**Міністерство освіти і науки України**

**Національний університет харчових технологій**

Кафедра інформаційних технологій, штучного інтелекту та кібербезпеки

**ЛАБОРАТОРНА РОБОТА № 7**

з дисципліни «Менеджмент розробки інноваційних проектів»

на тему: «УПРАВЛІННЯ РИЗИКАМИ В ІННОВАЦІЙНИХ ПРОЕКТАХ»

Виконав: Студент I курсу  
групи КН-1-3М

Кучерявий М. В.

Перевірив:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Київ — 2025**

**Визначення ризиків, критерії класифікації проектних ризиків**

**Ризик проєкту** — це подія або умова, яка, у разі настання, може мати позитивний або негативний вплив на одну або кілька цілей проєкту (зокрема, на терміни, вартість, якість або обсяг робіт).

**За джерелом походження** ризики поділяються на внутрішні та зовнішні. Внутрішні виникають у межах самого проєкту та можуть бути пов’язані з управлінськими помилками, нестачею ресурсів, технічними труднощами або проблемами в команді. Зовнішні ризики обумовлені факторами, що не залежать від команди проєкту, наприклад: зміни в законодавстві, політична нестабільність, економічна криза, форс-мажори.

**За впливом на проєкт** ризики поділяють на негативні та позитивні. Негативні ризики, або загрози, можуть зашкодити досягненню цілей проєкту, призвести до перевищення бюджету або затримки виконання. Позитивні ризики, або можливості, навпаки, відкривають нові перспективи, можуть сприяти економії ресурсів або покращенню результатів.

**За характером виникнення** ризики класифікуються як відомі (інтуїтивні) та приховані (невідомі). Відомі ризики — це ті, що базуються на попередньому досвіді або аналізі та легко передбачаються. Приховані ризики важко ідентифікувати, вони часто проявляються несподівано й потребують ретельного моніторингу.

**За ймовірністю настання** ризики поділяють на малоймовірні, імовірні та майже гарантовані. Ця класифікація допомагає визначити, наскільки реалістичною є поява певного ризику та які ресурси потрібно закладати на його подолання або запобігання.

**За масштабом впливу** виділяють ризики з низьким, середнім і високим рівнем впливу. Низький рівень означає незначний вплив на результати проєкту, середній — потребує корекційного втручання, а високий рівень загрожує серйозними наслідками, зокрема зупинкою реалізації проєкту.

**За сферою впливу** ризики бувають технічними, фінансовими, юридичними, організаційними та тимчасовими. Технічні пов’язані з помилками у технологіях чи обладнанні, фінансові — з нестабільністю бюджету, юридичні — з правовими аспектами, організаційні — з людським фактором, а тимчасові — з порушенням термінів або графіку.

**Цілі і процеси управління ризиками в інноваційних проектах**

**Управління ризиками в інноваційних проєктах** має на меті зменшення невизначеності та забезпечення стабільної реалізації новаторських ідей. Основною ціллю є виявлення потенційних загроз і можливостей, які можуть вплинути на досягнення цілей проєкту. Це особливо важливо в умовах інновацій, де ризики часто виникають через новизну технологій, нестабільність ринку чи обмеженість досвіду. Також управління ризиками спрямоване на мінімізацію можливих негативних наслідків, адаптацію проєкту до змін, збереження його інноваційного потенціалу та підтримку обґрунтованого прийняття управлінських рішень.

Процес управління ризиками в інноваційному проєкті починається з **ідентифікації ризиків**. На цьому етапі визначаються всі внутрішні та зовнішні чинники, які можуть загрожувати реалізації проєкту. Особлива увага приділяється таким аспектам, як технічна реалізованість, конкурентне середовище, доступ до фінансування та кадрові ресурси.

Наступним кроком є **аналіз ризиків**, у межах якого оцінюються ймовірність настання кожного ризику та масштаб його впливу. Використовуються якісні й кількісні методи аналізу — наприклад, експертні оцінки, SWOT-аналіз, діаграми впливу, аналіз сценаріїв тощо.

Після аналізу здійснюється **планування заходів реагування на ризики**. Для кожного значущого ризику обирається стратегія: уникнення (повне усунення), зниження (пом’якшення наслідків), перенесення (страхування або передача третій стороні) або прийняття (готовність до реалізації ризику з розробкою резервного плану).

Важливою складовою є **моніторинг і контроль ризиків**, що передбачає постійне спостереження за реалізацією проєкту, оновлення ризик-реєстру, виявлення нових ризиків та коригування планів реагування. В умовах інноваційної діяльності цей процес має бути гнучким і оперативним.

Останнім етапом є **документування та комунікація**. Уся інформація щодо виявлених ризиків, їх аналізу, планів реагування та результатів має бути зафіксована у відповідних документах і регулярно доводитися до ключових учасників проєкту. Це сприяє прозорості, підвищенню відповідальності та ефективнішому прийняттю рішень.

**Якісні методи оцінки ризиків (перелік і короткий опис )**

Якісні методи оцінки ризиків використовуються на ранніх етапах управління проєктом для виявлення, опису та попередньої оцінки потенційних загроз без використання точних числових даних. Одним із найпоширеніших методів є **SWOT-аналіз**, який полягає в оцінюванні сильних і слабких сторін проєкту, а також зовнішніх можливостей і загроз. Цей підхід дозволяє комплексно проаналізувати середовище проєкту та виявити потенційні ризики.

**Метод експертних оцінок** передбачає залучення досвідчених фахівців, які на основі власного досвіду формулюють можливі ризики та оцінюють їхній вплив. Подібним за змістом є **метод Delphi**, який полягає в багатократному анонімному опитуванні групи експертів із подальшим узгодженням їхніх відповідей до досягнення консенсусу.

**Мозковий штурм** — це групова сесія генерації ідей, під час якої учасники висувають усі можливі ризики без критики, що дозволяє зібрати широкий спектр припущень. Доповнити цю роботу можна за допомогою **інтерв’ю та анкетування** із членами команди, керівниками або замовниками проєкту, що допомагає зібрати індивідуальні погляди на можливі ризики.

Практичним інструментом є **контрольні списки ризиків (checklists)**, які складаються на основі досвіду попередніх проєктів і дають змогу швидко перевірити наявність типових загроз. Ще одним корисним методом є **аналіз причин і наслідків**, зокрема у формі діаграми Ішікави (риб’яча кістка), яка допомагає системно визначити, які фактори можуть призвести до певного ризику.

**Аналіз припущень** дозволяє перевірити правильність і стабільність гіпотез, що лежать в основі планування проєкту. Якщо припущення є ненадійними або неперевіреними, це може свідчити про наявність ризику. У свою чергу, **аналіз сценаріїв** допомагає змоделювати можливі варіанти розвитку подій, щоб передбачити наслідки реалізації тих чи інших ризиків.

Ще один метод — **SWIFT-аналіз (Structured What-If Technique)**, який полягає в послідовному формулюванні запитань типу «А що, як...?» з метою виявлення прихованих або недооцінених ризиків. Цей підхід зручний для обговорення потенційних ситуацій і розробки стратегій реагування.

Загалом, якісні методи не дають точної кількісної оцінки, але є надзвичайно корисними для початкового розуміння ризиків та формування основи для подальшого, більш глибокого аналізу.

**Кількісні методи оцінки ризиків (перелік і короткий опис )**

Кількісні методи оцінки ризиків дають змогу обчислити можливий вплив ризиків у числовій формі, що особливо важливо для ухвалення обґрунтованих управлінських рішень. Один із найпоширеніших методів — **аналіз очікуваної грошової вартості (EMV)**. Він передбачає множення ймовірності виникнення ризику на можливий фінансовий збиток або прибуток. Таким чином можна порівнювати ризики за величиною очікуваних втрат або вигоди.

**Дерева рішень** використовуються для візуалізації рішень і наслідків у вигляді дерева з різними гілками. Кожне відгалуження показує варіанти подій, імовірності та грошові наслідки, що дозволяє обрати оптимальне рішення на основі економічної доцільності.

**Аналіз чутливості** визначає, які змінні найбільше впливають на результат проєкту. Змінюючи окремі параметри (наприклад, вартість, тривалість робіт або ресурси), можна виявити ті, які є найбільш критичними для успіху проєкту.

**Аналіз сценаріїв** дає змогу оцінити результати проєкту в різних можливих умовах: оптимістичних, песимістичних і базових. Це допомагає підготуватися до різних ситуацій і оцінити вплив певних ризиків залежно від розвитку подій.

Найбільш глибокий інструмент — **метод Монте-Карло**, який використовує комп’ютерне моделювання з численними випадковими варіаціями параметрів. У результаті формується статистичний розподіл результатів проєкту, що дозволяє побачити ймовірність досягнення певних цілей.

**Факторний аналіз ризику** полягає в оцінюванні окремих факторів, що впливають на ризики, з визначенням їхньої ваги в загальному ризику проєкту. Метод може поєднуватися з експертними оцінками для формування більш точного уявлення про структуру ризиків.

**Індекси ризику** дозволяють обчислити інтегральний показник для кожного ризику, враховуючи ймовірність і рівень впливу. Такі індекси можуть бути подані у вигляді шкали чи таблиці, що полегшує пріоритезацію ризиків.

Усі ці методи спрямовані на те, щоб надати кількісні дані про ризики, що допомагає більш точно прогнозувати можливі втрати й оптимізувати рішення в управлінні проєктами.

**Пріоритезація ризиків та застосування принципу Парето**

**Пріоритезація ризиків** — це процес ранжування виявлених ризиків за ступенем їхнього потенційного впливу на проєкт, з урахуванням імовірності настання та серйозності наслідків. Метою є зосередження ресурсів і зусиль на найбільш значущих ризиках, які можуть критично вплинути на терміни, бюджет, якість або досягнення цілей проєкту. Найчастіше для пріоритезації використовують матрицю ризиків, де ризики розміщуються відповідно до їхньої ймовірності та наслідків — від незначних до критичних. Також застосовуються методи бальної оцінки (наприклад, шкала від 1 до 5), на основі яких обчислюється індекс ризику (Risk Priority Number).

Одним із ефективних підходів до пріоритезації є **принцип Парето (правило 80/20)**. Він базується на спостереженні, що приблизно 20% ризиків можуть спричиняти 80% негативних наслідків. Застосування цього принципу дозволяє виділити вузьке коло найбільш небезпечних або критичних ризиків, які потребують першочергової уваги. У практиці управління ризиками це може означати, що замість розпорошення ресурсів на усі ризики, команда зосереджується на кількох найважливіших, обмежуючи вплив більшості потенційних проблем.

Пріоритезація ризиків за принципом Парето допомагає ефективніше управляти часом, бюджетом та зусиллями команди, а також підвищує ймовірність успішного завершення проєкту шляхом зниження загального ризик-профілю.

**Стандарти з управління ризиками**

Існує низка міжнародних та галузевих стандартів, які регламентують управління ризиками і забезпечують уніфіковані підходи до їх ідентифікації, оцінки, контролю та мінімізації. Впровадження таких стандартів дозволяє організаціям систематизувати процес управління ризиками, підвищити його ефективність і забезпечити відповідність міжнародним вимогам.

Одним із найпоширеніших є **ISO 31000 – Risk Management. Principles and Guidelines**. Цей міжнародний стандарт, розроблений Міжнародною організацією зі стандартизації (ISO), встановлює загальні принципи, структуру та процеси управління ризиками. Він універсальний і підходить для будь-яких організацій, незалежно від їх розміру чи сфери діяльності. Основна ідея стандарту — інтеграція управління ризиками у всі управлінські процеси організації.

Специфічним для інформаційної безпеки є стандарт **ISO/IEC 27005**, який доповнює серію ISO/IEC 27000. Він детально описує процеси оцінки та управління ризиками, пов’язаними із захистом інформації та ІТ-інфраструктури.

Управління ризиками в проєктній діяльності регламентується у посібнику **PMBOK (Project Management Body of Knowledge)**, розробленому інститутом PMI. Він містить розділи, присвячені плануванню, ідентифікації, аналізу, реагуванню та моніторингу ризиків у проєктах.

Інтегрований підхід до корпоративного управління ризиками пропонує **COSO ERM Framework** — рамковий документ, розроблений Комітетом організацій-спонсорів Комісії Тредвея (COSO). Цей стандарт зосереджується на стратегічних, фінансових та репутаційних ризиках, допомагаючи організаціям підвищувати ефективність і прозорість управління.

Також важливими є стандарти, що регламентують управління ризиками в конкретних сферах: **ISO 22301** присвячений управлінню безперервністю бізнесу, допомагаючи організаціям протистояти аваріям, катастрофам і іншим надзвичайним ситуаціям; а **OHSAS 18001** (тепер замінений на **ISO 45001**) сфокусований на охороні праці та безпеці працівників.

Впровадження цих стандартів сприяє підвищенню зрілості систем управління ризиками в організаціях, а також забезпечує довіру партнерів і замовників за рахунок відповідності міжнародним і галузевим вимогам.

**Охарактеризувати та спробувати оцінити можливі ризики, що при захисті кваліфікаційної роботи щось «піде не так»**

Під час захисту кваліфікаційної роботи можуть виникнути різні ризики, які здатні вплинути на успішність заходу. Серед основних технічних проблем варто виділити несправність обладнання, такого як проектор або комп’ютер, а також можливу відсутність доступу до файлів презентації чи проблеми з інтернет-з’єднанням у випадку онлайн-захисту. Такі ризики можуть призвести до зупинки або затримки виступу.

Психологічні фактори також відіграють важливу роль. Нервозність, стрес та хвилювання можуть призвести до втрати концентрації, неправильного розподілу часу або забування важливих частин доповіді. Це може негативно позначитися на якості презентації та сприйнятті роботи комісією.

Іншим важливим видом ризиків є негативна реакція членів комісії. Це можуть бути несподівані або складні питання, критика, яка демотивує, або ситуації, коли відповіді не повністю відповідають очікуванням оцінювачів. Такі обставини можуть створити додатковий тиск і ускладнити захист.

Організаційні ризики пов’язані із затримками у початку захисту, зміною розкладу або відсутністю необхідних документів. Подібні проблеми можуть створити хаос і дезорганізацію, що теж вплине на загальне враження від захисту.

Для оцінки цих ризиків можна застосувати дерево рішень, де подія «щось піде не так» розбивається на категорії: технічні, психологічні та організаційні проблеми. Кожна гілка дерева деталізується на конкретні ризики, які оцінюються за ймовірністю та наслідками.

Також корисним є використання матриці ризиків, де кожному ризику присвоюється рівень ймовірності та серйозності наслідків. Наприклад, стрес і хвилювання мають високу ймовірність і середній рівень наслідків, що робить цей ризик пріоритетним для уваги. Несправність обладнання або відсутність файлів презентації можуть мати середню або низьку ймовірність, але високі наслідки, тому їх теж варто враховувати.

Загалом, пріоритет слід віддавати тим ризикам, які мають найвищий індекс ризику, тобто поєднують високу ймовірність із серйозними наслідками. Водночас, багато технічних та організаційних проблем можна мінімізувати завчасною підготовкою — перевіркою обладнання, створенням резервних копій і підтвердженням документації. Водночас робота з психологічною готовністю, наприклад, через тренування виступу та методи подолання стресу, допоможе знизити вплив внутрішніх факторів на якість захисту.