УДК [004.738.5:004.056]:330.131.5

КІЛЬКІСНА МОДЕЛЬ ДЛЯ ЕКОНОМІЧНОГО АНАЛІЗУ ЗАХОДІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНТЕРНЕТ-ПЛАТІЖНИХ СИСТЕМАХ

Оксана Володимирівна КЛЮВАК
провідний фахівець наукового відділу Львівського інституту банківської справи УБС НБУ (м. Київ)
E-mail: oksana_klyuvak@bigmir.net

Анотація. Запропоновано підхід до кількісної оцінки економічної ефективності від застосування заходів інформаційної безпеки в інтернет-платіжних системах. Проаналізовано ефективність застосування методів автентифікації в інтернет-платіжних системах на прикладі США із урахуванням запропонованого підходу.

Аннотация. Предложен подход к количественной оценки экономической эффективности от использования мер информационной безопасности в интернет-платежных системах. Проанализирована эффективность применения методов аутентификации в интернет-платежных системах на примере США с учетом предложенного подхода.

Ключові слова: *інтернет-платіжна система, автентифікаційні технології, ризик безпеки, показник окупності інвестицій.*
Ключевые слова: *интернет-платежная система, аутентификационные технологии, риск безопасности, показатель окупаемости инвестиций.*

Постановка проблеми. Віддаючи належне науковим напрацюванням у сфері інформаційної безпеки в електронній комерції, варто зазначити, що деякі аспекти безпеки проведення транзакцій та передачі автентифікаційних даних в інтернет-платіжних системах залишаються недостатньо вивченими та потребують ґрунтовного удосконалення, зокрема у сфері економічної обґрунтованості при впровадженні та застосуванні. При удосконаленні технологій забезпечення інформаційної безпеки проведення транзакцій в інтернет-платіжних системах слід враховувати не лише надійність технології, але й економічну ефективність насамперед від застосування технологій автентифікації.

Аналіз останніх досліджень та публікацій. У своїх дослідженнях питання використання інформаційних технологій, зокрема Інтернет-технологій, а також 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. зосереджують свою увагу на економічній ефективності впровадження систем захисту. Питання управління інформаційною безпекою та кількісної оцінки ризиків та втрат внаслідок Інтернет-шахрайств, зокрема в електронній комерції, містяться у працях таких вітчизняних та закордонних дослідників: Rok Bojanc, Borka Jerman-Blažič, Michel van Eeten, Johannes M. Bauer, Shirin Tabatabaie, Домарєв В. В

Метою статті є запропонувати підхід до кількісної оцінки економічної ефективності внаслідок застосування заходів безпеки під час проведення фінансової транзакції в Інтернет-платіжних системах. Враховуючи даний підхід, проаналізувати ефективність застосування методів автентифікації в Інтернет-платіжних системах на прикладі США.

Обґрунтування отриманих наукових результатів. Передумовою розробки заходів безпеки в інтернет-платіжних системах є припущення, що при порушенні захищеності активів завдається збиток усім учасникам інтернет-транзакції, а розробка, впровадження та використання заходів безпеки передбачає витрати. Заходи інформаційної безпеки в інтернет-платіжних системах, зокрема методи автентифікації, повинні бути не лише технічно та технологічно надійними, але й економічно ефективними, тобто враховувати виникнення ризиків під час розрахунків онлайн, а також попередити можливі втрати внаслідок шахрайських дій.

Розглянемо ризики, як можливість з певною імовірністю понести втрати суб'єктами інтернет-платіжних систем, а саме продавцями, по-

купцями, банками. Це може бути як прямий матеріальний збиток, так і непрямий збиток, що виражається, наприклад, у втраті репутації і довіри покупців до проведення транзакцій за допомогою карток. Так можна ствердити, що інформаційна безпека займається іміджевими питаннями, оскільки проблеми з безпекою, а також витік конфіденційної інформації вкрай негативно впливають на імідж та довіру до інтернет-продавців. Тому, оцінка ризиків - перший та необхідний етап в управлінні системою інформаційної безпеки.

Процедура оцінки ризику передбачає визначення вразливостей і загроз для кожного інформаційного активу (наприклад, автентифікаційні дані). Ризик безпеки R визначається як добуток ймовірності виникнення інциденту безпеки ρ та втрати внаслідок виникнення інциденту безпеки L:

$$R= \rho \cdot L \qquad (1)$$

Інцидент інформаційної безпеки в інтернет-платіжних системах визначимо як просту подію або набір небажаних або несподіваних подій, які можуть призвести до втрат під час проведення інтернет-транзакцій. Імовірність виникнення інциденту безпеки ρ ($0 \leq \rho \leq 1$) залежить від імовірності T($0 \leq \rho \leq 1$) виникнення загроз та вразливості ν:

$$\rho = T \cdot \nu \qquad (2)$$

Вразливість інтернет-платіжної системи сама по собі не спричиняє затрат, це лише умова, яка дозволяє загрозі впливати на активи. У випадку виникнення інциденту безпеки, суб'єкти інтернет-платіжних систем зазнають фінансових втрат L. Збиток L>0 вимірюється у грошових одиницях. Насправді, фінансовий збиток внаслідок інциденту безпеки досить важко оцінити. Труднощі викликає оцінка непрямих ризиків, що інколи є набагато більшими від прямих і можуть мати довготривалий негативний вплив на клієнтську базу, партнерів, фінансовий ринок, банки.

Кількісну оцінку збитку можна визначити за формулою 3:

$$L=L_{m\_chargeback}+ L_c + L_{m\_indirect} +L_{b\_indirect}, \qquad (3)$$

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 банків довготривалого характеру: втрата репутації, втрата довіри покупців-держателів карток.

Інцидент безпеки може призвести до простою інформаційної системи та послуг. Час простою включає час виявлення t_d інциденту безпеки та час налагодження та відновлення функцій системи t_r. Час t_d визначається, як період часу від моменту появи інциденту до моменту виявлення інциденту.

Таким чином, ствердимо, що неефективні засоби безпеки (зокрема, втрата конфіденційності даних покупця) в результаті призводять до зниження рівня довіри з боку покупців та втрати репутації. Зобразимо піраміду втрат у системах інтернет-платежів (рис.1).

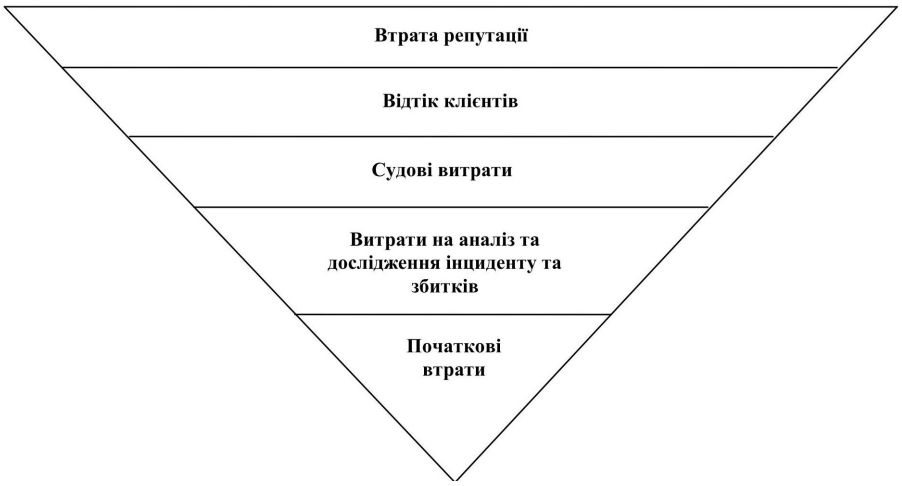

Рис. 1. Піраміда збитків внаслідок застосування неефективних заходів безпеки в інтернет-платіжних системах

Джерело: побудовано автором на основі [4-6]

Елементи формули 3 можна групувати відповідно до часових показників.

Показники $L_{m\_chargeback}$ та L_c залежні від часових показників t_d та t_r. Непрямі втрати від часу не залежать. Відобразимо це у формулі 4.

$$L=L_{m\_chargeback}\cdot t_r + L_c\cdot t_d\cdot t_r + L_{m\_indirect} + L_{b\_indirect} \quad (4)$$

Враховуючи формулу 2 і 4 ризики безпеки в інетернет-платіжних системах можна визначити за формулою 5:

$$R= T\cdot v\cdot(L_{m\_chargeback}\cdot t_r + L_c\cdot t_d\cdot t_r + L_{m\_indirect} + L_{b\_indirect}) \quad (5)$$

Ризик безпеки R відображає очікувані фінансові втрати, спричинені інцидентом безпеки та вимірюється у грошових одиницях [1-2].

Для подолання цього ризику виокремлюють наступні методи:

- зменшення ризику за допомогою відповідних технологій та інструментів (наприклад, «firewall», антивірусні програми) або впровадження відповідних заходів політики безпеки (наприклад паролі, інструменти строгої автентифікації, контроль доступу та ін.);

- передача ризику аутсорсинговим компаніям та його страхування;

- уникнення ризику шляхом усунення джерела загрози або впливу активу на ризик;

- прийняття ризику як частину бізнес-операцій. Може застосовуватися у випадку коли витрати на перенесення ризиків аутсорсинговим компаніям або страхування є більшими ніж загальні втрати.

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

- превентивні заходи безпеки s_p, котрі спрямовані на зменшення імовірності виникнення інциденту ρ (наприклад, антивірусне програмне забезпечення);

- заходи виявлення s_d, котрі зменшують час, який необхідний для виявлення інциденту t_d (системи виявлення атак, смс-оповіщення (підтвердження), автентифікація, хешування даних під час їхньої передачі).

- Інші заходи безпеки s_o , котрі зменшують збитки L внаслідок виникнення інциденту (смс-послуги, блокування коштів на рахунку, ефективна логістична система інтернет-продавця).

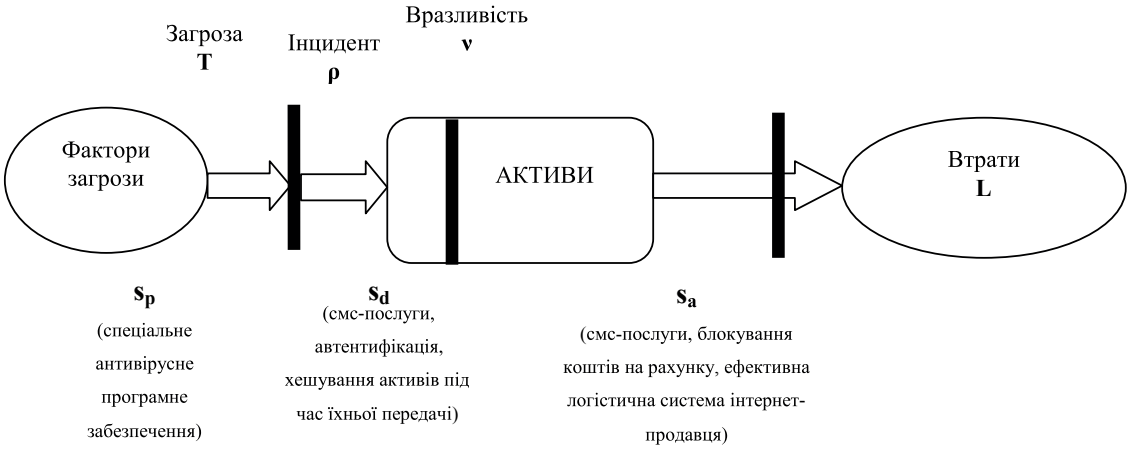

Рис. 2. Класифікація заходів інформаційної безпеки для інтернет-платіжних систем (власна розробка)

Кожен захід безпеки s(α,C) визначається двома кількісними параметрами ефективністю α(t) та вартістю C. Ефективність α(t)>0 демонструє вплив даного заходу безпеки на зменшення ризику. Вартість C визначається як інвестиції, виражені у грошовій формі.

Превентивні заходи безпеки s_p (α_p,C_p) зменшують імовірність виникнення інциденту ρ. За допомогою формули 2 можна продемонструвати залежність між інвестиціями C_p та превентивними заходами безпеки (формула 6):

$$P(T,v,Cp) = T^{v^{\alpha p Cp+1}} \quad (6)$$

Вважаємо, що при необмежених інвестиціях у превентивні заходи безпеки імовірність виникнення інциденту є нульовою (формула 7).

$$C_p \lim\to\infty\ P(T,v,Cp)=0 \quad (7)$$

Превентивні заходи безпеки s_p зменшують імовірність виникнення інциденту. Це може бути описано наступним чином:

Чим менший час, який використовується на спрацювання заходів безпеки $s_o(\alpha_{o,} C_o)$, тим менших збитків зазнаватимуть учасники інтернет-транзакції. Цього можна досягнути, інвестуючи певну суму коштів у ці заходи C_o. Час t_r, який витрачається на використання засобів безпеки безпеки s_o, можна визначити за допомогою формули 9:

$$t_r = e^{-\alpha_0 C_0} \quad (9)$$

Функція часу t_r є опуклою на інтрервалі $0 < C_o < C_{it\_security\_max.}$ $C_{it\_security\_max}$ вважаємо максимально заплановані кошти, які можна інвестувати у заходи безпеки на стадії виникнення інциденту, наприклад, для покупця – вартість послуги смс-оповіщення, для банку чи інтернет-продавці – кошти, заплановані у кошторисі. Тобто, мінімальний простій часу досягається за умови максимального інвестування коштів у засоби безпеки s_o (формула 10).

$$\frac{\partial t_r}{\partial C_0} \langle 0, \frac{\partial^2 t_r}{\partial C_p^{\,2}} \rangle 0 \quad (10)$$

Для заходів виявлення $s_d(\alpha_{d,} C_d)$ можна вивести наступну формулу:

$$t_r = e^{-\alpha_d C_d} \quad (11)$$

Функція часу t_d є опуклою на інтервалі $0 \le C_d < C_{it\_security\_max.}$ $C_{it\_security\_max}$ вважаємо витрати спрямовані на послуги смс-банкінгу, спеціальне програмне забезпечення безпечної передачі даних, на генерування банками для своїх клієнтів кодів спеціального призначення (формула 12).

$$\frac{\partial t_d}{\partial C_d} \langle 0, \frac{\partial^2 t_d}{\partial C_d^{\,2}} \rangle 0 \quad (12)$$

Слід, на нашу думку, також врахувати такі заходи безпеки як страхування ризиків. Про це, в першу чергу, мають подбати інтернет-продавці. Таким чином, у випадку настання інциденту, страхова компанія виплачує компенсацію К для покриття збитку. Застосуємо параметр К (С) до формули 4:

$$L = L_{m\_chargeback} \cdot t_r + L_c \cdot t_d + L_{m\_indirect} + L_{b\_indirect} - K \quad (13)$$

Враховуючи фактор часу (формули 9 та 11), збитки, які можуть понести учасники інтернет-транзакції, виразимо формулою 14:

$$L = L_{m\_chargeback} \cdot e^{-\alpha_0 C_0} + L_c \cdot e^{-\alpha_d C_d} + L_{m\_indirect} + L_{b\_indirect} - K \quad (14)$$

Враховуючи формули 6 та 14, тобто визначення імовірності виникнення інциденту ρ та розміру втрат внаслідок його настання, доповнимо формулу 5 та визначимо загальний ризик R:

$$R = T \cdot \nu^{\alpha_p C_p} \cdot [L_{m\_chargeback} \cdot e^{-\alpha_o Co} + L_c \cdot e^{-\alpha_d C_d} + L_{m\_indirect} + L_{b\_indirect} - K] \quad (15)$$

Для оцінки економічного ефекту від застосування відповідних заходів безпеки розглянемо показник окупності інвестицій (ROI). ROI показує скільки або що отримають продавець, покупець, банк в результаті затраченої певної суми грошей. Даний показник зіставляє вигоди від інвестицій В та затрачені кошти на заходи безпеки (вартість заходів) С. Якщо результат ROI становите додатне число, то це означатиме, що інвестиції є економічно обґрунтовані:

$$ROI = \frac{B - C}{C} \quad (16)$$

Варто зазначити, що оцінити окупність інвестицій у заходи безпеки є досить складно. Заходи безпеки, такі як антивірусне програмне забезпечення, різноманітні методи автентифікації, самі по собі не приносять прямих фінансових доходів.

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 у тому, що оцінка вартості заощадження коштів залежить від подій, які ще не відбулися. Вигоди від інвестицій у заходи безпеки В ототожнюються із зменшенням ризику за рахунок використання цих заходів. Це можна трактувати, як різницю між рівнями ризику до застосування заходу R_0 у формулі 5 та значенням ризику після застосування заходу R(C) у формулі 15:

$$B = R_0 - R(C) \quad (17)$$

Зменшений ризик у формулі 17 є технічним елементом вигоди. Крім того, на значення вигоди впливають організаційні елементи, такі як негативні наслідки заходів безпеки τ (наприклад, зменшення операційної можливості системи) та непрямі позитивні ефекти μ (наприклад, зростання іміджу, зменшення витрат на страхування та ін.):

$$B = R_0 - R(C) - \tau + \mu \quad (18)$$

Використовуючи формулу 18, застосуємо її до формули 16:

$$ROI = \frac{R_0 - R(C) - \tau + \mu - C}{C} \quad (19)$$

Відповідно формулу 19 можна застосувати до описаних вище превентивних заходів безпеки s_p, заходів виявлення s_d та інших заходів безпеки (формули 20-22) [101-102]:

$$ROI_p = \frac{T\nu\left(1-\nu^{\alpha^p C^p}\right)L - \tau + \mu - C_p}{C_p} \quad (20)$$

$$ROI_o = \frac{T\nu L_{m_{chargeback}}\left(1-e^{-\alpha_0 C_0}\right) - \tau + \mu - C_o}{C_o} \quad (21)$$

$$ROI_d = \frac{T\nu L_c\left(1-e^{-\alpha_d C_d}\right) - \tau + \mu - C_d}{C_d}$$

Розглянемо детальніше метод автентифікації (технологію 3-D Secur), як захід безпеки, залежно від рівня ризику. Найбільша частка транзакцій (80 %), які проводяться при допомозі 3-х доменної технології, вважаються низькоризиковими. У цій ситуації держатель картки проходить процес безперервної транзакції без додаткових автентифікаційних запитів від емітента. Причиною віднесення до цієї категорії ряду транзакцій є наявність у емітента історії транзакцій держателя картки на певному сайті продавця. 15-18 % транзакцій віднесено до середньоризикових. Під час таких транзакцій емітент ініціює використання додаткових методів автентифікації, таких як набір запитань до покупця, SMS одноразові паролі. Якщо покупець успішно проходить цей процес, то результатом стає абсолютна автентифікація. Якщо покупець не проходить успішно цей етап, емітент зазначає це у відповіді продавцю. Продавець у свою чергу вирішує проводити транзакцію поза технологією 3-D Secure. При високоризикових транзакціях покупець автоматично не проходить автентифікацію емітента. Емітент повідомляє продавця в межах протоколу «3-D secure» про помилкову автентифікацію. Зазвичай, отримуючи таке повідомлення, продавець транзакцію не продовжує. Звісно, такий розподіл відсотків (80%, 15-18 %, 2 %) притаманний американському ринку. В Україні переважають транзакції із середнім рівнем ризику. Це пояснюється недостатнім рівнем проникнення електронної комерції та розвитку технологій відстеження ризику, які базуються на транзакційних історіях (рис. 3) [3].

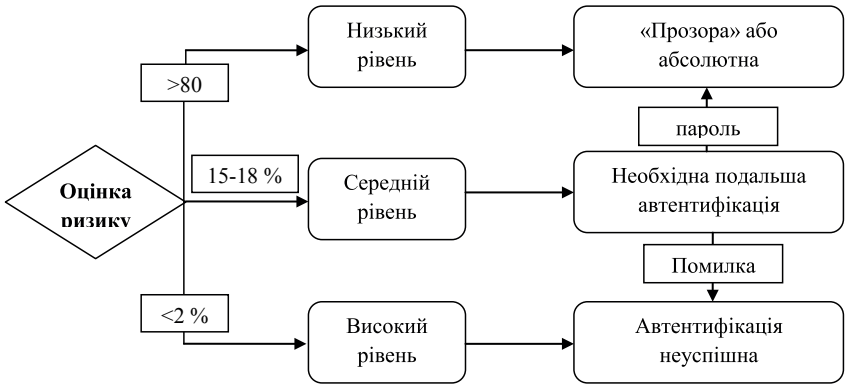

Рис. 3. Категорії інтернет-транзакцій залежно від рівня ризику

Джерело: побудовано на основі [3]

Для оцінки ефективності застосування методів автентифікації наведемо витрати інтернет-продавців на технології автентифікації по регіонах, починаючи з 2011 року, а також доходи та втрати американських інтернет-продавців (табл. 1, 2) [4-6].

Таблиця 1

Витрати на автентифікаційні технології

Витрати на технології автентифікації по регіонах (млрд. дол. США)	Роки							Середній темп приросту за 4 роки (2010-2013рр.,%)
	2010	2011	2012	2013	2014П	2015 П	2016 П	
Північна Америка	2,158	2,576	2,881	3,297	3,880	4,328	4,785	15,2 %
Європа	4,020	4,327	4,551	5,217	5,994	6,408	6,850	9,18 %
Латинська Америка	1,790	1,929	2,020	2,279	2,569	2,691	2,818	8,44 %
Близький Схід разом з Іраном та Афганістаном	2,147	2,453	2,754	3,171	3,678	4,119	4,625	13,88 %
Азіатсько-Тихоокеанський регіон	23,180	25,237	27,031	30,122	34,202	36,098	37,056	9,13 %

Джерело: розраховано автором на основі: [4-6].

Співставимо витрати американських продавців на автентифікаційні технології із доходами та втратами, які вони зазнавали внаслідок Інтернет-шахрайств (табл. 2).

Таблиця 2

Доходи від он-лайн продаж та втрати інтернет-продавців внаслідок онлайн шахрайств

	Роки						Середній темп приросту за 4 роки (2010-2013рр.,%)
	2010	2011	2012	2013	2014 П	2015 П	
Втрати від он-лайн шахрайств (млрд. дол. США)	1,7	2,43	2,3	2,46	-	-	14,85
Доходи від продаж (млрд. дол. США)	327,77	379,8	431	482,6	538,3	597,9	13,22%

Джерело: розраховано автором на основі [4-6].

Застосуємо дані із табл.1-2 до формули ефективності (формула 16), дещо її модифікувавши.

ROI = (Pm – Lm – Sa)/Sa, де (22)

Pm – середній обсяг доходів від продаж;

Lm – середній обсяг втрат від онлайн шахрайств;

Sa – середній обсяг витрат на технології автентифікації.

У даному випадку, ефективність застосування автентифікаційних технологій становить додатне число (114,82 млрд дол США), тобто в середньому за 4 роки це було незбитково для продавців. Проте втрати від онлайн шахрайств зростали за ці роки разом із зростанням доходів продавців. Варто зазначити, що середній темп приросту обсягів збитків від он-лайн шахрайств на 1,63 % більший від середнього темпу приросту доходів від продаж за період 2010-2013 рр.

Також можна спостерігати, що затрати на автентифікаційні технології американських інтернет-продавців є значно більшими, а ніж обсяги втрат від он-лайн шахрайств, що не суперечить формулам 6-8. Згідно поданих вище даних, інтернет-продавці застосовують в основному типові верифікаційні методи автентифікації міжнародних платіжних систем, за рахунок чого витрати на ці технології не є значними. Невелика частка продавців застосовують більш надійніші методи, т. з. «out-of-band» автентифікацію, що є більш надійнішою, проте і затратнішою [7].

Висновки. Таким чином, заходи безпеки, які застосовуються в інтернет-платіжних системах, повинні економічно обґрунтовуватися при впровадженні. Вигоди від їхнього застосування не повинні бути меншими, а ніж витрати, які спрямовуються на їх розробку та впровадження у процес реалізації інтернет-транзакцій. З мате-

матичної точки зору та відповідно до наведеного економічного аналізу заходів безпеки чим більше коштів затрачається на розробку, впровадження та реалізацію різних заходів безпеки суб'єктами інтернет-платіжних систем, тим менша імовірність виникнення інциденту безпеки, а у випадку виникнення інциденту – зменшення фінансових втрат. Іншими словами, збитки, які потенційно можуть зазнати учасники транзакції, не повинні перевищувати витрат на заходи безпеки. Для інтернет-продаців витрати в першу чергу повинні спрямовувати на ефективний ризик-менеджмент, логістичну систему та страхування ризиків. У випадку покупців, це – витрати на банківські послуги, наприклад смс-оповіщення. Витрати банків можуть бути пов'язані із витратами на страхування ризиків, технічних супровід транзакції, спеціальне програмне забезпечення. Але крім економічної обґрунтованості, слід враховувати рівень надійності впроваджених заходів безпеки на програмному рівні. З позицій надійності, ефективним заходом безпеки на програмному рівні являється хешування при передачі автентифікаційних даних, а також банківські послуги SMS-оповіщення.

Список використаних джерел

1. Rok Bojanc, Borka Jerman-Blazic Quantitative model for economic analyses of information security investment in an enterprise information system // Research papers Organizacija. Volume 45. — Number 6. — November – December 2012. — p. 276–288.

2. Одарченко Р. С., Лукін С. Ю. 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. Advantages of a risk-based authentication strategy for MasterCard SecureCode [Електронний ресурс]. — Режим доступу : http://www.mastercard.com/us/merchant/pdf/rba_secure_code_HR.pdf.

4. Офіційний сайт консалтингової компанії CEB (The Corporate Executive Board Company) TowerGroup Retail Banking and Cards Practice [Електронний ресурс]. — Режим доступу : http://www.executiveboard.com/.

5. True cost of fraud study. Merchants struggle against onslaught of high-cost identity fraud and oline fraud. — Annual Report LexisNexis. — September 2013. — p. 35

6. Card-Not-Present Fraud: A Primer on Trends and Authentication Processes\ A Smart Card Alliance Payments Council White Paper. — Publication Date: February 2014. — p.22.

7. Visa e-commerce merchants' guide to risk management. Tools and best practices for building a secure internet business [Електронний ресурс]. — Режим доступу : http://usa.visa.com/download/merchants/visa-risk-management-guide-ecommerce.pdf.