ДОДАТОК А

Копії публікацій

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗДОБУВАЧІВ ДРУГОГО (МАГІСТЕРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ КАФЕДРИ ЕКОНОМІЧНОЇ КІБЕРНЕТИКИ ТА УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ

Харків 2019

Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

ЗБІРНИК НАУКОВИХ ПРАЦЬ ЗДОБУВАЧІВ ДРУГОГО (МАГІСТЕРСЬКОГО) РІВНЯ ВИЩОЇ ОСВІТИ КАФЕДРИ ЕКОНОМІЧНОЇ КІБЕРНЕТИКИ ТА УПРАВЛІННЯ ЕКОНОМІЧНОЮ БЕЗПЕКОЮ

Рекомендовано рішенням НМР
Харківського національного
університету радіоелектроніки
Протокол від 24.02.2011 № 6

Харків 2019

УДК 65.012.8 + 658.5:330.4

Збірник наукових праць здобувачів другого (магістерського) рівня вищої освіти кафедри економічної кібернетики та управління економічною безпекою/ за ред. Т. В. Полозової та ін. Харків: Харківський національний університет радіоелектроніки, 2019. 133 с.

Збірник містить наукові статті здобувачів другого (магістерського) рівня вищої освіти кафедри економічної кібернетики та управління економічною безпекою Харківського національного університету радіоелектроніки, які навчаються за спеціальностями 051 Економіка освітньо-професійної програми «Економічна кібернетика» та 073 Менеджмент освітньо-професійної програми «Управління фінансово-економічною безпекою». Статті подано в авторській редакції.

ЗМІСТ

Лотвінова В.В.,
науковий керівник
Кирій В.В., к.е.н , доцент

ВИКОРИСТАННЯ РИЗИК-МЕНЕДЖМЕНТУ ДЛЯ ЗАБЕЗПЕЧЕННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ ІТ-ПІДПРИЄМСТВА

У статті розглянуті питання забезпечення безпеки ІТ-підприємства шляхом впровадження ризик-менеджменту. Метою статті є огляд кроків ризик-менеджменту для забезпечення економічної безпеки ІТ-підприємства.

This article focuses on risk management as an IT-enterprise security tool. The purpose of the article is to review the steps of risk management to ensure the economic security of an IT-company.

В умовах постійних загроз навколишнього середовища суб'єкти господарювання все частіше стикаються з проблемами забезпечення ефективності своєї діяльності, а це викликано тим, що виникаючі явища та тенденції розвитку навколишнього середовища найчастіше не мають позитивного впливу на функціонування суб'єктів господарювання. Ось чому виникає необхідність захисту позицій підприємства на конкурентних ринках, який забезпечить економічну безпеку суб'єкту господарювання, та є логічною відповіддю на негативні зміни зовнішнього середовища.

Термін «економічна безпека» вперше був використаний під час Великої депресії в Сполучених Штатах. У той час ідея економічної безпеки була пов'язана з окремими особами, і заходи щодо її забезпечення були спрямовані на гармонізацію соціальної ситуації в державі, а також на розвиток системи змін державних пенсійних доходів і соціального страхування безробітних. В Україні термін «економічна безпека» вперше згадується в період незалежності.

Економічна безпека підприємства – це система, в якій воно здатне адекватно і ефективно реагувати на всі існуючі загрози, як внутрішні, так і зовнішні. Економічна безпека підприємства визначається як складна категорія, яка використовує економічну здатність системи підприємства та створена на ньому для протидії дестабілізуючих впливів внутрішніх і зовнішніх факторів і забезпечення ефективного використання ресурсів (капіталу, персоналу, технологій, інформації тощо), наявних ринкових можливостей (конкурентоспроможність), а також виконує інші базові завдання в поточному періоді та в майбутньому. Існує також концепція «інтегрованої системи забезпечення економічної безпеки», яка включає в себе конкретний набір взаємозв'язних елементів (організаційного, економічного та правового характеру), який, у разі досягнення підприємством головних цілей бізнесу, забезпечує захист від реальних або потенційних загроз, які можуть привести до матеріального збитку [1].

Матеріальною основою економічної безпеки підприємства є його економічний потенціал, який визначає можливість захисту економічної системи від несприятливих впливів внутрішнього та зовнішнього середовища. Аналіз

численних зовнішніх небезпек та загроз, напрямків та об'єктів їх дій, можливих наслідків для бізнесу, пов'язаний із довготривалими дослідженнями. Тим не менш, кожне підприємство і, перш за все, його вищий менеджмент, враховуючи конкретну ситуацію, з якою стикаються у бізнесі, повинні визначити (передбачити) найбільш значущі (небезпечні) проблеми та розробити систему заходів щодо їх своєчасного виявлення, зменшення їх впливу, запобігання.

Для ІТ-компанії проектна діяльність є основним засобом отримання економічних вигід. Забезпечення безпеки кожного проекту є шляхом до забезпечення економічної безпеки ІТ-підприємства в цілому.

Відповідно до видання PMBOK (Project Management Body of Knowledge, Project Management), проект визначається як «тимчасове починання з початком і кінцем, і його потрібно використовувати для створення унікального продукту, послуги чи результату». Це визначення проекту означає, що проекти – це ті роботи, які не можуть тривати нескінченно і мають певну мету [2].

Проектом називають діяльність, яка спрямована на створення унікального продукту чи послуги, а тому діяльність, яка проводиться для здійснення рутинної діяльності, не може вважатися проектом [2].

Слід пам'ятати, що термін тимчасовий не поширюється на результат або послугу, що формується проектом. Наприклад, проект будівництва пам'ятника матиме тривалий період, тоді як результат, який є пам'ятником, зберігається нескінченно довго.

Проект це завжди унікальна діяльність. Звичайно, багато споруджених офісних будівель багато в чому схожі, але кожна окрема споруда по-своєму унікальна.

Нарешті, проект повинен поступово створюватися. З цього виходить, що проект прогресує поетапно і продовжується поступово. Також це означає, що бачення проекту вдосконалюється на кожному кроці, і в кінцевому підсумку визначається мета прогресу. З огляду на це бачимо, що проект спочатку визначається не в повній мірі, а потім, протягом прогресування проекту, переглядається з часом визначення та додається більше ясності до обсягу проекту, а також до основних припущень щодо проекту.

Фази проекту складають його життєвий цикл. Менеджерам проектів зручно ділити проект на фази для контролю та моніторингу. Кожна віха на кожному етапі потім розробляється та контролюється для її вчасного завершення. Основні етапи проекту залежать від типу проекту, який виконується.

Мета кожної фази проекту – це набір результатів, які узгоджуються до початку проекту. Наприклад, під час розробки програмного забезпечення на етапі формування вимог необхідно створити документи, що відносяться до вимог, описати фази проектування, проектні документи, тощо. Етап розробки проекту забезпечує завершений код, тоді як на етапі тестування йдеться про завершене тестування результатів [3].

Кожна фаза проекту пов'язана з певним етапом, і перелік результатів, як очікується, забезпечить кожна фаза, потім відстежується на відповідність вимогам та завершення. Життєвий цикл проекту складається з ініціювання,

виконання, контролю та закриття процесів, як описано в PMBOK [2] . Кожен з цих процесів необхідний для того, щоб проект залишався на вірному шляху виконання та був завершений відповідно до технічних умов.

Забезпечення безпеки проектів в IT-компанії досягається за допомогою розробки заходів з ризик-менеджменту.

Ризик-менеджмент – це процес виявлення, оцінки та контролю загроз капіталу та прибутку організації. Ці загрози чи ризики можуть виникати з найрізноманітніших джерел, включаючи фінансову невизначеність, юридичні зобов'язання, помилки стратегічного управління, аварії та стихійні лиха. Загрози безпеці IT-підприємства та ризики, пов'язані з даними, стали головним пріоритетом в розробці стратегії управління ризиками для IT-компаній. Як результат, план управління ризиками включає все більше процесів компанії щодо виявлення та контролю загроз її цифровим активам, включаючи власні корпоративні дані, особисту інформацію клієнта та інтелектуальну власність.

Усі ризики функціонування IT-підприємства можна розподілити по категоріям. Загальноприйнятим способом структурування категорій ризиків IT-компанії є використання ієрархічної структури ризиків (risk breakdown structure, RBS), яка є ієрархічним представленням потенційних джерел ризику. RBS допомагає команді проекту враховувати в повному обсязі джерела, з яких можуть виникати індивідуальні ризики проекту. Це може бути корисним при ідентифікації ризиків або в процесі розподілу за категоріями ідентифікованих ризиків. У тих випадках, коли RBS не використовується, організація може застосувати звичайну структуру категоризації ризиків, яка може приймати форму простого переліку категорій або структури, заснованої на цілях проекту.

Кожен бізнес стикається з ризиком виникнення несподіваних загроз, які можуть принести грошові збитки або призвести до її закриття. Управління ризиками дозволяє організаціям спробувати підготуватися до несподіваного шляхом мінімізації ризиків та додаткових витрат до того, як вони відбудуться.

Реалізуючи план управління ризиками та розглядаючи різні потенційні ризики чи події до їх виникнення, організація може заощадити гроші та захистити своє майбутнє. Саме тому надійний план управління ризиками допоможе компанії встановити процедури, щоб уникнути потенційних загроз, мінімізувати вплив у разі їх виникнення та справитись із результатами. Ця здатність розуміти та контролювати ризик дозволить організаціям відчувати себе впевненіше у своїх бізнес-рішеннях. Крім того, чіткі принципи корпоративного управління, які зосереджені на управлінні ризиками, можуть допомогти компанії досягти своїх фінансових цілей.

Усі плани управління ризиками включають ті ж кроки, які поєднуються для формування загального процесу управління ризиками, а саме:

– визначення контексту. Необхідно визначити обставини, в яких відбуватиметься процес. Критерії, що будуть використані для оцінки ризику, також повинні бути встановлені та визначена структура аналізу ризиків;

– ідентифікація ризиків. Компанії потрібно визначити потенційні ризики, які можуть негативно вплинути на конкретний процес чи проект;

– аналіз ризиків. Після ідентифікації ризиків компанія визначає шанси їх виникнення, а також можливі наслідки. Метою аналізу ризиків є подальше розуміння кожного конкретного випадку ризику та яким чином це може впливати на проекти та завдання компанії;

– оцінка ризиків. Також ризик потрібно додатково оцінити після визначення загальної ймовірності виникнення ризику в поєднанні з його загальним наслідком. Після цього компанія може приймати рішення щодо того, чи є ризик прийнятним і чи бажає компанія прийняти його;

– мінімізація ризиків. Під час цього кроку компанії необхідно оцінити свої ризики з найвищим рейтингом та розробити план їх мінімізації за допомогою контролю за ризиками. Ці плани включають процеси зменшення ризику, тактику запобігання ризикам та плани на випадок надзвичайних ситуацій у разі, якщо ризик буде реалізований;

– моніторинг ризиків. Частина плану мінімізації наслідків включає спостереження як за ризиками, так і за загальним планом постійного моніторингу та відстеження нових та існуючих ризиків;

– обговорення та консультації. Внутрішні та зовнішні зацікавлені особи повинні бути залучені у обговорення та консультації на кожному відповідному етапі процесу управління ризиками та стосовно проекту в цілому [2].

За допомогою розробленої стратегії ризик-менеджменту та виконання наведених вище кроків можна забезпечити економічну безпеку проектів та IT-підприємства в цілому. З цього випливає, що ризик-менеджмент є необхідною та невід'ємною частиною керування проектами.

Перелік джерел посилання

1. Ніколаюк С.І., Никифорчук Д.Й. Безпека суб'єктів підприємницької діяльності : курс лекцій. Київ: КНТ, 2005. 320 с.

2. Project management institute. A guide to the Project Management Body of Knowledge: book. Project Management Institute, Inc. Newtown, 2017. 762 p.

3. International Institute of Business Analysis. A guide to the Business Analysis Body of Knowledge: book. International Institute of Business Analysis, Toronto, 2015. 514 p.

ДОДАТОК Б

Таблиця Б.1 - Технічні терміни та скорочення

Термін	Визначення
Зацікавлена сторона	Особа або організація (наприклад споживач, спонсор, виконавча організація або громадськість), які активно залучені в проект, або на чиї інтереси можуть позитивно або негативно вплинути виконання чи завершення проекту. Зацікавлена сторона також може впливати на проект і його результати.
Ієрархічна структура ризиків	Ієрархічно організоване подання ідентифікованих ризиків проекту, розподілених за категоріями і підкатегоріями ризику, що вказує на різні області і джерела можливих ризиків. Ієрархічна структура ризиків часто буває адаптована під конкретні типи проектів.
PM	Менеджер проекту
BA	Бізнес-аналітик
TL	Технічний лід
CEO	Директор
HR	Спеціаліст з керування кадрами
Скоуп	Сукупність робіт, необхідних для завершення проекту
Флоу	Шляхи використання продукту
Спринт	Ітерація розробки (2 тижні)
Спайк	Час для вивчення проблеми та моделювання її вирішення
API	Опис способів, якими одна комп'ютерна програма може взаємодіяти з іншою програмою.

ДОДАТОК В

Таблиця В.1 - Ідентифікатор ризику, розподіл ролей і відповідальностей за технічні ризики

ID	Назва ризику	Відповідальний
TR1	Зацікавлені особи можуть додавати функції до продукту, які не були затверджені;	PM
TR2	Команда проекту може не визначити всі результати розробки, які можуть потребувати змін пізніше;	TL
TR3	Вимоги можуть бути неправильно проаналізовані та зрозумілі	BA
TR4	Команда проекту може не визначити всіх заходів, необхідних для створення результатів	TL, BA, PM
TR5	Помилково визначені зацікавлені сторони	BA
TR6	Неоднозначні вимоги	BA
TR7	Неповні вимоги	BA
TR8	Суперечливі вимоги	BA, TL
TR9	Незадокументовані припущення	BA
TR10	Недооцінка або переоцінка вартості проекту	PM
TR11	Недооцінка або переоцінка часових меж проекту	PM
TR12	Архітектурний ризик	TL
TR13	Якість даних	TL
TR14	Інтеграційний ризик	TL
TR15	Ризик партнера	TL, PM
TR16	Загрози безпеці	TL

ДОДАТОК Г

Таблиця Г.1 - Ідентифікатор ризику, розподіл ролей і відповідальностей за управлінські ризики

ID	Назва ризику	Відповідальний
MR1	Неорганізованість процесів.	CEO, PM
MR2	Неправильна оцінка часу або вартості проекту	CEO, PM, TL
MR3	Неналаштована комунікація з клієнтом	PM, BA
MR4	Структурні ризики	TL, BA
MR5	Компонентні ризики	TL, BA
MR6	Ризик невиконання платіжного календаря	CEO
MR7	Неможливість забезпечення кваліфікованого фахівця у встановлені терміни	CEO, PM, HR
MR8	Не пропрацьований план комунікації із заінтересованими особами	BA
MR9	Недостатня комунікація команди та заінтересованих осіб	PM, BA
MR10	Недостатнє розуміння доменної області бізнесу замовника	PM, BA

ДОДАТОК Д

Таблиця Д.1 - Ідентифікатор ризику, розподіл ролей і відповідальностей за комерційні ризики

ID	Назва ризику	Відповідальний
CR1	Недостатньо прописані пункти договору	CEO, PM
CR2	Невизначені строки оплати рахунків	CEO, PM
CR3	Обмеженість відповідальності за продукт, або надзвичайно велика відповідальність	CEO

Таблиця Д.2 - Ідентифікатор ризику, розподіл ролей і відповідальностей за зовнішні ризики

	Назва ризику	Відповідальний
ER1	Регуляторні ризики	CEO
ECR2	Ціноутворення	CEO
ER3	Інновації	CEO
ER4	Ресурси	CEO, HR
ER5	Політичний стан	CEO

ДОДАТОК Е

Таблиця Е.1 - Повний перелік термінів ризиків та проти ризикових заходів

Протиризиковий захід	Назва ризику	Періодичність або прогнозована дата	Граничний термін	Відповідальний
Скоуп моніторинг	Зацікавлені особи можуть додавати функції до продукту, які не були затверджені	Впродовж усього проекту	Кінець проекту	PM
Прорахунок усіх можливих флоу додатку	Команда проекту може не визначити всі результати розробки, які можуть потребувати змін пізніше	На стартових стадіях розробки	Кінець другого спринта	TL
Підтвердження вимог перед початком кожного спринта	Вимоги можуть бути неправильно проаналізовані та зрозумілі	Перед кожним спринтом	Кінець проекту	BA
Технічний спайк перед кожним спринтом	Команда проекту може не визначити всіх заходів, необхідних для створення результатів	Перед кожним спринтом	Кінець проекту	TL, BA, PM
Перевірка та підтвердження списку зацікавлених сторін	Помилково визначені зацікавлені сторони	На стартових стадіях розробки	Другий спринт	BA
Використання широкого рангу технік виявлення вимог та підтвердження їх	Неоднозначні вимоги	Перед кожним спринтом	Кінець проекту	BA
Використання широкого рангу технік виявлення вимог та підтвердження їх	Неповні вимоги	Перед кожним спринтом	Кінець проекту	BA

Протиризиковий захід	Назва ризику	Періодичність або прогнозована дата	Граничний термін	Відповідальний
Використання широкого рангу технік виявлення вимог та підтвердження їх, технічні перевірки можливості виконання вимог	Суперечливі вимоги	Перед кожним спринтом	Кінець проекту	BA, TL
Моніторинг припущень щодо кожної вимоги	Незадокументовані припущення	Перед кожним спринтом	Кінець проекту	BA
Використання адекватних технік оцінки вартості, без бажання зробити вартість більш привабливою,ніж у конкурентів	Недооцінка або переоцінка вартості проекту	с	Другий спринт	PM
Використання адекватних технік оцінки вартості, без бажання зробити часові межі більш привабливими, ніж у конкурентів	Недооцінка або переоцінка часових меж проекту	На стартових стадіях розробки	Другий спринт	PM
Технічний спайк на старті проекту, ввід фази вивчення	Архітектурний ризик	Старт проекту	Другий спринт	TL
Висока якість коду та детальне тестування	Якість даних	Впродовж усього проекту	Кінець проекту	TL
Технічний спайк, створення тестової, моделі додатку	Інтеграційний ризик	Стадія інтеграції зі сторонніми API	Кінець проекту	TL
Технічний спайк, створення тестової, моделі додатку	Ризик партнера	Стадія інтеграції зі сторонніми API	Кінець проекту	TL, PM
Використання високих стандарів захисту данних(fips 140)	Загрози безпеці	Впродовж життєвого циклу додатку	Впродовж життєвого циклу додатку	TL
Документування процесів за допомогою BPMN	Неорганізованість процесів	Впродовж усього проекту	Кінець проекту	CEO, PM

Протиризиковий захід	Назва ризику	Періодичність або прогнозована дата	Граничний термін	Відповідальний
Використання адекватних технік оцінки вартості, без бажання зробити часові межі більш привабливими, ніж у конкурентів	Неправильна оцінка часу або вартості проекту	На стартових стадіях розробки	Другий спринт	CEO, PM, TL
Створення плану коммунікації з клиентом та узгодження його з кліентом	Неналаштована комунікація з клієнтом	Впродовж усього проекту	Кінець проекту	PM, BA
Технічні спайки	Структурні ризики	Впродовж усього проекту	Впродовж життєвого циклу додатку	TL, BA
Технічні спайки	Компонентні ризики	Впродовж усього проекту	Впродовж життєвого циклу додатку	TL, BA
Обговорення платіжних зобов'язань та мір при невиконанні платіжного календаря	Ризик невиконання платіжного календаря	Впродовж усього проекту	Кінець проекту	CEO
Створення гідних трудових умов, мотивація розвитку, політика лояльності	Неможливість забезпечення кваліфікованого фахівця у встановлені терміни	Впродовж усього проекту	Кінець проекту	CEO, PM, HR
Створення документації плану коммунікації з клиентом та узгодження його з кліентом	Не пропрацьований план комунікації із заінтересованими особами	Впродовж усього проекту	Кінець проекту	BA
Створений та пропрацьований план комунікації з кліентом, пояснення необхідності коммунікації	Недостатня комунікація команди та заінтересованих осіб	Впродовж усього проекту	Кінець проекту	PM, BA
Вивчення доменної області бізнесу замовника	Недостатнє розуміння доменної області бізнесу замовника	На старті проекту	Кінець проекту	PM, BA

Протиризиковий захід	Назва ризику	Періодичність або прогнозована дата	Граничний термін	Відповідальний
Моделювання та документування усіх можливих дій усіх зацікавлених сторін	Недостатньо прописані пункти договору	Старт проекту	Кінець проекту	CEO, PM
Створення договору оплати рахунків	Невизначені строки оплати рахунків	Старт проекту	Другий спринт	CEO, PM
Обговорення та документування відповідальності за продукт	Обмеженість відповідальності за продукт, або надзвичайно велика відповідальність	Старт проекту	Впродовж усього життєвого циклу проекту	CEO
Розроблення запасного плану роботи організації	Регуляторні ризики	Впродовж усього життєвого циклу роботи організації	Впродовж усього життєвого циклу роботи організації	CEO
Постійний моніторинг IT ринку	Інновації	Впродовж усього життєвого циклу роботи організації	Впродовж усього життєвого циклу роботи організації	CEO
Створення гідних трудових умов, мотивація розвитку, політика лояльності	Ресурси	Впродовж усього життєвого циклу роботи організації	Впродовж усього життєвого циклу роботи організації	CEO, HR
Розроблення запасного плану роботи організації	Політичний стан	Впродовж усього життєвого циклу роботи організації	Впродовж усього життєвого циклу роботи організації	CEO