УДК [004.738.5:004.056]:330.131.5

ЕКОНОМІЧНИЙ АНАЛІЗ РІВНІВ ЕФЕКТИВНОСТІ ТА ЯКОСТІ ІНТЕРНЕТ-ПЛАТІЖНИХ СИСТЕМ ПІДПРИЄМСТВА

© 2015 **ЮЗЕВИЧ В. М., КЛЮВАК О. В.**

УДК [004.738.5:004.056]:330.131.5

Юзевич В. М., Клювак О. В. Економічний аналіз рівнів ефективності та якості інтернет-платіжних систем підприємства

Аналізуючи, систематизуючи і узагальнюючи наукові праці багатьох учених, автори розглянули ефективність та якість інтернет-платіжних систем підприємства (ІПСП) з позицій інформаційної безпеки та здійснили економічний аналіз їх рівнів. У результаті дослідження виокремлено основні заходи безпеки (превентивні заходи безпеки sp, заходи виявлення sd та інші заходи безпеки so , спрямовані на зменшення збитків L), які застосовуються для ефективного функціонування ІПСП, і запропоновано розрахунок показника окупності інвестицій (ROI) для кожного із зазначених видів заходів безпеки. Застосовано методику оцінювання ризику на основі статистичного підходу та наведено систему математичних співвідношень, яка являє собою економетричну модель для оптимізації інтернет-платіжних систем підприємства. Ця модель (ІПСП) враховує фактори якості, ефективності, ризику, корисності. Перспективою подальших досліджень у даному напрямі є впровадження розробленої економетричної моделі у практичну діяльність суб'єктів підприємництва.

Ключові слова: *інтернет-платіжна система підприємства (ІПСП), заходи інформаційної безпеки, показник окупності інвестицій, якість, ефективність, ризик, корисність, економетрична модель оптимізації.*
Рис.: *1.* ***Формул:*** *22.* ***Бібл.:*** *9.*

Юзевич Володимир Миколайович – *доктор фізико-математичних наук, професор, завідувач кафедри економіки підприємства та інформаційних технологій, Львівський університет бізнесу та права (вул. Кульпарківська, 99, Львів, 79021, Україна)*
E-mail: *yuzevych@ukr.net*

Клювак Оксана Володимирівна – *провідний фахівець наукового відділу, Львівський інститут банківської справи Університету банківської справи Національного банку України (пр. Т. Шевченка, 9, Львів, 79005, Україна)*
E-mail: *oksana_klyuvak@bigmir.net*

УДК [004.738.5:004.056]:330.131.5

Юзевич В. Н., Клювак О. В. Экономический анализ уровней эффективности и качества интернет-платежных систем предприятия

Анализируя, систематизируя и обобщая научные труды многих ученых, авторы рассмотрели эффективность и качество интернет-платежных систем предприятия (ИПСП) с позиций информационной безопасности, а также осуществили экономический анализ их уровней. В результате исследования выделены основные меры безопасности (превентивные меры безопасности sp, меры выявления sd и другие меры безопасности so, направленные на уменьшение убытков L), которые применяются для эффективного функционирования ИПСП, и предложен расчет показателя окупаемости инвестиций (ROI) для каждого из указанных видов меры безопасности. Применена методика оценки риска на основе статистического подхода и предложена система математических соотношений, которая представляет собой эконометрическую модель для оптимизации интернет-платежных систем предприятия. Эта модель (ИПСП) учитывает факторы качества, эффективности, риска, полезности. Перспективой дальнейших исследований в данном направлении является внедрение разработанной эконометрической модели в практическую деятельность субъектов предпринимательства.

Ключевые слова: *интернет-платежная система предприятия (ИПСП), меры информационной безопасности, показатель окупаемости инвестиций, качество, эффективность, риск, полезность, эконометрическая модель оптимизации.*
Рис.: *1.* ***Формул:*** *22.* ***Библ.:*** *9.*

Юзевич Владимир Николаевич – *доктор физико-математических наук, профессор, заведующий кафедрой экономики предприятия и информационных технологий, Львовский университет бизнеса и права (ул. Кульпарковская, 99, Львов, 79021, Украина)*
E-mail: *yuzevych@ukr.net*

Клювак Оксана Владимировна – *ведущий специалист научного отдела, Львовский институт банковского дела Университета банковского дела Национального банка Украины (пр. Т. Шевченко, 9, Львов, 79005, Украина)*
E-mail: *oksana_klyuvak@bigmir.net*

UDC [004.738.5:004.056]:330.131.5

Yuzevych V. M., Klyuvak O. V. Economic Analysis of the Levels of Efficiency and Quality of Internet Payment Systems of Enterprise

Analyzing, reviewing, and summarizing the scientific works of many scientists, the authors examined the efficiency and quality of Internet payment systems of enterprise (IPSE) in terms of information security, as well as carried out an economic analysis of their levels. As result of the study major security measures have been allocated (preventive security measures sp, measures to identify sd and other security measures so, aimed to mitigate the damages L), which are used for the efficient functioning of the IPSE, and a calculation of the rate of return on investment (ROI) for each of the types of security measures has been proposed. Methods of risk assessment based on statistical approach were applied, a system of mathematical ratios was proposed, which represents an econometric model for optimization of Internet payment systems of enterprise. This model (IPSE) takes into account factors of quality, efficiency, risk, usefulness. Prospect of further research in this area is introduction of the developed econometric model into practical activities of business entities.

Key words: *Internet payment system of enterprise (IPSE), measures of information security, rate of return on investment, quality, efficiency, risk, usefulness, econometric model of optimization.*
Pic.: *1.* ***Formulae:*** *22.* ***Bibl.:*** *9.*

Yuzevych Volodymyr M. *– Doctor of Sciences (Physics and Mathematics), Professor, Head of the Department of Business Economy and Information Technology, Lviv University of Business and Law (vul. Kulparkivska, 99, Lviv, 79021, Ukraine)*
E-mail: *yuzevych@ukr.net*

Klyuvak Oksana V. *– Leading Specialist of the Research Division, Lviv Institute of Banking of University of Banking of the National Bank of Ukraine (pr. T. Shevchenka, 9, Lviv, 79005, Ukraine)*
E-mail: *oksana_klyuvak@bigmir.net*

Від інтернет-платіжних систем (ІПС) вимагається надійність, тобто довіра користувачів. Учасники системи інтернет-платежів повинні бути упевнені, що відправлені гроші будуть зараховані правильно і протягом визначеного терміну, а інформація про фінансові транзакції не буде доступна третім особам. Упевненість у платежах вимагає високого рівня ефективності та якості систем із належним контролем. Досить часто

сучасним ІПС властива невідповідність основним вимогам ефективного та якісного функціонування, що характеризується повільністю, нестачею надійності, упевненості й/або значними витратами та низьким рівнем безпеки. Тому для суб'єктів підприємницької діяльності оцінка економічної ефективності рівня інформаційної безпеки та оптимізація ІПС стають одними із найважливіших завдань.

Віддаючи належне науковим напрацюванням у сфері функціонування інтернет-платіжних систем підприємства (ІПСП), варто зазначити, що аспекти ефективності та якості залишаються недостатньо вивченими та потребують ґрунтовного вдосконалення, зокрема у сфері захищеності автентифікаційних даних під час проведення інтернет-транзакцій, економічної обґрунтованості при впровадженні та застосуванні на підприємствах заходів інформаційної безпеки. Недостатньо дослідженими залишаються фактори якості, ефективності, ризику, корисності та шляхи оптимізації ІПСП.

У своїх дослідженнях питання безпеки електронного бізнесу розглядають такі вітчизняні науковці: Н. Сулік, Ю. Бондарчук, С. Савин, А. Берко, В. Висоцька та інші. Автори Одарченко Р. С., Лукін С. Ю., Tae Hwan. Shon, Paula M. C. Swatman зосереджують свою увагу на економічній ефективності впровадження систем захисту та критеріях ефективності для інтернет-платіжних систем, зокрема [1, 2]. Питання кількісної оцінки ризиків та втрат внаслідок інтернет-шахрайств містяться у працях таких вітчизняних і закордонних дослідників: Rok Bojanc, Borka Jerman-Blažič, Michel van Eeten, Johannes M. Bauer, Shirin Tabatabaie, В. В. Домарєв, С. О. Качанов [3, 4].

Варіанти результатів оптимізації виробничої програми вітчизняних підприємств, які дають змогу вдосконалювати якість продукції і системи управління, подано у працях [5, 6].

Основним завданням статті є дослідження рівнів ефективності та якості інтернет-платіжних систем підприємства з позицій інформаційної безпеки та розроблення економетричної моделі для оптимізації їхнього функціонування.

Передумовою розробки заходів безпеки в інтернет-платіжних системах є припущення, що при порушенні захищеності активів підприємства завдається збиток усім учасникам інтернет-транзакції, а розроблення, впровадження та використання заходів безпеки передбачає певні витрати. Заходи інформаційної безпеки в інтернет-платіжних системах, зокрема методи автентифікації, повинні враховувати виникнення ризиків, а також попередити можливі втрати внаслідок шахрайських дій.

Процедура оцінювання ризику передбачає визначення вразливостей і загроз для кожного інформаційного активу (наприклад, автентифікаційних даних). Ризик безпеки R визначається як добуток ймовірності виникнення інциденту безпеки ρ і втрати внаслідок виникнення інциденту безпеки L. Імовірність виникнення інциденту безпеки ρ ($0 \le \rho \le 1$) залежить від імовірності T ($0 \le \rho \le 1$) виникнення загроз і вразливості ν [2, 3]:

$$\rho = T \cdot \nu. \quad (1)$$

У випадку виникнення інциденту безпеки суб'єкти інтернет-платіжних систем зазнають фінансових втрат L. Насправді фінансовий збиток внаслідок інциденту безпеки досить важко оцінити. Труднощі викликає оцінка непрямих ризиків, що інколи суттєво перевищують прямі та можуть мати довготривалий негативний вплив на клієнтську базу, партнерів, фінансовий ринок, банки. Кількісну оцінку збитку можна визначити за формулою [2, 3]:

$$L = L_{m\_chargeback} + L_c + L_{m\_indirect} + L_{b\_indirect}, \quad (2)$$

де $L_{m\_chargeback}$ – збитки продавця, наприклад внаслідок «чарджбеку»;

L_c – збитки покупця у розмірі вартості придбаних товарів або наданих послуг шахраєм;

$L_{m\_indirect}$ – непрямі збитки продавця довготривалого характеру: переривання бізнес-процесів, втрата репутації, втрата довіри покупців;

$L_{b\_indirect}$ – непрямі збитки підприємств довготривалого характеру: втрата репутації, втрата довіри покупців-утримувачів карток.

Елементи формули (2) можна групувати відповідно до часових показників: час виявлення інциденту безпеки t_d, час налагодження та відновлення функцій системи t_r і період часу від моменту появи інциденту до моменту виявлення інциденту t_d. Показники $L_{m\_chargeback}$ і L_c залежні від часових показників t_d і t_r. Відобразимо це у формулі (3) [2, 3]:

$$L = L_{m\_chargeback} \cdot t_r + L_c \cdot t_d \cdot t_r + \\ + L_{m\_indirect} + L_{b\_indirect}. \quad (3)$$

Враховуючи формули (1) і (3), ризики безпеки в інтернет-платіжних системах можна визначити за формулою (4):

$$R = T \cdot \nu \cdot (L_{m\_chargeback} \cdot t_r + L_c \cdot t_d \cdot t_r + \\ + L_{m\_indirect} + L_{b\_indirect}). \quad (4)$$

Заходи безпеки, які доцільно застосовувати в інтернет-платіжних системах, можна класифікувати таким чином (*рис. 1*) [2, 3]:

- превентивні заходи безпеки s_p, які спрямовані на зменшення імовірності виникнення інциденту ρ;
- заходи виявлення s_d, котрі зменшують час, необхідний для виявлення інциденту t_d;
- інші заходи безпеки s_o, котрі зменшують збитки L внаслідок виникнення інциденту.

Кожен захід безпеки $s(\alpha, C)$ визначається двома кількісними параметрами – ефективністю $\alpha(t)$ і вартістю C. Ефективність $\alpha(t) > 0$ демонструє вплив даного заходу безпеки на зменшення ризику. Превентивні заходи безпеки $s_p(\alpha_p, C_p)$ зменшують імовірність виникнення інциденту ρ згідно з умовами:

$$\frac{\partial \rho}{\partial C_p} < 0, \frac{\partial^2 \rho}{\partial C_p^2} > 0. \quad (5)$$

Залежність між інвестиціями C_p і превентивними заходами безпеки можна продемонструвати за допомогою формули (6):

$$P(T, \nu, C_p) = T^{\alpha_p C_{p+1}}. \quad (6)$$

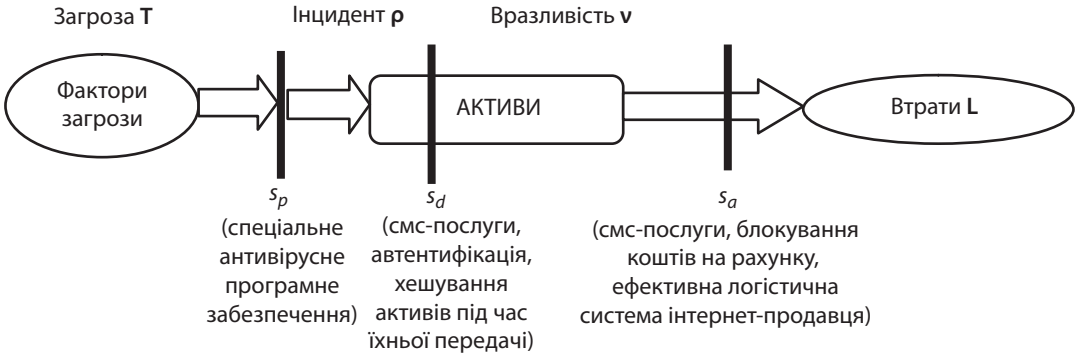

Рис. 1. Класифікація заходів інформаційної безпеки для інтернет-платіжних систем

Джерело: власна розробка.

Чим менший час, який використовується на спрацювання заходів безпеки $s_0(\alpha_0, C_0)$, тим менших збитків зазнаватимуть учасники інтернет-транзакції. Цього можна досягнути, інвестуючи в ці заходи певну суму коштів C_0. Час t_r, який витрачається на використання засобів безпеки s_o, можна визначити за допомогою формули (7):

$$t_r = \exp(-\alpha_0 \cdot C_0). \quad (7)$$

Аналогічно t_r визначається для заходів виявлення $s_d(\alpha_d, C_d)$ [2, 3, 8].

Функція часу t_r є опуклою на інтервалі $0 \le C_0 < C_{it\_security\_max}$. При цьому $C_{it\_security\_max}$ вважаємо максимально запланованими коштами, які можна інвестувати в заходи безпеки підприємства на стадії виникнення інциденту. Тобто, мінімальний простій часу досягається за умови максимального інвестування коштів у засоби безпеки s_0 (формула (8)):

$$\frac{\partial t_r}{\partial C_0} < 0, \frac{\partial^2 t_r}{\partial C_p^2} > 0. \quad (8)$$

Аналогічною є ситуація для функції часу t_d, пов'язаного із $C_{it\_security\_max}$-витратами, спрямованими на послуги смс-банкінгу, спеціальне програмне забезпечення безпечної передачі даних, на генерування підприємствами при передачі конфіденційної інформації та коштів для своїх клієнтів кодів спеціального призначення.

Про такі заходи безпеки, як страхування ризиків, у першу чергу, повинні подбати інтернет-продавці. У випадку настання інциденту страхова компанія виплачує компенсацію K для покриття збитку (формула (9)):

$$L = L_{m\_chargeback} \cdot t_r + L_c \cdot t_d + L_{m\_indirect} + L_{b\_indirect} - K. \quad (9)$$

Враховуючи фактор часу, збитки, які можуть понести учасники інтернет-транзакції, виразимо формулою (10):

$$L = L_{m\_chargeback} \cdot e^{-\alpha_0 C_0} + L_c \cdot e^{-\alpha_d C_d} + L_{m\_indirect} - K. \quad (10)$$

Таким чином, визначимо загальний ризик R (11):

$$R = T \cdot v^{\alpha_p C_p} \cdot \left[L_{m\_chargeback} \cdot e^{-\alpha_0 C_0} + L_c \cdot e^{-\alpha_d C_d} + L_{m\_indirect} + L_{b\_indirect} - K \right]. \quad (11)$$

Показник окупності інвестицій (*ROI*) показує, скільки або що отримають продавець, покупець, підприємство в результаті затраченої певної суми грошей. За допомогою даного показника зіставляють вигоди від інвестицій B і витрачені кошти на заходи безпеки (вартість заходів) C.

Загалом, вигоди від інвестицій у заходи безпеки розглядаються як збереження коштів за рахунок зменшення імовірності виникнення інцидентів та їхніх наслідків. Ці вигоди зазвичай достатньо складно точно спрогнозувати. Проблема полягає в тому, що оцінка вартості заощадження коштів залежить від подій, які ще не відбулися. Вигоди від інвестицій у заходи безпеки B визначаються як різниця між рівнями ризику до застосування заходу R_0 і значенням ризику після застосування заходу $R(C)$ (формула (12)):

$$B = R_0 - R(C). \quad (12)$$

Використовуючи співвідношення (12), визначимо *ROI*:

$$ROI = \frac{R_0 - R(C) - \tau + \mu - C}{C}, \quad (13)$$

де τ – негативні наслідки заходів безпеки (наприклад, зменшення операційної можливості системи), μ – непрямі позитивні ефекти (наприклад, зростання іміджу, зменшення витрат на страхування тощо).

Відповідно формулу (13) можна вдосконалити і застосувати до описаних вище превентивних заходів безпеки s_p, заходів виявлення s_d та інших заходів безпеки:

$$ROI_p = \frac{T \cdot v(1 - v^{\alpha_p C_p})L - \tau + \mu - C_p}{C_p}, \quad (14)$$

$$ROI_o = \frac{T \cdot v \cdot L_{m\_chargeback}(1 - e^{-\alpha_0 C_0}) - \tau + \mu - C_o}{C_o}, \quad (15)$$

$$ROI_d = \frac{T \cdot v \cdot L_c(1 - e^{-\alpha_d C_d}) - \tau + \mu - C_d}{C_d}. \quad (16)$$

Аналогічні до (14) – (16) співвідношення частково відображені у працях [2, 3, 8, 9].

Для вдосконалення ефективності інтернет-платіжних систем підприємства з урахуванням фактора часу використаємо співвідношення [5]:

$$E_a = \frac{Fv}{Fw}; \; E_t = \frac{Fv_t}{Fw_t}; \; \Delta E_t = E_a - E_t, \quad (17)$$

де E_a – ефективність в початковий момент часу $t = 0$; E_t – ефективність в актуальний момент часу t; F_w – запланований вхід (потік інформації, коштів); Fw_t – фактичний вхід в момент часу t; ΔE_t – зміна ефективності в часі.

Для оптимізації інформаційних та платіжних потоків $P_k(X_i)$ підприємства і покращення системи захисту використаємо аналогічно з [6] функціонал якості з урахуванням оберненого зв'язку:

$$J(P_k(X_i), FB(X_i)) = \int_{t_0}^{t_k} f(\bar{y}, \bar{u}, \bar{s})\, dt \Rightarrow opt, \quad (18)$$

де $\bar{y}$ – вектор заданих впливів ($y_j(t)$ – компоненти вектора, $j = 1, 2, \ldots, n$); $\bar{u}$ – вектор керувань; $\bar{s}$ – вектор невизначених збурень; $[t_0, t_k]$ – інтервал часу, в якому розглядається процес (формування оптимальних значень інформаційних та фінансових потоків $P_k(X_i)$, $k = 1, 2, \ldots, m$); m – загальне число інформаційних та фінансових потоків, які мають відношення до даного підприємства; $f(\bar{y}, \bar{u}, \bar{s})$ – функція, що відображає показник якості; $FB(X_i)$ – функція, яка характеризує обернений зв'язок (*Feed-back*) між потоками P_i та оточенням підприємства (контрагентами) з урахуванням думок експертів. Тут символ *opt* відповідає умові оптимальності функціоналу.

Для оптимізації ризиків врахуємо такі фактори [4]: якості (18) та надійності – *jn*, інформаційної ємності – *ij* і фактор ризику – *rz*.

Для кожного з цих факторів означимо функцію корисності P_{jn}, P_{ij}, P_{rz} [4]. Зокрема, $P_{rz} = P_{r^*} - P_r(\bar{X}_v, \bar{Y}_p)$, де P_{r^*} – постійне значення параметра, який відповідає початковим умовам ($P_{r^*} > P_r(\bar{X}_v, \bar{Y}_p)$); вектор $\bar{X}_v$ – початкові умови (сукупність заданих даних на вході ІПСП); $\bar{Y}_p$ – множина величин, які характеризують прийняте рішення щодо оптимізації ІПСП.

Інтегральну корисність P_{int} подамо у вигляді виразу [4]:

$$P_{int} = k_{v1}P_{jn} + k_{v2}P_{ij} + k_{v3}P_{rz}, \quad k_{v1} + k_{v2} + k_{v3} = 1, \quad (19)$$

де k_{v1}, k_{v2}, k_{v3} – коефіцієнти вагомості, які визначають експертним методом.

Для P_{int}, яка відповідає ІПСП, запишемо умову екстремуму аналогічно [4]:

$$P_{int} \Rightarrow \max. \quad (20)$$

Для реалізації методики оцінювання ризику на основі статистичного підходу вводимо параметр $\Psi(R)$ та відповідний інтегральний критерій для кожної складової P_{jn}, P_{ij}, P_{rz} (19) по аналогії з працею [9]:

$$\Psi(R) = \sqrt{(\delta_Z)^2 + (S_{ZV})^2 + (\delta_{as})^2 + (\delta_{ex})^2} \Rightarrow \min. \quad (21)$$

Тут враховано множину показників: коефіцієнт варіації δ_Z, коефіцієнт семіваріації S_{ZV}, коефіцієнт варіації асиметрії δ_{as}, коефіцієнт варіації ексцесу δ_{ex}.

Вираз (21) розглядаємо як критеріальне співвідношення для ризиків R(С) і оцінюємо складові $\Psi(R, P_{jn})$, $\Psi(R, P_{ij})$, $\Psi(R, P_r)$, а також інтегральний ризик з розширеною низкою параметрів $\Psi(R, P_{jn}, P_{ij}, P_r)$ за результатами урахування співвідношень (1) – (16).

Ефективність інноваційної продукції підприємства, від якої залежить розмір корисного ефекту, що одержується при використанні ІПСП за призначенням $M(E)$, розміром витрат ресурсів на розробку і застосування ІПСП $M(Z)$ і розміром можливих пов'язаних з ризиком втрат $M(\Psi, R)$.

Множина параметрів $M(J(P_k(X_i), FB(X_i)), \Psi(R, P_{jn}, P_{ij}, P_r), E_a)$, що характеризує якість J (18), ризики $\Psi(R, P_{jn}, P_{ij}, P_r)$ (21) та ефективність E_a ІПСП, потребує раціонального об'єднання, систематизації, упорядкування, оптимізації:

$$M(J, E_a) = M(E) \cdot M(Z) \cdot M(\Psi, R) \times \times M\left(P_k(X_i), FB(X_i)\right) \Rightarrow opt. \quad (22)$$

Множина параметрів (22), доповнена співвідношеннями (1) – (21), є основою економетричної моделі для оптимізації інтернет-платіжних систем підприємства. Модель ІПСП (1) – (22) враховує фактори якості (18), ефективності (17), ризику (1) – (16), (21), корисності (19), (20).

ВИСНОВКИ

Таким чином, на теперішній час безпека є чи найважливішим критерієм ефективного та якісного функціонування інтернет-платіжних систем підприємства, адже саме її рівень формує репутацію підприємства, рівень довіри споживачів, обсяг втрат при проведені фінансових інтернет-транзакцій та, як наслідок, обсяг прибутку. Вигоди від застосування заходів інформаційної безпеки не повинні бути меншими, ніж витрати, які спрямовуються на їх (ІПСП) розробку та впровадження у процес реалізації інтернет-транзакцій. З наведеного економічного аналізу заходів безпеки випливає, що чим більше коштів затрачається на розробку, впровадження та реалізацію різних заходів безпеки суб'єктами інтернет-платіжних систем, тим менша імовірність інциденту безпеки, а у випадку інциденту – зменшення фінансових втрат. Для інтернет-продавців витрати в першу чергу повинні спрямовуватися на ефективний ризик-менеджмент, логістичну систему та страхування ризиків. У випадку покупців, це – витрати на банківські послуги, наприклад смс-повідомлення, антивірусне програмне забезпечення. Витрати підприємств можуть бути пов'язані із витратами на страхування ризиків, технічний супровід транзакції, спеціальне програмне забезпечення.

Для оптимізації інтернет-платіжних систем підприємства запропоновано систему математичних співвідношень (1) – (22), яка являє собою економетричну модель. Ця модель (ІПСП) враховує фактори якості, ефективності, ризику, корисності. ■

ЛІТЕРАТУРА

1. Танцюра М. Ю. Забезпечення ефективності системи інформаційної безпеки підприємства (на прикладі туристичних підприємств АР Крим) : автореф. дис. … канд. екон. наук: 08.00.04 «Економіка та управління підприємствами (підприємства туристично-рекреаційного комплексу)» / М. Ю. Танцюра ; Тавр. нац. ун-т ім. В. І. Вернадського. – Сімферополь : Б. в., 2012. – 19 с.

2. Одарченко Р. С. Економічна ефективність впровадження систем захисту стільникових мереж 4G / Р. С. Одарченко, С. Ю. Лукін // Системи обробки інформації. – 2012. – Випуск 4 (102), том 2. – С. 51 – 55.

3. Bojanc R. Quantitative model for economic analyses of information security investment in an enterprise information system / Rok Bojanc, Borka Jerman-Blazic // Research papers Organizacija. Volume 45. – No. 6. – November – December 2012. – P. 276 – 288.

4. Качанов С. О. Методика оцінки ризику від провадження господарської діяльності / С. О. Качанов // Управління проектами та розвиток виробництва : зб. наук. пр. – Луганськ : Східноукр. нац. ун-т ім. В. Даля, 2009. – № 2 (30). – С. 109 – 112.

5. Семчук Ж. В. Розвиток систем управління якістю продукції машинобудівних підприємств : автореф. дис. … канд. екон. наук: 08.00.04 «Економіка та управління підприємствами» / Ж. В. Семчук. – Львів : Б. в., 2011. – 24 с.

6. Krap N. P. Methodological aspects of management of projects of tourist flows / N. P. Krap, V. M. Yuzevych // Modern scientific research and their practical application. Research Bulletin SWorld. Published by S. V. Kupriyenko. – 2013. – Volume J2130, November. – P. 155 – 160.

7. True cost of fraud study. Merchants struggle against onslaught of high-cost identity fraud and oline fraud // Annual Report LexisNexis. – September 2013. – P. 35.

8. Visa e-commerce merchants' guide to risk management. Tools and best practices for building a secure internet business [Electronic resource]. – Mode of access : http://usa.visa.com/download/merchants/visa-risk-management-guide-ecommerce.pdf

9. Качанов С. О. Розробка механізму побудови нормативної документації з системної реалізації державного нагляду і контролю : автореф. дис. … канд. техн. наук: спец. 05.01.02 «Стандартизація, сертифікація та метрологічне забезпечення» / С. О. Качанов. – Львів, 2009. – 20 с.

REFERENCES

Bojanc, R., and Jerman-Blazic, B. "Quantitative model for economic analyses of information security investment in an enterprise information system". *Research papers Organizacija,* vol. 45, no. 6 (2012): 276-288.

Kachanov, S. O. "Metodyka otsinky ryzyku vid provadzhennia hospodarskoi diialnosti" [Methods of assessing the risk of economic activities]. *Upravlinnia proektamy ta rozvytok vyrobnytstva*, no. 2 (30) (2009): 109-112.

Krap, N. P., and Yuzevych, V. M. "Methodological aspects of management of projects of tourist flows". *Modern scientific research and their practical application,* vol. J2130 (2013): 155-160.

Kachanov, S. O. "Rozrobka mekhanizmu pobudovy normatyvnoi dokumentatsii z systemnoi realizatsii derzhavnoho nahliadu i kontroliu" [Development of the regulatory mechanism of construction documentation system implementation of state supervision and control]. *Avtoref. dys. ... kand. tekhn. nauk: 05.01.02*, 2009.

Odarchenko, R. S., and Lukin, S. Yu. "Ekonomichna efektyvnist vprovadzhennia system zakhystu stilnykovykh merezh 4G" [Cost-effectiveness of implementation of protection 4G cellular networks]. *Systemy obrobky informatsii,* vol. 2, no. 4 (102) (2012): 51-55.

Semchuk, Zh. V. "Rozvytok system upravlinnia iakistiu produktsii mashynobudivnykh pidpryiemstv" [Development of quality management systems engineering enterprises]. *Avtoref. dys. … kand. ekon. nauk: 08.00.04*, 2011.

"True cost of fraud study. Merchants struggle against onslaught of high-cost identity fraud and oline fraud". *Annual Report Lexis Nexis*, 2013.

Tantsiura, M. Yu. "Zabezpechennia efektyvnosti systemy informatsiinoi bezpeky pidpryiemstva (na prykladi turystychnykh pidpryiemstv AR Krym)" [Ensure the effectiveness of information security company (for example tourism enterprises Crimea)]. *Avtoref. dys. … kand. ekonomich. nauk: 08.00.04*, 2012.

"Visa e-commerce merchants' guide to risk management. Tools and best practices for building a secure internet business". http://usa.visa.com/download/merchants/visa-risk-management-guide-ecommerce.pdf