МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»
Кафедра кібербезпеки

Клєвцєвич Н.А

ПРАКТИКУМ
з дисципліни
«АНАЛІЗ РИЗИКІВ ІТ-ПІДПРИЄМСТВ»
для студентів ІІІ курсу денної форми навчання
спеціальності 073 «Менеджмент»
ОП «ІТ-менеджмент та маркетинг»

ОДЕСА 2024

УДК 657.1.012

Рекомендовано навчально-методичною радою
Національного університету «Одеська юридична академія»
Протокол № від 2024 року

Рецензенти:

Кібік Ольга Миколаївна – завідувач кафедри Національної економіки Національного університету «Одеська юридична академія», доктор економічних наук, професор, академік Транспортної академії України

Карпінська Ганна Володимирівна - кандидат економічних наук, с.н.с., с.н.с. відділу розвитку підприємництва ДУ «Інститут ринку і економіко - екологічних досліджень Національної академії наук України

Автор:

Клєвцєвич Наталія Анатоліївна - кандидат економічних наук, доцент, доцент кафедри кібербезпеки Національного університету «Одеська юридична академія», ORCID: https://orcid.org/0000-0002-2010-4814

Практикум з дисципліни «Аналіз ризиків ІТ-підприємств» для студентів ІІІ курсу денної форми навчання спеціальності 073 «Менеджмент» ОП «ІТ-менеджмент та маркетинг» [Електронне видання] / Н.А. Клєвцєвич; кафедра кібербезпеки НУ «Одеська юридична академія». - Одеса, 2024. - 42 с.

Практикум з дисципліни «Аналіз ризиків ІТ-підприємств» спрямований на формування практичних навичок у студентів щодо виявлення, оцінки та управління ризиками в ІТ-сфері. Основна мета курсу – навчити майбутніх спеціалістів визначати потенційні загрози для підприємств, розробляти стратегії їх мінімізації та впроваджувати ефективні механізми захисту бізнесу від негативних впливів. Ключові аспекти, які охоплює практикум: ідентифікація ризиків – аналіз потенційних загроз у різних сферах діяльності ІТ-компаній; оцінка ризиків – використання методик для оцінки ймовірності настання ризиків та їх впливу на бізнес-процеси; розробка стратегії управління ризиками – формування та впровадження планів реагування на ризики; моніторинг та контроль ризиків – постійний аналіз ефективності застосованих заходів для зменшення ризиків. Даний курс допомагає студентам отримати необхідні знання та вміння для роботи в умовах високої конкурентоспроможності та швидких технологічних змін.

УДК 657.1.012

ЗМІСТ

ВСТУП

Вивчення дисципліни «Аналіз ризиків ІТ-підприємств» є надзвичайно актуальним для сучасних студентів, оскільки ІТ-сектор залишається одним із напрямів бізнесу, що найбільш динамічно розвиваються. В умовах глобалізації та постійних технологічних змін підприємства стикаються з різними загрозами, включаючи кіберзлочинність, витоки даних, технічні збої та регуляторні вимоги. Саме тому майбутнім фахівцям важливо володіти інструментами та знаннями для:

1. Виявлення нових загроз – у швидкозмінному світі ІТ-ризики постійно трансформуються, і студенти мають бути готовими до їхнього швидкого розпізнання.
2. Захисту інформаційних активів – правильне управління ризиками дозволяє зменшити ймовірність втрати критично важливих даних та порушення роботи систем.
3. Побудови ефективних систем кібербезпеки – вивчення дисципліни сприяє розумінню того, як налаштувати архітектуру безпеки на підприємстві для протидії різноманітним загрозам.
4. Оцінки впливу ризиків на бізнес – аналіз ризиків допомагає зрозуміти, які загрози можуть найбільш серйозно вплинути на стратегію та прибутковість компанії.
5. Підвищення конкурентоспроможності – здатність управління ризиками підвищує стійкість компанії на ринку, що дозволяє ІТ-підприємствам працювати ефективніше.

Таким чином, ця дисципліна дає студентам важливі знання, що допоможуть їм успішно будувати кар’єру в сфері ІТ і зберігати підприємства від негативних наслідків ризиків.

Тема 1. Вступ до аналізу ризиків ІТ підприємств

Метою практичного заняття на тему **«Вступ до аналізу ризиків ІТ підприємств»** є ознайомлення студентів з основними поняттями та принципами аналізу ризиків у сфері інформаційних технологій. Під час заняття студенти мають отримати загальне розуміння, що таке ризики в ІТ-секторі, які види ризиків існують, а також як їх можна виявляти та оцінювати.

Основні завдання заняття включають:

1. Ознайомлення з базовими поняттями – що таке ризик, як він виникає та як впливає на роботу ІТ-підприємств.
2. Класифікація ризиків – розгляд різних типів ризиків: технологічні, операційні, фінансові, регуляторні та інші.
3. Методи ідентифікації ризиків – студенти дізнаються про інструменти та техніки для виявлення потенційних загроз на підприємстві.
4. Огляд процесу управління ризиками – знайомство зі стандартними етапами управління ризиками: ідентифікація, оцінка, розробка стратегії, впровадження заходів та моніторинг.
5. Практичні приклади – аналіз конкретних випадків ризиків на реальних прикладах ІТ-підприємств для кращого розуміння теорії.

Після заняття студенти повинні мати уявлення про основи аналізу ризиків і бути готовими до більш глибокого вивчення даної теми.

Питання для обговорення

1. Що таке ризик в контексті ІТ-підприємства, і як його можна визначити?
2. Які основні види ризиків можуть виникати на ІТ-підприємстві?
3. Чим відрізняються технологічні ризики від операційних? Наведіть приклади.
4. Як глобалізація та цифровізація впливають на зростання ризиків в ІТ-секторі?
5. Які методи ідентифікації ризиків ви знаєте? Який з них, на вашу думку, є найбільш ефективним?
6. Що таке управління ризиками? Які етапи включає цей процес?
7. Які інструменти оцінки ризиків використовуються на ІТ-підприємствах? Чим відрізняються якісні та кількісні методи оцінки?

8. Як ви думаєте, які ризики є найважчими для прогнозування на IT-підприємствах?
9. Які наслідки може мати неправильне управління ризиками для IT-компанії?
10. Як законодавчі та етичні аспекти можуть впливати на процес управління ризиками на підприємствах?

Завдання

Завдання 1. Ідентифікація ризиків

Завдання: студенти мають скласти список можливих ризиків для уявного або реального IT-підприємства. Сфери для розгляду: технічні проблеми, людський фактор, кібербезпека, правові ризики. Поясніть, чому саме ці ризики можуть бути важливими для підприємства.

Завдання 2. Класифікація ризиків

Завдання: розподілити виявлені ризики на категорії: фінансові, технологічні, операційні, правові та регуляторні. Для кожного ризику вказати потенційні наслідки та ймовірність його виникнення.

Завдання 3. Оцінка ризиків

Завдання: використовуючи методику FMEA (Аналіз видів і наслідків відмов), оцініть рівень важливості кожного ризику з попереднього завдання. Вкажіть можливі наслідки, ймовірність виникнення та можливість контролю для кожного ризику. На основі цього оцініть їх пріоритетність.

Завдання 4.Розробка стратегії управління ризиками:

Завдання: студенти повинні запропонувати стратегії мінімізації або усунення для кожного з ризиків, ідентифікованих у попередніх завданнях. Наприклад, технічні ризики можуть бути мінімізовані за рахунок резервного копіювання даних або оновлення систем безпеки.

Завдання 5. Практичний кейс

Завдання: проаналізуйте приклад випадку з відомим IT-підприємством, яке зіткнулося з серйозними ризиками. Опишіть, які ризики були не враховані, і які заходи могли б допомогти уникнути негативних наслідків.

Одним із відомих прикладів серйозних ризиків, з якими зіткнулося IT-підприємство, є витік даних компанії Equifax у 2017 році. Це одна з найбільших кредитних організацій у США, яка збирає і зберігає фінансову інформацію мільйонів людей.

Опис випадку:

У вересні 2017 року було виявлено, що хакери отримали доступ до чутливої інформації 147 мільйонів клієнтів компанії, включаючи номери соціального страхування, дати народження та номери кредитних карток. Ця кібератака стала однією з найбільших у світі за масштабами втрат конфіденційних даних.

Ризики, з якими зіткнулося підприємство:

1. Кібербезпека: Основний ризик полягав у вразливості системи кібербезпеки. Хакери скористалися відомою вразливістю в програмному забезпеченні Apache Struts, яке використовувала Equifax. Компанія не встигла вчасно оновити програмне забезпечення, хоча вразливість була відома за кілька місяців до атаки.
2. Репутаційний ризик: Через цей витік компанія втратила довіру як серед клієнтів, так і партнерів. Витік настільки серйозно пошкодив репутацію компанії, що багато клієнтів почали шукати альтернативи.
3. Фінансові ризики: Наслідки для Equifax включали значні фінансові втрати. Компанія була змушена заплатити понад 700 мільйонів доларів за угоду з урядом США, щоб покрити збитки клієнтам та вирішити правові питання.
4. Правові ризики: Компанія зіткнулася з численними судовими позовами від постраждалих клієнтів, а також урядовими розслідуваннями, що викликало додаткові витрати на юридичну підтримку та регуляторні штрафи.

Тестові завдання з теми.

1. *Що таке ризик в контексті IT-підприємств?*

a) Неочікуване зростання прибутку
b) Потенційна загроза для досягнення цілей підприємства
c) Заплановане зменшення витрат
d) Впровадження нових технологій

2. *Який з наведених ризиків є технологічним?*

a) Порушення постачання обладнання
b) Неправильне управління фінансами
c) Невиконання вимог законодавства
d) Вразливість програмного забезпечення

3. *Який етап є першим у процесі управління ризиками?*

a) Розробка стратегії управління
b) Оцінка ризиків
c) Ідентифікація ризиків
d) Моніторинг і контроль

4. *Що є основною метою оцінки ризиків?*

a) Визначення ймовірності та впливу ризику
b) Усунення всіх ризиків
c) Впровадження нових ризиків
d) Збільшення прибутків компанії

5. *Який метод допомагає оцінити вплив і ймовірність виникнення ризику?*

a) SWOT-аналіз
b) FMEA (Аналіз видів і наслідків відмов)
c) PEST-аналіз
d) ABC-аналіз

Тема 2. Ідентифікація ризиків ІТ підприємств

Метою практичного заняття на тему **«Ідентифікація ризиків ІТ-підприємств»** є навчити студентів визначати та аналізувати потенційні ризики, з якими можуть зіткнутися ІТ-компанії, а також розвивати навички застосування різних методик для їхньої ідентифікації. Це заняття має на меті допомогти студентам краще зрозуміти процес виявлення ризиків на ранніх етапах, що дозволяє уникнути або мінімізувати негативні наслідки.

Основні завдання заняття:

1. Ознайомлення з основними категоріями ризиків: технологічні, операційні, фінансові, регуляторні та людські ризики.
2. Навчання інструментам ідентифікації ризиків: використання таких технік, як інтерв'ю з експертами, аналіз бізнес-процесів, "мозковий штурм" і чек-листи.
3. Вивчення реальних прикладів: аналіз конкретних кейсів з ІТ-підприємств, щоб зрозуміти, як вчасна ідентифікація допомагає уникнути катастрофічних втрат.
4. Практичні вправи: студенти повинні самостійно визначити потенційні ризики для уявного ІТ-підприємства і обговорити їх.

Питання для обговорення

1. Чому ідентифікація ризиків є важливим етапом у процесі управління ризиками ІТ-підприємства?
2. Які основні типи ризиків можуть виникати на ІТ-підприємствах, і які з них є найбільш критичними?
3. Як відрізняються підходи до ідентифікації технологічних та операційних ризиків?
4. Які методи ідентифікації ризиків використовуються на ІТ-підприємствах? Який із них є найбільш ефективним у вашій думці?
5. Як зміни в технологіях та інноваціях впливають на типи та кількість ризиків для ІТ-компаній?
6. Чому людський фактор є однією з найсерйозніших загроз для ІТ-безпеки? Наведіть приклади.
7. Як можна оцінити вплив неідентифікованих ризиків на роботу ІТ-підприємства?

8. Які інструменти автоматизації можна використовувати для ідентифікації ризиків у сучасних IT-системах?
9. Як ви думаєте, чи всі ризики можна передбачити на етапі ідентифікації? Що робити з непередбачуваними ризиками?
10. Яким чином ідентифікація ризиків впливає на стратегію розвитку IT-підприємства в довгостроковій перспективі?

Завдання

З*авдання 1: Ідентифікація ризиків у реальному кейсі*

Опис: проаналізуйте кейс IT-компанії, що зіткнулася з проблемами. Ідентифікуйте ключові ризики, які могли б загрожувати цьому підприємству.

Вимоги: визначити не менше 5 ризиків і розподілити їх за категоріями (технологічні, фінансові, операційні тощо).

Кейси: Кібератака на компанію Sony Pictures Entertainment

Опис ситуації:

У листопаді 2014 року компанія **Sony Pictures Entertainment** стала жертвою потужної кібератаки, яка призвела до значних втрат і репутаційних втрат. Хакери, що назвали себе **Guardians of Peace**, зламали внутрішні системи компанії, отримали доступ до конфіденційної інформації та викрали значні обсяги даних, включаючи сценарії фільмів, електронну пошту співробітників та персональні дані.

Проблеми:

1. *Витік даних*: Хакери оприлюднили листи, що містили особисті та професійні коментарі співробітників, що викликало великий скандал.
2. *Технічний збій*: Через атаку було зупинено роботу багатьох комп'ютерних систем і сервісів, що призвело до значних затримок у виробництві та випуску фільмів.
3. *Фінансові втрати*: Оцінюється, що атака призвела до витрат на суму понад 100 мільйонів доларів на відновлення систем, юридичні послуги та компенсації.
4. *Репутаційні втрати*: Втрата довіри з боку партнерів, інвесторів і громадськості, що негативно позначилося на бренді.

Реакція компанії:

- *Вжиття заходів безпеки*: Sony вжила серйозні заходи для посилення кібербезпеки, включаючи поліпшення систем шифрування, навчання співробітників і вдосконалення протоколів реагування на інциденти.
- *Судові дії:* компанія подала позови проти інших сторон, які могли бути причетні до витоку даних.

- *Публічні вибачення*: керівництво Sony публічно вибачилося перед співробітниками та клієнтами за виниклі незручності.

Завдання 2: Використання чек-листів для ідентифікації ризиків

Опис: створіть чек-лист для оцінки потенційних ризиків на уявному IT-підприємстві. Включіть в нього основні аспекти бізнесу, такі як технічна інфраструктура, безпека даних, регуляторні вимоги тощо.

Вимоги: чек-лист має містити щонайменше 10 пунктів з поясненням, як кожен ризик може вплинути на підприємство.

Приклад чек-листа для оцінки потенційних ризиків

1. Технічні ризики

Чи є застарілі сервери або мережеве обладнання, які можуть спричинити збої в роботі?

Чи існують проблеми з сумісністю програмного забезпечення або його оновленнями?

Чи є резервні копії даних і чи регулярно перевіряється їх працездатність?

Чи використовуються хмарні рішення, і як здійснюється контроль над даними в хмарі?

Чи є проблеми з продуктивністю IT-інфраструктури під час пікових навантажень?

2. Кібербезпека

Чи належним чином захищені дані компанії (шифрування, контроль доступу)?

Чи проводиться регулярний моніторинг можливих кіберзагроз і атак?

Чи регулярно оновлюється антивірусне програмне забезпечення та системи безпеки?

Чи використовується двофакторна аутентифікація для критичних систем?

Чи здійснюється навчання співробітників щодо основ кібербезпеки та запобігання фішинговим атакам?

3. Операційні ризики

Чи достатньо персоналу для підтримки стабільної роботи IT-систем і проєктів?

Чи існує ризик втрати ключових співробітників і як це може вплинути на функціонування підприємства?

Чи належним чином документовані всі внутрішні процеси?

Чи існують ризики простою через технічні збої або зовнішні фактори (наприклад, проблеми з інтернет-провайдером)?

Чи є план дій у разі технічної аварії або інших непередбачених обставин?

4. Юридичні та регуляторні ризики

Чи відповідає IT-інфраструктура вимогам законодавства щодо захисту даних (GDPR, локальні закони)?

Чи існує ризик юридичних претензій у разі витоку персональних даних?

Чи є угоди про конфіденційність та захист інтелектуальної власності у відносинах з партнерами та підрядниками?

Чи перевіряються нові контракти на відповідність стандартам безпеки?

5. Фінансові ризики

Чи існує ризик перевищення бюджету на обслуговування ІТ-інфраструктури?

Чи передбачено достатній бюджет на оновлення обладнання та програмного забезпечення?

Чи є фінансові резерви для покриття можливих втрат через технічні збої або кібератаки?

Чи аналізуються довгострокові витрати на підтримку ІТ-інфраструктури?

6. Проєктні ризики

Чи існує чіткий план управління ризиками в ІТ-проєктах?

Чи є ризик перевищення термінів виконання ІТ-проєктів?

Чи існує ризик зриву взаємодії з підрядниками або постачальниками?

Чи регулярно проводяться оцінки прогресу та якості виконання проєктів?

7. Інфраструктурні ризики

Чи є фізичний захист ІТ-інфраструктури (системи контролю доступу, камери спостереження)?

Чи існує план безперебійного живлення на випадок аварійного вимкнення електроенергії?

Чи забезпечено захист серверного обладнання від природних катастроф (затоплення, пожежа)?

8. Соціальні та репутаційні ризики

Чи існує ризик пошкодження репутації компанії через витік даних або кіберінцидент?

Чи є комунікаційний план на випадок кризи або публічних звинувачень?

Чи проводиться моніторинг соціальних медіа для відстеження репутації компанії?

Завдання 3: Аналіз людського фактора

Опис: проведіть аналіз ризиків, пов’язаних з людським фактором (наприклад, помилки персоналу, недостатня підготовка, неправильне поводження з даними). Запропонуйте стратегії для зменшення впливу цих ризиків.

Вимоги: визначити 3-5 ризиків і описати, як можна мінімізувати їх вплив.

Завдання 4: Ідентифікація ризиків для стартапу

Опис: уявіть, що ви консультуєте ІТ-стартап, який займається розробкою мобільних додатків. Ідентифікуйте ризики, з якими може зіткнутися стартап на початковому етапі розвитку (наприклад, нестача фінансування, помилки в програмному коді, ризики конфіденційності даних).

Вимоги: описати не менше 5 потенційних ризиків, які можуть вплинути на стартап.

Завдання 5: Створення схеми процесу ідентифікації ризиків

Опис: розробіть схему процесу ідентифікації ризиків для ІТ-підприємства, починаючи від збору інформації до категоризації ризиків. На

схемі має бути показано основні етапи та інструменти, які можна використовувати на кожному з них.

Вимоги: схема повинна містити не менше 4-5 ключових етапів з поясненням кожного.

Тестові завдання

1. *Яка з наведених кібератак найчастіше використовує фішинг?*

a) Вірусна атака
b) Атака «людини посередині»
c) Вірус-вимагач
d) Соціальна інженерія

2. *Яка з наведених технологій є найефективнішою для шифрування даних?*

a) HTTPS
b) VPN
c) AES
d) SSL

3. *Який з наступних етапів є першим кроком у плані реагування на інциденти?*

a) Виявлення інциденту
b) Оцінка збитків
c) Відновлення системи
d) Повідомлення зацікавлених сторін

4. *Яка з наступних методологій є популярною для управління проектами в IT?*

a) Agile
b) Waterfall
c) Six Sigma
d) Обидва a і b

5. *Яка з наведених методів аутентифікації є найбільш надійною?*

a) Пароль
b) Відбиток пальця
c) Питання безпеки
d) SMS-код

Тема 3. Кількісні методи оцінки ризиків

Метою заняття на тему **«Кількісні методи оцінки ризиків»** є надати студентам знання та навички, необхідні для розуміння та застосування кількісних методів оцінки ризиків у різних сферах діяльності, зокрема в бізнесі, фінансах та управлінні проектами.

Завдання:

1. Ознайомити студентів з основними концепціями та термінами, пов'язаними з оцінкою ризиків.
2. Розглянути різні кількісні методи оцінки ризиків, такі як:
    - Метод монте-карло
    - Аналіз чутливості
    - Статистичні методи (регресійний аналіз, кореляційний аналіз)
    - Метод дерева рішень
3. Навчити студентів використовувати ці методи для аналізу реальних ситуацій і прийняття обґрунтованих рішень.
4. Розвинути навички критичного мислення при оцінці ризиків та прийнятті рішень на основі кількісних даних.
5. Провести практичні вправи, що дозволяють студентам застосовувати набуті знання в практичних сценаріях.

Питання для обговорення

1. Що таке ризик, і які його основні складові?
2. Які переваги та недоліки використання кількісних методів оцінки ризиків порівняно з якісними методами?
3. Як метод Монте-Карло може бути використаний для оцінки ризиків у фінансових проектах?
4. Яка роль статистичних методів (регресійний аналіз, кореляційний аналіз) у кількісній оцінці ризиків?
5. У яких випадках використання дерева рішень може бути більш ефективним для оцінки ризиків?
6. Які практичні приклади використання кількісних методів оцінки ризиків ви можете навести з реального життя?
7. Як ви оцінюєте важливість розуміння та застосування кількісних методів оцінки ризиків у сучасному бізнес-середовищі?

8. Які етичні питання можуть виникати при оцінці ризиків, особливо в контексті фінансових рішень?
9. Які нові тенденції в галузі кількісної оцінки ризиків ви бачите?
10. Як ви вважаєте, які навички та знання є найважливішими для фахівців, які займаються оцінкою ризиків?

Завдання

Завдання 1: Розрахунок ризику

Ситуація: у компанії планується запуск нового продукту. Вартість розробки складає 100 000 доларів, а прогнозований дохід — 200 000 доларів. Однак є 20% ймовірність того, що продажі не виправдають очікування, і компанія втратить 50 000 доларів.

Запитання:

1. Розрахуйте очікуваний прибуток або збиток від запуску продукту.
2. Чи варто продовжувати проект, враховуючи отримані дані?

Завдання 2: Аналіз чутливості

Ситуація: Ви є аналітиком, який оцінює проект з інвестиціями в 500 000 доларів. Проект має прогнозовану внутрішню норму прибутковості (IRR) 15%. Однак існує невизначеність в очікуваних грошових потоках.

Запитання:

1. Визначте, як зміна грошових потоків на 10% вплине на IRR проекту.
2. Чи змінилася б ваша оцінка проекту в разі такого сценарію?

Завдання 3: Метод Монте-Карло

Завдання: використовуючи метод Монте-Карло, змоделюйте сценарій ризику для фінансового проекту, в якому:

- Імовірність позитивного результату — 60% з очікуваним прибутком у 100 000 доларів.
- Імовірність негативного результату — 40% з очікуваним збитком у 50 000 доларів.

Запитання:

1. Запустіть 1000 симуляцій і розрахуйте очікуваний результат проекту.
2. Які рекомендації ви б дали на основі отриманих результатів?

Завдання 4: Дерево рішень

Ситуація: Ви повинні вирішити, чи інвестувати в нову технологію. Інвестиція коштує 200 000 доларів. Є дві основні гілки: успіх (70% ймовірність) і невдача (30% ймовірність).

Запитання:

1. Розрахуйте очікуване значення (EV) інвестиції, якщо успіх приносить 400 000 доларів, а невдача — 100 000 доларів збитку.

2. Яке рішення ви б прийняли на основі розрахунків?

Завдання 5: Вплив зовнішніх факторів

Ситуація: ризики для вашого проекту можуть бути пов’язані з економічними змінами (інфляція, зміна валютних курсів тощо).

Запитання:

1. Складіть список можливих зовнішніх ризиків і їхнього впливу на ваш проект.
2. Розробіть кількісну модель для оцінки впливу одного з цих ризиків на фінансові результати проекту.

Тестові питання

1. *Яка з наведених формул найкраще описує ризик?*

a) Ризик = Витрати + Прибуток
b) Ризик = Ймовірність × Вплив
c) Ризик = Доходи - Витрати
d) Ризик = (Прибуток - Витрати) / Витрати

2. *Для чого використовується метод Монте-Карло в оцінці ризиків?*

a) Для створення якісних описів ризиків
b) Для моделювання різноманітних сценаріїв за допомогою випадкових вибірок
c) Для управління проектами
d) Для побудови графіків

3. *Яка з наступних ситуацій є прикладом аналізу чутливості?*

a) Визначення ймовірності негативного сценарію
b) Оцінка впливу зміни цін на прибутковість проекту
c) Ідентифікація всіх ризиків у проекті
d) Розробка плану управління ризиками

4. *Яка з наведених компонентів є частиною дерева рішень?*

a) Ризик
b) Кошторис
c) Вузли та гілки
d) Проектний план

5. *Яка з наступних характеристик найбільше відповідає внутрішній нормі прибутковості (IRR)?*

a) Це середня ставка прибутковості проекту
b) Це ставка, при якій чистий дисконтований дохід (NPV) проекту дорівнює нулю
c) Це ставка, що враховує інфляцію
d) Це ставка, яка визначається на основі зовнішніх фінансових ринків

Тема 4. Якісні методи оцінки ризиків

Метою заняття на тему «**Якісні методи оцінки ризиків**» надати студентам розуміння основних якісних методів оцінки ризиків, їх застосування та значення в управлінні ризиками в різних сферах діяльності, зокрема в бізнесі, фінансах і проектному управлінні.

Завдання:

1. Ознайомити студентів з основними поняттями та термінами, пов'язаними з якісною оцінкою ризиків.
2. Розглянути різні якісні методи оцінки ризиків, такі як:
    - SWOT-аналіз
    - Метод експертних оцінок
    - Аналіз сценаріїв
    - Метод мозкового штурму
3. Навчити студентів ідентифікувати та класифікувати ризики за допомогою якісних методів.
4. Розвинути навички критичного мислення та аналізу при оцінці ризиків, акцентуючи увагу на важливості якісних даних у прийнятті рішень.
5. Провести практичні вправи, що дозволяють студентам застосовувати набуті знання на реальних прикладах.

Питання для обговорення:

1. Що таке якісна оцінка ризиків, і чим вона відрізняється від кількісної?
2. Як SWOT-аналіз може допомогти в ідентифікації ризиків?
3. Яка роль експертних оцінок у якісній оцінці ризиків?
4. Які основні етапи проведення аналізу сценаріїв, і як цей метод може бути застосований у вашій сфері?
5. Які стратегії можна використовувати для мозкового штурму, щоб генерувати ідеї щодо потенційних ризиків?

6. Чи можуть якісні методи оцінки ризиків бути доповнені кількісними даними?
7. Які етичні міркування слід враховувати при проведенні якісної оцінки ризиків?
8. Які нові тенденції в галузі якісних методів оцінки ризиків ви помічаєте?
9. Які практичні приклади ви можете навести, де якісні методи оцінки ризиків виявилися ефективними?
10. Які навички та знання є найбільш важливими для фахівців, які займаються якісною оцінкою ризиків?

Завдання

Завдання 1: SWOT-аналіз

Ситуація: компанія планує запустити новий продукт на ринок.

Завдання:

1. Проведіть SWOT-аналіз, визначивши:
   - Сильні сторони (Strengths)
   - Слабкі сторони (Weaknesses)
   - Можливості (Opportunities)
   - Загрози (Threats)
2. Напишіть короткий звіт з рекомендаціями щодо управління ризиками на основі результатів аналізу.

Завдання 2: Експертні оцінки

Ситуація: Ви є частиною команди, яка аналізує потенційні ризики для нового проекту.

Завдання:

1. Залучіть трьох експертів у вашій організації (або використайте фіктивних експертів) для оцінки ризиків.
2. Проведіть інтерв'ю з кожним експертом, запитуючи про ймовірність і вплив основних ризиків.
3. Підготуйте звіт, в якому представите результати експертних оцінок та рекомендації щодо управління ризиками.

Завдання 3: Аналіз сценаріїв

Ситуація: компанія розглядає можливість виходу на новий ринок.

Завдання:

1. Складіть три різні сценарії (оптимістичний, песимістичний і реалістичний) для виходу на новий ринок.

2. Для кожного сценарію визначте можливі ризики, а також їхній потенційний вплив на бізнес.

3. Підготуйте презентацію, в якій узагальните результати аналізу сценаріїв та обґрунтуйте рекомендації.

Завдання 4: Мозковий штурм

*Ситуація***:** ваша команда має зібратися для генерування ідей щодо потенційних ризиків у проекті.

Завдання:

1. Організуйте мозковий штурм на тему ризиків вашого проекту.
2. Визначте правила для мозкового штурму (наприклад, жодних критичних зауважень, всі ідеї приймаються).
3. Запишіть усі ідеї, а потім класифікуйте їх за категоріями (фінансові, технологічні, юридичні тощо).
4. Підготуйте звіт із зібраними ризиками та рекомендаціями для їх управління.

Завдання 5: Презентація якісних методів

*Завдання***:**

1. Підготуйте презентацію про один з якісних методів оцінки ризиків (SWOT-аналіз, метод експертних оцінок, аналіз сценаріїв, мозковий штурм тощо).
2. Уключіть такі елементи:
    - Опис методу
    - Процес його застосування
    - Приклади його використання
    - Переваги та недоліки
3. Проведіть презентацію для класу та відповідайте на запитання.

Тестові завдання

*1. Якісні методи оцінки ризиків в основному використовуються для***:**

a) Оцінки ймовірності ризиків
b) Кількісного визначення фінансових втрат
c) Ідентифікації та оцінки ризиків без використання числових даних
d) Створення математичних моделей ризиків

2. Яка з наведених частин не є елементом SWOT-аналізу?

a) Сильні сторони
b) Загрози
c) Слабкі сторони
d) Прибуток

3. Яка з наступних характеристик найбільше відповідає методу експертних оцінок?

a) Використання статистичних даних для оцінки ризиків
b) Оцінка ризиків на основі думок і досвіду фахівців
c) Використання комп'ютерних моделей для прогнозування ризиків
d) Аналіз історичних даних для виявлення тенденцій

4. Яка з наведених ситуацій найкраще ілюструє метод аналізу сценаріїв?

a) Визначення всіх можливих ризиків у проекті
b) Оцінка впливу зміни ринку на бізнес
c) Створення й оцінка кількох альтернативних майбутніх ситуацій
d) Розробка плану управління ризиками

5. *Яка з наведених переваг є основною для використання якісних методів оцінки ризиків?*

a) Вони завжди забезпечують точні фінансові розрахунки
b) Вони дозволяють швидко ідентифікувати ризики в умовах невизначеності
c) Вони не потребують залучення фахівців
d) Вони є найбільш дорогими з усіх методів оцінки ризиків

Тема 5. Управління ризиками інформаційної безпеки

Основною метою заняття на тему «Управління ризиками інформаційної безпеки» навчити студентів основам управління ризиками в інформаційній безпеці, включаючи ідентифікацію, оцінку та управління ризиками, що впливають на конфіденційність, цілісність і доступність інформації в організаціях.

Завдання:

1. Ознайомити студентів з основними поняттями та термінами, пов'язаними з управлінням ризиками інформаційної безпеки.
2. Розглянути методи і інструменти для ідентифікації ризиків, включаючи оцінку вразливостей та загроз.

3. Навчити студентів методам оцінки ризиків, зокрема якісним і кількісним підходам.
4. Обговорити стратегії управління ризиками, включаючи уникнення, зменшення, прийняття та перенесення ризиків.
5. Провести практичні вправи, в яких студенти можуть застосувати отримані знання на реальних прикладах, розглянувши сценарії загроз та вразливостей в інформаційних системах.

Питання для обговорення

1. Які основні елементи управління ризиками інформаційної безпеки?
2. Які типи загроз можуть вплинути на інформаційну безпеку організації?
3. Як можна ідентифікувати вразливості в інформаційних системах?
4. Які переваги та недоліки є у якісних і кількісних методах оцінки ризиків?
5. Які стратегії управління ризиками ви вважаєте найбільш ефективними?
6. Як впливають нові технології, такі як штучний інтелект або блокчейн, на управління ризиками інформаційної безпеки?
7. Яку роль відіграє навчання та підвищення обізнаності співробітників у зменшенні ризиків інформаційної безпеки?
8. Які етичні питання виникають при управлінні ризиками інформаційної безпеки?
9. Як слід реагувати на інциденти інформаційної безпеки?
10. Які нові тренди в управлінні ризиками інформаційної безпеки ви помічаєте?

Завдання

Завдання 1: Аналіз ризиків

Ситуація: Ви є керівником проекту в IT-компанії, яка розробляє новий продукт.

Проект: Розробка платформи для дистанційного навчання

Огляд проекту: проект має на меті створення інноваційної платформи для дистанційного навчання, що забезпечує інтерактивний та зручний навчальний досвід для студентів та викладачів. Платформа буде використовувати новітні технології, включаючи штучний інтелект, для персоналізації навчання, автоматизації оцінювання та надання аналітики щодо успішності учнів.

Цілі проекту:

1. Розробити зручний інтерфейс для студентів і викладачів, який забезпечить легкий доступ до навчальних матеріалів та ресурсів.

2. Інтегрувати функціонал для відео-конференцій, чату та обговорень, що дозволить студентам взаємодіяти між собою та з викладачами.

3. Створити систему оцінювання та зворотного зв'язку, що автоматизує процес перевірки домашніх завдань та тестів.

4. Використати алгоритми штучного інтелекту для персоналізації навчальних траєкторій в залежності від потреб кожного студента.

5. Забезпечити високий рівень безпеки даних, включаючи шифрування та захист особистої інформації.

Ключові етапи проекту:

1. Дослідження ринку:
    - Аналіз конкурентів і вивчення потреб цільової аудиторії (студентів, викладачів, навчальних закладів).
    - Визначення функціональних вимог до платформи.
2. Проектування:
    - Розробка архітектури системи та створення прототипів інтерфейсу.
    - Визначення технологій, які будуть використовуватися (фреймворки, мови програмування, бази даних).
3. Розробка:
    - Написання коду та реалізація всіх функціональних модулів платформи.
    - Проведення внутрішнього тестування для виявлення та виправлення помилок.
4. Тестування:
    - Проведення бета-тестування з залученням реальних користувачів (студентів та викладачів).
    - Збір відгуків та вдосконалення платформи на основі отриманих даних.
5. Запуск:
    - Офіційний запуск платформи на ринку та активна промоція продукту.
    - Проведення навчальних сесій для викладачів та студентів щодо використання платформи.
6. Підтримка та оновлення:
    - Забезпечення технічної підтримки користувачів.
    - Регулярне оновлення платформи з урахуванням нових технологій та зворотного зв'язку від користувачів.

Очікувані результати:

- Створення конкурентоспроможного продукту, що забезпечує ефективне дистанційне навчання.
- Збільшення кількості користувачів платформи завдяки унікальним функціям та простоті у використанні.
- Позитивний вплив на навчальний процес, підвищення успішності студентів та задоволеності викладачів.

Команда проекту:

- Менеджер проекту: Відповідає за загальне управління проектом, контроль за термінами виконання та бюджетом.
- Розробники: Створюють функціонал платформи, працюють над кодуванням та тестуванням.
- UX/UI дизайнери: Розробляють інтерфейс та покращують користувацький досвід.
- Аналітики: Збирають дані про ринок та потреби користувачів, аналізують результати тестування.
- Спеціалісти з безпеки: Відповідають за забезпечення безпеки даних користувачів та системи в цілому.

Завдання:

1. Проведіть ідентифікацію ризиків, що можуть вплинути на безпеку інформації в рамках цього проекту.
2. Складіть список не менше ніж п'яти ризиків, вказавши їх потенційний вплив і ймовірність виникнення.
3. Оцініть ризики за шкалою від 1 до 5 (1 — низький ризик, 5 — високий ризик) і розробіть рекомендації щодо їх управління.

Завдання 2: Розробка політики безпеки

Ситуація: організація планує впровадити нову політику інформаційної безпеки.

Завдання:

1. На основі аналізу існуючих загроз та вразливостей, розробіть проект політики інформаційної безпеки.
2. Включіть такі елементи:
    - Мета та обґрунтування політики
    - Основні правила доступу до інформаційних систем
    - Процедури реагування на інциденти
3. Презентуйте свою політику перед класом та отримайте зворотний зв'язок.

Завдання 3: Сценарії інцидентів

Ситуація: організація стала жертвою кібератаки.

Завдання:

1. Розробіть три різні сценарії можливих інцидентів інформаційної безпеки (наприклад, витік даних, атака на відмову в обслуговуванні, фішинг).
2. Для кожного сценарію визначте:
    - Потенційний вплив на бізнес
    - Кроки для виявлення інциденту
    - Процедури реагування на інцидент
3. Обговоріть ваші сценарії з колегами в класі та проаналізуйте можливі вдосконалення.

Завдання 4: Оцінка вразливостей

Ситуація: організація проводить регулярні оцінки вразливостей системи.

Завдання:

1. Проведіть оцінку вразливостей для конкретної інформаційної системи (можете використати фіктивну систему).
2. Визначте можливі вразливості та оцініть їхній ризик (високий, середній, низький).
3. Розробіть рекомендації щодо усунення виявлених вразливостей.

Завдання 5: Навчальний семінар

Завдання:

1. Підготуйте короткий семінар (10-15 хвилин) на тему "Кращі практики управління ризиками інформаційної безпеки".
2. Включіть такі елементи:
    - Визначення ризиків і їх вплив на бізнес
    - Підходи до управління ризиками
    - Реальні приклади впровадження управлінських практик
3. Презентуйте семінар перед класом і відповідайте на запитання.

Тестові завдання

1. *Яка з наведених нижче загроз є прикладом кібератаки?*

a) Витік даних через ненадійний Wi-Fi
b) Помилка користувача при вводі даних
c) Відмова обладнання
d) Пожежа в серверній кімнаті

2. *Який з наведених методів є якісним підходом до оцінки ризиків?*

a) Визначення фінансових втрат
b) Метод SWOT-аналізу
c) Використання статистичних даних
d) Моделювання сценаріїв

3. *Яка стратегія управління ризиками передбачає зменшення ймовірності або впливу ризику?*

a) Уникнення
b) Прийняття
c) Зменшення
d) Перенесення

4. Що є основною метою навчання співробітників в контексті інформаційної безпеки?

a) Зниження витрат
b) Підвищення продуктивності
c) Зменшення ризиків людських помилок
d) Підвищення технічних навичок

5. Який з наведених етапів є першим у процесі управління ризиками?

a) Реагування на інциденти
b) Ідентифікація ризиків
c) Оцінка ризиків
d) Розробка стратегії управління

Тема 6. Управління проектними ризиками в ІТ

Метою заняття на тему **«Управління проектними ризиками в ІТ»** є ознайомлення студентів з основами управління ризиками в контексті ІТ-проектів. Студенти навчаться ідентифікувати, оцінювати та управляти ризиками, які можуть вплинути на успішність проектів у сфері інформаційних технологій.

Завдання:

1. Аналіз ризиків проекту: студенти отримують опис фіктивного ІТ-проекту (наприклад, розробка мобільного додатку) і повинні визначити можливі ризики, їх вплив та ймовірність виникнення.

2. Розробка плану управління ризиками: на основі виявлених ризиків студенти повинні створити план управління ризиками, в якому включити рекомендації щодо їх уникнення або зменшення.

3. Сценарії ризиків: студенти повинні розробити три різні сценарії ризиків, що можуть вплинути на проект, та визначити потенційні наслідки для проекту.

Питання для обговорення

1. Які типи ризиків є найбільш поширеними в IT-проектах, і чому?
2. Які методи ідентифікації ризиків є найефективнішими в IT-проектах?
3. Як можна оцінити ймовірність виникнення та вплив ризиків на проект?
4. Чи важливо розробляти план управління ризиками на етапі ініціації проекту? Чому?
5. Які наслідки можуть бути від ігнорування цього етапу?
6. Які стратегії управління ризиками (усунення, зменшення, перенесення, прийняття) є найбільш доречними в різних ситуаціях?
7. Як вибрати правильну стратегію для конкретного ризику?
8. Як організувати процес моніторингу ризиків протягом життєвого циклу проекту?
9. Яку роль грає комунікація в управлінні ризиками?
10. Як забезпечити ефективний обмін інформацією про ризики в команді?

Завдання

Завдання 1: Аналіз ризиків IT-проекту

*Опис***:** Студентам надається опис фіктивного IT-проекту, наприклад, розробка нової системи управління проектами.

Завдання:

- Визначте та опишіть принаймні п’ять потенційних ризиків, які можуть виникнути в цьому проекті.
- Оцініть ймовірність виникнення кожного ризику та його потенційний вплив на проект (високий, середній, низький).

Проєкт: ProjectMaster

Мета проєкту: створення сучасної хмарної системи управління проєктами, яка допоможе командам з різних галузей ефективніше координувати роботу, контролювати дедлайни, розподіляти завдання та відстежувати продуктивність. Система буде адаптована для різних розмірів компаній і зможе інтегруватися з іншими популярними інструментами (наприклад, Slack, Google Drive, Jira).

Основні функції:

1. Дашборд проєктів: інтуїтивно зрозумілий інтерфейс для перегляду поточних та запланованих проєктів, статусів завдань, термінів виконання та ресурсів.
2. Управління завданнями: можливість створювати, призначати та відстежувати завдання для кожного учасника проєкту з індивідуальними термінами виконання.

3. Інтеграція з популярними інструментами: підтримка інтеграції з такими платформами як Slack, Google Drive, Microsoft Teams, Trello та інші.
4. Календар: Вбудований календар з відображенням дедлайнів, подій і зустрічей, синхронізований із зовнішніми календарями (Google, Outlook).
5. Аналітика продуктивності: модуль для оцінки ефективності роботи команди, кількості виконаних завдань, аналізу термінів.
6. Система повідомлень: автоматичні сповіщення про дедлайни, прогрес у виконанні завдань, необхідні дії, щоб команди могли залишатися в курсі змін.
7. Мобільна версія: кросплатформний мобільний додаток для зручного доступу до системи з мобільних пристроїв, планшетів.
8. Ролі та права доступу: гнучка система керування правами доступу для різних ролей (адміністратор, менеджер, виконавець).
9. Захист даних: система зберігання даних відповідно до стандартів безпеки (шифрування, автентифікація) та дотримання вимог GDPR.

Команда проєкту:

- Керівник проєкту: відповідає за загальне управління проєктом, узгодження вимог замовника, контроль термінів та координацію командної роботи.
- Аналітики: займаються збором вимог від кінцевих користувачів, розробкою специфікацій та функціоналу.
- Розробники: програмісти, що працюють над реалізацією системи, поділені на фронтенд і бекенд команди.
- Тестувальники: відповідальні за забезпечення якості продукту, тестування функціоналу, виявлення багів та збоїв у роботі системи.
- Дизайнери: розробляють користувацький інтерфейс, роблять акцент на зручності використання системи.
- DevOps-інженери: Забезпечують розгортання і підтримку інфраструктури проєкту, хмарні рішення, автоматизацію CI/CD.
- Фахівці з безпеки: працюють над тим, щоб система відповідала стандартам інформаційної безпеки.

Ключові етапи проєкту:

1. Етап планування:
    - Аналіз ринку конкурентів.
    - Визначення вимог і розробка технічного завдання.
    - Складання календарного плану розробки.
2. Етап розробки:
    - Створення прототипу системи управління проєктами.
    - Реалізація базових функцій (створення проєктів, завдань, дашборд).
    - Інтеграція з зовнішніми сервісами та платформами.
3. Етап тестування:
    - Проведення внутрішнього тестування функціоналу.
    - Виправлення помилок, оптимізація системи.
    - Тестування продуктивності та безпеки.
4. Етап запуску:
    - Публічний реліз системи в хмарі.
    - Впровадження серед перших користувачів та збір зворотного зв’язку.

   - Навчання та підтримка клієнтів.
5. Етап супроводу:
   - Технічна підтримка, розв'язання проблем користувачів.
   - Регулярні оновлення та додавання нових функцій відповідно до зворотного зв'язку.

Очікувані ризики:

1. Технічні ризики: збої в хмарному середовищі, проблеми з масштабуванням під навантаженням.
2. Фінансові ризики: перевищення бюджету через затримки у розробці або потребу в додаткових ресурсах.
3. Юридичні ризики: проблеми з відповідністю вимогам GDPR або іншим регуляторним актам.
4. Ризики кібербезпеки: потенційні атаки на сервери або злом користувацьких акаунтів.

Очікувані результати:

- Створення конкурентоздатної системи управління проєктами з широким функціоналом для малого і середнього бізнесу.
- Успішний запуск на ринку з подальшою підтримкою та розвитком платформи.
- Залучення перших 100 компаній-користувачів протягом першого року.

Цей фіктивний проєкт демонструє всі ключові етапи, ризики та виклики, з яким

Завдання 2: Розробка плану управління ризиками

Опис: на основі ризиків, виявлених у першому завданні.

Завдання:

- Розробіть план управління ризиками, в якому для кожного ризику визначте:
  - Стратегію управління (усунення, зменшення, перенесення, прийняття).
  - Дії, які потрібно вжити для реалізації стратегії.
  - Відповідальних осіб за управління ризиками.

Завдання 3: Сценарії ризиків

Опис: студенти працюють в групах.

Завдання:

- Розробіть три різні сценарії ризиків для обраного IT-проекту.
- Для кожного сценарію опишіть можливі наслідки для проекту та запропонуйте шляхи їх уникнення або пом'якшення.

Завдання 4: Оцінка ризиків

Опис: використовуючи методи оцінки ризиків.

Завдання:

- Оберіть один з ризиків, виявлених у завданні 1, і проведіть більш детальну оцінку.
- Використайте матрицю ризиків для візуалізації ймовірності та впливу ризику.
- Визначте, чи слід вживати заходів для управління цим ризиком.

Завдання 5: Презентація управлінської стратегії

Опис: кожна група студентів представляє свій проект.

Завдання:

- Підготуйте коротку презентацію (5-7 хвилин) про ваш проект, включаючи аналіз ризиків, план управління ризиками та обрані стратегії.
- Обговоріть, як ви плануєте моніторити ризики протягом реалізації проекту.

Тестові питання

1. *Який з наступних ризиків є типовим для IT-проектів?*

a) Зміна законодавства
b) Витік інформаці
c) Технічні збої
d) Усі вищезгадан

2. *Який з методів є найбільш поширеним для ідентифікації ризиків?*

a) SWOT-аналіз
b) Ризиковий реєстр
c) Бенчмаркінг
d) Дерево рішень

3. *Яка з наведених стратегій управління ризиками полягає в перенесенні ризику на іншу сторону?*

a) Уникнення
b) Прийняття
c) Зменшення
d) Перенесення

4**.** *Який етап управління ризиками включає визначення відповідальних осіб?*

a) Ідентифікація
b) Оцінка
c) Планування

d) Моніторинг

5. *Яка з наступних метрик може використовуватися для оцінки ризиків?*

a) ROI (повернення інвестицій)
b) PERT (метод оцінки і перегляду програми)
c) KPI (ключові показники ефективності)
d) Точка беззбитковості

Тема 7. Ризики в управлінні IT інфраструктурою

Метою заняття на тему «Ризики в управлінні IT інфраструктурою» є ознайомлення студентів із основними ризиками, які виникають при управлінні IT інфраструктурою, а також розвиток навичок і знань, необхідних для їх ідентифікації, оцінки та управління.

Завдання:

1. Розуміння типів ризиків
2. Оцінка впливу ризиків
3. Розробка стратегій управління ризиками
4. Вивчення методів моніторингу ризиків
5. Аналіз реальних випадків
6. Розвиток критичного мислення:

Завдяки цим цілям студенти отримають комплексне уявлення про ризики в управлінні IT інфраструктурою та набудуть практичних навичок для їх ефективного управління, що є важливим аспектом у сучасному бізнес-середовищі.

Питання для обговорення

1. Які основні ризики виникають при управлінні IT інфраструктурою в організації?
2. Які методи ідентифікації ризиків є найефективнішими в контексті IT інфраструктури?
3. Як оцінювати ймовірність виникнення та потенційний вплив ризиків?
4. Які стратегії управління ризиками є найбільш доцільними для IT інфраструктури?

5. Як впливають зміни в технологічному середовищі на ризики IT інфраструктури?
6. Які виклики можуть виникати при впровадженні стратегій управління ризиками?
7. Яка роль комунікації у управлінні ризиками в IT інфраструктурі?
8. Які новітні тенденції у сфері кібербезпеки слід враховувати при управлінні ризиками IT інфраструктури?
9. Як проводити моніторинг ризиків у процесі управління IT інфраструктурою?
10. Які уроки можна винести з реальних випадків ризиків, що виникали в організаціях?

Завдання

Завдання 1: Ідентифікація ризиків

Опис: студентам надається опис фіктивної IT-інфраструктури, наприклад, компанії, що використовує хмарні технології, локальні сервери та мобільні пристрої.

Завдання:

- ідентифікуйте не менше п’яти ризиків, які можуть виникнути у цій інфраструктурі4
- для кожного ризику вкажіть можливі наслідки для бізнесу.

Опис фіктивної IT-інфраструктури компанії

Загальна інформація про компанію

Назва компанії: TechInnovate
Тип бізнесу: Розробка програмного забезпечення та надання IT-послуг
Розмір: Середня компанія з 200 працівниками
Місцезнаходження: Офіси в Україні та США
IT-інфраструктура

1. Хмарні технології:
    - Хостинг: Компанія використовує хмарні сервіси Amazon Web Services (AWS) для розміщення своїх веб-додатків та баз даних. Це забезпечує масштабованість та високу доступність.
    - Програмне забезпечення як послуга (SaaS): Використання Google Workspace для колективної роботи, електронної пошти та обміну файлами.
    - Зберігання даних: Використання хмарних рішень для резервного копіювання даних, включаючи рішення на основі Google Drive та Dropbox.
2. Локальні сервери:
    - Сервери: Компанія має локальні сервери для зберігання чутливих даних, таких як фінансова інформація та особисті дані клієнтів. Ці сервери розташовані в закритій серверній кімнаті з контролем доступу.
    - Програмне забезпечення: Використання внутрішніх систем для управління проектами, таких як Jira, а також власні розроблені програми для обліку робочого часу та витрат.
3. Мобільні пристрої:

- Смартфони та планшети: Співробітники компанії забезпечені смартфонами для доступу до корпоративних ресурсів, комунікаційних платформ (Slack, Microsoft Teams) та бізнес-додатків.
- Безпека мобільних пристроїв: Впровадження політик безпеки, таких як шифрування даних на пристроях, використання VPN для підключення до корпоративної мережі та управління мобільними пристроями (MDM) для контролю за доступом.

Архітектура мережі

- Локальна мережа (LAN): Компанія має потужну локальну мережу з Wi-Fi з доступом до серверів та хмарних ресурсів.
- Віртуальна приватна мережа (VPN): Для віддалених працівників налаштована VPN для забезпечення безпечного доступу до внутрішніх ресурсів компанії.

Програмне забезпечення та інструменти

- Управління проектами: Jira та Asana для управління проектами та задачами.
- Контроль версій: GitLab для версійного контролю коду та співпраці між розробниками.
- Клієнтське обслуговування: Використання CRM-системи Salesforce для управління взаємовідносинами з клієнтами.

Завдання 2: Оцінка ризиків

Опис: На основі ризиків, виявлених у першому завданні.

Завдання:

- оцініть ймовірність виникнення кожного ризику та його потенційний вплив на бізнес-процеси.
- використайте матрицю ризиків для візуалізації оцінок.

Завдання 3: Розробка плану управління ризиками

Опис: Використовуючи результати оцінки ризиків.

Завдання:

- Розробіть план управління ризиками для виявлених ризиків, в якому визначте стратегії для їх усунення, зменшення, перенесення або прийняття.
- Вкажіть, хто буде відповідальним за реалізацію кожної стратегії.

Результати оцінки ризиків для IT-інфраструктури компанії TechInnovate

Виявлені ризики

Кіберзагрози:

Вид: Зловмисне програмне забезпечення (Malware)
Ймовірність: Висока
Вплив: Високий (може призвести до втрати даних та фінансових витрат)

Технічні збої:

Вид: Вимкнення електроенергії або збої в роботі серверів
Ймовірність: Середня
Вплив: Високий (втрата доступу до критично важливих систем)

Витік даних:

Вид: Неправомірний доступ до чутливих даних через неналежний контроль
Ймовірність: Середня
Вплив: Високий (репутаційні втрати та юридичні наслідки)

Людський фактор:

Вид: Помилки співробітників, що можуть призвести до втрати даних або порушення безпеки
Ймовірність: Висока
Вплив: Середній (може спричинити тимчасові затримки в роботі)
Недостатня підготовленість до надзвичайних ситуацій:

Вид: Відсутність плану відновлення після катастрофи
Ймовірність: Висока
Вплив: Високий (затримки у відновленні бізнесу)

Завдання 4: Сценарії ризиків

Опис: Студенти працюють у групах.

Завдання:

- Розробіть три різні сценарії ризиків для обраної IT-інфраструктури.
- Для кожного сценарію опишіть можливі наслідки та заплануйте дії для пом'якшення ризику.

Опис IT-інфраструктури компанії TechInnovate

1. Загальна структура
   - Тип бізнесу: Розробка програмного забезпечення, консалтинг, технічна підтримка.
   - Розмір: Середня компанія з 200 працівниками, що працюють в офісі та віддалено.
   - Географія: Офіси в Україні та США, з можливістю віддаленої роботи.
2. Компоненти IT-інфраструктури

a. Хмарні технології
   - Провайдери: Використання Amazon Web Services (AWS) для хостингу веб-додатків і баз даних, а також Google Cloud Platform (GCP) для аналітики та зберігання даних.
   - Сервіси:
     - Хостинг: Веб-сервери для розміщення корпоративного сайту та додатків.
     - Бази даних: Використання Amazon RDS (Relational Database Service) для управління даними.
     - Резервне копіювання: Автоматизовані системи резервного копіювання на AWS S3.

b. Локальні сервери
   - Сервери: Наявність локальних серверів для зберігання чутливих даних та внутрішніх систем.
     - Програмне забезпечення: Внутрішні системи для управління проектами (Jira), фінансами (QuickBooks) та комунікаціями (Microsoft Teams).
     - Системи безпеки: Використання міжмережевих екранів (firewalls) та антивірусного програмного забезпечення для захисту локальних систем.

c. Мобільні пристрої
   - Пристрої: Співробітники використовують смартфони (iOS та Android) для доступу до корпоративних ресурсів.
   - Захист: Впровадження політик безпеки для мобільних пристроїв, включаючи шифрування даних та використання VPN для підключення до корпоративної мережі.

d. Мережева інфраструктура
   - Локальна мережа (LAN): Сучасні маршрутизатори та комутатори для забезпечення швидкого та безперебійного з'єднання в офісі.
   - Wi-Fi: Безпечна бездротова мережа з обмеженим доступом для гостей та клієнтів.
   - Віртуальна приватна мережа (VPN): Залишає можливість безпечного віддаленого доступу до внутрішніх систем.

3. Програмне забезпечення та інструменти
   - Управління проектами: Використання Jira для планування, відстеження та звітування про проекти.
   - Кодова база: GitLab для контролю версій, управління кодом та колективної роботи над проектами.
   - Комунікаційні інструменти: Microsoft Teams та Slack для внутрішньої комунікації та обміну інформацією між командами.
4. Безпека та управління ризиками
   - Політики безпеки: Внутрішні політики щодо управління доступом, управління паролями та безпеки даних.
   - Навчання персоналу: Регулярні тренінги для співробітників з кібербезпеки та управління ризиками.
   - Моніторинг: Впровадження систем моніторингу безпеки для виявлення та реагування на загрози в реальному часі.
5. Інфраструктура підтримки
   - Технічна підтримка: Команда з IT-підтримки, що забезпечує вирішення проблем з обладнанням та програмним забезпеченням.
   - План відновлення: Наявність документації та процедур для відновлення систем у разі збою або атаки.

Завдання 5: Дослідження справжнього випадку

Опис: студенти обирають реальний випадок IT-компанії, що стикалася з ризиками в управлінні інфраструктурою.

Завдання:

- Підготуйте доповідь про цей випадок, вказуючи типи ризиків, які виникли, і способи їх управління.
- Які висновки та уроки можна винести з цього випадку?

Завдання 6: Презентація результатів

Опис: кожна група студентів представляє свої результати.

Завдання:

- Підготуйте коротку презентацію (5-7 хвилин) про вашу роботу, включаючи аналіз ризиків, оцінку та план управління ризиками.
- Обговоріть, як ви плануєте моніторити ризики протягом управління IT інфраструктурою.

Тема 8. Оцінка та управління ризиками кібербезпеки

Метою заняття на тему «Оцінка та управління ризиками кібербезпеки» Є забезпечення систематичний підхід до виявлення, аналізу та зменшення потенційних загроз для інформаційних систем і даних організації. Це важливий етап у створенні безпечної IT-інфраструктури, яка може захистити компанію від різних кіберзагроз, включаючи зловмисне програмне забезпечення, фішинг, атаки на сервери та інші види кібернетичних атак.

Завдання:

1. Виявлення ризиків

2. Оцінка впливу
3. Розробка стратегій управління
4. Моніторинг і відстеження
5. Навчання персоналу

Питання для обговорення

1. Які основні типи кіберзагроз, з якими може стикатися наша організація?
2. Як можна ефективно ідентифікувати вразливості в нашій IT-інфраструктурі?
3. Які критерії слід використовувати для оцінки потенційного впливу кіберзагроз на бізнес?
4. Як вплив кіберінцидентів може відрізнятися залежно від типу даних, що зберігаються?
5. Які заходи безпеки є найефективнішими для зменшення ризиків кібербезпеки?
6. Як визначити пріоритети для впровадження заходів управління ризиками?
7. Які інструменти моніторингу та реагування на інциденти ви вважаєте найкращими для нашої організації?
8. Як можна забезпечити швидке реагування на кіберінциденти?
9. Яку роль відіграє навчання персоналу в управлінні ризиками кібербезпеки?
10. Які теми навчання є критично важливими для підвищення обізнаності?

Завдання

Завдання 1: Оцінка ризиків

Опис: розробіть матрицю ризиків для визначення потенційних загроз і їх впливу на бізнес.

Кроки:

1. Ідентифікуйте 5–10 потенційних кіберзагроз.
2. Оцініть ймовірність та вплив кожної загрози (високий, середній, низький).
3. Складіть матрицю ризиків та надайте рекомендації щодо управління ними.

Завдання 2: Розробка плану управління ризиками

Опис: створіть план управління ризиками кібербезпеки для вашої організації.

Кроки:

1. Визначте цілі та обсяги управління ризиками.
2. Розробіть стратегії для зменшення ризиків (наприклад, технологічні, організаційні).
3. Опишіть процедури моніторингу та звітності.

Завдання 3: Симуляція кіберінциденту

Опис: організуйте симуляцію кіберінциденту для вашої організації, щоб перевірити готовність до реагування.

Кроки:

1. Створіть сценарій кіберінциденту (наприклад, фішинг або атака DDoS).
2. Проведіть симуляцію та зафіксуйте дії учасників.
3. Напишіть звіт про результати симуляції та рекомендації щодо поліпшення.

Завдання 4: Навчальний матеріал

*Опис***:** розробіть навчальний матеріал для співробітників щодо основ кібербезпеки.

Кроки:

1. Визначте ключові теми, які повинні бути висвітлені (фішинг, паролі, безпека мобільних пристроїв).
2. Створіть презентацію або інший формат навчального матеріалу.
3. Проведіть навчання та оцініть ефективність за допомогою тестування.

Завдання 5: Аналіз економічних ризиків

Опис: виконайте аналіз економічних ризиків для вибраної IT-інфраструктури компанії.

Кроки:

1. Визначте основні компоненти IT-інфраструктури (системи, технології, послуги).
2. Ідентифікуйте можливі економічні ризики (зміни цін на послуги, витрати на обслуговування, коливання валюти).
3. Оцініть вплив цих ризиків на загальний бюджет компанії.

Завдання 6: Розробка стратегії управління витратами

Опис: розробіть стратегію управління витратами в IT-інфраструктурі компанії.

Кроки:

1. Проаналізуйте поточні витрати на IT (обладнання, програмне забезпечення, обслуговування).
2. Визначте можливості для оптимізації витрат (перегляд контрактів, заміна застарілого обладнання).
3. Напишіть звіт з рекомендаціями щодо зменшення витрат.

Завдання 7: Оцінка фінансової стійкості

Опис: Оцініть фінансову стійкість компанії в умовах змін на ринку IT.

Кроки:

1. Зберіть дані про доходи та витрати компанії за останні кілька років.
2. Визначте ключові показники фінансової стійкості (рентабельність, ліквідність).
3. Напишіть аналіз можливих економічних ризиків, пов'язаних зі змінами в технологічному середовищі.

Завдання 8: Вплив технологічних змін на бюджет

Опис: Проаналізуйте, як технологічні зміни можуть вплинути на бюджет IT-компанії.

Кроки:

1. Ідентифікуйте ключові технологічні зміни (перехід на хмарні рішення, нові програмні платформи).
2. Оцініть потенційні витрати на впровадження цих змін (інвестиції, навчання персоналу).
3. Напишіть звіт про те, як ці зміни можуть вплинути на фінансовий стан компанії.

Тестові питання

1. *Який з наступних варіантів є прикладом економічного ризику в IT-інфраструктурі?*

a)) Атака шкідливого програмного забезпечення
b) Зміна цін на програмне забезпечення
c) Погіршення якості коду
d) Витік конфіденційних даних

2. *Який з наведених методів є найбільш ефективним для управління витратами на IT?*

a) Збільшення кількості співробітників
b) Перегляд контрактів з постачальниками
c) Впровадження нових технологій без аналізу витрат
d) Ігнорування зміни ринку

3. *Який показник найкраще характеризує фінансову стійкість компанії?*

a) Кількість користувачів продукту
b) Рентабельність
c) Технічні характеристики обладнання
d) Кількість інвестицій у нові технології

4. *Яка з наведених стратегій може допомогти зменшити економічні ризики в IT?*

a) Збільшення витрат на рекламу
b) Диверсифікація постачальників
c) Зменшення кількості проектів
d) Використання застарілих технологій

5. *Який з факторів не є економічним ризиком для IT-компанії?*

a) Зміни в законодавстві
b) Невдача проекту через перевищення бюджету
c) Витік даних клієнтів
d) Конкуренція на ринку

Тема 9. Сучасні тенденції та перспективи в управлінні ризиками IT підприємств

Метою заняття на тему: **"Сучасні тенденції та перспективи в управлінні ризиками IT підприємств"**є дослідження та аналіз новітніх тенденцій в управлінні ризиками IT підприємств, а також оцінка їхнього впливу на поточні бізнес-процеси та перспективи розвитку компаній. Студенти повинні зрозуміти, як сучасні інструменти та стратегії можуть допомогти в ідентифікації, оцінці та мінімізації ризиків в умовах швидко мінливого технологічного середовища. Особлива увага приділяється впровадженню автоматизації, штучного інтелекту, хмарних рішень і

кібербезпеки, а також впливу глобальних тенденцій, таких як цифрова трансформація та віддалена робота, на управління ризиками ІТ.

Завдання:

1. Ідентифікація ключових ризиків ІТ підприємств.
2. Аналіз сучасних трендів у сфері кібербезпеки та управління ризиками.
3. Оцінка нових технологій (ШІ, блокчейн) для прогнозування та запобігання ризикам.
4. Розробка стратегій мінімізації ризиків у хмарних середовищах та віддаленій роботі.
5. Ознайомлення з нормативними вимогами та міжнародними стандартами інформаційної безпеки.

Питання для обговорення

1. Які основні сучасні тенденції впливають на управління ризиками в ІТ?
2. Як новітні технології (штучний інтелект, машинне навчання, автоматизація) змінюють підходи до управління ризиками?
3. Як впровадження хмарних технологій впливає на управління ІТ-ризиками?
4. Які ризики виникають при переході на хмарні рішення, і як їх можна мінімізувати?
5. Яку роль відіграє кібербезпека в сучасному управлінні ІТ-ризиками?
6. Як нові кіберзагрози змінюють підходи до безпеки ІТ-інфраструктури?
7. Як цифрова трансформація та автоматизація бізнес-процесів впливають на ризики ІТ-підприємств?
8. Чи є ризик збільшення залежності від технологій? Які способи управління цим ризиком?
9. Які переваги та недоліки використання штучного інтелекту в управлінні ризиками ІТ?
10. Наскільки автоматизовані системи можуть бути ефективнішими за людський контроль?

Завдання

Завдання 1: Дослідження сучасних тенденцій в управлінні ІТ-ризиками

Опис: проведіть аналіз сучасних тенденцій в управлінні ІТ-ризиками у глобальному масштабі.

Кроки:

1. Виберіть три сучасні тенденції (наприклад, штучний інтелект в управлінні ризиками, хмарні рішення, автоматизація).

2. Опишіть, як кожна з цих тенденцій впливає на управління ризиками в IT-підприємствах.
3. Оцініть можливі переваги та виклики для бізнесу при застосуванні цих тенденцій.

Завдання 2: Оцінка ризиків впровадження хмарних технологій

Опис: оцініть основні ризики, пов'язані з переходом компанії на хмарні рішення.

Кроки:

1. Виберіть одну або декілька IT-систем компанії, які можуть бути переведені на хмарну платформу.
2. Визначте ризики, що виникають під час цього процесу (наприклад, питання безпеки, затримки в міграції, зміна вартості).
3. Запропонуйте стратегії для мінімізації виявлених ризиків.

Завдання 3: Розробка стратегії управління кіберризиками

Опис: розробіть стратегію управління кіберризиками для компанії, що використовує хмарні сервіси, локальні сервери та мобільні пристрої.

Кроки:

1. Ідентифікуйте основні вразливості та загрози для IT-інфраструктури компанії.
2. Створіть план дій для мінімізації кіберризиків, зокрема запропонуйте використання сучасних інструментів кібербезпеки.
3. Опишіть способи моніторингу та реагування на кіберзагрози.

Завдання 4: Оцінка впливу цифрової трансформації на IT-інфраструктуру

Опис: оцініть, як цифрова трансформація може вплинути на ризики та витрати компанії.

Кроки:

1. Проаналізуйте можливі зміни, що можуть виникнути внаслідок впровадження цифрових технологій.
2. Оцініть ризики, пов'язані з адаптацією до нових інструментів (навчання співробітників, сумісність систем, додаткові витрати).
3. Розробіть рекомендації щодо ефективного управління цими ризиками.

Завдання 5: Розробка плану дій на випадок технічних збоїв

Опис: розробіть план дій для мінімізації економічних втрат у випадку технічних збоїв в IT-інфраструктурі.
Кроки:

1. Виберіть ключові компоненти IT-інфраструктури (сервери, мережі, хмарні сервіси).
2. Визначте ризики, пов'язані з можливими технічними збоями.
3. Розробіть план аварійного відновлення та економічну оцінку потенційних втрат.

Тестові завдання

1. *Яка з наведених технологій найбільше впливає на автоматизацію управління IT-рисками?*
   a) Віртуальна реальність
   b) Штучний інтелект
   c) Графічний дизайн
   d) Веб-розробка
2. *Який з факторів є основним ризиком для компаній, що переходять на хмарні технології?*

a) Висока вартість обладнання
b) Проблеми з безпекою даних
c) Недостатня кількість персоналу
d) Застарілі програмні рішення

3. *Яка з наведених технологій є однією з основних тенденцій для підвищення безпеки в управлінні IT-інфраструктурою?*

a) Блокчейн
b) Розширена реальність
c) Доповнена реальність
d) Гейміфікація

4. *Яке основне завдання цифрової трансформації в контексті управління IT-рисками?*

a) Збільшення кількості співробітників
b) Мінімізація технічних та кіберризиків
c) Підвищення витрат на технології
d) Оптимізація документації

5. *Який основний ризик виникає внаслідок використання мобільних пристроїв в корпоративній IT-інфраструктурі?*

a) Низька швидкість передачі даних
b) Підвищений ризик витоку даних
c) Недоступність мобільних додатків
d) Висока вартість обслуговування

Рекомендована література

1. Гранатуров В.М., Литовченко І.В., Харічков С.К. Аналіз підприємницьких ризиків: проблеми визначення, класифікації та кількісні оцінки : монографія. Одеса : Ін-т проблем ринку та екон.-екол. досліджень НАН України, 2003. 164 с.
2. Бондар О. В. Ситуаційний менеджмент : навч. посіб. 2-ге вид., перероб та доповн. Київ : Центр учбової літератури, 2012. 388 с.
3. Чуприна І. В. Поняття та класифікація ризиків в підприємницькій діяльності. Збірник наукових праць ВНАУ. Сер. Економічні науки. 2012. №4(70). С. 187-194.
4. Донець Л.І., Шепеленко О.В., Баранцева С.М., Сергєєва О.В., Веремейчик О.Ф. Обґрунтування господарських рішень та оцінювання ризиків : навч. посіб. / за заг. ред. Донець Л.І. Київ : Центр учбової літератури, 2012. 472 с.
5. Вербіцька І. І. Ризик-менеджмент як сучасна система управління ризиками підприємницьких структур. Сталий розвиток економіки. 2013. № 5(22). С. 282-291.
6. Вишневська О. А. Підприємницький ризик в управлінні конкурентоспроможністю підприємства. Економіка і суспільство. 2016. № 7. С. 232- 237.
7. Олійник Л.В., Скідченко А.О. Аналіз шляхів подолання підприємницьких ризиків на прикладі ТОВ «НОВА ПОШТА». Економіка і організація управління. 2020. № 2(38). С. 68–80
8. ІТ-маркетинг : навчальний посібник / С. А. Горбаченко, О. В. Дикий, О. М. Кібік, Н. А. Клєвцєвич, Н. С. Разінкін ; Нац. ун-т «Одеська юрид. академія». Одеса : Видавництво «Юридика», 2024. 218 с.
9. Бізнес-планування : навч. посіб./ Л. В. Боденчук, С. А. Горбаченко, Н. А. Клєвцєвич, І. В. Ліганенко. О: Фенікс. 2022. 272 с
10. Горбаченко С.А. Особливості впровадження управлінських інновацій суб'єктами підприємництва ІТ-сфери. Європейський вектор економічного розвитку. 2021. №1 (30). С. 18-24

Іноземні публікації

1. Aven, Terje Foundations of Risk Analysis: A Knowledge and Decision-Oriented Perspective Видання: John Wiley & Sons, 2003, Чичестер, Велика Британія. 224 с.
2. Hubbard, Douglas W**.** *The Failure of Risk Management:* Why It's Broken and How to Fix It Видання: John Wiley & Sons, 2009, Нью-Йорк. 304 с.

3. *Hopkin, Paul* Fundamentals of Risk Management: Understanding, Evaluating, and Implementing Effective Risk Management Видання: Kogan Page, 2017, Лондон. 488 с.
4. Kaplan, Robert S., Mikes, Anette Risk Management – The Revealing Hand *Стаття у:* Journal of Applied Corporate Finance, Vol. 26, No. 1, 2014, С.8-20.
5. Jorion, Philippe Value at Risk: The New Benchmark for Managing Financial Risk Видання: McGraw-Hill, 3-є видання, 2006, Нью-Йорк. 600 с.
6. ISO 31000:2018 Risk Management – Guidelines Міжнародна організація зі стандартизації (ISO), 2018, Женева. 16 с.
7. Haimes, Yacov Risk Modeling, Assessment, and Management Видання: John Wiley & Sons, 4-те видання, 2015, Нью-Йорк. 720 с.
8. Flage, Roger, et al. Risk Assessment in Engineering: Principles, System Representation, and Risk Criteria *Видання:* Springer, 2020, Швейцарія. 276 с.

База даних Scopus –

1. Effectiveness of Emergency Management in Public Organizations: A Paradigm from a European Civil Protection Mechanism
   Authors: Stavros Kalogiannidis, Dimitrios Kalfas, Olympia Papaevangelou, Fotios Chatzitheodoridis
   Published: *Journal of Risk Analysis and Crisis Response*, Vol. 14, No. 3, 2024
   Pages: Available online Journal of Risk Analysis and Crisis Response
2. **Fire Risk Model for Fires in Ro-Ro Ship Spaces**
   Authors: Sixten Dahlbom, Stina Andersson, Eric De Carvalho, Leon Lewandowski, Franz Evegren
   Published: *Journal of Risk Analysis and Crisis Response*, Vol. 14, No. 3, 2024
   Pages: Available online Journal of Risk Analysis and Crisis Response
3. Risk and Decision Analysis
   This journal covers topics related to mathematical models and decision-making under uncertainty. It is indexed in *Scopus* and publishes articles focused on risk management strategies, resilience, and forecasting in diverse sectors.
   Published by IOS Press
   For more details, visit the IOS Press Journal Page.

Навчально-методичне видання

Клєвцєвич Н.А.

ПРАКТИКУМ

з дисципліни

«АНАЛІЗ РИЗИКІВ ІТ-ПІДПРИЄМСТВ»

для студентів ІІІ курсу всіх форми навчання

спеціальності 073 «Менеджмент»

ОП «ІТ-менеджмент та маркетинг»

В авторській редакції