УДК 007.3

О.В. Гетманець, Д.В. Шмирьов

Управління проектами при побудові інформаційних систем

Національна Академія СБ України

Викладені погляди щодо використання теорії управління проектами у проектуванні систем захисту інформації. Наведено програмний інструментарій для аналізу систем управління проектами.

Ключові слова: управління проектами, системи захисту інформації, інформаційні технології, управління ризиками, аналіз систем, проектування систем.

Постановка проблеми. Питання управління окремими проектами та портфелями проектів, внаслідок бурхливого розвитку та постійного підвищенням складності інформаційних технологій, стають на теперішній час все більш актуальними. Не винятком є і проектування систем захисту інформації (далі - СЗІ). Чим більш складною та інтелектуальною є СЗІ, тим більш керованим повинен бути процес її створення і функціонування. У цьому сенсі може бути плодотворним використання теорії управління проектами при вирішенні задач створення СЗІ.

Аналіз шляхів управління проектів. Втілення технологій управління проектами в Україні переживає період бурхливого росту, який розпочався наприкінці дев'яностих років минулого сторіччя. Із розвитком технологій управління проектами простежуються цікаві закономірності у практиці використання цього напрямку діяльності. По-перше, виявилася пряма залежність між рівнем конкуренції на певному сегменті ринку та зацікавленістю технологіями управлінням проектами. По-друге, укрупнення компаній практично завжди супроводжується формалізацією політики управління, інтеграцією зусиль по взаємодії різних керуючих ланок та, як наслідок, широким втіленням єдиних методологій глибокого управління проектами та портфелями проектів.

Під проектом будемо розуміти комплекс взаємопов'язаних заходів, що призначені для досягнення протягом певного часу при встановленому бюджеті поставлених задач із чітко визначеними цілями.

Для успішного управління проектом необхідно постійно знаходити баланс між взаємосуперечливими характеристиками:

- зміст проекту, час, витрати і якість;
- вимоги до проекту та очікування від нього у різних ключових учасників;
- несумісність результатів та очікувань проекту.

Зміст принципу керування проектом можна розділити на більш-менш самостійні блоки. Одним з таких блоків є управління ризиками проекту. Розглянемо цій блок більш детально.

Під управлінням ризиками проекту будемо розуміти опис дій по ідентифікації та аналізу проектних ризиків, а також методи реагування на них.

У загальному випадку проектні ризики можуть мати як негативні, так і позитивні наслідки, але останні у даній роботі враховуватись не будуть.

Процес управління ризиками включає в себе наступні етапи:

- ідентифікація ризиків;
- кількісна оцінка ризиків;
- розробка методів реагування;

- контроль ризиків;
- контроль реагування.

Ідентифікація ризиків.

На цьому етапі необхідно визначити ступінь деталізації, тобто визначити, які існують інформаційні і технічні ресурси зі складу інформаційної системи (далі - ІС) та з якою детальністю вони повинні розглядатися в процесі управління ризиком.

На цьому етапі повинна здійснюватися ідентифікація та оцінка цінностей, в ході якої виявляються та призначаються вартість ресурсів ІС. Цінності можуть бути визначені на основі впливів наслідків для організації. Оцінка ризиків передбачає не тільки вартість ресурсів, а й наслідків в разі здійснення загроз. Вартість ресурсів може бути представлена у вигляді потенційних втрат.

Завершує цей етап безпосередньа ідентифікація загроз і визначення їх ймовірностей.

Кількісна оцінка ризиків.

Міра ризику може розглядатися, як опис видів несприятливих факторів, впливу яких може зазнати ІС, та ймовірності їх реалізації. Результат цього процесу повинен визначити ступінь ризику для певних цінностей.

Розробка методів реагування.

Мета цього етапу – вибір відповідних заходів і засобів захисту. Цей етап може бути виконаним із використанням перевірки прийнятності ризику. Перевірка прийнятності ризику – це діяльність, що порівнює поточну міру ризику за критеріями прийнятності із відповідними граничними значеннями та призводить до визначення того, наскільки адекватний поточний рівень ризику.

Контроль ризиків.

На цьому етапі повинно відбуватись відслідковування поточних рівнів раніше ідентифікованих ризиків і ходу заходів, що направлені на стримування цих ризиків, ідентифікація нових ризиків.

Контроль реагування.

На цьому етапі повинні відслідковуватися зміни у факторах ризику.

Система управління ризиками при проектуванні інформаційної системи повинна стати невід'ємною частиною загального процесу проектування. Одним з основних документів системи управління ризиками є карта ризиків (таблиця 1).

Таблиця 1

Карта ризиків

Ідентифікатор ризику	Унікальне позначення (найменування ризику)
Класифікація ризику	Загальна характеристика типу впливу, якого може завдати ризик
Умови появи ризику	Опис умов появи загроз
Тригери ризику	Часові або параметричні індикатори
Ймовірність появи ризику	Вірогідна величина (0…1)
Загроза ризику	Кількісна міра загрози ризику
Очікувана величина ризику	Добуток ймовірності реалізації ризику на загрозу ризику
Зв'язані ризики	Перелік ідентифікаторів інших ризиків, які знаходяться з даним ризиком у залежності з описом цієї залежності
Заходи стримування ризику	Опис заходів, що повинні стримувати ідентифікований ризик

Які переваги може дати використання теорії управління проектами? Одна з переваг – це можливість використання міжнародних стандартів. Це насамперед прийнятий у 2000 році міжнародний стандарт управління інформаційною безпекою «International Standard ISO/IEC 17799. Information technology – Code of practice for information security management». Цей стандарт розроблений Британським інститутом стандартів і включає в себе модель системи менеджменту, що описує загальну організацію, класифікацію даних, системи доступу, напрямки планування, використання оцінки ризику в контексті інформаційної безпеки.

Аналіз існуючих продуктів управління проектами. Ще одна з переваг використання теорії управління проектами – це використання розвинутого інформаційного бізнес-середовища, що включає в себе велику кількість програмного інструментарію для розробки та ведення проектів. Цей інструментарій може стати потужною зброєю для організації комплексного захисту інформації. Нижче наведено короткий огляд ринку засобів розробки управління проектами та портфелями проектів.

Компанія Microsoft представлена продуктами Microsoft Project та Microsoft's Enterprise Project Management. Ці продукти найбільш відомі на ринку України та успішно використовуються для автоматизації етапів робот над проектом: складання плану, графічне представлення структури, збір та аналіз відомостей, управління графіком, управління ресурсами, управління витратами, складання звіту, управління ризиками.

Високу функціональність має Oracle Projects компанії Oracle. За допомогою цієї системи можливе планування із використанням структури «дроблення» робіт для більш точного розрахунку вартості проекту. Передбачено аналіз портфелю проектів за кількома критеріями з подальшим ранжуванням та врахуванням різних сценаріїв розвитку подій. Систему Oracle Projects зручно використовувати великим організаціям, що ведуть велику кількість проектів.

Відомими є продукти компанії IBM – Rational Unified Process та IBM Tivoli Unified Process. В означених системах багато уваги приділено здійсненню інтегрованої політики управління портфелем проектів. Також підходять великим організаціям.

Крім названих продуктів можна виділити продукцію компаній Artemis, Borland, Compuware, Mercury, PlanViev, Primavera, SAP.

Використовуючи зазначений програмний інструментарій, значно легше обрати варіант системи комплексного захисту інформації. Так, в залежності від конфіденційності інформації, що обробляється в організації, рівня її критичності, величини можливих збитків від реалізації загроз, матеріальних та інших ресурсів, що є у розпорядженні організації, а також інших чинників, є можливість обґрунтування пропозицій щодо доцільності застосування певних варіантів забезпечення інформаційної безпеки, а саме:

- досягнення необхідного рівня інформаційної безпеки за мінімальних затрат і допустимого рівня обмежень на технології зберігання, обробки та передавання інформації в організації;
- досягнення необхідного рівня захищеності інформації за допустимих затрат і заданого рівня обмежень на технології зберігання, обробки та передавання інформації в організації;
- досягнення максимального рівня захищеності інформації за необхідних затрат і мінімального рівня обмежень на технології зберігання, обробки та передавання інформації в організації.

Висновки

Таким чином, використання теорії управління проектами та відповідного програмно-аналітичного інструментарію є доцільним та може суттєво допомагати вирішувати складні завдання щодо забезпечення надійного захисту інформації із дотриманням прозорості та гнучкості. Останнє є важливим у разі необхідності аудиту системи захисту інформації за міжнародними стандартами.

Література

1. Богуш, В.М., Юдін О.К. Інформаційна безпека держави [Текст] / В.М. Богуш, О.К. Юдін– К.: МК-Прес, 2005. – 432 с.
2. Черников, А. Заглянем в 2009 г.: на очереди – управление портфелем проектов [Текст] / А. Черников // Компьютерное обозрение. – 2006 г. - №43. – С. 26-30.

Рецензент: кандидат технічних наук, доцент Сидоренко Н.Ф.
Державне науково-виробниче підприємство «Об`єднання «Комунар»»

Поступила в редакцію 05.09.2011

Управление проектами при построении информационных систем

Представлены тезисы применения теории управления проектами при проектировании систем защиты информации, а также программный инструментарий для анализа систем управления проектами.

Ключевые слова: управление проектами, системы защиты информации, информационные технологи, управление рисками, анализ систем, проектирование систем.

Project management rules in development of information systems

Project management rules implementation is introduced in design process of security systems. Software tools for analysis of project management systems are described.

Keywords: project management, security systems, information technology, risk management, system analysis, system design.