УДК 681.3.06

Є.В. Буров, О.О. Кочіашвілі
Національний університет "Львівська політехніка",
кафедра інформаційних систем та мереж

КЕРУВАННЯ ПРОЕКТАМИ З ВРАХУВАННЯМ РИЗИКІВ

Розглянуто задачу керування проектами з врахуванням ризиків. Запропоновано математичну модель для прогнозування ризиків на підставі досвіду.

This paper proposes a mathematical model for risk assessment based on previous projects experience.

1. Постановка проблеми у загальному вигляді

У сучасному світі індустрії програмного забезпечення кожен проект з розробки програмного забезпечення містить певні ризики. Відомо, що протягом виконання проектів можуть виникнути певні проблеми. Керування ризиками має попереджати ризики, які можуть супроводжувати проектування, розглядати і прогнозувати можливі негативні події, а також визначати, як діяти у разі таких подій. Велика кількість організацій зосереджується на прогнозованих вигодах проекту, не звертаючи увагу на його ризики і забуваючи про критичну реальність: *кожен* проект може завершитись поразкою – замовник відмовиться від проекту або бюджет буде перевищено. Водночас, на початку проекту неможливо передбачити всі деталі або ж володіти повною інформацією, необхідною для його виконання. Тому питання про визначення ризиків і керування ними є актуальним і дуже важливим.

2. Зв'язок висвітленої проблеми із важливими науковими чи практичними завданнями.

Під час керування проектами найперше завдання – оцінювання ризиків, пов'язаних з проектом, і керування цими ризиками. Ризики мають властивість бути великими на початку проекту і зменшуватись в кінці проекту. Відповідно, важливо, щоб робота з мінімізації ризиків проводилася з самого початку проектування. Необхідно, щоб це робилось на ранній стадії проекту, коли затрати на мінімізацію ризику є малими, ніж на пізній стадії, коли, можливо, ризик вже виник, і витрати є великими. Отже, ризик необхідно визначити на початковому етапі проекту і контролювати його на подальших етапах [1].

Невід'ємним правилом RUP (Rational Unified Process) – раціонального уніфікованого процесу – є ідентифікація і засоби з обробки найризикованіших частин проекту на ранній його стадії. Список ризиків призначений для того, щоб фіксувати найімовірніші ризики з метою досягнення успіху проекту. Список ризиків ідентифікує в спадному порядку пріоритетності події, які б могли привести до значних негативних наслідків. Для кожного ризику визначають план дій, які би зменшили ймовірність його виникнення. Він визначає робочу активність під час проектування і є основою для організації всіх етапів проекту [7].

Ризик – це подія або умова, яка негативно впливатиме на проект, якщо виникне.

Ризики виникають через неточності прийнятих за проектом рішень. Суттєвим аспектом прийняття успішних рішень є контролювання і зменшення ризиків, які є невід'ємною частиною проекту. Більшість людей асоціює поняття ризику з можливістю втрат щодо вартості проекту, контролювання, функціональності, якості або часових меж завершення проекту. Однак, до ризиків проектування належать також втрати вигоди в сприятливих обставинах, а також неточності прийнятих рішень, що може призвести до втрати прибутку за проектом [5].

2.1. Типи ризиків

Технічні, управлінські, експлуатаційні, середовищні і тестувальні ризики – всі вони загрожують успіху розробки програмного продукту.

Хоча існують й інші ризики, названі вище є найпоширенішими та оцінюваними в проектах з розробки, вдосконалення і тестування, зокрема автоматизованого тестування програмних продуктів.

2.1.1. Технічний ризик (Technical risk)

Цей ризик виникає під час проектування, адже не існує проектів, де не виникає жодної проблеми. У цьому випадку має бути поставлено два основні запитання:

1. Чи дійсно відомо, в чому полягає проблема?
2. Чи цю проблему можна вирішити?

Проблему визначають на етапі аналізу логіки функціонування системи, на етапі збирання і визначення вимог до програмного продукту. Дуже часто проект розпочинається з нечіткого уявлення про те, що має бути зроблено і якими повинні бути результати. Отже, з самого початку, розробники проекту мають завдання, яке є нечітким і може постійно ззмінюватись. Вони не знають, в якому напрямку вони прямують або як досягти результатів, але вони щось роблять. Визначення вимог до проекту і контроль за ними є завданнями керівника проекту. Не йдеться про те, щоб абсолютно всі вимоги були відомі до початку будь-якої роботи, але всі вони мають бути відомі перед тим, як твердити, що проект повністю завершений. Те, що проблема є відомою, не означає, що вона може бути вирішена. Рішення можуть виявитися дуже дорогими або можуть негативно впливати на проект загалом. Ці ризики необхідно проаналізувати і визначити проблему на етапі ініціювання проекту якомога раніше.

Іншим аспектом технічного ризику є випадок, коли знайдене рішення є поза межами сучасних технологічних можливостей. Хоча від керівника проекту не вимагають бути експертом у всіх існуючих технологіях, він відповідає за те, що технологічні питання будуть адресовані відповідним людям. Якщо компанії невідомо, в чому полягає реальна проблема або чи є вона поза межами певної технології, проект приречений ще перед своїм початком.

2.1.2. Управлінський ризик (Managerial risk)

Протягом життєвого циклу проекту зустрічаються такі управлінські ризики:

- ризик графіка виконання проекту;
- фінансовий ризик;
- ризик персоналу;
- ризик якості;
- ризик конфігураційного менеджменту.

Ризик графіка виконання проекту (Schedule risk). Напевно, найбільшим ризиком в керуванні проектами є неточне визначення графіка виконання проекту. Ризик графіка виконання проекту починається з вихідної (і часто незмінюваної) оцінки розмірів проекту, його критичності, складності, значущості, необхідності, а також складності його виконання. Існує багато випадків проектів, що значно виходили за межі, встановлені графіком і тому були зроблені неякісно або не повністю завершені, чи завершені якісно, але з суттєвим запізненням. Не лише керівник проекту, але й системний архітектор, програмісти, а також аналітики з гарантування якості (Quality Assurance) повинні бути активно залучені до процесу оцінювання розмірів проекту для того, щоб запобігти протермінуванню графіка виконання проекту. Вони також повинні надавати консультації з метою контролю за поточним станом проекту й дотриманням графіка у міру розробки, кодування і тестування програмного продукту.

Фінансовий ризик (Financial risk). Фінансовий ризик нерозривно пов'язаний з ризиком графіка виконання проекту. Неправильно оцінені і визначені графіки негативно впливають на точність фінансових оцінок. Це не свідчення того, що лише встановлення графіка роботи впливає на фінансові ризики. Багато однакових факторів , що впливають на оцінку графіка, також впливають на фінансову оцінку. Це повинно братися до уваги, коли оцінюють вартість проекту. Керівник проекту повинен постійно аналізувати інформацію стосовно загрози виникнення фінансових ризиків [3].

Ризик персоналу (Personnel risk). Технічний ризик, який виникає через проблему розуміння і технологічних можливостей, може перетворитися в ризик персоналу. Для того, щоб визначити, чи існує ризик персоналу, керівник проекту повинен відповісти на такі запитання:

- Чи є достатньо кваліфікованих співробітників, яким можна адресувати цю проблему?
- Чи вони мають достатню кваліфікацію, щоб вирішити цю проблему?

Якщо такого персоналу дуже мало або якщо досвід роботи є невеликим, це може поставити під загрозу успішне завершення проекту [3].

Ризик конфігураційного менеджменту (CM risk). Розробка і постачання програмного продукту потребують, щоб всі його частини були взаємоузгоджені і відповідали затвердженим вимогам до продукту. Вочевидь, переважно проблем не виникає, якщо програмний продукт є автономним програмним продуктом. Однак, програмне забезпечення фактично ніколи не є автономним. Принаймні, воно повинно функціонувати на певній обчислюваній платформі сумісно з іншим програмним забезпеченням, таким як операційна система. У деяких проектах програмне забезпечення є частиною більшої системи, яка може задіяти й інше програмне забезпечення і містити апаратні засоби як частину продукту, що підлягає здаванню. Від найменшої зміни програмного забезпечення до розробки найбільшої системи гарантування того, що програмне забезпечення, що підлягає здаванню, функціонує правильно в програмному середовищі, яке його оточує, є головним ризиком конфігураційного менеджменту. Працівник з якості повинен співпрацювати з розробниками, керівником проекту, а також з працівниками, які відповідають за конфігураційний менеджмент, для забезпечення гарантії, що конфігураційні проблеми не загрожують проекту [3].

Ризик якості (Quality risk). Ризик якості полягає в тому, що завершений програмний продукт міститиме дефекти або не буде чітко і повністю виконано поставлені до нього вимоги. Важливим запитанням щодо ризику є те, наскільки якісним має бути продукт, що здається. Часто шукають компроміс між якістю і часовими межами чи вартістю. У деяких випадках вдалим комерційним рішенням буде здати продукт, який не є абсолютно близький до своїх якісних цілей для того, щоб задовольнити потреби ринку та вимоги замовника. В інших випадках критичність продукту диктує, що бюджет або графік проекту (або і бюджет, і графік) будуть перевищені для того, щоб зробити високоякісний продукт. Сторонами, що впливають на компромісне рішення, можуть бути керівництво, маркетинг, фінансовий відділ, користувач, аналітики з якості тощо, залежно від специфіки ситуації [3].

Поточний контроль за проектом. Найкраще запобігти виникненню управлінських ризиків можна шляхом розпізнавання загроз і поточного контролю за проектом для того, щоб виявити виникнення загроз. Початкове розпізнавання потенційних загроз може сприяти спеціальному плануванню проекта з врахуваням ризиків. У міру продовження проекту постійний контроль за потенційними ризиками сприятиме вчасному розпізнаванню ризикованих ситуацій і впровадженню планів відповідних ризикам дій [10].

2.1.3. Експлуатаційний ризик (Operational risk)

Існують такі три експлуатаційні ризики:

1. Незадовільний рівень освіти або підготовки користувача;
2. Неправильне використання (спеціально або випадково) програмного продукту;
3. Незадовільне технічне обслуговування продукту.

Освіта користувача (User education). Освіта користувача – це один з трьох вищевикладених ризиків, виникненню якого найлегше запобігти. Очікується розуміння ролі користувача з самого початку проекту. Це розуміння повинно означати можливі вимоги до підготовки і освіти для правильного і вмілого використання нового продукту. Можна звернутися до працівника з якості, щоб він оцінив потреби в підготовці працівників, спробував використати продукт з метою знаходження потенційних помилок у використанні продукту або дефектів продукту, або навіть здійснив формальний прогін системи, використовуючи лише надані документи та інструкції з використання програмного продукту [3].

Неправильне використання програмного продукту (Software Misuse). Важче запобігти ризику неправильного використання продукту його користувачем. Попередження і вбудований в програмне

забезпечення захист від загальних випадкових помилок з боку користувача – це такі дії, які часто можуть запобігти виникненню ризика. Спеціальне неправильне використання продукту зазвичай не можна передбачити і важко зупинити у випадках, коли воно може бути передбачене. У цих випадках чіткі формулювання належних меж проекту і використання продукту і конкретні попередження про можливі наслідки неправильного використання можуть бути єдиним захистом компанії, що розробляє продукт [3].

Технічне обслуговування (Maintenance). Технічне обслуговування програмного продукту є ризикованішим, ніж сама розробка продукту. І працівники з контролю якості, і працівники гарантування якості мають безпосередньо виявляти та запобігати ризикам з технічного обслуговування.

Роль працівників з контролю за якістю полягає в перевірці того, що кожен процес технічного обслуговування перевіряють, тестують й аналізують, а конфігурацію правильно встановлюють до завершення процесу технічного обслуговування.

Роль працівників з гарантування якості полягає в контролюванні процесів технічного обслуговування, щоб розпізнати ознаки частин продукту з помилками, визначити слабкі частини процесу технічного обслуговування і передбачити потенційні, але ще не знайдені проблеми технічного обслуговування [3].

2.1.4. Ризик середовища (Environment risk)

Найкращі програмні системи світу є некорисними, якщо їх неможливо запустити. Це здається достатньо елементарним твердженням, але захист центру даних є часто останнім аспектом, про який хвилюється організація. Центром даних називаємо приміщення організації, яка розробляє програмний продукт, де знаходяться всі сервери, що використовуються організацією і містять основну інформацію. Центр даних знаходиться в постійному ризику пошкодження від пожежі чи від води, і якщо приймаються якісь профілактичні заходи, то переважно в цьому напрямку. Крім цього, більшість центрів даних не враховують можливості обробки даних в разі зупинки роботи через тяжкі пошкодження. На жаль, для малої кількості центрів даних передбачено пристрої з тимчасового оброблення даних у випадках, коли центр даних зазнав пошкоджень.

Формальним аналізом ризиків визначено декілька типів пошкоджень, центру даних і відповідний рівень захисту для запобігання цим пошкодженням. Це є фізичні ризики: ризик пожежі, ризик затоплення. Також це можуть бути погодні ризики: можливість тяжких погодних пошкоджень є реальним фактором в місцевостях з частими ураганами і торнадо, аналогічно як і в місцевостях, де тяжкі снігопади можуть зруйнувати дахи і завадити проїзду на шляхах.

Не всі ризики можна попередити: деякі з них неминучі і не можливі профілактичні заходи. Інші можуть спричинити настільки малий негативний ефект, що їх можна проігнорувати. Однак, кожен ризик необхідно ідентифікувати перед тим, як приймати такі рішення. Аналіз ризиків допомагає компанії визначити, як найкраще витратити гроші. Однаково важливо визначити, що якийсь окремий фактор є малим або неважливим ризиком, а також знайти ті фактори, які дійсно становлять ризик. Як тільки ризики та їх вартість у разі виникнення відомі, можна вживати профілактичних або захисних заходів [3].

2.1.5. Ризик тестування (Testing risk)

Цей ризик пов'язаний з ситуацією, коли система протестована не повністю, або навпаки, коли проводиться надлишкове тестування і, відповідно, зростають витрати. Працівник з контролю якості грає ключову роль у запобіганні ризику тестування. Якісно складені тест-план і процес тестування сприяють зменшенню неповного або повторного тестування. Коли припинити тестування – залежить від типів дефектів, які все ще виявляються на етапі тестування, відповідальності, якщо такі дефекти будуть знайдені користувачем, вартості додаткового тестування тощо. Розглядаються можливості здавання продукту з невідомими або не знайденими дефектами; наслідки здавання продукту з відомими, але не виправленими дефектами; вартість, продовження тестування. Результати аналізу подають відповідальному керівництву для прийняття кінцевого рішення: чи визнавати ризик, чи продовжувати тестування [3].

2.2. Проективний процес керування ризиками

Якість виконання проектів підтримують ідентифікацією, оцінюванням можливих ризиків на проектах і відслідковуванням тих ризиків, що виникли під час проектування. В інформаційній системі має бути реалізовано проективний процес керування ризиками.

Ризик належить до майбутніх умов і обставин, які є поза контролем колективу проектувальників і які негативно впливають на проект, якщо виникають. Іншими словами, якщо проблема – це така негативна ситуація, що вже існує і яку необхідно вирішувати, то ризик – це потенційна майбутня проблема, яка ще не виникла.

Реактивний керівник проекту намагається вирішити ці проблеми, коли вони виникають. Проективний керівник проекту намагається розв'язати потенційні проблеми до їх виникнення. Не всі проблеми можна завчасно передбачити; і деякі потенційні проблеми, виникнення яких здається малоймовірним, насправді виникають. Однак, більшість проблем можна передбачити завчасно шляхом проективного керування ризиками. Керівник проекту має оцінювати ризик разом з колективом і клієнтом, попереджувати клієнта і колектив проектувальників про середні або важкі ризики, які можуть спричинити майбутні проблеми.

Ідентифікація ризиків є проективним методом забезпечення успіху проекту і підтримання якості виконання проекту шляхом підтримки проекту згідно з графіком і бюджетом. Метою керування ризиками є ідентифікація факторів ризиків проекту і створення плану керування ризиками для мінімізації ймовірності того, що виникнення ризику зашкодить проекту. Вперше ризики оцінюють на етапі визначення обсягу робіт з проектування. Додатково ідентифікувати ризики необхідно протягом проектування відповідно до графіка (щомісячно або щоквартально) або на етапі завершення проекту. Щоб почати процес ідентифікації ризиків, можна ідентифікувати ті області проекту, які можуть бути потенційними проблемами, і скласти список ризиків. Потім складають план керування ризиками, зменшуючи тим потенційні проблеми і готуючись до будь-яких непередбачених випадків.

3. Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання цієї проблеми і на які спирається автор

За результатами аналізу найпоширеніших типів ризиків, що виникають під час розробки програмного забезпечення і з врахуванням проективного процесу керування ризиками було розроблено критерії і вимоги до інформаційної системи для керування проектами і проведено подальші системні оцінювання і дослідження (таблиця).

Аналіз існуючих інформаційних систем

Критерій	Існуючі інформаційні системи	
	Microsoft Project 2003	Software Planner
Можливість підтримки виконання багатьох проектів одночасно	Так	Так
Зазначення для кожного проекту планованої дати його початку і завершення	Так	Ні
Зазначення для кожного проекту реальної дати його початку і завершення	Так	Ні
Зазначення для кожного проекту переліку завдань, що необхідно виконати	Так	Так
Зазначення для кожного завдання планованої дати його початку і завершення	Так	Так
Зазначення для кожного завдання реальної дати його початку і завершення	Так	Так
Оцінювання ймовірності виникнення ризиків, їх впливу і затрат на основі попередніх проектів	Ні	Ні
Можливість роботи без Project Server	Ні	Так
Перерахування ризиків на проекті	Так	Так
Пов'язання ризиків з завданнями	Так	Так
Оцінювання впливу ризиків на проект	Так	Ні
Генерування діаграм, які показують статус проекту відносно прогнозованого	Ні	Ні

За вказаними критеріями було оцінено інформаційні системи, які широко використовуються для підтримки виконання проектів – Microsoft Project і Software Planner.

Microsoft Project – гнучкий інструмент для того, щоби керувати проектами, який належить до найпопулярніших на ринку програмних продуктів для планування проектів.

Software Planner – доступний через мережу програмний інструмент для керування всіма стадіями проекту. Software Planner дає змогу відслідковувати вимоги клієнта, сценарії тестування, дефекти, задачі, які необхідно виконати і відправити клієнту. Software Planner надає можливість колективу співпрацювати, спільно використовуючи документи, проводячи обговорення і керуючи їх розкладом.

Розглянемо кожен з оцінюваних критеріїв (див. таблицю) детальніше.

1. Можливість підтримки виконання багатьох проектів одночасно.

Інформаційна система повинна надавати можливість вводити інформацію про нові проекти, містити інформацію про проекти, що виконуються, а також про проекти, що вже завершилися.

Microsoft Project і Software Planner відповідають цьому критерію.

2. Зазначення для кожного проекту планованої дати його початку і завершення.

В інформаційній системі має існувати можливість визначити для кожного проекту плановані дати його початку і завершення.

Microsoft Project відповідає цьому критерію, Software Planner – не відповідає: у цій інформаційній системі немає можливості конкретно вказати плановані дати початку і завершення проекту.

3. Зазначення для кожного проекту реальної дати його прочатку і завершення.

Інформаційна ситема повинна надавати можливість у процесі роботи над проектом вказати реальні дати його початку і завершення. Порівняння цих дат з плановаными приводить до формування висновків про успішність (або неуспішність) виконання проекту і впливає на формування рішень керівника проекту під час планування наступних проектів.

У Microsoft Project існує можливість змінити плановані дати проекту, можна вважати цю процедуру введенням реальних дат виконання проекту. Software Planner не відповідає цьому критерію – у цій інформаційній системі немає можливості конкретно вказати для проекту реальні дати його початку і завершення.

4. Визначення для кожного проекту переліку завдань, що необхідно виконати.

Для кожного проекту повинна існувати можливість переліку завдань, що мають бути виконані в межах проекту.

Microsoft Project і Software Planner відповідають даному критерію.

5. Зазначення для кожного завдання планованої дати його початку і завершення.

Інформаційна система повинна забезпечувати можливість задання для кожного завдання дат його планованого початку і завершення.

Microsoft Project і Software Planner відповідають цьому критерію.

6. Зазначення для кожного завдання реальної дати його початку і завершення.

Інформаційна система повинна надавати можливість у процесі роботи над проектом вказувати реальні дати початку і завершення роботи за завданнями проекту. Порівнюючи ці дати з плановаными, роблять висновки про успішність (або неуспішність) виконання проекту (або окремого завдання) та визначають (керівник проекту) час, необхідний для виконання наступних проектів.

У Microsoft Project існує можливість змінити плановані дати завдання, можна вважати цю процедуру введенням реальних дат виконання проекту. Але не існує окремого поняття "планована дата" і "реальна дата", що є недоліком Microsoft Project. Software Planner відповідає цьому критерію – у цій інформаційній системі є можливість вказати для завдання реальні дати його початку і завершення.

7. Оцінювання ймовірності виникнення ризиків, їх впливу і затрат на основі попередніх проектів.

Це є дуже важливий критерій, адже необхідним фактором під час планування проектів, планування часу, який потрібно виділити на виконання того чи іншого завдання, є врахування досвіду роботи з попередніми проектами, які вже завершилися. Необхідно скласти перелік ризиків, ймовірність виникнення кожного ризику, кількість часу, що додається на виконання певного завдання, якщо даний ризик станеться. Під час аналізу цієї інформації важливу роль має відігравати аналіз інформації про попередні проекти. Але жодна з інформаційних систем, що розглядаються, не

надає можливість аналізувати ризики (їх ймовірностей і затрат часу, якщо ці ризики стануться) на основі попередніх даних. Характеристики ризиків як за всім проектом, так і за окремими завданнями вводяться в дані системи керівником проекту на основі його суб'єктивної оцінки, а суб'єктивна оцінка не завжди буває правильною.

8. Можливість роботи без Project Server.

Project Server – це допоміжний програмний продукт, який (якщо його спеціально налаштувати) надає можливість сумісного планування і звітування статусу з виконання проекту між членами робочої групи, менеджерами проектів та іншими зацікавленими сторонами, шляхом роботи і обміну інформацією на проекті через веб-сайт. Тобто цей сайт потрібно створити, належно сконфігурувати і налаштувати. Це потребує додаткового часу, програмного середовища і створення мережі. Тобто створення Project Server може бути не завжди доцільним і вигідним.

Microsoft Project не відповідає цьому критерію, адже ризики в Microsoft Project не можуть бути створені без Project Server – система дає повідомлення про помилку "A Project Server URL has not been specified. Please specify a Project Server URL in the Collaborate tab of the Tools Options dialog." Software Planner відповідає цьому критерію. Робота з системою можлива без використання Project Server.

9. Перерахування ризиків проекту.

Інформаційна система повинна надавати можливість перелічити для кожного проекту ризики, які можуть вплинути на терміни його виконання.

Як Microsoft Project, так і Software Planner відповідають цьому критерію. У Microsoft Project існують спеціальні форми для переліку ризиків проекту і зазначення їх характеристик. У Software Planner не передбачено автоматичних засобів для створення ризиків і переліку їх характеристик. Існує лише можливість зберігати для цього проекту спеціальний Word-документ, в якому надається інформація про ризики, що можуть виникнути під час проектування. Система Software Planner пропонує зберігати ризики і додаткову інформацію про них у вигляді звичайної таблиці.

10. Пов'язання ризиків з завданнями.

Інформаційна система повинна також надавати можливість перелічити для кожного завдання ризики, які можуть вплинути на терміни його виконання. Як Microsoft Project, так і Software Planner відповідають цьому критерію (ризики перелічуються аналогічно, як для усього проекту).

11. Оцінювання впливу ризиків на проект.

Інформаційна система повинна підрахувати, скільки загалом часу піде на виконання як усього проекту, так і окремих завдань з врахуванням ризиків, виходячи з характеристик ризиків (їх ймовірностей і часу, що піде на виконання тих завдань, де ці ризики можуть виникнути).

У Microsoft Project такий підрахунок здійснює система. Software Planner не забезпечує автоматичного підрахунку часу, що планується на виконання проекту.

12. Генерування діаграм, які показують статус проекту відносно прогнозованого.

Інформаційна система повинна генерувати різноманітні діаграми, які зображають статус проекту відносно того, що планувався, і дають змогу керівнику проекта побачити, де відбуваються відхилення від планованого графіка роботи.

Жодна з інформаційних систем, що розглядаються, не відповідає цьому критерію.

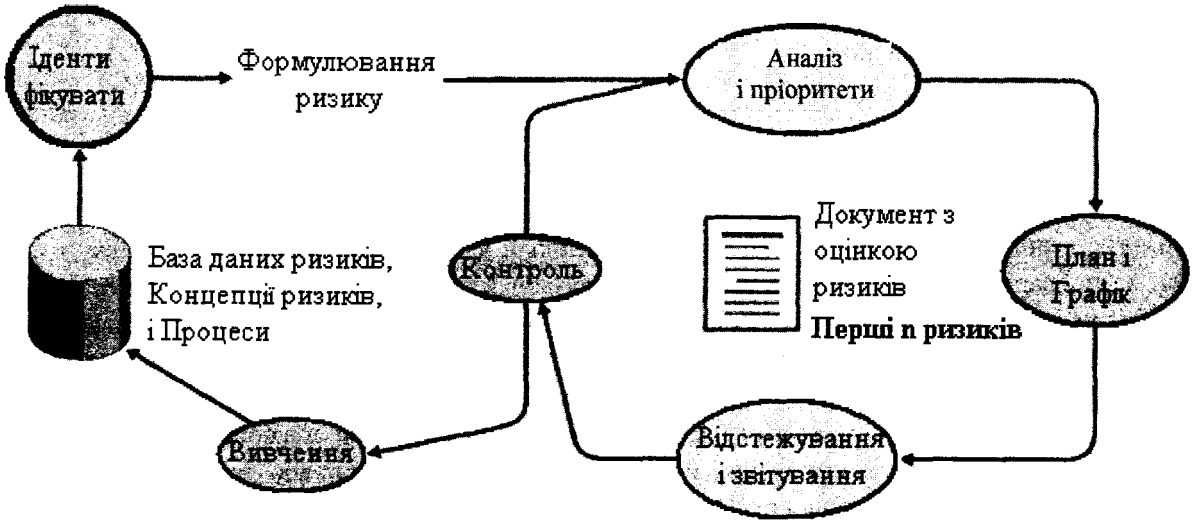
Отже, оцінивши існуючі інформаційні системи для підтримки виконання проектів, можна зробити висновок, що вони не повністю відповідають поставленим критеріям. Жодна з систем, що розглядалися, не задовольняє головного критерію, що нас цікавить, – оцінювання ймовірності виникнення ризиків, їх впливу і затрат на основі попередніх проектів. Тому доцільно розробити нову інформаційну систему, яка буде відповідати всім вищепереліченим критеріям.

4. Виділення не вирішених раніше частин загальної проблеми, котрим присвячено статтю

Керування ризиками – це процес ідентифікації, аналізу і запобігання ризикам під час виконання проекту, щоб вони не стали проблемами і не спричинили втрат.

Процес керування ризиками компанії Microsoft – Microsoft® Solutions Framework (MSF), який зображено на рисунку, є прогресивним методом, який колектив використовує протягом виконання

проекту. Колектив постійно оцінює, що може бути зроблено неправильно і як мінімізувати будь-які втрати. MSF пропагандує відслідковування ризику шляхом використання формальних документів для оцінки ризиків і пріоретизації ризиків.



MSF процес керування ризиками

MSF процес керування ризиками визначає шість кроків, за допомогою яких колектив керує поточними ризиками, планує і виконує стратегії керування і документує знання, набуті на поточному проекті, для майбутніх проектів. Є такі шість кроків MSF процесу керування ризиками:

4.1. Ідентифікація ризику

На цьому кроці визначають ризики та інформують колектив про потенційні проблеми [5].

Не існує широко застосовуваного стандартного методу для ідентифікації ризиків. Досвід у попередніх, схожих проектах або програмних продуктах є суттєвим засобом для ідентифікації ризиків. Також колективне обговорення проблем: "що станеться, якщо", інші запитання тощо можуть сприяти знаходженню потенційних можливостей виникнення ризику.

Щойно ризик або можливість ризику, якими б нереальними вони здавалися, є визначені, вони мають бути занотовані та оцінені [3].

4.2. Аналіз ризиків і визначення пріоритетів

На цьому кроці визначають:

- Можливі витрати у разі виникнення ризику;
- Ймовірність виникнення ризику;
- Вплив ризику;
- Вартість прийняття відповідних дій у разі виникнення ризику.

Визначення розміру можливих витрат. Для кожного ідентифікованого ризику має бути визначено потенційні витрати: скільки часу або коштів піде на подолання ризику, якщо він виникне.

Визначення ймовірності виникнення ризику. Ймовірність виникнення має бути визначено для кожного ризику, що був ідентифікований. Цю величину визначають або на основі попереднього досвіду виникнення ризиків на певних типах завдань, або ж на основі експертної оцінки когось з кваліфікованих працівників, наприклад, керівника проекту.

Визначення впливу ризику. Вплив ризику – це добуток розміру можливих витрат і ймовірності виникнення ризику. Вплив ризику необхідно визначити для кожного ризику для того, щоб врахувати витрати, визначити пріоритети і методи подолання ризиків.

Вартість заходів з відповіді на ризик. Це завдання є близьким до оцінки вартості і графіка проекту. Оцінка розміру витрат та їх впливу на бюджет і відповідна зміна графіка повинні бути пораховані для кожного визначеного ризику [3].

4.3. Планування ризиків і встановлення графіків

Як тільки вплив ризику визначено, повинна бути визначена відповідь на ризик – план дій, що мають виконуватись, якщо виникне цей ризик. На основі впливу ризику й оціненої вартості відповіді на нього кожному ризику присвоюється один з таких типів з точки зору відповіді на ризик:

- Виключення (Elimination);
- Уникнення (Avoidance);
- Пом'якшення (Mitigation);
- Прийняття (Acceptance).

Виключення. Ризику присвоюється тип "Виключення", коли величина впливу ризику є неприйнятно великою або коли вартість ліквідації ризику є надзвичайно високою. У випадку малої або незначної вартості відповіді на ризик цей ризик зазвичай також виключають.

Уникнення. Відповідно до значення терміна "Уникнення" означає виконання альтернативних кроків для того, щоб зменшити ймовірність виникнення ризику до нуля або числа, наближеного до нуля.

Пом'якшення. "Пом'якшення" – це зменшення впливу ризику. Цього може бути досягнуто зменшенням ймовірності виникнення ризиків, зменшенням розміру втрат або обидвома шляхами.

Прийняття. У випадку надзвичайно малої ймовірності виникнення або дуже малого розміру витрат може бути прийняте рішення про ігнорування ("Прийняття") ризику. Це рішення може також бути досягнуто, якщо вартість виключення ризику, його уникнення або пом'якшення є неприйнятно великою [3].

4.4. Відслідковування і звітування ризиків

Цей крок означає контроль статусу ризиків і стану планів для пом'якшення цих ризиків [5].

Дуже важливим етапом в процесі керування ризиками є створення спеціального плану керування ризиками на проекті. У цьому плані вказують всі визначені ризики і плановані відповіді на ці ризики. Процес керування ризиками і засоби його вдосконалення також обов'язково мають бути викладені в плані.

4.5. Контроль ризиків

На цьому кроці відбувається виконання плану для пом'якшення ризиків і звітування про стан ризиків колективу і замовнику.

4.6. Вивчення ризиків

Вивчення ризиків передбачає ведення документів, що містять уроки, засвоєні на етапі виконання проектів, з метою майбутнього використання цього досвіду колективом і організацією в нових проектах.

Кроки процесу керування ризиками є логічними кроками; вони не обов'язково повинні виконуватись у вказаному порядку. Колективи часто повторюють кроки ідентифікації, аналізу і планування для певних наборів ризиків, періодично повертаючись до кроку дослідження ризиків.

Отже, проведенням аналізу проблем керування проектами доходимо висновку про те, що кожен аспект розробки і підтримки програмного забезпечення містить ризики. Ризики поділяються на технічний, управлінський, експлуатаційний, ризик середовища і ризик тестування. Управлінський ризик містить ризик графіка виконання проекту, фінансовий ризик, ризик персоналу, ризик конфігураційного менеджменту, ризик якості. Експлуатаційний ризик складається з таких ризиків: освіта користувача, неправильне використання програмного продукту, технічне обслуговування. Кожен тип ризику може впливати на інші типи, тобто жоден з них не є відокремленим.

Керування ризиками – це процес, що складається з шести кроків: ідентифікація ризиків, їхнє оцінювання і відповідь на ризики, планування послідовності дій, які потрібно буде виконати, якщо ризик виникне, а також контроль ризиків протягом проектування і вивчення ризиків і проведення аналізу набутого досвіду щодо попередження ризиків. Визначення фактичної відповіді для кожного виду ризику є важливим етапом і передбачає розгляд впливу ризику і вартості вдіповіді на цей вплив.

Процес керування ризиками завершується складанням плану керування ризиками, який окреслює досвід роботи з ризиками під час проектування з метою використання цього досвіду організацією для нових проектів.

Під час проектування потрібно запобігти якомога більшій кількості ризиків, наскільки це можливо. Для цього необхідно чітко розуміти вимоги до проекту. Шляхом передбачення ризиків керівник проекту має можливість їх попереджувати. З використанням різних таблиць і діаграм і веденням поточної документації щодо проекту або використанням спеціального програмного засобу для цього керівник проекту буде готовий оперувати елементами ризику.

Ризики аналізують з різними цілями на різних етапах проектування з автоматизованого тестування програмних систем. Спочатку аналіз ризиків застосовують на фазі первинного аналізу для визначення пріоритетів та часу на виконання завдань проекту. Цей процес допомагає досягти консенсусу між потребами в тестуванні різних компонент програмних систем і фокусує роботу з планування тестування на найважливіших компонентах. Також це допомагає оцінити розмір роботи з тестування і підготувати оцінку бюджету проекту і графіка роботи. Початковий графік тестування зазвичай складають на етапі початку проектування за послідовністю проміжних завдань проекту. Це допомагає точніше спланувати ресурси для написання тестових сценаріїв і проведення безпосереднього автоматизованого тестування системи на етапі тестування. Протягом проектування керівник проекту складає поточну документацію, аналізує, які ризики вже виникли, який негативний вплив вони спричинили, змінює пріоритетність ризиків. На етапі завершення проекту колектив аналізує і документує досвід роботи з ризиками під час проектування для того, щоб ця інформація могла бути використана в майбутньому для інших проектів.

5. Формулювання цілей статті (постановка задачі)

Основна задача інформаційної системи керування проектами з врахуванням ризиків – надати інформацію керівникові проекту для того, щоб правильно спланувати час на виконання проекту, залежно від досвіду роботи над попередніми проектами, і від ризиків, що можуть статися. Центральну роль у системі керування ризиками на основі досвіду відіграє математична модель, покладена в основу системи.

6. Виклад основного матеріалу дослідження з повним обґрунтуванням отриманих наукових результатів

З врахуванням викладених критеріїв і вимог до інформаційної системи, а також процесу керування ризиками розроблено математичну і концептуальну модель нової інформаційної системи для керування проектами із застосуванням аналізу ризиків і досвіду виконання попередніх проектів.

6.1. Математична модель

Побудова математичної моделі зводиться до визначення формул, за якими інформаційна система буде рекомендувати керівникові проекту час, необхідний на виконання певного проекту, який планують розпочати.

Припускаємо, що всі ризики, прив'язані до завдань проекту, є незалежними випадковими подіями. Тоді рекомендований системою час визначатиметься за формулою:

$$FT = \sum_{i=1}^{N} (TT_i + \sum_{j=1}^{M} p_{ij} TR_{ij}),$$

де FT – загальний час, який інформаційною системою рекомендовано виділити на виконання проекту, год.; TT_i – рекомендований час, необхідний на виконання і-го завдання проекту T_i (якщо не справдиться жоден ризик), год.; N – кількість завдань проектування; p_{ij} – ймовірність випадкової події виникнення j-го ризику R_j на *i*-му завданні T_i; TR_{ij} – розмір втрат від j-го ризику R_j, якщо він виникне на і-му завданні T_i, год.; M – кількість ризиків, що можуть виникнути на завданні T_i.

Добуток $p_{ij}TR_{ij}$ визначає вплив j-го ризику R_j на час виконання і-го завдання T_i, тобто проекту загалом (збільшує час виконання).

Величини p_{ij}, TR_{ij} надаються системою за результатами аналізу попередніх проектів, проте керівник проекту має можливість змінити значення цих величин, якщо він вважає це доцільним.

Час TT_i, який система рекомендує витратити на завдання T_i, обчислюють за такою формулою:

$$TT_i = HU_i \cdot TS_i,$$

де HU_i – час, який витрачають на виконання одиниці роботи (одиниця вимірювання завдання T_i); цю інформацію система зчитує з бази даних одиниць вимірювання, год.; TS_i – кількість одиниць завдання T_i (кількість одиниць вимірювання завдання).

Коли завдання завершене, керівник проекту його закриває. Тоді інформаційна система аналізує, чи на закритому завданні виник ризик, виходячи з інформації, введеної в систему керівником проекту.

Якщо завдання T_i було закрите і на ньому виник ризик R_j, то ймовірність виникнення цього ризику p_{ij}=1, якщо ризик не виник p_{ij}=0.

Після того, як завдання закрите, система так модифікує інформацію за ризиками і завданнями.

Зчитується розмір втрат від цього ризику R_j на завданні T_i:

$$TR_{ij}=k,$$

де k – дійсна кількість годин, витрачена на подолання ризику, якщо він виник.

Для кожного ризику R_j, асоційованого з завданням T_i, j=1.. M , в базі даних ризиків модифікується ймовірність виникнення ризику R_j:

$$p_j = \frac{\sum_{i=1}^{L} p_{ij}}{L},$$

де p_j – ймовірність виникнення ризику R_j; p_{ij} – дійсна ймовірність виникнення ризику R_j на завданні T_i; L – кількість різних завдань, що є закриті і на яких виник ризик R_j.

Аналогічно для кожного ризику R_j, асоційованого з завданням T_i, j=1.. M , в базі даних ризиків модифікується розмір втрат для ризику TR_j:

$$TR_j = \frac{\sum_{i=1}^{L} TR_{ij}}{L},$$

де TR_j – ймовірність виникнення ризику R_j; TR_{ij} – дійсна ймовірність виникнення ризику R_j на завданні T_i; L – кількість різних завдань, що є закриті і на яких виник ризик R_j.

Модифікована інформація про ймовірності виникнення ризиків і розмір витрат для цих ризиків використовуватимуть для аналізу ризиків на нових завданнях і нових проектах.

Для закритого завдання T_i система модифікує базу даних одиниць вимірювання цього завдання за формулою:

$$HUN_i = HU_i + \frac{TTR_i}{TS_i},$$

де HU_i – "старий" час, який витрачався на виконання одиниці роботи (одиниця вимірювання завдання T_i); цю інформацію система зчитує з бази даних одиниць вимірювання, год.; HUN_i –

"новий" час, який витрачається на виконання одиниці роботи (одиниця вимірювання завдання T_i), год.; TTR_i – дійсний час, який витрачено на виконання і-го завдання проекту T_i, год.; TS_i – кількість одиниць завдання T_i (кількість одиниць вимірювання завдання).

Модифікована інформація про час, необхідний для виконання одиниці завдання, використовуватиметься для створення графіків і планування часу на нових проектах.

6.2. Концептуальна модель

На цьому етапі проектують нову інформаційну систему за критеріями, обмеженнями і вимогами, поставленими в главі 2, на основі побудованої математичної моделі.

Було побудовано модель способів використання інформаційної системи, створено діаграми потоків даних і розроблено концептуальну модель бази даних, створено макет інформаційної системи, яка полегшує для керівника проекту процес керування ризиками і проектом загалом, збільшує точність оцінювання бюджету і графіків нових проектів, сприяє ефективному плануванню і аналізу.

7. Висновки з даного дослідження і перспективи подальших розвідок у цьому напрямку

Кожен проект з розробки програмного забезпечення містить ризики, але розпізнаючи і аналізуючи ризики на проекті на ранній стадії, можна ефективно протидіяти цим ризикам шляхом прийняття певних рішень з метою успішного виконання проекту.

На проектах потрібно запобігти якомога більшій кількості ризиків, наскільки це можливо. Для цього необхідно чітко розуміти проект і вимоги до нього. Передбаченням ризиків керінник проекту має можливість їх попереджувати. Використовуючи різні таблиці і діаграми, а також поточну проектну документацію або спеціальний програмний засіб для цього, керівник проекту буде готовий оперувати елементами ризику.

У процесі роботи:

- Проаналізовано проблеми керування проектами і способи їх подолання з використанням аналізу ризиків;
- Досліджено основні типи ризиків, які є найпоширенішими під час розробки програмного забезпечення;
- Проаналізовано проективний процес керування ризиками і доведено ефективність його використання;
- Згідно з визначеними критеріями (вимогами і обмеженнями) проаналізовано існуючі програмні системи для керування проектами з врахуванням проектних ризиків і зроблено висновок, що розглянуті системи не повністю задовольняють визначені критерії;
- Побудовано математичну модель нової інформаційної системи, яка реалізує новітній підхід автоматичного застосування досвіду попередніх проектів для підвищення ефективності процесу керування ризиками під час виконання нових проектів.

Розроблена математична модель є основою нової інформаційної системи, яка підвищує ефективність і точність планування проектів, спрощує реалізацію проективного процесу керування ризиками; надає дані про досвід виконання попередніх проектів, використання якого зменшує ймовірність виникнення ризиків на майбутнє і, відповідно, сприяє успішному їх завершенню. Система може бути ефективно застосована для проектів різного спрямування: для підтримки якості їх виконання, не лише для проектів з розробки програмного забезпечення. В роботі розглядався підхід до ризиків як до незалежних випадкових подій, що мають певні ймовірності виникнення. Надалі доцільно сконцентрувати увагу на реалізації в інформаційній системі можливості встановлення залежностей між ризиками проектів, що сприятиме точнішому аналізу і плануванню проектів.

1. Hall P., "Overcoming residence to risk management", STQA Magazine, January/February 2003. – 23-26 pp. 2. Higuera R. P., Dorofee A. J., Walker J. A., William R. C., "Team Risk Management: A New Model for Customer-Supplier Relationships", QMS, July 1994. – 448 pp. 3. Horch J., "Practical Guide to

Software Quality Management, Second Edition," Artech House, 2003. – 226 pp. 4. Kirkpatrick R. J., Walker J. A., Firth R., "Software Development Risk Management: An SEI Appraisal (SEI Technical Review'92)", Software Engineering Institute, Carnegie Mellon University, 1992. – 240 pp. 5. MCSD Self-Paced Training Kit: Analyzing Requirements and Defining Microsoft .NET Solution Architectures, www.microsoft.com/mspress. 6. Probasco L., "The Ten Essentials of RUP The Essence of an Effective Development Process". 7. Rowe W. D., "An Anatomy of Risk', 1988. – 16 pp. 8. Tuffley D., "Risk Management Standard", Tuffley Computer Services, July 1999. – 8 pp. 9. Van Scoy R. L., "Software Development Risk: Opportunity, Not Problem", Software Engineering Institute (CMU/SEI-92-TR-30, ADA 258743), September 1992. – 225 pp. 10."Best Practices for Software Projects – Risk Management", Pragmatic Software Newsletters, July 2004.

УДК 004:339.166.5

О. Б. Вовк, В.С. Якушев
Національний університет "Львівська політехніка",
кафедра інформаційних систем та мереж

ОЦІНКА ВАРТОСТІ ПРАВ ОБ'ЄКТІВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ У ГАЛУЗІ КОМП'ЮТЕРНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ

Наведено характеристику основних визначень об'єктів інтелектуальної власності у галузі комп'ютерних технологій. Показано взаємозв'язок між такими поняттями, як "зміст" та "інтелектуальна власність", оцінено інтелектуальний капітал.

In article it is resulted the characteristic of the basic definitions of the object intellectual property in sphere of computer technologies. It is shown interrelation between such concepts as "contents" and "the intellectual property". It is made an estimation of the intellectual capital in sphere of computer technologies.

1. Вступ

Від вирішення проблеми створення ефективної системи охорони і захисту прав об'єктів інтелектуальної власності (ОІВ) загалом і у сфері комп'ютерних інформаційних технологій зокрема залежить успішність побудови інноваційної моделі розвитку України, її модернізації, підвищення конкурентоспроможності у світовій соціально-економічній системі. Такі тенденції є першорядними у створенні світової технології XXI століття — технології, що базується на знаннях. Необхідним є також функціонування цивілізованого ринкового середовища, де і підприємці, і споживачі були б надійно захищені від недобросовісної конкуренції, пов'язаної з неправомірним використанням прав на ОІВ, виробництвом неліцензованих товарів, а також контрафактних примірників ОІВ, зокрема комп'ютерних програм і баз даних. Ця проблема є особливо актуальною з огляду на те, що під час відтермінування запровадження економічних санкцій з боку США чітко обумовлювалось продовження заходів, які підтверджували б рішучість України у боротьбі з порушеннями прав інтелектуальної власності.

2. Постановка проблеми

Проблеми охорони і захисту прав ОІВ в Україні

Проблеми охорони і захисту прав ОІВ сьогодні вийшли в світі на перший план і стали вже не просто юридичними або економічними питаннями, а і проблемами політичних взаємовідносин країн. Внаслідок неосяжної інтелектуалізації сучасного суспільства за останнє десятиліття, що перш