінні ризиками підприємства

У сучасних умовах господарювання ефективність функціонування всієї економічної системи та дії її суб'єктів не можуть бути повністю a priori визначені та розраховані, тобто діяльність кожного підприємства завжди пов'язана із ризиком та можливими втратами. У цьому разі виникає потреба в певному механізмі, який би дозволив найраціональнішим способом врахувати ризик та мінімізувати втрати. Таким механізмом є ризик-менеджмент (управління ризиком). Тому управління ризиком у системі ринкових відносин представляється об'єктивно необхідною задачею, вирішення якої вимагає нових підходів щодо вдосконалення теоретико-методологічних засад і розширення практики застосування.

В порівнянні з економічно розвиненими країнами Заходу в Україні поняття ризик-менеджмент адекватно сприймається не більше ніж 15% власників крупного і середнього бізнесу. Як правило, українські «топи» вважають, що всі проблеми в період кризи на їх підприємстві пов'язані лише із зовнішніми чинниками, а модель внутрішнього управління компанією є досконалною і управлінських помилок менеджмент не допускає в принципі. Попит на ризик-менеджмент сьогодні високий з боку компаній, що найдинамічніше розвивалися в до кризовий період. Хоча в міру поглиблення кризисних явищ все більша кількість власників середнього бізнесу розуміє необхідність повноцінного впровадження ризик-менеджменту на підконтрольних підприємствах.

1.2.1 Таксометрія поняття ризик-менеджмент

Наукова література по-різному тлумачить поняття управління ризиком, визначає його риси, властивості, елементи, функції та етапи. Неоднозначність

підходів пояснюється використанням різних методичних засад при вивченні цієї проблеми, оскільки управління ризиком - складне багатоаспектне і багаторівневе явище, яке характеризується складовими, що мають різноспрямований вплив на об'єкт управління.

Найбільш поширеним є визначення ризик-менеджменту як системи управління ризиком та економічними, точніше фінансовими відносинами, які виникають у процесі управління.

Управління ризиком - багатоетапний процес, мета якого зменшити чи компенсувати збитки для об'єкта при настанні несприятливих подій [8, с. 16]. Як вважає О. Л. Устенко, управління ризиком - це процес впливу на суб'єкт господарювання, при якому забезпечується максимально широкий діапазон охоплення можливих ризиків, їх обґрунтоване прийняття та зведення ступеня їх впливу до мінімальних меж, а також розробка стратегії поведінки даного суб'єкта в разі реалізації конкретних видів ризику.

З точки зору В. М. Гранатурова, управління ризиком можна охарактеризувати як сукупність методів, прийомів, заходів, що дозволяють певною мірою прогнозувати настання ризикованих подій і вживати заходів щодо виключення або зниження негативних наслідків їх настання [3, с. 7].

Штефанич Д. А. визначає управління підприємницьким ризиком як сукупність дій економічного, організаційного і технічного характеру, спрямованих на встановлення видів, факторів, джерел ризику, оцінку величини, розробку і реалізацію заходів щодо зменшення його рівня та запобігання можливих втрат [5].

Згідно зі стандартом AS/NZS Standard 4360:1999 процес ризик-менеджменту визначається як систематичне використання наявних у розпорядженні менеджерів методів, способів і прийомів для вирішення завдань, що стосуються ризиків: установлення контексту, аналізу (виявлення й оцінки), впливу, моніторингу і комунікації [10].

Узагальнюючи представлені точки зору провідних науковців щодо управління ризиками та враховуючи основні положення теорії управління, автори пропонують розглядати управління ризиком як процес впливу на об'єкт господарювання, при якому забезпечується охоплення максимально широкого діапазону можливих ризиків і використання всіх методів впливу на них в процесі прийняття управлінських рішень та зведення ступеню впливу виявлених ризиків до мінімальних або прийнятних меж. Результатом цих дій стає розроблення стратегії поведінки об'єкта управління в разі настання конкретних подій, які викликають дію різних видів ризику.

Таким чином, ризик-менеджмент - це сукупність принципів, методів і форм управління організацією та її поведінкою в зовнішньому середовищі в умовах невизначеності та конфліктності.

1.2.2 Завдання, мета та функції ризик-менеджменту

У рамках ризик-менеджменту вирішуються три основні завдання: профілактика виникнення ризиків; мінімізація збитку, спричиненого ризиками; максимізація додаткового прибутку, який отримує підприємство внаслідок управління ризиками.

Основна мета ризик-менеджменту - це зменшення або ліквідація можливих втрат від ризику, тому визначення принципів та функцій управління ризиком мають суттєве значення для застосування ризик-менеджменту на підприємстві. Ризик-менеджмент базується на таких основних принципах:

- принцип масштабності (максимізації);
- принцип мінімізації;
- принцип адекватної реакції;
- принцип розумного прийняття.

Ризик-менеджмент виконує функції, притаманні будь-якій управлінській діяльності, але при цьому специфіка їх виконання визначається об'єктом управління. Це функції прогнозування (планування), організації, контролю, регулювання, координації та мотивації.

Інтеграція ризик-менеджменту в загальний процес управління виражається, зокрема, в тому, що до управління ризиками залучаються практично всі підрозділи компанії: до ідентифікації і аналізу ризику представники функціональних підрозділів залучаються як експерти; вони ж займаються розробкою заходів щодо управління «своїми» ризиками і власне управлінням цими ризиками (тобто моніторингом їх рівня, реалізацією заходів щодо запобігання настанню і ліквідації наслідків ризикових подій). При цьому за службою ризик-менеджменту залишаються функції координації і контролю, а також консолідація і аналіз інформації про ризикові події і розробка необхідних дій. Фактично, контролюючи ризики, служба ризик-менеджменту контролює весь процес управління організацією в цілому, виконуючи, тим самим, функцію внутрішнього контролю. Враховуючи те, що контроль є одним із складових процесу управління, служба ризик-менеджменту спільно з іншими функціональними підрозділами здійснює процес управління організацією, керуючись при цьому критерієм «доходність/ризик».

Крім того, коли говорять про «інтегрований ризик-менеджмент», мають також на увазі доцільність централізованого управління всіма ризиками організації в силу:

1) взаємозв'язку ризиків;

2) необхідності контролю сумарного рівня ризику;

3) необхідності контролю сумарних витрат на управління ризиками.

Управління ризиком не зводиться виключно до дії на джерело ризику з метою зниження рівня можливих втрат. Управляти можна не лише внутрішніми,

але і зовнішніми ризиками. Типовими прикладами такого роду можуть служити: ухилення від ризику, страхування ризику, хеджування валютних ризиків і так далі. На рис. 1.7 наочно наведено логіку управління підприємницькими ризиками

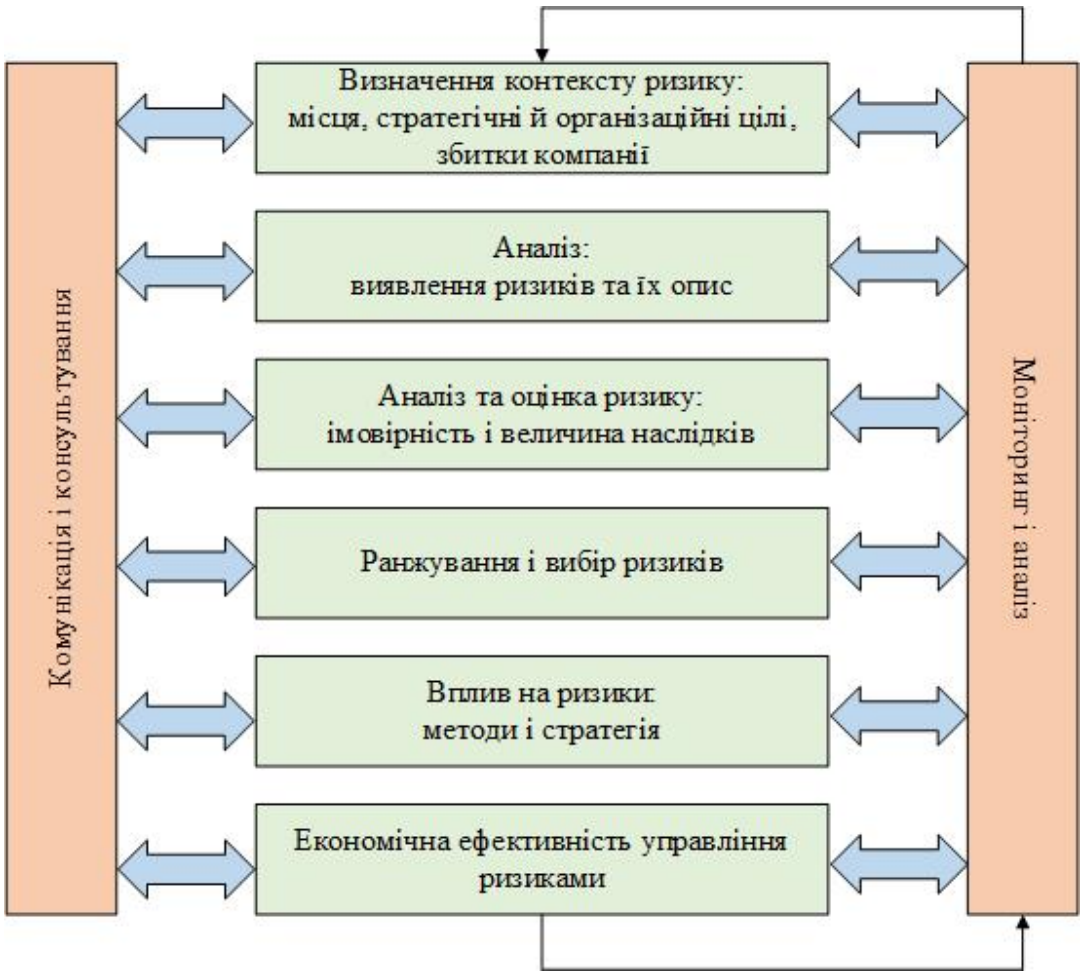


Рисунок 1.7 - Логіка управління підприємницькими ризиками

Ризик-менеджмент виконує певні функції. Розрізняють функцій ризик-менеджменту двох типів:

1) функції об'єкту управління;

2) функції суб'єкта управління.

До функцій об'єкту управління в ризик-менеджменті відноситься організація дозволу ризику; ризикових вкладень капіталу; роботи зі зниження величини ризику; процесу страхування ризику; економічних стосунків і зв'язків між суб'єктами господарського процесу.

До функцій суб'єкта управління в ризик-менеджменті відносяться: прогнозування; організація; регулювання; координація; стимулювання; контроль.

Прогнозування у ризик-менеджменті є розробкою на перспективу змін фінансового стану об'єкту в цілому і його підсистем. Прогнозування – це передбачення певної події. Воно не ставить своїм завданням безпосередньо здійснити на практиці розроблені прогнози. Особливістю прогнозування є також альтернативність в побудові фінансових показників і параметрів, що визначає різні варіанти розвитку фінансового стану об'єкту управління на основі тенденцій, що намітилися.

1.2.3 Етапи ризик-менеджменту компанії

На першому етапі ризик-менеджменту доцільною є оцінка господарської ситуації. Відбувається визначення цілі підприємницької діяльності в умовах ризику. Такі цілі повинні бути чіткими, конкретизованими та співставними з величиною ризику та капіталом.

На етапі діагностики проблеми збирають інформацію про структуру та властивості об'єкта, визначають стратегічні і тактичні цілі компанії, аналізують стан та перспективи розвитку зовнішнього середовища.

Визначення можливих факторів та чинників ризиків передбачає збір та обробку даних по всіх аспектах діяльності організації, відбувається оцінка ймовірності настання ризикових подій, визначення площин підвищеного ризику, визначення ступеня впливу ризику. Спочатку визначають найбільш імовірні та

небезпечні ризики, поступово переходячи до найменш імовірних, формуючи портфель ризиків. Виявлення ризиків може здійснюватися через застосування комплексу формальних і неформальних підходів, методів, заснованих на використанні суб'єктивної чи об'єктивної інформації. Наявної інформації має бути достатньо для прийняття адекватних рішень на наступних етапах ризик-менеджменту.

Аналіз ризику - один із найважливіших етапів управління ризиком, мета якого - одержання необхідної інформації щодо структури та властивостей об'єкта ризику та виявлення основних видів ризику, що впливають на цей об'єкт. Ризик доцільніше і вигідніше завчасно виявити, попередити або уникнути, ніж потім за допомогою управлінського впливу мінімізувати його наслідки.

Аналіз ризику складається із виявлення ризику та його оцінювання. При виявленні ризику (якісна складова) визначаються всі ризики, які впливають на дану систему. Головне - не пропустити важливі обставини і детально описати всі існуючі ризики. Виявлення ризику включає два етапи: збір інформації про структуру і властивості об'єкта та виявлення небезпек та інцидентів.

Якісний аналіз ризику.

На цьому етапі здійснюється експертне оцінювання рівнів виявлених ризиків шляхом оцінки вірогідності настання ризикових подій і величини можливих втрат. Основним результатом є список ризиків, з якого за принципом Паретто виділяються ризики, що підлягають подальшому аналізу і управлінню. Будується карта ризику – двовимірна матриця, в якій найважливіші ризики організації розміщуються відповідно до вірогідності виникнення і рівня збитку.

Кількісний аналіз ризику.

На цьому етапі будуються моделі кількісної оцінки рівнів рисок, що підлягають управлінню. У простому випадку рівень риски, що розуміється як математичне чекання (середнє значення) величини можливих втрат, визначається

як твір вірогідності настання ризикової події на відповідну величину втрат. В більшості випадків вживання такого універсального підходу не представляється можливим, і тому для оцінки конкретних видів рисок розробляються спеціальні моделі і показники їх оцінки (метод Монте-Карло, імітаційне моделювання, аналіз дерева рішень і т.д).

Оцінювання - кількісний опис виявлених ризиків, у процесі якого визначаються такі характеристики, як імовірність настання несприятливих подій та розмір можливих збитків [8]. Крім того, формується набір сценаріїв розвитку несприятливих подій і для різних ризиків можуть бути побудовані функції розподілу вірогідності понесення збитків.

Виявлення та оцінювання ризиків взаємно пов'язані між собою. Іноді аналіз йде у двох протилежних напрямах - від оцінки до виявлення і навпаки. У першому випадку вже є зафіксовані збитки, тому необхідно виявити причини їх настання. У другому випадку на основі аналізу системи виявляються можливі ризики і можливі наслідки їх дій. Другий варіант можна розглядати як упереджувальне управління ризиком. Застосування профілактичних заходів сприяє зниженню витрат на ризик-менеджмент.

У процесі оцінювання одне із найважливіших місць займає розробка системи показників оцінки рівня ризику. Ця система повинна відповідати наступним вимогам: будуватися на теорії імовірності, оскільки ризик - категорія імовірнісна; визначати різні за змістом та формою показники ризику, які б дозволяли найкращим чином врахувати всі можливі сценарії розвитку подій.

В залежності від обраного алгоритму дій, до схеми ризик-менеджменту можуть додатися етапи вибору методів управління ризиками (вибір конкретних методів управління, планів реагування на них; складання списку ризиків, що підлягають моніторингу; складання список вторинних ризиків; складання договорів на передачу ризику (аутсорсинг, страхування і так далі) та етап

моніторінгу та контролю. На останньому етапі проводиться періодичний аудит (оцінка ефективності) системи управління ризиками, також на періодичній основі складаються огляди ризиків організації, вносяться необхідні корективи в плани і процедури реагування на ризики.

Створення самостійного незалежного підрозділу, який ініціює, координує і контролює процес управління ризиками, прийнято називати «активним ризик-менеджментом». Як показує зарубіжна практика, саме цей підхід виявляється в більшості випадків оптимальним, причому, що важливо, у тому числі і за вартістю реалізації.

Так званий «пасивний ризик-менеджмент» передбачає залучення зовнішніх консультантів, які здійснюють необхідну роботу з ідентифікації і аналізу ризику, підбирають відповідні методи управління ключовими ризиками і диференційовано розподіляють їх по підрозділах компанії. При цьому всі необхідні рішення проводяться через керівні органи, але окремий підрозділ ризик-менеджменту не створюється. Недоліки цього підходу очевидні: після від'їзду консультантів система ризик-менеджменту перестає працювати.

Надзвичайно важливо також визначити місце, яке відводиться внутрішньому аудиту. У «COSO ERM Framework» міститься вказівка на незалежність ризик-менеджменту і внутрішнього аудиту:

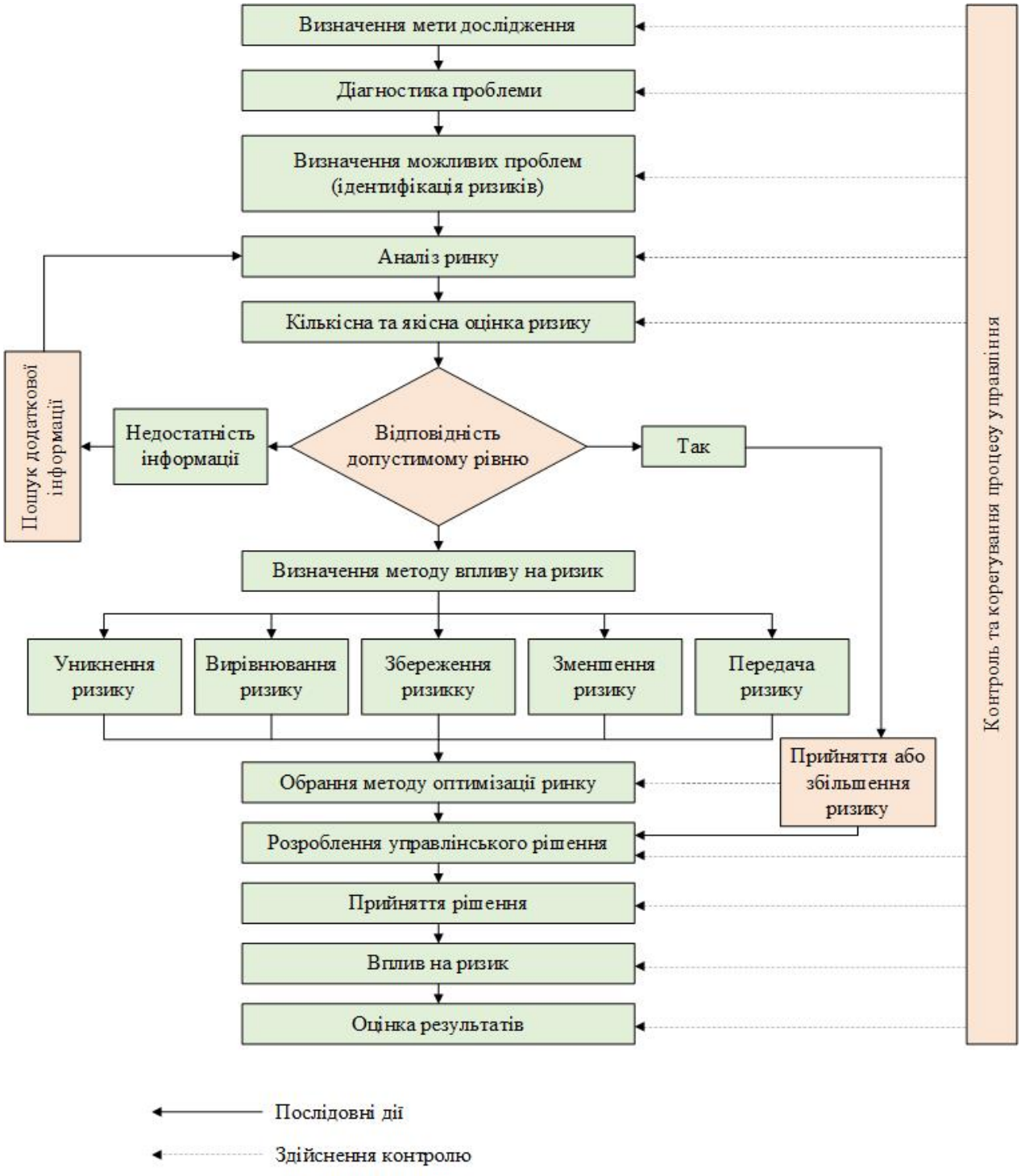


Рисунок 1.8 - Етапи реалізації процесу управління ризиком

«Внутрішні аудитори грають важливу роль в моніторингу системи управління ризиками (ERM), але не мають основного обов'язку реалізації і підтримки функціонування цієї системи». Основне завдання внутрішнього аудиту – оцінка ефективності системи управління ризиками і внутрішнього контролю і виробітку рекомендацій з оптимізації системи. Тоді як власником процесу і основним споживачем інформації ризик-менеджменту є виконавче керівництво компанії, внутрішній аудит – це незалежний від менеджменту інструмент ради директорів. Відповідно внутрішній аудит і ризик-менеджмент не рекомендується об'єднувати в одному підрозділі.

Відмінність ризик орієнтованого внутрішнього аудиту від традиційного:

Традиційний внутрішній аудит – це контроль по факту, тобто предметом його аналізу є ризикові події, що вже настали.

Ризик-орієнтований внутрішній аудит передбачає також і попереджувальний контроль, тобто виявлення потенційних проблемних ситуацій і розробку рекомендацій з їх недопущення.

1.2.4 Ключові показники, відповідальні за ризик

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 його детальніше.

1.2.5 Карта ризиків (ризик-профіль) та побудова радару загроз

Карта ризиків (risk tap) - 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 (рис. 1.9). Числа на поле карти ризиків відповідають порядковим номерам в реєстрі ризиків компанії.

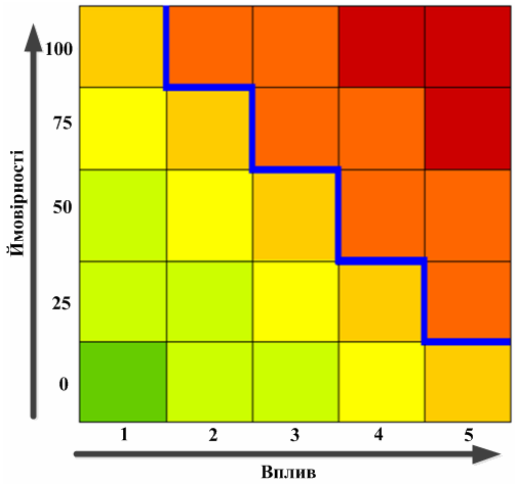


Рисунок 1.9 - Карта ризиків

Карта ризиків допомагає на єдиній основі виявляти схильності компанії до ризиків (risk appetites) на всіх напрямках її діяльності, визначити критично важливі ризики, пом'якшити їх і забезпечити управління ними; розробити динамічну фінансову модель компанії, яка включала б всі основні ризики, що впливають на розмір прибутку.

Існує два способи вимірювання ризиків: категорійний (описовий) і кількісний (ранжируваних). Перший має на увазі використання вербальних (словесних) вимірювачів типу «сильний» - «слабкий». В рамках категорійного підходу «ймовірність» описується так:

майже неможливо - може бути - ймовірно - майже напевно.

А «серйозність наслідків»:

незначна - помірна - значна - висока.

Кількісний підхід має на увазі використання умовних балів. Таким чином, ймовірність виникнення ризикової події і серйозність наслідків буде описуватися так:

1 бал - найнижча ймовірність виникнення / незначні наслідки;

5 балів - найвища ймовірність виникнення / найбільш руйнівні наслідки.

Як приклад розглянемо ризик-профіль компанії UGI (рис. 1.10).

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

Рисунок 1.10 - 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).

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 грунтуються 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.

Як показує практика професіоналів ризик-менеджменту, таких як Zurich International і Price Waterhouse Coopers, підхід «зверху вниз» є досить ефективним рішенням для складання карти ризиків. Наприклад, Zurich International - компанія з надання фінансових послуг - сповідує фірмову методологію «тотального ризик-про- филирования» (Total Risk Profiling), а Price Waterhouse Coopers, аудиторська компанія, використовує метод ORCA (Objectives, Risk, Control / Processes and Alignment, «Завдання, ризик, засоби контролю І процеси і регулювання»), засновані саме на підході «зверху вниз».

Для аналізу рівня внутрішніх і зовнішніх ризиків середнього / малого підприємства можна використовувати радар ризиків. Побудова радара складається з таких етапів.

1 етап. Визначення параметрів оцінки внутрішнього і зовнішнього ризиків для функціонування підприємства. Експертне виставляння ступеня вираження даних параметрів.

На першому етапі визначаються основні параметри, які є підставою оцінки внутрішнього і зовнішнього ризиків для функціонування підприємства. Шляхом опитування керівництва і співробітників підприємства визначаються ті чинники, які набирають в груповий оцінці найбільшу вагу (по частоті згадувань). Вони і розглядаються в якості параметрів внутрішніх і зовнішніх ризиків для функціонування підприємства.

2 етап. Складання таблиці експертних оцінок ризиків.

Далі всі отримані дані обробляються, з усіх аналізованих ризиків виділяються найбільш значущі по впливу на діяльність підприємства, останні зводяться в окремі таблиці, і розраховується середнє значення параметрів оцінки внутрішніх і зовнішніх ризиків функціонування підприємства.

3 етап. Побудова радара ризиків. Взявши середнє значення кожного параметра оцінки внутрішніх і зовнішніх ризиків функціонування підприємства, можна побудувати радар основних ризиків (рис. 4.9). Виходячи з споконвічно певною мірою вираження параметрів ризиків функціонування підприємства: (від 0 до 5 - небезпечна ризикова ситуація для підприємства; 5 - необхідно проявити обережність; від 5 до 10 - безпечна ситуація для діяльності підприємства), з побудованого радара одразу візуально видно, на що необхідно, в першу чергу, звернути увагу керівництву підприємства, щоб забезпечити його сталий і рентабельне функціонування. Для аналізу ризиків діяльності підприємства можна використовувати не тільки радар ризиків, а й так звану матрицю управління ризиками.

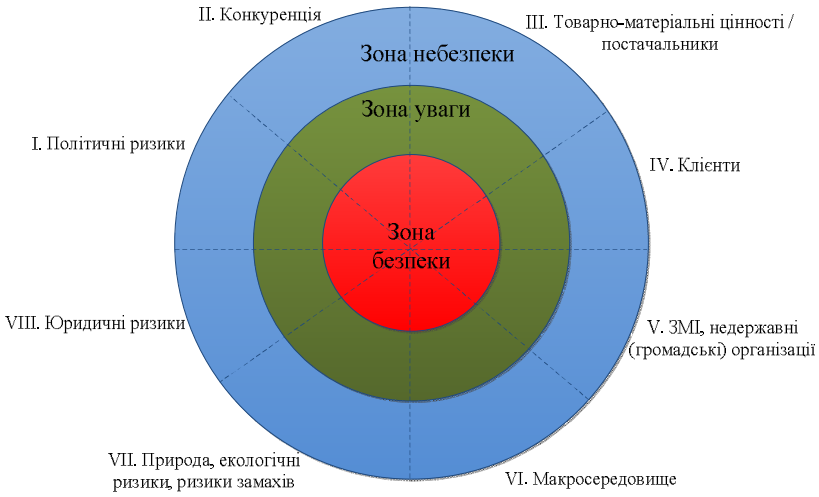


Рисунок 1.11 – Радар зовнішніх ризиків функціонування підприємства

1.2.6 Приклад впровадження ризик-менеджменту з побудовою радару загроз

Сучасне підприємство перебуває одночасно у різних “шарах” господарську діяльність. З погляду процесів – це маркетинг, продажі, виробництво, зберігання та логістичні питання, взаємодія з партнерами та клієнтами. З погляду структури – це робота з кадрами, контрагентами та партнерами, робота з інформацією, стан безпеки загалом у компанії, інформаційна інфраструктура тощо. Кількість складових залежить тільки від масштабів компанії, виду господарської діяльності, планів розвитку, навколишніх загроз та ризиків. Передбачається, що на базовому рівні, шаблонно, можна виділити 5 основних сегментів на підприємстві – кадри, робота з контрагентами, фізичний захист та технічні засоби охорони, IT-сегмент, документи та персональні дані.

На рис. представлений радар загроз, який є візуалізацією поточного стану безпеки підприємства. Приклад радара погроз показаний на рис. 1.12.

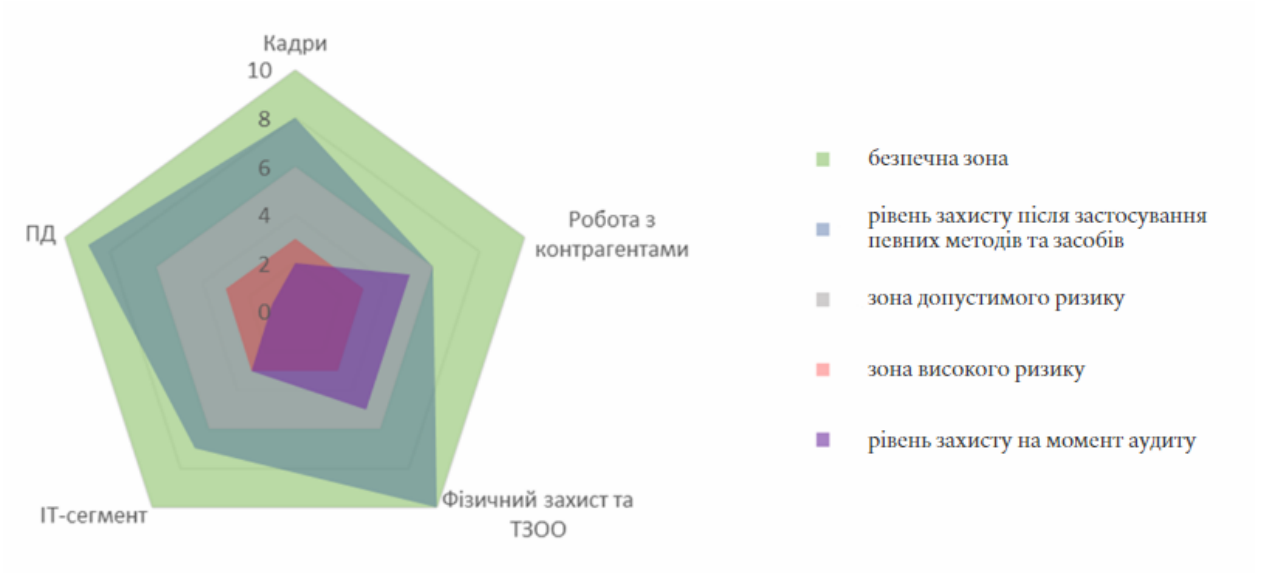


Рисунок 1.12 – Приклад радара загроз із зазначенням рівнів захисту

Щоб побудувати такий радар ризику та оцінити стан рівня безпеки підприємства, необхідно отримати відповіді на ряд питань.

По кожному з напрямків сформовано 10 питань, відповіді на які показують загальний стан напряму, при цьому мінімальний бал – 0, максимальний бал – 10. Відповідно, мінімальний бал – 0, максимальний бал – 10. Як видно з представленого на рис. , представлено наступне зонування:

– початковий рівень захисту (вихідні дані);

– поточний рівень захисту (результат роботи);

– зона високого ризику (показник ≤3);

– зона допустимого ризику (значення в діапазоні 3 – 7);

– безпечна зона (показник ≥7).

Далі алгоритм наступний:

1. Заповнюємо опитувальні листи за 5-ма напрямками, в результаті з'ясовуємо початковий рівень захисту.

2. Аналізуємо, у які зони ризику потрапляють наші результати – високого, допустимого ризику чи безпечну зону.

3. Напрямки, що потрапили в червоний сектор (зона високого ризику) за допомогою методів та засобів захисту виводимо, як мінімум, у зону допустимого ризику.

4. Оцінюємо ситуацію і досягаємо такого результату (застосовуючи оптимальні методи та засоби захисту), при якому показники представлених напрямків компанії з червоної зони в жовту та далі – в зелену зону. Оптимальний % жовтого сектора (зона допустимого ризику) – трохи більше 25%. Питання, на підставі яких визначається початковий рівень захисту підприємства, представлено в Додатку №Б.

В результаті анкетування отримуємо таблицю, приклад якої представлено нижче.

Таблиця 1.4 – Приклад анкетування для отримання радару загроз

	№ питання	7		№ питання	7		№ питання	7		№ питання	7		№ питання	7
КАДРИ	1	1	КОНТРАГЕНТИ	1	0	ФІЗИЧНИЙ ЗАХИСТ ТА ТЗОО	1	0	IT-ІНФРАСТРУКТУРА	1	1	ПЕРСОНАЛЬНІ ДАНІ	1	1
	2	1		2	0		2	0		2	1		2	1
	3	1		3	0		3	0		3	0		3	1
	4	0		4	1		4	1		4	0		4	0
	5	0		5	0		5	0		5	0		5	0,5
	6	1		6	0,5		6	0,5		6	1		6	0
	7	1		7	1		7	1		7	1		7	0
	8	0,75		8	0		8	0		8	1		8	1
	9	0		9	0		9	0		9	0		9	0
	10	0,5		10	0		10	0		10	1		10	1

Далі візуалізуємо інформацію та представляємо її у вигляді радару загроз. Результат представлено на рис.1.13.

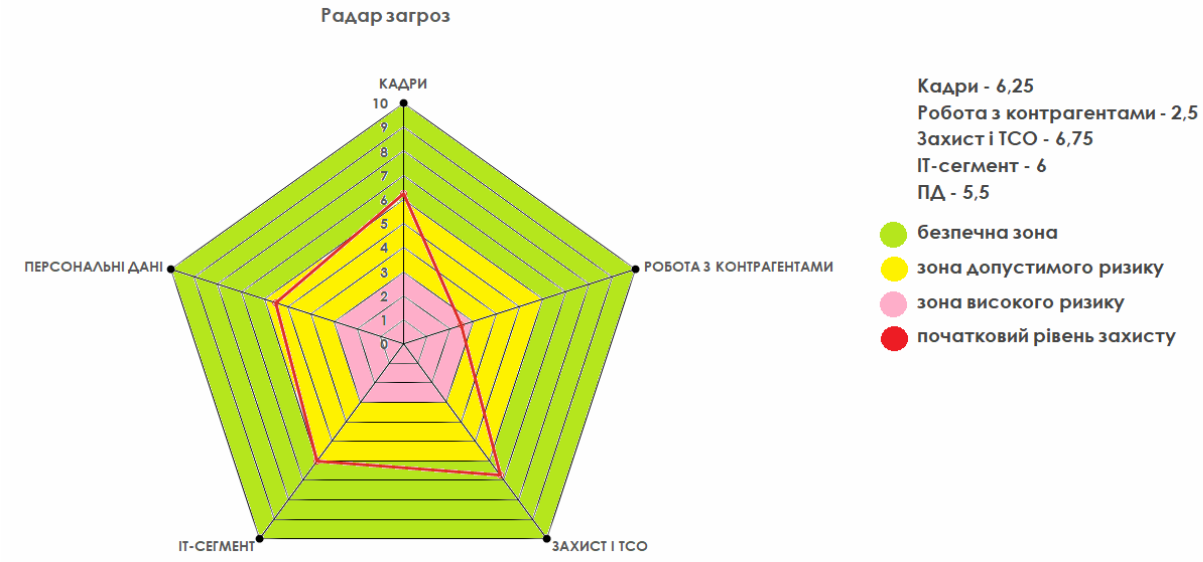


Рисунок 1.13 – Приклад радару загроз із зазначенням початкового рівня захисту компанії

Вибір оптимальних методів та засобів захисту ґрунтується на застосуванні шаблонів, представлених у Додатку Б ВКР. Будь-який метод чи засіб, який ми вибираємо, має певний бал, який змінює розміщення на радарі загроз. Приклади набору балів представлені нижче в тематичних таблицях.

В табл. 1.5 наведені методи і засоби захисту, які спрямовані на підвищення рівня захисту напряму Робота з контрагентами.

Таблиця 1.5 – Напрям Робота з контрагентами

Дія	Використання	Результат	Бал	Витрати
Перевірка контрагентів інструментами конкурентної розвідки	Перевірка контрагентів на надійність, чесність, добросовісність	Відсіювання недобросовісних контрагентів	0,35	2000
Контролювати такі моменти, як сімейність контрагентів, вплив родинних зв'язків на підприємство, лобіювання інтересів контрагентів, порушення договірних зобов'язань, шахрайство з документами	Боротьба з шахрайством	Виключення впливу родинних зв'язків, юридична відповідальність за лобіювання інтересів контрагентів та порушення договірних зобов'язань	1	0
Юридична відповідальність за факти крадіжок матеріально-товарних цінностей, шахрайство, роботу на користь контрагентів, отримання відкатів	Боротьба з шахрайством	Інформування кожного співробітника про юридичну відповідальність з подальшим звільнення	0,25	0
Офіційні договірні відносини	Боротьба з шахрайством	Юридична і економічна фіксація рахунків, договорів, контрактів	0,25	0
СБ підприємства підпорядковується власнику	Конфіденційність	Співробітники СБ напряму розмовляють з власником підприємства	0,25	0

Впроваджені дій дозволять ефективно боротися з шахрайством на підприємстві та підвищать загальний рівень захисту, але оскільки, підприємство «Голіаф» займається фінансовим кредитуванням напрям Робота з контрагентами не потребує високого рівня захисту.

В табл. 1.6 наведені методи і засоби захисту, які спрямовані на підвищення рівня захисту напряму Персональні дані.

Таблиця 1.6 – Напрям Персональні дані

Дія	Використання	Результат	Бал	Витрати
Навчання співробітників в сфері захисту КІ і ПД	Профілактичні підготовки співробітників	Покращення навиків роботи і захисту КІ і ПД	0,5	0
Впровадження положення про КТ	Конфіденційність	Підвищення рівня конфіденційності	0,5	1000
Облік осіб, допущених до роботи з ПД та КТ підприємства	Захист від несанкціонованого доступу	Невелика кількість перевірених людей з підвищеним рівнем доступу до інформації	0,25	5000
Використання шредерів	Знищення паперової документації	Використання шредерів для правильного знищення паперової документації	0,35	16000
Контроль знищення паперової документації	Контроль за знищенням паперової документації	Своєчасне знищення потрібних документів	0,25	3000
Контроль вхідної та вихідної документації	Контроль всієї документації	Контроль вхідної та вихідної документації	0,25	0
Впровадження регламенту захисту ПД GDRP	Несанкціонований доступ	Підвищення рівня захисту ПД	0,5	0

Впроваджені дії дозволять швидко и без особливих складнощів підняти рівень захисту напрямку Персональних даних. Персональні дані є важливим аспектом підприємства.

В табл. 1.7 наведені методи і засоби захисту, які спрямовані на підвищення рівня захисту напрямку ІТ.

Таблиця 1.7 – Напрям ІТ

Дія	Використання	Результат	Бал	Витрати
Поділ корпоративної мережі на гостьові та робочі сегменти	Розділення на робочу та громадську зону	Завдяки розділенню зон, підвищується рівень безпеки мережі	0,25	0
Періодичне резервування даних	Зберігання резервних копій даних	У випадку людської помилки, збою приладів, шкідливого ПЗ, хакерської атаки копії даних не постраждають і можуть бути відновленими.	0,25	1000
Використання антивірусних програм	Захист від шкідливого ПЗ	Дозволяє перевіряти файли на наявність шкідливого коду	0,25	1000
Навчання персоналу питань комп’ютерної грамотності	Профілактичні підготовки співробітників	Покращення навиків роботи і захисту інформації	0,25	0
Розташування сервера за межами підприємства	Стабільність	У випадку сбою роботи на підприємстві, роботу можна продовжити в іншому місці	0,25	4000
Застосування парольної політики	Підвищення захисту доступності	Базовий і обов’язковий спосіб підвищення захисту робочого ПК.	0,25	0
Захист від соціальної інженерії	Профілактичні підготовки співробітників	Інформування кожного співробітника про соціальну інженерію	0,25	0
Захист бездротових точок доступу	Захист від несанкціонованого доступу	Підвищення рівня захисту бездротових точок доступу	0,25	0
Використання шифрування	Підвищити рівень складності	Використовуючи це програмне забезпечення,	0,25	0

	отримання інформації	можна сховати від неавторизованих осіб будь-яку інформацію		

Напрям ІТ є важливим аспектом підприємства, тому за допомогою впровадженим діям можна вдосконалити и забезпечити стабільну роботу підприємства.

В табл. 1.8 наведені методи і засоби захисту, які спрямовані на підвищення рівня захисту напрямку Кадрів.

Таблиця 1.8 – Напрям Кадрів

Дія	Використання	Результат	Бал	Витрати
Застосування методів і засобів конкурентної розвідки	Перевірка кандидата на надійність, чесність, добросовісність	Відсіювання недобросовісних кандидатів	0,25	2000
Системне навчання персоналу підприємства з питань безпеки	Профілактичні підготовки співробітників	Покращення навиків роботи і захисту інформації	0,25	0
Офіційне працевлаштування	Боротьба з шахрайством	Юридична фіксація контрактів	0,25	0
Впровадження положення про комерційну таємницю	Конфіденційність	Підвищення рівня конфіденційності	0,25	1000
Надання старшим співробітникам статусу «матеріально-відповідних осіб»	Відповідальність за молодших співробітниках	«Старша» особа несе часткову відповідальність за дії молодших співробітників	0,25	2000

За допомогою обраних методів захисту можливо досить безболісно підвищити рівень безпеки напряму Кадрів.

В табл. 1.9 наведені методи і засоби захисту, які спрямовані на підвищення рівня захисту напрямку Фізичний захист і ТЗО.

Таблиця 1.9 – Напрям Захист і ТЗО

Дія	Використання	Результат	Бал	Витрати
Застосування якісних рішень для організації інженерно-технічного захисту підприємства	Стабільність	Використання продуманих і якісних технічних рішень може гарантувати стабільну роботу підприємства	0,25	0
Поділ трафіку систем відеоспостереження та корпоративної мережі передачі даних	Розподілення трафіку	Завдяки розділенню трафіка, підвищується рівень безпеки підприємства	0,4	5000
Заміна обладнання ТСО на більш технологічне і ефективне	Вдосконалення технічної апаратури	Нове обладнення підвищить рівень безпеки, а також може зробити деякі технічні питання більш ефективними і економічними	0,3	300 000
Залежно від специфіки об'єкта - застосування рубіжної політики безпеки	Підвищення захисту	Підвищення рівня безпеки навколо підприємства	0,35	50 000
Захищена прокладка комунікацій ТСО і мереж передачі даних	Підвищити рівень складності отримання інформації	Підвищення складності зовнішньої взаємодії з прокладеною комунікацію	0,35	25 000

Напрям Фізичний захист і ТЗО має досить високий бал захисту, щоб підтримувати цей рівень потрібно систематично обновлювати технічне обладнення та підвищити рівень складності взаємодії ззовні підприємства. После применения методов и средств защиты обновим радар для понимания текущей ситуации. Результаты представлены на рис.1.14.

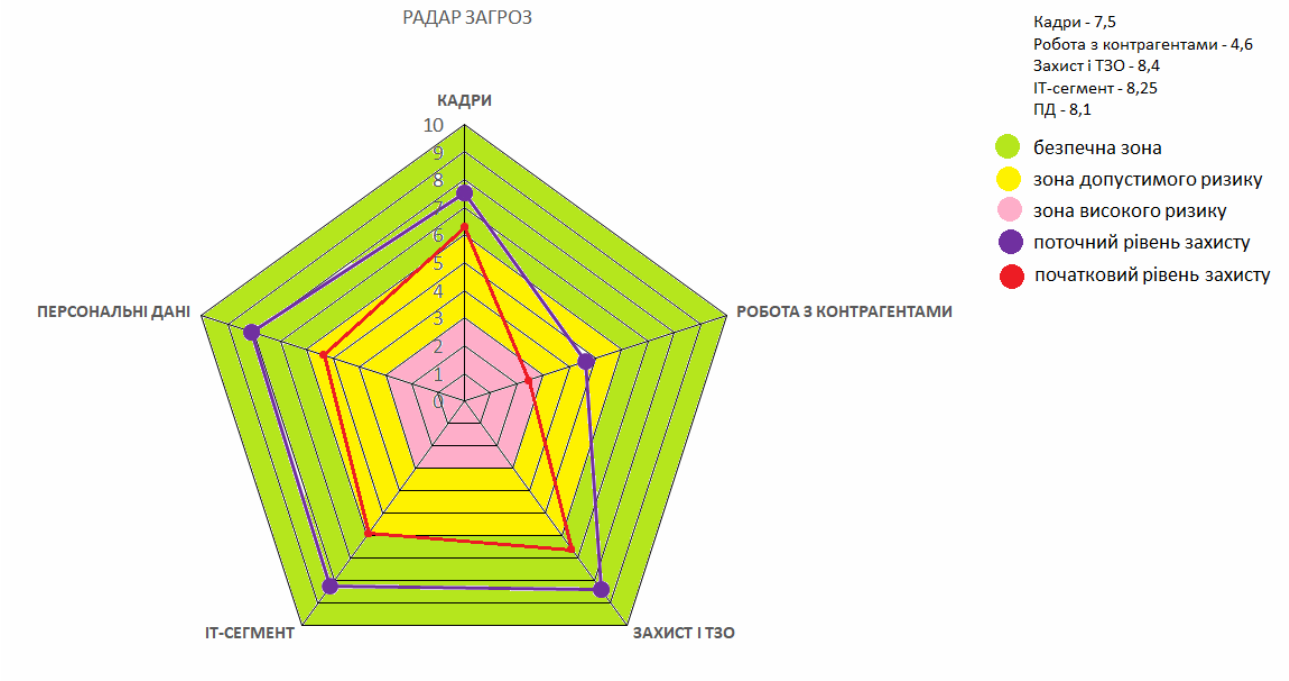


Рисунок 1.14 – Оновлений радар загроз

Впроваджені методи і засоби захисту інформації покращали кожний з основних напрямів підприємства. В табл. 1.10 показані нові значення радару загроз.

Таблиця 1.10 – Нові значення захисту

Напрям	Початкове значення	Поточне значення	Поточна зона
Кадри	6.25	7,5	Безпечна
Робота з контрагентами	2,5	4,6	Допустима
Захист і ТЗО	6,75	8,4	Безпечна
ІТ-сегмент	6	8,25	Безпечна
Персональні дані	5,5	8,1	Безпечна

Вибраний спосіб дозволяє оцінювати поточний рівень захисту підприємства, а набір методів та засобів захисту підвищувати рівень захисту підприємства.

Візуалізація через радар загроз дозволяє застосовувати даний у широкій сфері господарську діяльність непрофесіоналами у сфері безпеки, причому експрес-методом. Цей підхід може бути широко застосований власниками компаній, топ-менеджерами, підприємцями різних груп тощо.

2 ОХОРОНА ПРАЦІ

Охорона праці є важливою складовою процесу працевлаштування в будь-якій сфері діяльності, включаючи інформаційні технології. У програмістській галузі, де працівники проводять багато часу за комп'ютером, забезпечення безпечних умов праці відіграє важливу роль у збереженні здоров'я та підтриманні продуктивності. Цей розділ розгляне основні правові та законодавчі акти, що регулюють забезпечення безпечних умов праці для програмістів.

Аналіз небезпечних і шкідливих факторів, що впливають на програміста при розробці даного програмного комплексу.

Вплив ергономіки: Погано спроектоване робоче місце може призводити до напруги м'язів, зморшки, болю в спині, зниження зорової гостроти і змін в позі тіла. Для зменшення цього впливу важливо забезпечити комфортне робоче місце з належною посадкою, належно розташованою клавіатурою, монітором і мишею. Регулярні перерви для розтягування і вправ можуть допомогти зменшити навантаження на м'язи і очі.

Вплив випромінювання: При розробці програмного комплексу може бути використано різне обладнання, яке випромінює електромагнітні поля. Довготривалий вплив випромінювання може бути шкідливим для здоров'я, спричиняти головні

Гігієнічні вимоги до виробничого середовища.

Забезпечення безпечних умов праці для програмістів є важливим завданням, яке вимагає дотримання відповідних законодавчих вимог та обов'язків як з боку роботодавців, так і працівників. Належне виконання цих вимог сприяє збереженню здоров'я працівників, підвищенню продуктивності та створенню безпечного та комфортного робочого середовища.

Вимоги до приміщення.

Площа приміщення: Приміщення повинно мати достатню площу для розміщення робочого місця програміста. Загальна площа повинна враховувати необхідний простір для комп'ютера, столу, стільця та інших обладнань, що використовуються під час роботи.

Освітлення.

Освітлення: Приміщення має бути добре освітлене. Наявність природного світла є бажаною, але в разі його відсутності необхідно забезпечити належне штучне освітлення. Освітлення повинно бути рівномірним, без блисків та тіней, що можуть впливати на зорову активність програміста.

Шум.

Вплив шуму: Розробка програмного комплексу може супроводжуватися шумом від обладнання, вентиляційних систем і спілкування з колегами. Довготривалий вплив шуму може призвести до стресу, погіршення концентрації, погіршення слуху тощо. Рекомендується використовувати засоби індивідуального захисту, такі як навушники або ватні чепчики, для зменшення рівня шуму.

Вимоги до організації робочого місця працівника.

Організація робочого місця: розміщення монітора, клавіатури, миші та інших пристроїв з урахуванням ергономіки та забезпечення комфорту працівника.

Паузи та розумні перерви: рекомендації щодо регулярних перерв для відпочинку та фізичних вправ, які допомагають запобігти напругам м'язів і суглобів.

Захист від шкідливих впливів: використання спеціальних екранних фільтрів, захисту від електромагнітного випромінювання та інших небезпечних факторів

Згідно з законодавством, роботодавець зобов'язаний:

Забезпечити безпечні та здорові умови праці для програмістів, уключаючи відповідне обладнання та інструменти, необхідні для виконання роботи.

Проводити навчання та інструктажі з охорони праці для нових працівників та організовувати періодичне навчання для всього персоналу.

Забезпечити наявність необхідних засобів індивідуального захисту, таких як окуляри, клавіатурні підставки, планшети для роботи з графічними планшетами тощо.

Регулярно проводити технічний огляд обладнання та інструментів для виявлення можливих недоліків чи потенційно небезпечних ситуацій.

Захист від шкідливих впливів: використання спеціальних екранних фільтрів, захисту від електромагнітного випромінювання та інших небезпечних факторів

Створити процедури для повідомлення про небезпечні ситуації, включаючи механізми подання скарг та повідомлень про проблеми з охороною праці.

Мікроклімат.

Температура повітря: Згідно з нормами, оптимальна температура для офісних приміщень знаходиться в діапазоні 20-24°C. Програмістам слід забезпечувати комфортну температуру, яка не спричиняє перегрівання або охолодження організму.

Вологість повітря: Вологість повітря також має важливе значення для комфорту та здоров'я. Рекомендований рівень вологості знаходиться в діапазоні 40-60%. Висока вологість може спричиняти дискомфорт і сприяти розвитку плісняви та інших проблем з повітряними шляхами. Низька вологість може впливати на шкіру, слизові оболонки та стан дихальної системи.

Швидкість руху повітря: Швидкість руху повітря повинна бути такою, щоб не викликати дратівливість, віяння або холод. Рекомендоване значення швидкості руху повітря становить 0,1-0,25 м/с.

Очищення повітря: Програмістам рекомендується забезпечувати наявність ефективних систем очищення повітря, особливо в разі роботи в закритих

приміщеннях з обмеженим доступом до свіжого повітря. Це може включати використання фільтрів повітря та систем вентиляції з позитивним тисненням.

Вентиляція: забезпечення достатнього притоку свіжого повітря та видалення небезпечних речовин, що можуть утворюватися при роботі з комп'ютером.

Електробезпека.

Встановлення безпечних електричних систем: Робоче місце програміста повинно мати належно встановлену та заземлену електричну систему. Електропроводка повинна відповідати електробезпечним стандартам та нормам.

Заземлення та ізоляція: Усе електричне обладнання повинно бути належно заземлене, щоб уникнути можливості ураження електричним струмом. Крім того, повинна бути забезпечена належна ізоляція електропроводів та обладнання.

Безпека при роботі з електрообладнанням: Програміст повинен отримати необхідне навчання та інструктаж щодо безпечної роботи з електрообладнанням. Це включає правила вимикання та увімкнення обладнання, уникання перевантаження електричних мереж та правила безпеки при використанні кабелів, розеток та інших електричних пристроїв.

Перевірка та обслуговування: Електрообладнання повинно періодично перевірятися на відповідність стандартам безпеки. Регулярне технічне обслуговування та перевірка електричного обладнання зменшує ризик виникнення небезпечних ситуацій.

Пожежна безпека.

Пожежна сигналізація та системи пожежогасіння: Приміщення, де працює програміст, повинно бути обладнане пожежною сигналізацією та системами пожежогасіння. Це можуть бути пожежні тривожні пристрої, пожежні датчики, вогнегасники та інші пристрої для виявлення та припинення пожежі.

Евакуаційні шляхи та плани: Приміщення повинно мати належно обозначені та вільні евакуаційні шляхи. Плани евакуації повинні бути розроблені та вивчені

всіма працівниками. Також слід проводити регулярні практичні тренування евакуації.

Вогнезахисне обладнання та матеріали: Програмістам слід уникати використання вогненебезпечних матеріалів у своїй роботі. Кабелі, розетки та інше електрообладнання повинні бути відповідно сертифіковані та відповідати пожежно-безпечним вимогам.

Зберігання та утилізація матеріалів: Програмісти повинні зберігати легкозаймисті матеріали, такі як папір, відходи або лакофарбові речовини, у безпечних контейнерах та місцях для зберігання. Утилізація відходів повинна проводитися відповідно до встановлених правил та норм.

ВИСНОВОК

Аудит ІБ сьогодні – це найбільш ефективний інструмент для розуміння поточного рівня захищеності підприємства. У поєднанні з ризик-менеджментом аудит стає замкнутим циклічним процесом, де за циклом безперервного вдосконалення йде визначення поточного стану безпеки на підприємстві, аналіз та ранжування ризиків, картографування, побудова радара загроз. Все це дає можливість виділити збалансований бюджет та обрати оптимальні методи та засоби захисту:

1. Розглянуто ключові аспекти управління та природу внутрішніх та зовнішніх ризиків компанії.

2. Проаналізовано роль аудиту в діяльності компанії – визначення, цілі, види тощо.

3. Розглянуто проведення інвентаризацію ІТ-ресурсів компанії.

4. Показано структуру аудиту в фокусі принципу неперервності бізнесу.

5. В рамках вивчення ризик-менеджменту показано завдання, мету, функції та основні етапи.

6. Представлено карту ризиків та на її основі побудовано радар загроз підприємства в аспекті 5-ти базових напрямів.

ПЕРЕЛІК ПОСИЛАНЬ

1. Клочков М. Аудит сетевой и телекоммуникационной инфраструктуры // Jet Info. - 2005. - №4.

2. Инвентаризация IT - ресурсов как шаг к информационной безопасности предприятий. // Защита информации. INSIDE. – 2015. – №2. – С. 73–75.

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

4. Петренко С.А., Беляев А.В. Программа BCM: уроки выживания компании. // Защита Информации. Inside. – 2007. – № 4. – С. 38–34.

5. Стайкуца С.В., Аверьянов В.А. Анализ IT-инфраструктуры современного предприятия с позиции "жизненного" цикла // 71-ша науково-технічна конференція професорсько-викладацького складу, науковців, аспірантів та студентів. - Одесса: ОНАС им. А.С. Попова, 2016.

6. Стайкуца С. В. Аналіз основних ризиків IT-інфраструктури підприємства / С. В. Стайкуца, В.Й. Кільдішев, В.Г. Дергач // Сборник тезисов третьей всеукраинской научно-практической конференции "Перспективные направления защиты информации", ОНАС им. А.С.Попова. – 2017. – С. 76–79.

7. 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.

8. Гаджиєв М.М. Робота з ризиками як метод підвищення рівня безпеки сучасного підприємства / М.М. Гаджиєв, С. В. Стайкуца, О.П.Мельник,

М.М.Горпиненко // Матеріали 73-ї науково-технічної конференції професорсько-викладацького складу, науковців та студентів ОНАЗ ім. О.С. Попова. – 2018

9. Рой Я. В. Аудит інформаційної безпеки - основа ефективного захисту інформації / Я. В. Рой, Н. П. Мазур, П. М. Складанний. // Кібербезпека: освіта, наука, техніка. – 2018. – №1. – С. 86–93.

10. Аудит информационной безопасности [Електронний ресурс] // Корпоративний сайт Amika. – 2021. – Режим доступу до ресурсу: https://amica.ua/ru/information-security-audit/.

11. Стайкуца С.В., Методичні вказівки до виконання курсового проекту з дисципліни «Сучасна теорія та техніка ІБ» / Стайкуца С. - Одеса: ДУІТЗ, 2021. – 16 с.

12. Савчук В. Основы риск-менеджмента предприятий / Володимир Савчук., 2019. – 280 с.

13. Мостенська, Т. Л. Ризик-менеджмент як інструмент управління господарським ризиком підприємства / Т. Л. Мостенська, Н. С. Скопенко // Вісник Запорізького національного університету. Економічні науки. — 2010. — № 3. – С. 72–79.

14. Головач Т. В., Грушевицька А. Б., Швид В. В.: Ризик-менеджмент: зміст і організація на підприємстві. Вісник Хмельницького національного університету, 2009, 3: 157-163.

15. Морозов Д. ИТ-инфраструктура современных компаний: общие тенденции / Дмитрий Морозов. // Intelligent Enterprise/Корпоративные системы. – 2013.

16. Жизненный цикл системы. Информационно-аналитические системы и сети. Ч. 1: Информационно-аналитические системы /О.И. Алдохина, О.Г. Басалаева; Кемерово: КемГУКИ, 2010. – 148 с.

17. Клочков М. Аудит сетевой и телекоммуникационной инфраструктуры // Jet Info. - 2005. - №4.

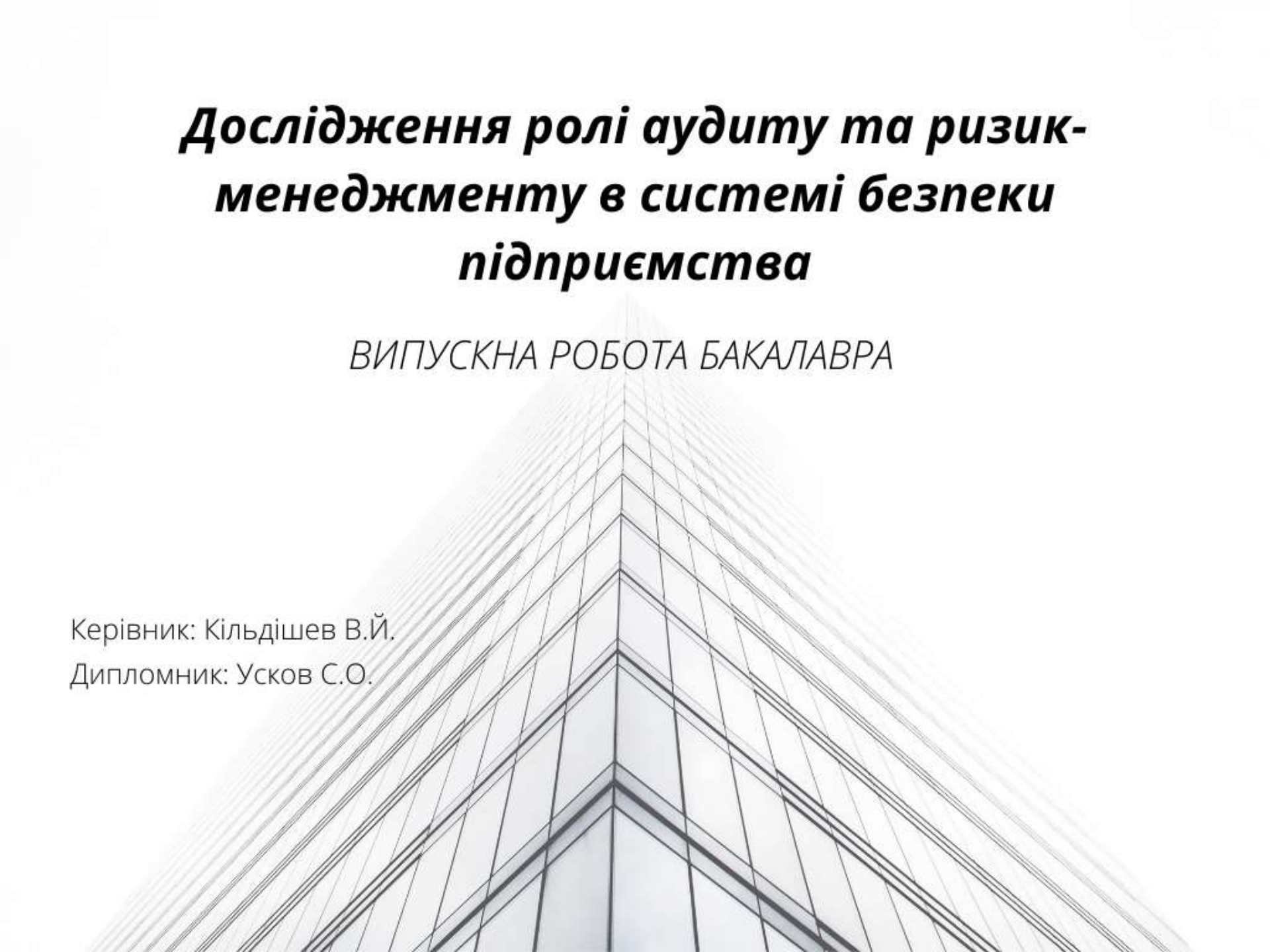
18. Инвентаризация IT - ресурсов как шаг к информационной безопасности предприятий. // Защита информации. INSIDE. – 2015. – №2. – С. 73–75.

19. Рекомендация МСЭ-Т X.1205. Безопасность электросвязи. Обзор кибер без опасности. - Женева, 2009. - 66 стор.

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

Дослідження ролі аудиту та ризик-менеджменту в системі безпеки підприємства

ВИПУСКНА РОБОТА БАКАЛАВРА



Керівник: Кільдішев В.Й.

Дипломник: Усков С.О.

Ризик (risk)

потенційна небезпека заподіяння шкоди підприємству в результаті реалізації певної загрози його стабільної діяльності з використанням вразливостей активу або групи активів даного підприємства

Кількісна класифікація ризиків

Базова класифікація ризиків підприємства

Аудит

Процес збору та аналізу інформації для якісної або кількісної оцінки рівня стану

- Підтоговка ТЗ на проектування
- Розробка та впровадження системи захисту
- Впорядкування існуючих заходів захисту інформації
- Приведення діючої системи безпеки у відповідність вимогам українського або міжнародного законодавства,
- Розслідування інциденту

Аудит ІБ організації

Систематичний, незалежний та документований процес отримання свідоцтв діяльності організації щодо забезпечення інформаційної безпеки та встановлення ступеня виконання в організації критеріїв інформаційної безпеки

Цілі аудиту ІБ організації:

01

Аналіз можливостей

Аналіз можливості здійснення загроз безпеці по відношенню до інформаційних систем

02

Визначення рівня захищеності ІБ

Визначення рівня захищеності ІБ та виявлення слабких місць у системі захисту

03

Формування рекомендацій

Формування рекомендацій щодо підвищення ефективності механізмів безпеки ІБ

04

Оцінка

Оцінка повноти виконання законодавчих вимог, стандартів, нормативних документів

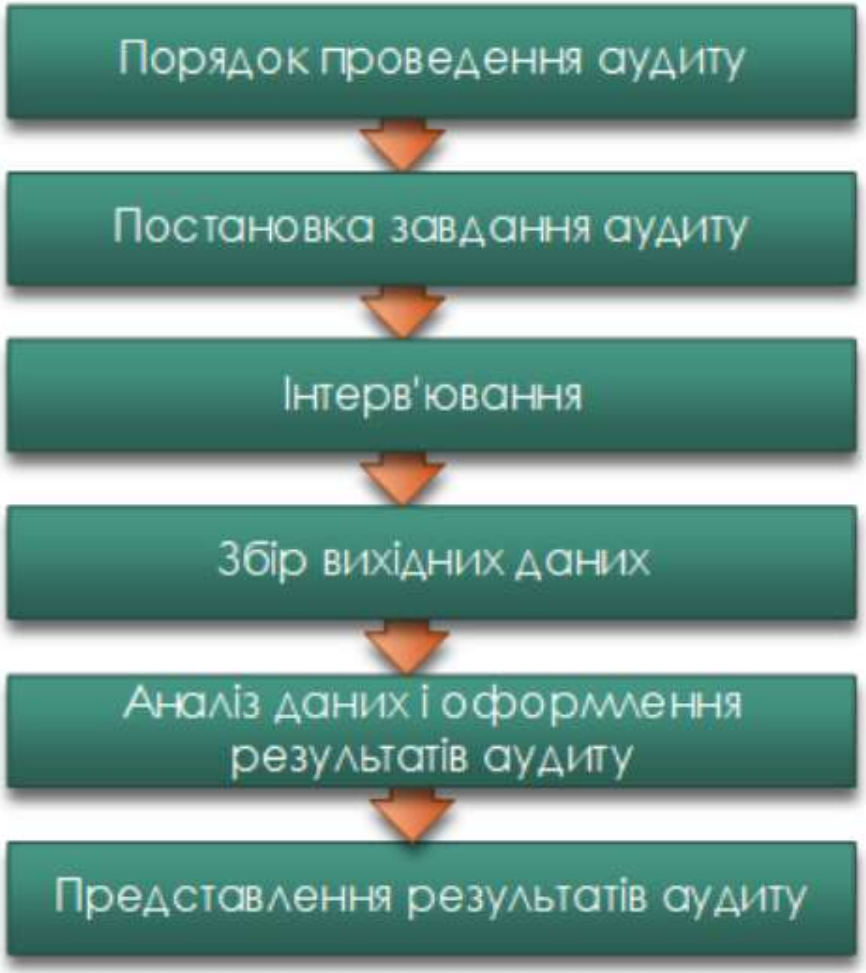
Способи проведення аудиту

Аудит власними силами:

Плюси	Мінуси
1. Ясне розуміння процесів, що відбуваються, і специфіки ІС 2. Відомості про систему та підсумки аудиту не залишають компанію 3. Відсутні фінансові витрати	1. Відсутність кваліфікованого персоналу та обширного досвіду в аудиті 2. Нестача часу у співробітників 3. Суб'єктивність оцінки

Аудит зовнішніми силами:

Плюси	Мінуси
1. Незалежна оцінка 2. Наявність великого досвіду у сфері аудиту 3. Високий рівень експертизи	1. Відомості про систему та підсумки аудиту знаходяться у підрядника 2. Складність вибору підрядника 3. Висока вартість роботи



Етап аналізу даних та оформлення результатів:

–перевірка зібраних даних;
–аналіз структури ТИ;
–аналіз конфігураційних файлів;
–аналіз операційного стану;
–підготовка аналітичного звіту;
–підготовка експлуатаційної документації;
–презентація результатів.

Перелік відомостей, потрібних для проведення аудиту

Перелік вихідних даних, необхідних для аудиту безпеки

Тип інформації	Склад вихідних даних
Організаційно-розпорядча документація з питань інформаційної безпеки	• Політика інформаційної безпеки ІС; • Керівні документи (накази, розпорядження, інструкції) з питань зберігання, порядку доступу і передачі інформації; • Регламенти роботи користувачів з інформаційними ресурсами ІС
Інформація про апаратне забезпечення хостів	• Перелік серверів, робочих станцій і комунікаційного устаткування, встановленого в ІС; • Апаратні конфігурації серверів і робочих станцій; • Відомості по периферійному обладнанню
Інформація про загальносистемне ПЗ	• Відомості про ОС, встановлену на робочих станціях і серверах; • Відомості про СУБД, встановлену в ІС
Інформація про прикладне ПЗ	• Перелік прикладного ПЗ загального і спеціального призначення, встановленого в ІС; • Опис функціональних завдань, що вирішуються за допомогою прикладного ПЗ
Інформація про засоби захисту, що встановлені в ІС	• Виробник засобів захисту; • Конфігураційні налаштування засобів захисту; • Схема встановлення засобів захисту
Інформація про топологію ІС	• Карта локальної обчислювальної мережі, включаючи схему розподілу серверів і робочих станцій за сегментами мережі; • Типи каналів зв'язку, що використовується в ІС • Використовувані в ІС мережеві протоколи; • Схема інформаційних потоків ІС

Складові частини IT-аудиту

Проведення інвентаризації

***Інвентаризація**, як рішення для збільшення "життєвого" циклу IT-інфраструктури, дозволяє виявити програмне забезпечення з вичерпаним терміном підтримки, морально-застаріле обладнання, несанкціоновані програмні і апаратні засоби*

- оперативність реагування на поточні події
- ефективне управляти апаратними та програмними ресурсами, які є на балансі
- можливість виявлення виходу з ладу або розкрадання врахованого обладнання
- виявлення стороннього (шкідливого) обладнання

Проведення інвентаризації

Скрипти зі збору інформації

Стікери з матричним кодом, QR-кодом

АПК інвентарізації

Інструменти проведення інвентаризації IT-інфраструктури

Alloy Discovery

- Збір докладної інформації про комп'ютери та пристрої в мережі.
- Аудит віддалених мереж і сайтів.
- Аудит які не підключені до мережі комп'ютерів за допомогою знімних носіїв.
- Аудит віддалених серверів і комп'ютерів під управлінням Linux і травні.
- Аналіз зібраної інформації
- Плановий аудит з застосуванням різних налаштувань і декількох розкладів.
- Інвентаризація програмного забезпечення.

Altiris Client Management Suite

- Управління життєвим циклом комп'ютерів в різнорідних середовищах.
- Точна ідентифікація та інвентаризація авторизованих і неавторизованих пристроїв.
- Комплексне управління програмним забезпеченням.
- Позасмугове управління.
- Віддалений контроль.
- Автоматизація IT-процесів,
- Адаптація нових технологій.

Програмні рішення для проведення інвентаризації та їх основні функції

Ризик-менеджмент (risk management)

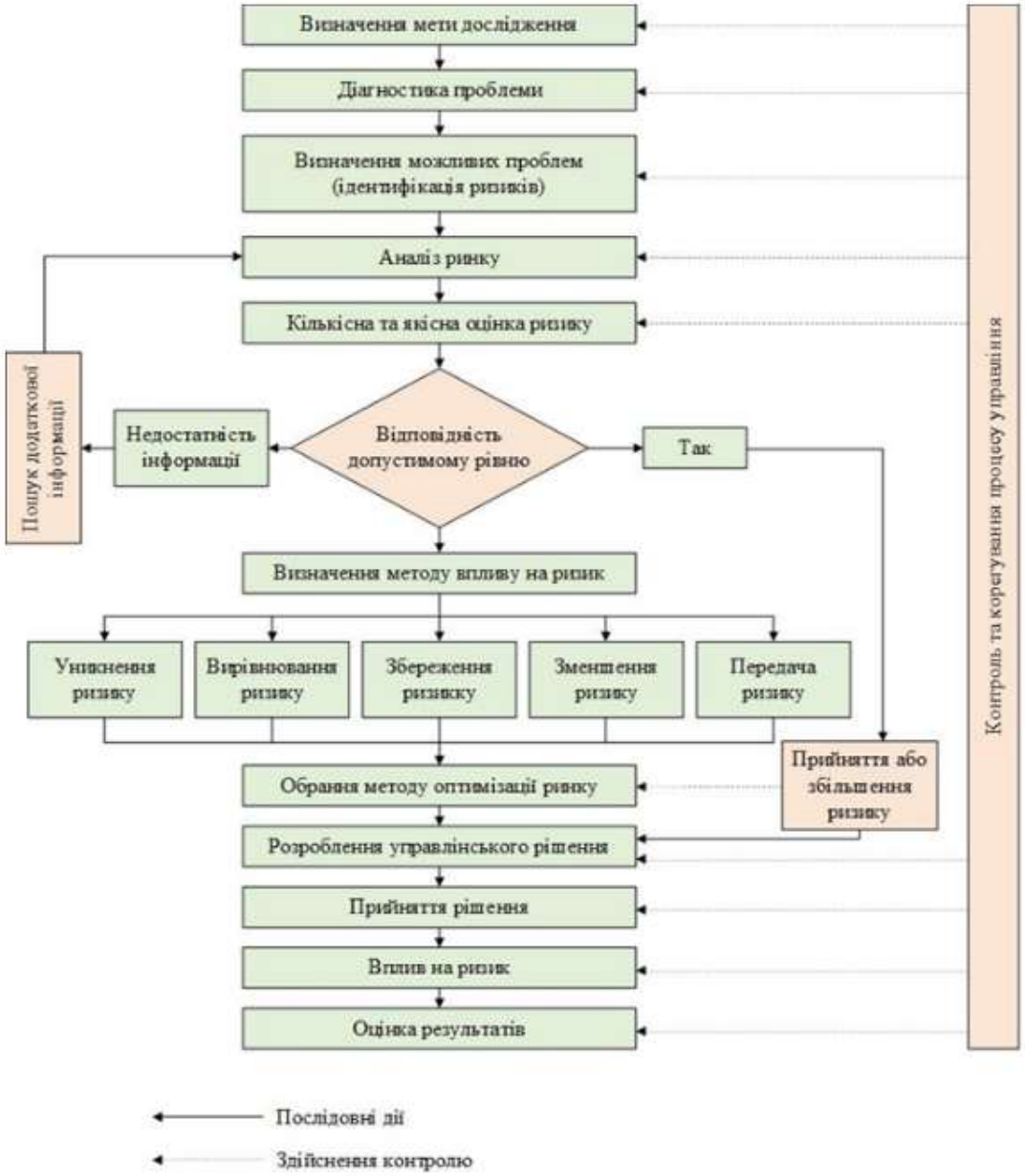
система управління ризиком, що передбачає повний процес ідентифікації, контролю, усунення або зменшення наслідків небезпечних подій, які можуть мати негативний вплив на стабільне функціонування підприємства

Основна мета ризик-менеджменту

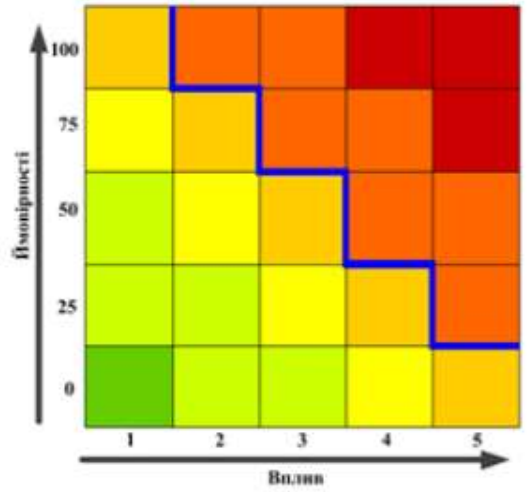
це зменшення або ліквідація можливих втрат від ризику, тому визначення принципів та функцій управління ризиком мають суттєве значення для застосування ризик-менеджменту на підприємстві

Основні принципи та функції ризик-менеджменту

Етапи реалізації процесу управління ризиком



Карта ризиків

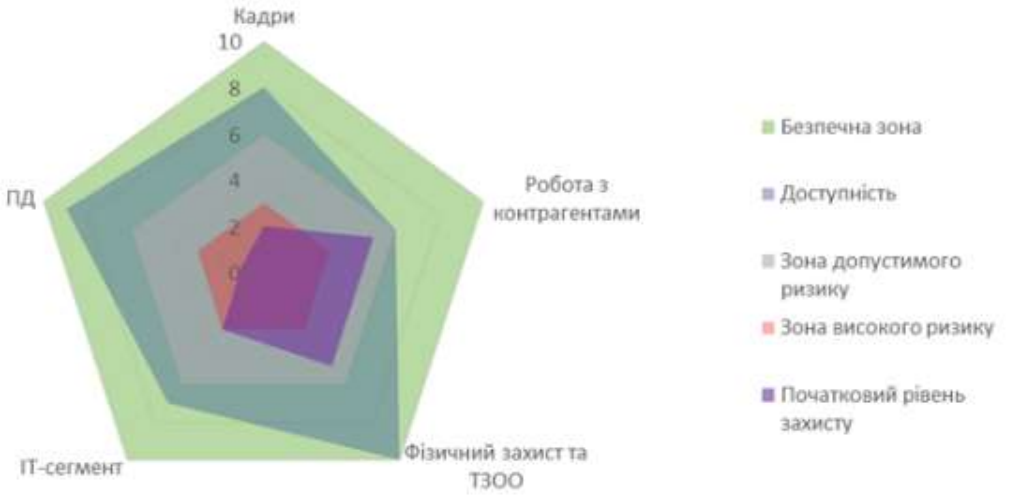


Координати карти ризиків:
Вплив (значимість, втрати) - ймовірність.
Для впливу (значимості, втрати):
1 - незначний ризик;
2 - допустимий ризик;
3 - підвищений ризик;
4 - критичний ризик;
5 - катастрофічний ризик.
Для ймовірності (частоти реалізації):
0 - ризик напевно не реалізується;
25 - ризик, швидше 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 шести категоріям ймовірності
Жирна ламана лінія - критична межа терпимості до ризику

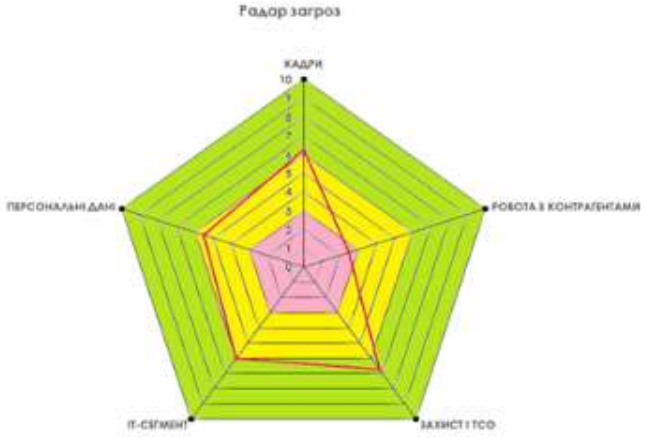
Анкетування та побудова радару загроз

Кадри
Робота з контрагентами
Фізичний захист та ТЗО
IT-сегмент
Документи та ПД



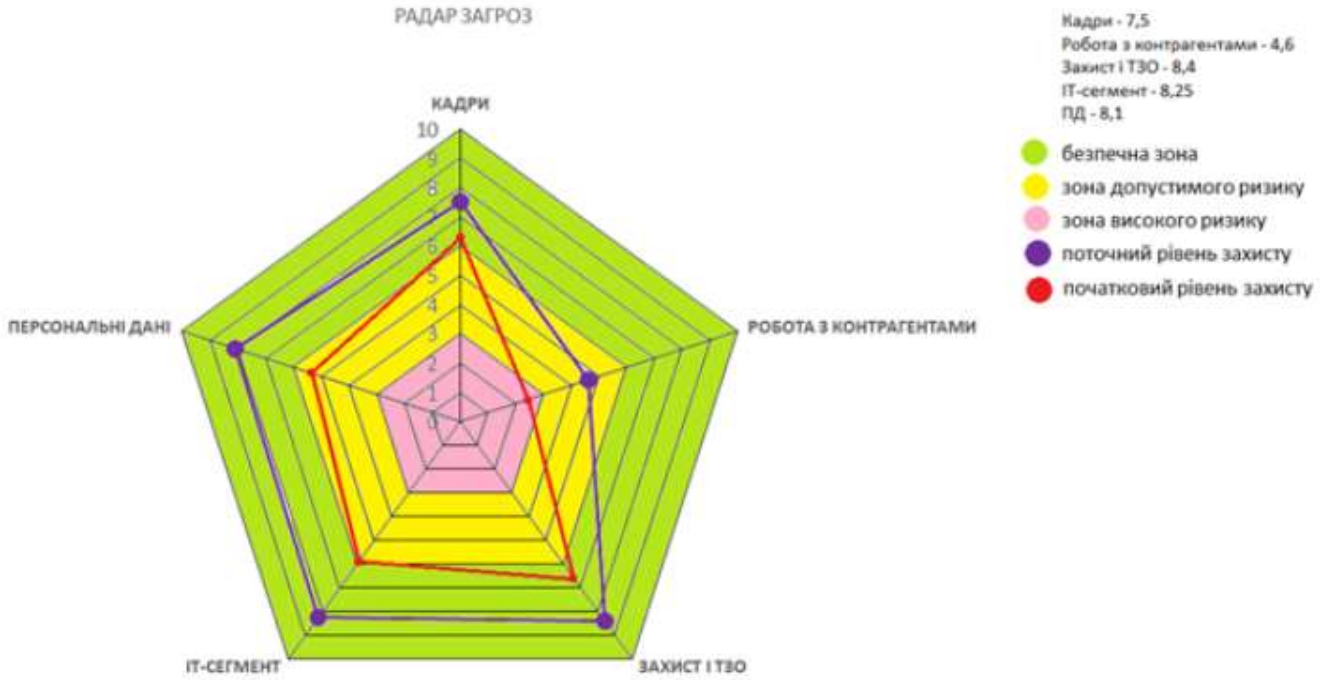
Таблиця з результатами анкетування

	№ питання	7		№ питання	7		№ питання	7		№ питання	7		№ питання	7
КАДРИ	1	1	КОНТРАГЕНТИ	1	0	ФІЗИЧНИЙ ЗАХИСТ ТА ТЗОО	1	0	IT-ІНФРАСТРУКТУРА	1	1	ПЕРСОНАЛЬНІ ДАНІ	1	1
	2	1		2	0		2	0		2	1		2	1
	3	1		3	0		3	0		3	0		3	1
	4	0		4	1		4	1		4	0		4	0
	5	0		5	0		5	0		5	0		5	0,5
	6	1		6	0,5		6	0,5		6	1		6	0
	7	1		7	1		7	1		7	1		7	0
	8	0,75		8	0		8	0		8	1		8	1
	9	0		9	0		9	0		9	0		9	0
	10	0,5		10	0		10	0		10	1		10	1



Візуалізація у вигляді радару загроз

Порівняння показників до та після застосування механізмів захисту



Напрям	Початкове значення	Поточне значення	Поточна зона
Кадри	6,25	7,50	Безпечна
Робота з контрагентами	2,50	4,60	Допустима
Захист і ТЗО	6,75	8,40	Безпечна
IT-сегмент	6,00	8,25	Безпечна
Персональні дані	5,50	8,10	Безпечна

Порівняння показників до та після застосування механізмів захисту

ДЯКУЮ ЗА УВАГУ!

UNICHECK

Ім'я користувача:
Наталія Вікторівна Копусь

ID перевірки:
1015516686

Дата перевірки:
08.06.2023 22:10:46 EEST

Тип перевірки:
Doc vs Internet + Library

Дата звіту:
08.06.2023 22:15:28 EEST

ID користувача:
100011688

Назва документа: 2БКС-27_Сергій_Усков

Кількість сторінок: 51 Кількість слів: 8569 Кількість символів: 68223 Розмір файлу: 1.24 MB ID файлу: 1015171321

Виявлено модифікації тексту (можуть впливати на відсоток схожості)

46.5%
Схожість

Найбільша схожість: 17.8% з Інтернет-джерелом (https://elibrary.kubg.edu.ua/id/eprint/25663/1/%D0%AF_%D0%A0%D0..

46.5% Джерела з Інтернету | 736 ..... Сторінка 53

Не знайдено джерел з Бібліотеки

0% Цитат

Вилучення цитат вимкнене

Вилучення списку бібліографічних посилань вимкнене

0%
Вилучень

Немає вилучених джерел

Модифікації

Виявлено модифікації тексту. Детальна інформація доступна в онлайн-звіті.

Замінені символи | 6

Підозріле форматування | 8 сторінок

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

Ми, що нижче підписалися,

Усков Сергій Олександрович,
здобувач освіти гр. 2БКС-27, та

Кільдішев Віталій Йосипович,
керівник дипломного проекту,

не заперечуємо щодо розміщення електронного варіанту пояснювальної записки до випускної кваліфікаційної роботи фахового молодшого бакалавра / бакалавра / молодшого спеціаліста на тему:

«Дослідження ролі аудиту та ризик-менеджменту в системі безпеки підприємства» (автор роботи – Усков С.О., керівник роботи – Кільдішев В.Й.)

виконаного у ВСП «Одеський технічний фаховий коледж Одеського національного технологічного університету» в 2023 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 _____ / *Усков С.О.*/

Керівник _____ / *Кільдішев В.Й* /

«15» 06 2023 р.

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

ВІДГУК

керівника про кваліфікаційну роботу бакалавра

Ускова Сергія Олександровича

(прізвище, ім`я та по батькові здобувача/здобувачки освіти)

Освітньо-професійна програма *«Комп'ютерна інженерія»*

Спеціальність *123 «Комп'ютерна інженерія»*

Тема кваліфікаційної роботи

«Дослідження ролі аудиту та ризик-менеджменту в системі безпеки підприємства»

ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

а) обсяг і якість виконання роботи (розрахунково-пояснювальної записки)

Пояснювальна записка виконана якісно, у достатньому обсязі, відповідно до індивідуального завдання та теми дипломного проекту, розділи пояснювальної записки відповідають етапам рішення завдання, поставленого у дипломному проекті

Презентація виконана якісно, у достатньому обсязі. Презентація наочно демонструє результати роботи.

б) самостійність роботи над кваліфікаційною роботою

Студент самостійно обрав напрям та тематику кваліфікаційної роботи. Провів аналіз елементи аудиту безпеки та ризик-менеджменту на прикладі ІТ-компанії. Для підвищення рівня захисту проведено аналіз ролі аудиту в діяльності компанії – визначення, цілі, види тощо. Розглянуто природу, сутність та типологію ризиків та питання аудиту в фокусі напрямку неперервності бізнесу BCM.

в) теоретична підготовка бакалавра

відповідає вимогам, що надаються до бакалавра зі спеціальності «Комп'ютерна інженерія»

г) вміння розв`язувати виробничі та конструкторські питання

У кваліфікаційній роботі розглянуто ключові аспекти управління та природу внутрішніх та зовнішніх ризиків компанії. Розглянуто проведення інвентаризації IT-ресурсів компанії. Досить глибоко вивчив питання впровадження ризик-менеджменту та побудови радару загроз.

Оцінка розрахункової частини відмінно

Оцінка графічної (презентаційної) частини відмінно

Загальна оцінка відмінно

Прізвище, ім'я, по батькові керівника роботи Кільдішев Віталій Йосипович

Місце роботи і посада керівника роботи к.т.н., доцент кафедри кібербезпеки та технічного захисту інформації ДУІТЗ

«15» 06 2023 р. (підпис) (прізвище та ініціали керівника)

ВСП «ОДЕСЬКИЙ ТЕХНІЧНИЙ ФАХОВИЙ КОЛЕДЖ ОНТУ»

РЕЦЕНЗІЯ

на кваліфікаційну роботу бакалавра
відділення комп'ютерних систем

Ускова Сергія Олександровича

(прізвище, ім`я та по батькові)

Напрямку підготовки *123 «Комп'ютерна інженерія»*

Керівник кваліфікаційної роботи *Кільдішев Віталій Йосипович*

(прізвище, ім`я та по батькові)

Тема кваліфікаційної роботи *«Дослідження ролі аудиту та ризик-менеджменту в системі безпеки підприємства»*

Обсяг пояснювальної записки _____ сторінок

Обсяг графічної (презентаційної) частини проекту _____ аркушів (слайдів)

ХАРАКТЕРИСТИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

а) заключення про ступінь відповідності виконаної роботи завданню

Робота відповідає технічному завданню до дипломного проекту. Виконана у відповідності з вимогами.

б) характеристика виконання кожного розділу роботи

При виконанні дипломного проекту студент продемонстрував уміння використовувати останні досягнення науки та техніки, уміння працювати з літературою. Так, студент грамотно дослідив та проаналізував аудиту та ризик-менеджменту в системі безпеки підприємства.

в) оцінка якості виконання графічної (презентаційної) частини роботи і пояснювальної записки

Графічна частина відповідає вимогам, виконана якісно та відображає основні елементи проектування системи. Розглянуто карту ризиків та на її основі побудовано радар загроз підприємства в аспекті 5-ти базових напрямів. Представлено структуру аудиту в фокусі принципу неперервності бізнесу. В рамках вивчення ризик-менеджменту показано завдання, мету, функції та основні етапи.

г) перелік позитивних якостей роботи

Тема дипломного проекту є актуальною, виконана у достатньому обсязі, якісно, відповідно до поставленого завдання.

д) основні недоліки роботи У тексті пояснювальної записки відсутні посилання на використану літературу, для підвищення ефективності захисту було б доцільним представити радар загроз в більшій кількості напрямів.

Оцінка розрахункової частини 5 (відмінно)

Оцінка графічної (презентаційної) частини 4 (добре)

Загальна оцінка 5 (відмінно)

Прізвище, ім'я та по батькові рецензента Василіу Євген Вікторович

Місце роботи і посада рецензента Державний університет інтелектуальних технологій і зв'язку, д.т.н., проф. кафедри КБ та ТЗІ, декан факультету інформаційних технологій та кібербезпеки

«16» 06 2023 р.

(підпис)

ПІДПИС ПОСВІДЧУЮ
НАЧАЛЬНИК ВІДДІЛУ
КАДРІВ ДУІТЗ

ВІДДІЛ КАДРІВ