Електронне наукове фахове видання "Ефективна економіка" включено до переліку наукових фахових видань України з питань економіки (Наказ Міністерства освіти і науки України від 29.12.2014 № 1528)

Ефективна ЕКОНОМІКА

Дніпропетровський державний аграрно-економічний університет

№ 10, 2016 Назад Головна

0 0 0 0 0 0 0 0

УДК 338.47

М. В. Шашина,
кандидат економічних наук, доцент кафедри економіки і підприємництва
НТУ України «Київський політехнічний інститут ім. Ігоря Сікорського», м. Київ
В. В. Володін,
магістр, НТУ України «Київський політехнічний інститут ім. Ігоря Сікорського», м. Київ

ІНФОРМАЦІЙНА СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

M. Shashina,
PhD, Associate Professor of Department of Economics and Business
National Technical University of Ukraine " Igor Sikorsky Kyiv Polytechnic Institute ", Kyiv
V. Volodin,
magister, National Technical University of Ukraine «Igor Sikorsky Kyiv polytechnic institute», Kyiv

INFORMATIONAL COMPONENT OF ECONOMC SECURITY

Для сучасного суспільства на перший план виходять інформація, передача нових знань, технічних та наукових ідей. Як результат, з'являється необхідність у пошуку шляхів вимірювання, управління, оптимізації витрат та покращення сервісу захисту інформації, з метою обгрунтування адекватності заходів захисту бізнеса підприємства. У статті проведено аналіз підходів щодо оцінки сукупної вартості володіння для підсистем інформаційної безпеки. Розкрито та деталізовано поняття інормаційної безпеки підприємства. Визначено взаємозв'язок між витратами на інформаційну безпеку підприємства та рівнем його захищеності. Наведеного приклад типового розподілу витрат на економічну безпеку та його оптимізація. Досліджено методики оцінки витрат на інформаційну безпеку та надано алгоритм прийняття рішень щодо розробки методики оцінки витрат на інформаційну безпеку.

For modern society on the fore is information, transfering of new knowledge, technical and scientific ideas. As a result, necessary to find ways to measure, manage, optimize costs and improve information protection service in order to reasoning the adequacy of steps in the case of protection enterprise business. The article analyzes approaches TCO assessment for information security subsystems. Concept of informational security were disclosed and detalied. Also, we identified the correlation between costs on the company informational security and by general level of company protection. Showed, as an example, typical costs distribution on the economic security and its optimization. Studied cost method of valuation information security and presented algorithm and decision-making metod to develop cost valuation for IS.

Ключові слова: *Інформаційна безпека, економічні аспекти, сукупна вартість володіння, оцінка витрат на інформаційну безпеку.*

Keywords: *Information security, economic aspects, the total cost of ownership, assessment costs for information security.*

Постановка проблеми. Необхідність розгляду інформаційної складової економічної безпеки та її економічних аспектів обумовлено зростаючою важливістю інформації в цілому в суспільстві та економіки, в тому числі, потребою захисту економічних інтересів підприємства та держави.

Ринок інформаційних технологій останні декілька років динамічно розвивається, за оцінками експертів його ріст перевищує 10% в рік. При цьому сектор інформаційної безпеки розвивається ще більшими темпами – більше ніж на 25% в рік. Все це можна пояснити двома факторами: зросла увага керівництва до забезпечення інформаційної безпеки та недостатній рівень інформаційних безпек в сучасних інформаційних технологіях.

Впровадження сучасних інформаційних технологій звичайно пов'язане із значними інвестиціями і, відповідно, з необхідністю обгрунтування ефективності цих інвестицій. З іншого боку, щоб планувати бюджет на основі реальних комерційних показників, потрібно ясно уявляти собі статті витрат і чинники, які їх формують. Особливо гостро ця проблема стоїть при інтеграції даних систем, коли необхідно управляти інфраструктурою декількох напрямів діяльності підприємства.

Темпи росту сектора інформаційної безпеки за часом почнуть сповільнюватись, так як вони не зможуть перебувати постійно в такому режимі, тобто через певний проміжок часу питання витрат на забезпечення інформаційної складової економічної безпеки набере надзвичайної актуальності.

Аналіз останніх досліджень: Дослідженню інформаційної складової економічної безпеки підприємства присвячено праці науковців: R. Witty, J. Dubiel, J. Girard, J. Graff, A. Hallawell, B. Hildreth, N. MacDonald, W. Malik, J. Pescatore, M. Reynolds, K. Russell, A. Weintraub, V. Wheatman[1], Сімонов С.В.[2] Кузьмін А.С., Бочков С.І., Івін Ю.Е.[3], Скрипкін К.Г. [4], Петренко С.А [6], Костава В.А. [7].

Формулювання цілей статті(постановка завдання): Дослідження інформаційної складової економічної безпеки, задля визначення шляхів оптимізації витрат на економічну безпеку підприємства, а також визначення взаємозв'язку між витратами на інформаційну безпеку та рівнем захищеності підприємства в цілому Для досягнення поставлених цілей дослідити існуючі методики оцінки витрат на інформаційну безпеку та проаналізувати існуючі підходи до оцінки сукупної вартості володіння.

Виклад основного матеріалу дослідження. В умовах інформаційної ери, коли ведеться інформаційна війна, змусило не те що підприємства продумувати

свою інформаційну стратегію, а й державам приділяти більш прискіпливу увагу інформаційній безпеці.

В загальному розумінні поняття «економічної безпеки підприємства» тлумачиться як здатність мобілізації та найбільш оптимального управління корпоративними ресурсами підприємства, з метою найбільш ефективного їх використання і забезпечення стійкого функціонування, його активну протидію будь-яким негативним чинникам впливу на власну економічну безпеку[1].

Динамічність розвитку інформаційних технологій, тобто збільшення вимог до забезпечення інформаціної безпеки, яку одну із складових економічної безпеки зумовило те, що уже сьогодні витрати на забезпечення режиму інформаційної безпеки складають 30% всіх затрат на інформаційні системи, що змушує власників підприємств задумуватись над економічними аспектами забезпечення інформаційної безпеки. Із збільшенням зацікавленості власників інформаційною безпекою(ІБ) та її вартістю, перед технічними працівниками постає питання обгрунтування затрат на підвищення рівня забезпечення ІБ, тобто як пояснити керівництву доцільність/ефективність інвестицій в ІБ. У практиці зарубіжних компаній основою для вирішення даного питання є методика оцінки сукупної вартості володіння ІТ.

Методика сукупної вартості володіння ІТ, можна сказати, що дана методика дозволяє керівництву служб інформаційної безпеки обгрунтовувати бюджет на ІБ, доводити ефективність роботи працівників служби ІБ, тобто дана методика може використовуватись як доказ економічної ефективності наявних систем захисту інформації. Також дана методика робить систему захисту ІБ вимірюваною, з'являється можливість оперативно вирішувати задачі контроля і корекції показників економічної ефективності, тобто самого показника сукупної вартості володіння.

Сукупна вартість володіння – це сума прямих та непрямих витрат, які несе власник системи за період її життєвого циклу. Життєвий цикл, на якому розгдлядаються прямі на непрямі витрати. *Прямі витрати* включають в себе три основні складові:

- Основні витрати: створення ІС; обладнання (сервери, клієнтські місця, периферія, мережеві компоненти); програмне забезпечення; додатки, утиліти, керуюче програмне забезпечення; модернізація;
- Експлуатаційні витрати: управління задачами (система, мережа, масиви пам'яті); підпримка працездатності системи(персонал, довідкова служба, навчання, закупівля, розробка інфраструктури);
- Інші витрати: створення комунікацій – глобальні мережі, взаємодія постачальника сервісу, дистанційний доступ, інтернет, доступ клієнта; управління і підпримка – аутсорсинг, супровід.

В свою чергу *непрямі витрати* – це видатки на контроль, відправлення й одержання пошти, телефонні розмови, уведення інформації, переклади, видатки на приміщення, втрати від планових і позапланових простоїв, комунальні послуги.

Підхід до оцінки СВВ базується на результатах аудиту структури і поведінки корпоративної системи захисту інформації та інформаційних систем в цілому, включаючи, звісно ж, дії працівників служб автоматизації, інформаційної безпеки та користувачів інформаційної системи. Збір та аналіз статистики по структурі витрат проводиться протягом 12 місяців. Отримані дані оцінюються по ряду критерії та порівнюються з аналогічними підприємства галузі. За допомогою даної методики оцінюється та порівнюється ступінь захищеності ІС, звернути увагу на критичні точки в організації захисту й потім на основі отриманих даних побудувати економічну стратегію розвитку інформаційної безпеки. Звісно ж не потрібно забувати, що це зарубіжна методика й вона потребує адаптації під українське ринкове середовище, правову базу й т.п[2].

В загальному виразі визначення витрат підприємства на ІБ можна згрупувати на вирішення 3-ох завдань:

- Оцінка поточного рівня СВВ системи захисту інформації та інформаційних систем(ІС) в цілому (збір інформації та розрахунок показників СВВ компанії);
- Аудит ІБ підприємства на основі порівння СВВ компанії та рекомендованого рівня;
- Формування цільвої моделі.

Зобразимо кожне із перерахованих завдань (рис.1).

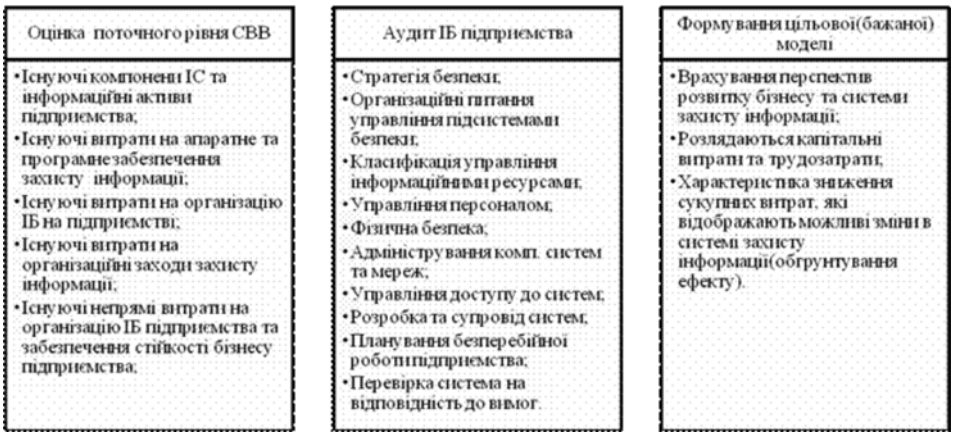

Рис. 1. Завдання визначення витрат підприємства

Як зазначилось в формувані бажаної моделі, що суттєвим для власників є зниження сукупних витрати або ж їх оптимізація. Тобто, можна сказати, що за допомогою даної методики можна визначити не тільки вартість певних елементів і зв'язків системи захисту інформації протягом їх життєвого циклу, а й допоможе відділу ІБ вимірювати, керувати, знижувати, оптимізувати витрати та покращувати рівень сервіса захисту інформації, з метою адекватності заходів захисту бізнесу підприємства. Але ми ж розуміємо, що кожна методика має певні межі свого застосування. Розглянемо межі застосування СВВ. Постановка задачі аналізу ефективності інвестицій на забезпеченні ІБ залежить від рівня зрілості компанії. Приведемо можливу класифікацію організації по рівню зрілості:

- Анархія;
- Фолькльор;
- Стандарти;
- Вимірюваний;
- Оптимізуємий.

Зрозуміло, що така методика є дієвою на останніх 2-х рівнях, бути частково корисною на рівні «Стандарти» і бути некорисною на перших 2-х рівнях. При використанні економічних методів аналізу ефективності інвестицій в ІБ потрібно пам'ятати, що існують «неекономічні» змінні, які є не менш важливими при аргументації прийняття певних рішень, наприклад:

- Структура організації та особливості системи управління;
- Обізнаність та залученість керівництва в розвиток інформаційних технологій;
- Особливості стратегії організації;
- Позиції керівництва відділів ІТ та ІБ в компанії;
- Роль ІТ у виробничому процесі;
- Інцеденти, які траплялись в сфері ІБ з тяжкими наслідками.

Дані фактори потрібно обов'язково включати на рівні з економічними при складанні аналітичних матеріалів.

Далі логічним є розглянути як можна визначити прямі та непрямі витрати на ІБ з врахування специфіки українських компаній. Задача, яку ми перед собою ставимо – це те, щоб затребуваний рівень захисту ресурсів справді досягався й відповідав очікуванням керівництва компанії. У зв'язку з цим необхідно відповісти на низку основних питань. При цьому ми припускаємо, що керівництво компанії проводить роботи по впровадженню на підприємство систему захисту інформації[3].

Визначені всі об'єкти і цілі захисту, загрози інформаційній безпеці і мірі для протидії, закуплені та встановлені необхідні засоби захисту інформації. Питання, пов'язані із затратами на ІБ, є наступними:

- Що таке витрати на інформаційну безпеку ?
- Чи неминучими є витрати на інформаційну безпеку ?
- Яка залежність між затратами на ІБ та досяжним рівнем ІБ ?
- Чи складають витрати на ІБ істотну частину від обороту компанії ?
- Яку користь принесе аналіз витрат на ІБ?

Коротко розглянемо можливі відповіді на поставлені питання.

Що ж таке витрати на інформаційну безпеку ? . Як правило витрати на ІБ поділяються на наступні категорії :

- Організаційні витрати – витрати на формування і підтримку ланок управління системою захисту інформації;
- Витрати на контроль – конкретне і підтверджене досягнуто рівня захищеності ресурсів підприємства;
- Внутрішні витрати на ліквідацію наслідків порушення політики інформаційної безпеки (ППБ) – витрати понесені підприємством в результаті того, що потрібний рівень не був досягнутий;
- Зовнішні витрати на ліквідацію наслідків порушення політики інформаційної безпеки – компенсації втрат при ППБ у випадках пов'язаниз із витіканням інформації, втратою іміджа, тощо;
- Витрати на технічне обслуговування систем захисту інформації і заходів попередження ППБ – витрати на попереджувальні заходи

Поділити дані затрати можна на одиничні та систематичні. Класифікація витрат умовна, так як все залежить від особливостей конкретної компанії. Основне при визначенні затрат є взаєморозуміння та згода за статтями витрат в середині підприємства[4].

З приводу *наступного питання* можна чітко відповісти, що повністю уникнути витрат на ІБ неможливо, але, звісно ж, їх можна звести до прийнятного рівня. Тобто їх можна поділити на необхідні та ті, які можна зменшити/виключити. До останніх можна віднести ті затрати, які при відсутності порушень політики безпеки або зменшаться, тобто негативний вплив порушень зменшиться. Що ж до необхідних – такі затрати, які потрібні навіть коли рівень загроз безпеки досить низький, отже це затрати на підтримку досягнутого рівня захищеності інформаційного середовища.

Наступним є *визначення залежності між ІБ та рівнем захищенності*. Сума всіх витрат підвищення рівня захищенності від загроз інформаційної безпеки складає Загальні витрати на безпеку. Взаємозв'язок між всіма витратами на безпеку, загальними витратами на безпеку і рівнем захищенності інформаційного середовища підприємства можна зобразати за допомогою функції рис. 2.[5].

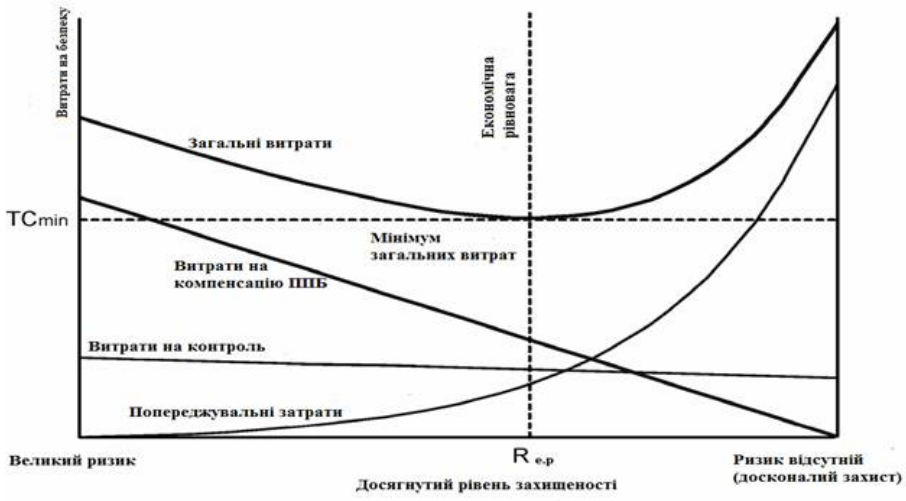

Рис.2. Взаємозв'язок між витратами на безпеку та досяжним рівнем захищеності

Загальні витрати на безпеку складаються з витрат на попереджувальні заходи, витрат на контроль і поповнення втрат (зовнішніх і внутрішніх). Зі зміною рівня захищеності інформаційного середовища змінюються величини складових загальних витрат і, відповідно, їх сума – загальні витрати на безпеку. Ми не включаємо в даному випадку одноразові витрати на формування політики інформаційної безпеки підприємства, оскільки припускаємо, що така політика вже розроблена.

Зниження загальних витрат. На рис. 2 зображено, що досяжний рівень захищеності вимірюється в категоріях «великий ризик» та «ризик відсутній». Розглядаючи ліву сторону графіку, ми може спостерігати, що загальні витрати досить високі, в основному це пов'язано із високими втратами на компенсацію при порушенні політики безпеки. Витрати на обслуговування системи безпеки досить малі. Якщо ж ми будем рухатись вправо по графіку, то досяжний рівень захищеності буде збільшуватись за рахунок збільшення об'ємів попереджувальних заходів, які, в свою чергу, пов'язані з обслуговуванням системи захисту. Витрати на компенсацію ППБ(порушень політики безпеки) зменшуються за рахунок попереджувальних дій. Як зображено на графіку , на даній стадії затрати на втрати падають швидше, аніж зростають витрати на поперджувальні заходи. Результатом цього є те, що загальні витрати на безпеку зменшуються. Зміни об'єму витрат на контроль є незначними[6].

Збільшення загальних витрат. Якщо рухатись по графіку вправо за точку економічної рівноваги(досяжний рівень захищеноті збільшується) ситуація починає змінюватись. Намагаючись досягти стабільності зниження затрат на компенсацію порушень політики безпеки, ми бачимо, що витрати на попереджувальні заходи зростають все швидше. З цього виходить, що істотна кількість ресурсів повинно витратитись для досягнення незначного зниження рівня ризику.

Потрібно також сказати, що графік (рис.2) відображає загальний випадок, так як побудований з врахуванням деяких припущень, які не завжди відповідають реальним ситуаціям.

Перше припущення заключається в тому, що попереджувальна діяльність по технічному обслуговування і попередження політики безпеки підприємства діє згідно того, що в першу чергу розглядаються ті проблеми, рішення яких дасть найбільший ефект по зниженню рівня ризику

Друге припущення заключається в тому, що точка економічної рівноваги не змінюється в часі. На практиці дане припущення часто не виконується. Основні фактори:

- Ефективність попереджувальної діяльності невелика. В даній моделі, що така діяльність дозволяє не повторяти вже допущені помилки. На практиці це не так, для досягнення потрібного ефекта потрібні набагато більші затрати. В результаті цього точка екон.рівноваги зміщується вправо;
- Старіння системи ІБ;
- Розробники засобів захисту не поспівають за активністю злочинців. Крім того інформатизація підприємства може зпричинити нові проблеми, які потребують додаткових попереджувальних затрат. Це може змістити економічну рівновагу в напрямку лівого краю графіка[7].

Проведемо оцінку частини витрат на ІБ в обороті компанії.

Там де витрати на ІБ належним чином враховані, то вони можуть складати від 2% до 20% і більше від об'єму продажів(обороту). Дана оцінка приведена з даних компаній, які спеціалізуються в області захисту інформації на основі аналізу стану захищеності інформаційного середовища підприємства в галузі зв'язку.

Таблиця 1.
Типовий розподіл витрат, пов'язаних з ІБ

Затрати на втрати (зовнішні та внутрішні)	70% від загальних витрат на безпеку
Витрати на контроль	25% від загальних витрат на безпеку
Витрата на попереджувальні заходи	5% від загальних витрат на безпеку

Припустимо, що вказані витрати на безпеку складають 10% від загального обороту. Потім припускаємо, що за рахунок збільшення об'єму попереджувальних заходів, тобто збільшуємо витрати на попереджувальні заходи, за рахунок чого вдалось знизити загальні витрати на безпеку до 6% від обороту.

Таблиця 2.
Приклад розподілу загальних витрат на безпеку

Затрати на втрати (зовнішні та внутрішні)	50% від загальних витрат на безпеку
Витрати на контроль	25% від загальних витрат на безпеку
Витрати на попереджувальні затрати	25% від загальних витрат на безпеку

Загальні витрати на забезпечення ІБ склали тільки 60% від їх початкової величини. По відношенню до первісних загальних витрат на ІБ нове їх розподілення буде виглядати наступним чином:

Таблиця 3.
Приклад співвідношення розподілу загальних витра на ІБ

Затрати на втрати (зовнішні та внутрішні)	$\frac{50 * 60}{100}$	30% від первісної величини загальних витрат на безпеку
Витрати на контроль	$\frac{25 * 60}{100}$	15% від первісної величини загальних витрат на безпеку
Витрати на попереджувальні затрати	$\frac{25 * 60}{100}$	15% від первісної величини загальних витрат на безпеку

Тобто виходячи з отриманих даних можна зробити висновок про 40% економії загальних витрат на безпеку.

При оцінці витрат на систему безпеки на будь-якому підприємстві необхідно враховувати відсоткове співвідношення загальних витрат на безпеку і загального обсягу продажів.

Висновки. Згідно проведеного аналізу можна сказати, що поряд із методикою СВВ можна використовувати різні методи для розрахунку повернення інвестицій. Як правило, для оцінки дохідної частини спочатку аналізують ті цілі, завдання і напрями бізнесу, які потрібно досягти за допомогою впровадження або реорганізації існуючих проектів в області системної інтеграції, автоматизації та інформаційної безпеки. Далі використовують деякі вимірні показники ефективності бізнесу для оцінки окремо по кожному рішенню. Зазначені показники не потрібно вигадувати, вони існують в надлишку. Далі можна використовувати методики розрахунку коефіцієнтів повернення інвестицій в інфраструктуру підприємства (ROI), наприклад, Gartner Group. Сьогодні існує велика кількість методик і технологій розрахунку, і виміру різних показників економічної ефективності.

Список літератури.

1. R. Witty, J. Dubiel, J. Girard, J. Graff, A. Hallawell, B. Hildreth, N. MacDonald, W. Malik, J. Pescatore, M. Reynolds, K. Russell, A. Weintraub, V. Wheatman. The Price of Information Security. Gartner Research, Strategic Analysis Report,K-11-65- 34, June 2001.

2. Симонов С.В. Технологии и инструментарий для управления рисками М.: Jet Info №2, 2003.

3. Кузьмин А.С., Бочков С.И., Ивин Ю.Э. Методы обеспечения информационной безопасности в АТМ-сетях. // «Электросвязь», - М:, № 9, 2001. – С. 28-32.

4. Скрипкин К.Г. Экономическая эффективность информационных систем. М.: ДМК Пресс, 2002.

5. Технико-экономическое обоснование эффективности инвестиций в ИТ. Рекомендации по формированию ИТ-бюджетов. Оценка совокупной стоимости владения (ТСО) ИТ [Електронний ресурс] - Режим доступа: http://www.topsbi.ru/default.asp?artID=775&mode=print

6. Петренко С.А. Симонов С.В. Экономически оправданная безопасность. Управление информационными рисками. Изд. ДМК, Москва, 2003.

7. Костава В.А. Анализ методов эффективности информационных систем, конспект лекций, лекция 3. [Електронний ресурс] – Режим доступу: http://inf-man.ru

References.

1. R. Witty, J. Dubiel, J. Girard, J. Graff, A. Hallawell, B. Hildreth, N. MacDonald, W. Malik, J. Pescatore, M. Reynolds, K. Russell, A. Weintraub, V. Wheatman (2001). "The Price of Information Security". *Gartner Research, Strategic Analysis Report,*K-11-65- 34.

2. Simonov S.V. (2003)"Tehnologii i instrumentarij dlja upravlenija riskami" M.: Jet Info vol.2.

3. Kuz'min A.S., Bochkov S.I., Ivin Ju.Je. (2001). "Metody obespechenija informacionnoj bezopasnosti v ATM-setjah". Jelektrosvjaz', vol.9, . pp.. 28-32.

4. Skripkin K.G.(2002) Jekonomicheskaja jeffektivnost' informacionnyh sistem. *DMK Press*.

5. "Tehniko-jekonomicheskoe obosnovanie jeffektivnosti investicij v IT. Rekomendacii po formirovaniju IT-bjudzhetov. Ocenka sovokupnoj stoimosti vladenija (TSO) IT", Business integrator [Online], available at: http://www.topsbi.ru/default.asp?artID=775&mode=print (Accessed 10 Sept. 16).

6. Petrenko C.A. Simonov S.V.(2003) "Jekonomicheski opravdannaja bezopasnost". Upravlenie informacionnymi riskami, DMK, Moskva, RU.

7. Kostava V.A. Analiz metodov jeffektivnosti informacionnyh sistem, konspekt lekcij, lekcija 3. [Online] available at: http://inf-man.ru (Accessed 8 Sept. 16).

Стаття надійшла до редакції 24.09.2016 р.