УДК 004.942 DOI: 10.30748/zhups.2018.56.25

С.П. Євсеєв[1], Р.В. Корольов[2], А.С. Комишан[1],
І.В. Бонь[2], С.Г. Солоненко[2], В.В. Богульський[2]

[1] *Харківський національний економічний університет ім. Семена Кузнеця, Харків*
[2] *Харківський національний університет Повітряних Сил ім. І. Кожедуба, Харків*

ВЕРИФІКАЦІЯ МЕТОДИКИ ОЦІНЮВАННЯ ФУНКЦІОНАЛЬНОЇ ЕФЕКТИВНОСТІ ПЕРЕДАЧІ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ В АВТОМАТИЗОВАНИХ БАНКІВСЬКИХ СИСТЕМАХ

Розглядається верифікація методики оцінювання емерджентних властивостей функціональної ефективності АБС на основі комплексного показника якості, який базується на основних показниках безпеки та надійності, що в свою чергу забезпечує протидію гібридним загрозам на банківські інформаційні ресурси та елементи інфраструктури автоматизованих банківських систем. Для оцінки комплексного показника функціональної ефективності запропоновані опорні таблиці, що дозволяють виділити діапазони зміни необхідних параметрів і визначити їх в умовних балах. Такий підхід дозволяє без значних економічних, обчислювальних та людських ресурсів враховувати не тільки технічні, але й економічні параметри ТЗЗІ АБС, що дозволяє точніше оцінювати її функціональну ефективність, враховувати результати досліджень при масштабуванні мережі АБС, виборі ТЗЗІ щодо побудови та підтримання КСЗІ, аналіз протидії загрозам на складові безпеки (ІБ, КБ, БІ) БІР, їх гібридність і синергізм, мінімізацію затрат та дієвий контроль за програмними засобами КСЗІ АБС.

Ключові слова: *банківські інформаційні ресурси, автоматизована банківська система, методика функціональної ефективності передачі даних в АБС, гібридність, синергізм.*

Вступ

Постановка проблеми. Зміни останнього десятиліття, що відбулися в організаціях банківського сектору (ОБС) призвели до об'єднання інформаційних та комп'ютерних мереж в єдиний інформаційний та кібернетичний простір. Інтеграційні процеси розвитку АБС обумовили істотно розширили спектр електронних послуг державних і комерційних банків світу та України. У результаті, суттєво трансформувалися і загрози у такому національному інформаційному ресурсі держави, як банківські інформаційні ресурси (БІР).

Загрози набули ознак гібридності. Від суто загроз інформаційній, кібернетичній безпеці та безпеці інформації БІР прояви ознак гібридності почали виникати унаслідок одночасного впливу на об'єкт захисту – БІР, за рахунок виникнення явища синергізму.

На основі загального поняття якості стандарту ISO 8402 були визначені основні терміни в області якості послуг зв'язку (Quality of Service, QoS), вперше опубліковані в Рекомендації МСЕ-Т Е.800 [1]. У роботах [2–3] розглянуті вимоги стандартів за основними технічними показниками якості обслуговування – надійності і безпеки. У стандарті ISO 9000 діє до: 2015 [4] визначені основні концепції і принципи управління якістю, в стандарті [5] – типові вимоги до автоматизованих систем. В цілому якість послуги характеризується сукупністю наступних основних споживчих властивостей [3]: забезпеченістю, зручністю використання, дієвістю, безпекою та іншими властивостями, специфічними для кожної послуги.

Таким чином, актуальним завданням є не тільки оцінка технічних компонент функціональної ефективності АБС, але і вплив економічних аспектів на інвестиційну політику в ОБС по забезпеченню безпеки конфіденційної інформації.

Запропонована методика оцінювання функціональної ефективності передачі БІР на основі комплексного показника дозволяє отримати емерджентні властивості на основі синтезу комплексного показника ефективності інвестицій в забезпечення безпеки банківських інформаційних ресурсів, результатів оцінювання сучасних загроз на БІР та елементи інфраструктури АБС, їх гібридність та синергізм, результатів оцінювання експрес-методом стійкості і ефективності програмної (програмно-апаратної) реалізації криптографічних алгоритмів.

Аналіз останніх досліджень [6–10; 21–24] **і публікацій** [11–17] показав, що для забезпечення складових безпеки: інформаційної безпеки (ІБ), кібербезпеки (КБ), безпеки інформації (БІ), як правило використовуються криптографічні механізми на основі процедур симетричною і несиметричною криптографії, однак вибір з пропонованого безлічі програмно-апаратних / програмних засобів є складним завданням. Проведений аналіз стандартів в роботах [18; 23; 25] показав, що ключовим моментом принципів управління ІБ є оцінювання ризиків. Практика показує, що сьогодні можна чітко виділити дві основні групи методів оцінювання ризиків безпеки [18; 23; 25]. Перша група методів дозволяє встановити рівень ризику шляхом оцінювання ступеня відповідності визначеному набору

вимог щодо забезпечення інформаційної безпеки. Друга група методів оцінювання ризиків ІБ базується на визначенні ймовірності реалізації атак, а також рівнів їх збитку. В даному випадку значення ризику обчислюється окремо для кожної загрози і в загальному випадку є як добуток імовірності реалізації загрози на величину потенційних збитків від цієї загрози. Значення шкоди визначається власником інформації, а ймовірність реалізації загрози обчислюється групою експертів, які проводять процедуру аудиту. Відмінною рисою методів першої і другої груп є застосування різних шкал для визначення величини ризику. У першому випадку ризик і всі його параметри виражаються в числових, тобто кількісних значеннях. У другому випадку використовуються якісні шкали. Для порівняльного аналізу як правило використовуються різні методики Vaughn-Hennig-Siraj, NIST STS822, OCIPEP, OCTAVE, CISWG, Erkan Kahraman, проте їх застосування вимагає, як тимчасових, так і економічних витрат [18; 23; 25].

Метою статті є проведення верифікації запропонованих рішень формування оцінки функціональної ефективності передачі даних в АБС на основі комплексного показника.

Основний розділ

Експеримент здійснено з дотриманням основних вимог, що висуваються до його проведення, а саме: розроблено план експерименту, програму експерименту та приведено аналіз його результатів. *Метою експерименту є* перевірка адекватності методики оцінювання ефективності функціонування АБС на основі комплексного показника оцінювання якості обслуговування об'єктів автоматизованої банківської системи щодо відбору альтернативних варіантів можливих стратегічних рішень з питань безпеки. *Об'єктом дослідження* визначено рівень загроз на складові безпеки (ІБ, КБ, БІ) БІР, що забезпечує мінімізацію інвестицій в побудову систем безпеки БІР.

Основними завданнями експерименту визначено такі:

– визначення ймовірності впливу загроз ІБ, КБ, БІ на безпеку БІР;

– визначення залежностей між елементами інфраструктури АБС, інформаційними активами БІР, загрозами ІБ, КБ, БІ та ТЗЗІ на основі удосконаленої моделі інфраструктури АБС, синергетичної моделі загроз, удосконаленої моделі зловмисника;

– визначення узагальненого показника рівня безпеки БІР на основі удосконаленої моделі оцінювання рівня захищеності БІР;

– оцінювання інвестицій в безпеку БІР, яка відрізняється від відомих комплексованих економічних показників інвестицій в безпеку БІР з урахуванням гібридності та синергізму атак на складові безпеки (ІБ, КБ, БІ);

– дослідження адекватності методики оцінювання ефективності функціонування АБС на основі комплексного показника оцінювання якості обслуговування об'єктів автоматизованої банківської системи щодо відбору альтернативних варіантів можливих стратегічних рішень з питань безпеки.

Обґрунтування вибору множини загроз на БІР. Керуючись створеною в роботі [25] методологією побудови системи безпеки БІР, яка як множину загроз на БІР виберемо загрози з веб-ресурсу (http://bdu.fstec.ru/threat) рис. 1.

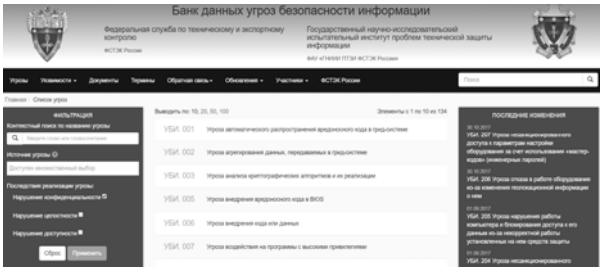

Рис. 1. Вибір множини загроз з ресурсу "Банк даних загроз безпеці інформації"

Розроблений **програмний застосунок експерименту** регламентує порядок його організації та проведення:

Етап 1. *Визначення ймовірності впливу загроз ІБ, КБ, БІ на безпеку БІР:*

Крок 1. Формування метричних коефіцієнтів загроз експертами за послугами безпеки:

$$w^j = \frac{1}{K}\sum_{i=1}^{N}\sum_{k=1}^{K} w_{ik}^j , \qquad (1)$$

де w_{ik}^j – значення метричного коефіцієнта, виставленого k-м експертом для i-ї загрози j-ї послуги безпеки; N – кількість загроз; K – кількість експертів.

На рис. 2 наведена таблиця побудови метричних коефіцієнтів за складовими послуг безпеки за всіма загрозами на БІР у програмному ресурсі (http://skl.hneu.edu.ua/).

На основі введеної метрики розраховуються основні показники метрики загроз: математичне сподівання – μ i-ї загрози, $i \in [1; N]$, де N – кількість загроз у класифікаторі, дисперсія – σ i-ї загрози, $i \in [1; N]$.

При розрахунках враховується можливість отримання в класифікаторі залежних загроз (коди загроз збігаються), тоді спочатку знаходиться повна ймовірність залежних загроз, а після цього обчислюються основні показники для незалежних загроз. У дод. Е наведені результати дослідження загроз БІР на основі запропонованого класифікатору (рис. 3–6).

Крок 1.2. Формування ідентифікаторів загроз за складовими класифікатора. На даному кроці експерти формують цифрове значення (код) ідентифікато-

ра загрози за відповідними складовими класифікатора. Складовими класифікатора є:

– складова безпеки БІР ОБС: ІБ (01), БІ (02), КБ (03);

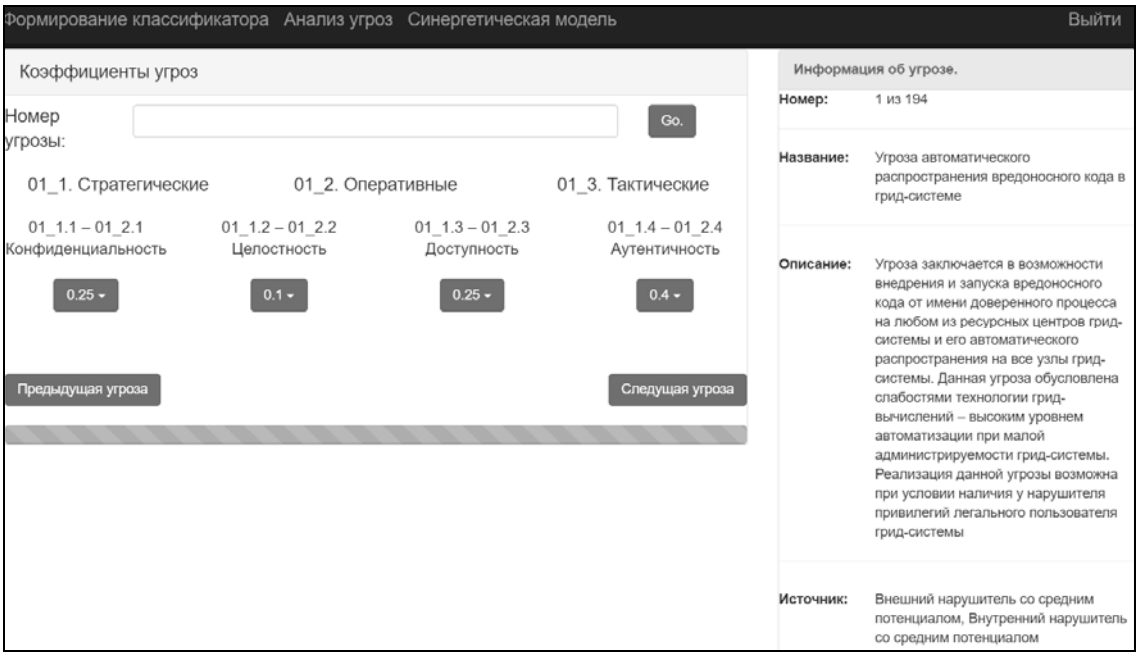

Рис. 2. Формування метричних коефіцієнтів загроз експертами

– характер напрямків: нормативно-правовий (01), організаційний (02), інженерно-технічний (03);

– основні особливості інформації: конфіденційність (01), цілісність (02), доступність (03), автентичність (04);

– рівні ієрархії інфраструктури АБС: FL – фізичний рівень (01), NL – мережевий рівень (02), OSL – рівень операційних систем (ОС) (03), DBL – рівень систем управління базами даних (04), BL – рівень банківських технологічних застосунків і сервісів (05) (рис. 3).

Крок 1.3 Вибір вагових коефіцієнтів α_i, що визначають умови прояву і-ї загрози (табл. 1, рис. 4). Запропоноване значення вагових коефіцієнтів α_i виникнення і-ї загрози визначається на основі метрики експертів за кожною складовою послуги безпеки, з ранжуванням отриманого результату.

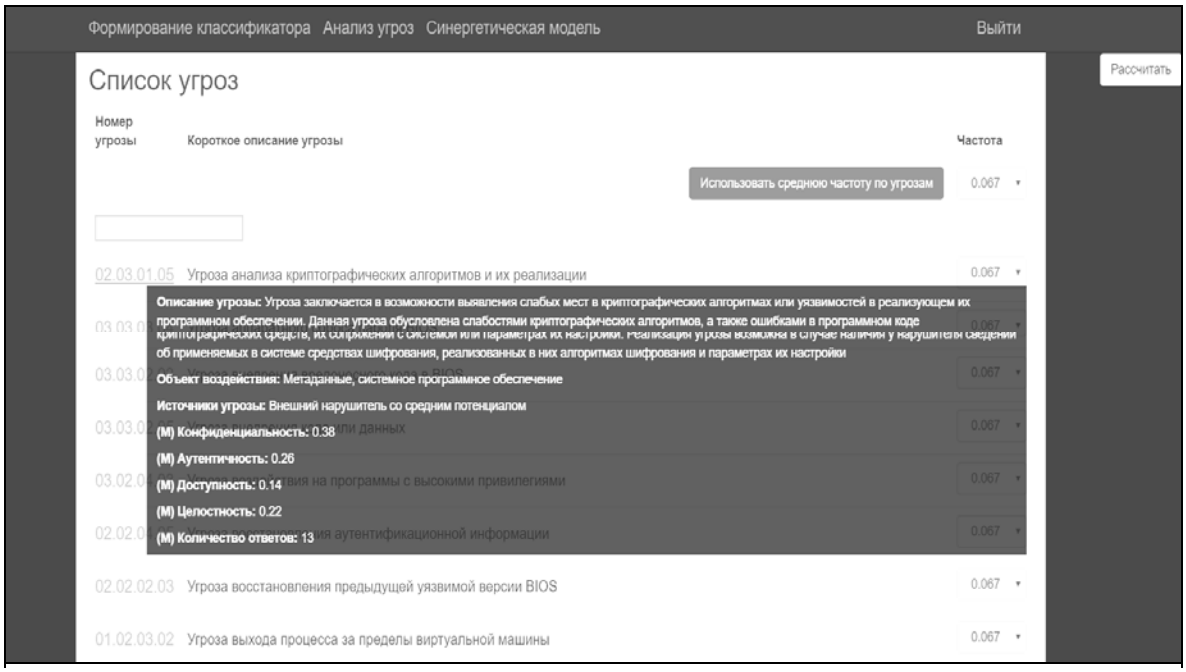

Рис. 3. Формування класифікатора за складовими

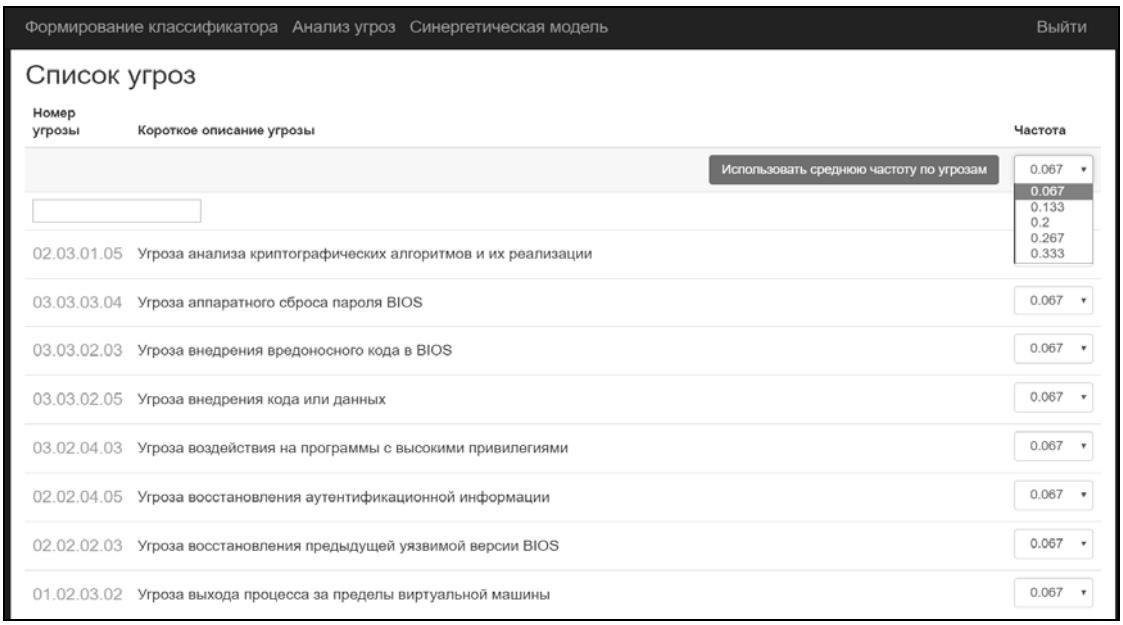

Рис. 4. Вибір вагових коефіцієнтів α_i, що визначають умови прояву і-ї загрози

Таблиця 1

Таблиця визначення ймовірності виникнення загроз залежно від частоти їх прояву

Вагові коефіцієнти α_i	Умови прояву загрози
0,067	загроза проявляється не частіше ніж один раз на 5 років
0,133	загроза проявляється не частіше ніж один раз на рік
0,2	загроза проявляється не частіше ніж один раз на місяць
0,267	загроза проявляється не частіше ніж один раз на тиждень
0,333	загроза проявляється щодня

Крок 1.4. Визначення реалізації кожної і-ї загрози з урахуванням імовірності прояву атаки її виникнення здійснюється за виразом:

$$w_i^j P_i^j = \frac{1}{K} P_i^j \sum_{k=1}^{N} w_{ik}^j . \qquad (2)$$

Для кожної послуги безпеки та і-ї загрози:

$w_i^C \alpha_i^C = \frac{1}{K} \alpha_i^C \sum_{k=1}^{K} w_{ik}^C$ – послуга конфіденційність;

$w_i^I \alpha_i^I = \frac{1}{K} \alpha_i^I \sum_{k=1}^{K} w_{ik}^I$ – послуга цілісність;

$w_i^A \alpha_i^A = \frac{1}{K} \alpha_i^A \sum_{k=1}^{K} w_{ik}^A$ – послуга доступність;

$w_i^{Au} \alpha_i^{Au} = \frac{1}{K} \alpha_i^{Au} \sum_{k=1}^{K} w_{ik}^{Au}$ – послуга автентичність,

де w_{ik}^C, w_{ik}^I, w_{ik}^A, w_{ik}^{Au} – експертні вагові коефіцієнти послуг безпеки: конфіденційності, цілісності, доступності, автентичності, α_i^C, α_i^I, α_i^A, α_i^{Au} – ваговий коефіцієнт послуги безпеки: конфіденційності, цілісності, доступності, автентичності прояву атаки і-ї загрози (рис. 5).

Крок 1.5. Визначення реалізації виникнення декількох загроз на певну послугу безпеки визначається з урахуванням виразу (2):

$$W_{synerg}^C = \sum_{i=1}^{M} w_i^C \alpha_i^C = 0,009 + 0,142 + 0,099 = 0,25$$ –

послуга конфіденційність;

$$W_{synerg}^I = \sum_{i=1}^{M} w_i^I \alpha_i^I = 0,112 + 0,155 + 0,061 = 0,328$$ –

послуга цілісність; (3)

$$W_{synerg}^A = \sum_{i=1}^{M} w_i^A \alpha_i^A = 0,108 + 0,123 + 0,088 = 0,319$$ –

послуга доступність;

$$W_{synerg}^{Au} = \sum_{i=1}^{M} w_i^{Au} \alpha_i^{Au} = 0,126 + 0,047 + 0,141 = 0,314$$ –

послуга автентичність,

де M – загальна кількість загроз в класифікаторі.

Крок. 1.6. Визначення узагальненої синергетичної загрози на БІР з урахуванням виразу (3) визначається:

$$W_{synerg}^{IB} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) P_i =$$
$$= 0,009 \times 0,112 \times 0,108 \times 0,126 = 0,0000137;$$
$$W_{synerg}^{KB} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) P_i = \qquad (4)$$
$$= 0,142 \times 0,155 \times 0,123 \times 0,047 = 0,0001272;$$
$$W_{synerg}^{BI} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) P_i =$$
$$= 0,099 \times 0,061 \times 0,088 \times 0,141 = 0,0000749.$$

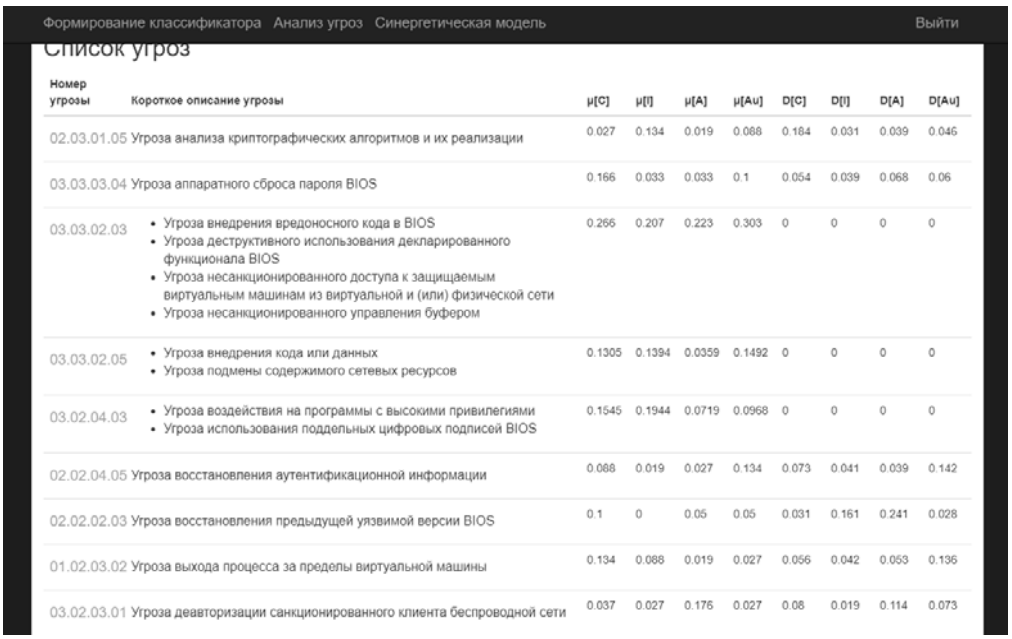

Рис. 5. Результати оцінювання основних показників кожної загрози (μ, σ)

Крок. 1.7. Визначення узагальненої синергетичної загрози на БІР:

$$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \bigcup W_{synerg}^{KB} \bigcup W_{synerg}^{BI} = \\ = 0,0002 + 0,0014 + 0,0007 = \mathbf{0,000216}. \quad (5)$$

Крок 1.8. Визначення узагальненої синергетичної загрози з урахуванням їх гібридності визначається, (рис. 6, табл. 2):

$$W_{synerg}^{hybrid\ C,I,A,Au} = W_{synerg}^{C} \bigcap W_{synerg}^{I} \bigcap W_{synerg}^{A} \bigcap W_{synerg}^{Au} = \\ = 0,471 \times 0,566 \times 0,542 \times 0,53 = \mathbf{0,008214}. \quad (6)$$

Таблиця 2

Результати оцінки синергії та гібридності загроз

складові безпеки	послуги безпеки				
	C, W_{synerg}^{C}	I, W_{synerg}^{I}	A, W_{synerg}^{A}	Au, W_{synerg}^{Au}	Підсумок
ІВ, W_{synerg}^{IB}	0,009	0,112	0,108	0,126	0,0000137
КВ, W_{synerg}^{KB}	0,142	0,155	0,123	0,047	0,0001272
ВІ, W_{synerg}^{BI}	0,099	0,061	0,088	0,141	0,0000749
Підсумок	0,25	0,328	0,319	0,314	
$W_{synerg}^{IB,KB,BI} = \mathbf{0,000216}$			$W_{synerg}^{hybrid\ C,I,A,Au} = \mathbf{0,008214}$		

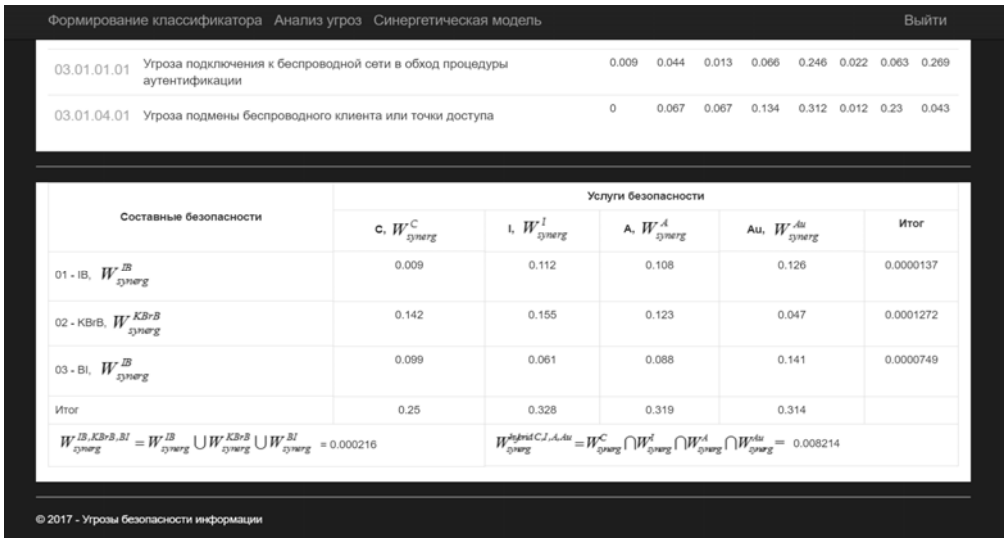

Рис. 6. Результати оцінки загроз на основі синергетичного підходу

Етап 2. *Визначення залежностей між елементами інфраструктури АБС, інформаційними активами БІР, загрозами ІБ, КБ, БІ та ТЗЗІ на основі удосконаленої моделі інфраструктури АБС, синергетичної моделі* загроз*, удосконаленої моделі зловмисника:*

На основі сформованої множини загроз ІБ, КБ, БІ на БІР та моделі ієрархії АБС – $G^{ABS} = \{\{O^{ABS}\}, \{L^{ABS}\}, \{I_A\}\}$, де $\{O^{ABS}\}$ – множина об'єктів середовища АБС, що описують елементи АБС і їх приналежність до рівнів ієрархії АБС, формується

$\{L^{ABS}\}$ – множина зв'язків між елементами АБС, $\{I_A\}$ – множина інформаційних активів БІР (рис. 7).

Крок 2.1. Визначення зв'язку між інформаційними активами БІР $\{I_A\}$ та елементами інфраструктури АБС $A^{ABS} = \left\|a_{ij}^{ABS}\right\|$. Кожен елемент $I_{A_i} \in \{I_A\}$ описується вектором $I_{A_i} = \left(Type, A^C, A^I, A^A, A^{Au}, C_Y\right)$, Type – тип інформаційного активу, описується множиною базових значень Type = {BT, PID, RrD, KT, StO, Ol, YI, PD}, де BT – банківська таємниця, PID – платіжні документи, KrD – кредитні документи, KT – комерційна таємниця , StO – статистичні звіти, Ol – загальнодоступна інформація, YI – керуюча інформація, PD – персональні дані. Значення A^C – конфіденційність, A^I – цілісність, A^A – доступність, A^{Au} – автентичність, CY – безперервність – властивостппрі інформації, які необхідно забезпечувати. Вони приймають значення 1 – якщо властивість необхідно, 0 – в іншому випадку (рис. 7);

Крок 2.2. Визначення зв'язку між інформаційними активами $\{I_A\}$ й об'єктами середовища (рис. 7, табл. 3, 4).

Кожен елемент $O_l \in \{O^{ABS}\}$ описується вектором $O_l = \{Y^{ABS}, IO\}$, де Y^{ABS} – рівень ієрархії інформаційної структури, яка визначається множиною Y^{ABS} = {FL, NL, OSL, DBL, BL}, де FL – фізичний рівень, NL – мережевий рівень, OSL – рівень операційних систем (ОС), DBL – рівень систем управління базами даних, BL – рівень банківських технологічних додатків і сервісів. Для визначення типу зв'язку та існуючих відношень I^{OR} між інформаційними активами та об'єктами середовища використання використовується правило:

$$IO^R = \left\|IO_{il}^R\right\|, \qquad (7)$$

де IO_{il}^R – відображає наявність і тип зв'язку між i-м інформаційним активом і l-м об'єктом середовища АБС. При цьому $\forall i \in \{I_A\}$, а $\forall l \in \{O^{ABS}\}$:

$$IO_{il}^R = \begin{cases} 0 - \text{зв'язок відсутній;} \\ cs - \text{включає і зберігає;} \\ pt - \text{обробляє або передає;} \\ so - \text{підтримує функціонування.} \end{cases}.$$

Кожному параметру присвоюються вагові категорії за правилом Фішберна [30], заснованому на тому, що зміна вагових коефіцієнтів критеріїв підкоряється спадній арифметичній прогресії.

При цьому перший критерій (i = 1), розташований першим в строго упорядкованому за важливістю ранжируваному ряду критеріїв i = 1, 2, ..., n, є найбільш важливим і має найбільший ваговий коефіцієнт. Це правило задається виразом:

$$w_i = \frac{2(N-n+1)}{N(N+1)},$$

де w_i – ваговий коефіцієнт Фішберна; N – загальна кількість параметрів; n – порядковий номер параметра; i – кількість параметрів.

Відповідно до виразу Фішберна маємо:

$$w_1 = \frac{2 \times N}{N(N+1)}; \quad w_N = \frac{2}{N(N+1)}; \quad \gamma = \frac{w_1}{w_N} = N,$$

де γ – кратність відмінності вагових коефіцієнтів один від одного.

Таким чином, $cs = 0,5$, $pt = 0,22$; $so = 0,17$.

Рис. 7. Визначення взаємозв'язку між інформаційними активами БІР, послугами безпеки та елементами удосконаленої інфраструктури АБС

Крок. 2.3. Визначення комплексування множини загроз на основі синергетичної моделі загроз й удосконаленої моделі зловмисника.

Синергетична модель загроз формально описується виразом [23]:

$$GR^{ABS} = \left\{\{DF^{ABS}\}, \{T_{risk}\}, \{T_P\}, \{T_U\}, \{VH\}\right\}, \quad (8)$$

де $\{DF^{ABS}\}$ – множина джерел загроз; $\{T_{risk}\}$ – якісний показник ризику; $\{T_P\}$ – множина базових термів ймовірності реалізації хоча б однієї загрози j-му активу; $\{T_U\}$ – множина базових термів величини збитку від реалізації погрози; $\{VH\}$ – множина деструктивних станів елементів АБС.

Таблиця 3

Надання послуг інформаційним активам БІР

Назва, I_{A_i}	C	I	A	Au
BT	1	1	1	1
PID	1	1	1	1
KrD	1	1	1	1
KT	1	1	1	1
StO	0	1	1	1
Ol	0	1	1	0
YI	0	1	1	1
PD	1	1	1	1

Таблиця 4

Взаємозв'язок інформаційних активів БІР з елементами узагальненої інфраструктури АБС

Назва, I_{A_i}	Фізичний рівень	Мережевий рівень	Рівень ОС	Рівень СУБД	Рівень ПЗ
BT	pt	pt	so	cs	so
PID	pt	pt	so	cs	so
KrD	pt	pt	so	cs	so
KT	pt	pt	so	cs	so
StO	pt	pt	so	cs	so
Ol	pt	pt	so	cs	so
YI	pt	pt	so	cs	so
PD	pt	pt	so	cs	so

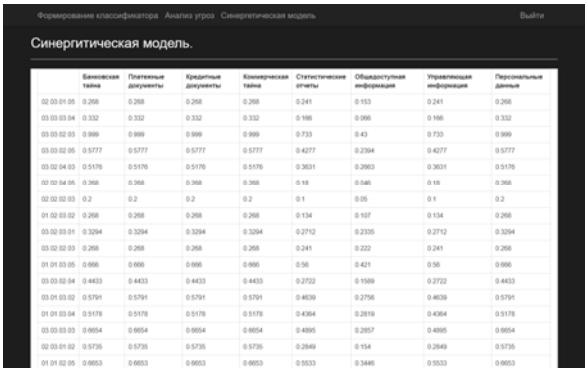

Рис. 8. Ймовірність виникнення і-ї загрози на інформаційні активи БІР

Удосконалена модель визначена п'ятьма категоріями зловмисника та формально описується виразом [20; 25]:

$$G_{IA}^{ABS} = \left\{ aid_i, pur_i, T_{IA}, S_{max_i}, pr_j, MS_i^{ABS} \right\} \forall i \in n, \forall j \in m, \quad (9)$$

де aid_i – ідентифікатор зловмисника (категорія зловмисника); pur_i – мета зловмисника; T_{IA} – час успішної реалізації загрози; S_{max_i} – ймовірнісний збиток системи; pr_j – ймовірність реалізації хоча б однієї загрози j-му активу, MS_i^{ABS} – рекомендації щодо виявлення, реагування ТЗЗІ.

На основі запропонованих моделей здійснюється комплексування множини загроз (рис. 8, табл. 5):

$$DF^{ABS} = \left\{ V^{NS} \right\} \cup \left\{ V^{AS} \right\},$$

де $\left\{ V^{AS} \right\} = \left\{ V^{ASIB} \right\} \cap \left\{ V^{ASKB} \right\} \cap \left\{ V^{ASBI} \right\}$, де $\left\{ V^{NS} \right\}$ – клас природних джерел загроз; $\left\{ V^{AS} \right\}$ – клас антропогенних загроз, де $\left\{ V^{ASIB} \right\}$ – множина загроз ІБ; $\left\{ V^{ASKB} \right\}$ – множина загроз КБ; $\left\{ V^{ASBI} \right\}$ – множина загроз БІ.

Крок 2.4. Визначення ціни повного ризику всіх активів БІР. Ціна повного ризику дорівнює сумі цін ризику всіх активів (табл. 2):

$$R_{повн} = \sum_{j=1}^{n} R_j, \quad (10)$$

де $R_j = pr_j \times q_j$, де pr_j – ймовірність реалізації хоча б однієї загрози j-му активу, q_j – збиток.

Крок 2.5. Визначення ймовірності реалізації хоча б однієї загрози для кожного активу БІР. Розрахунок ймовірності реалізації хоча б однієї загрози для кожного активу виконується за виразом (рис.8, табл. 5):

$$p_{rj} = 1 - \prod_{i=1}^{m} \left(1 - pr_{ij}\right), \quad (11)$$

де pr_{ij} – ймовірність реалізації і-ї загрози j-му активу.

Таблиця 5

Визначення ймовірності реалізації хоча б однієї загрози для кожного активу БІР

ID загрози	BT	PID	KrD	KT	StO	Ol	YI	PD
02.03.01.05	0,268	0,268	0,268	0,268	0,241	0,153	0,241	0,268
03.03.03.04	0,332	0,332	0,332	0,332	0,166	0,066	0,166	0,332
03.03.02.03	0,332	0,332	0,332	0,332	0,249	0,166	0,249	0,332
03.03.02.05	0,333	0,333	0,333	0,333	0,223	0,113	0,223	0,333
03.02.04.03	0,332	0,332	0,332	0,332	0,222	0,189	0,222	0,332
02.02.04.05	0,268	0,268	0,268	0,268	0,18	0,046	0,18	0,268
02.02.02.03	0,2	0,2	0,2	0,2	0,1	0,05	0,1	0,2
01.02.03.02	0,268	0,268	0,268	0,268	0,134	0,107	0,134	0,268
03.02.03.01	0,267	0,267	0,267	0,267	0,23	0,203	0,23	0,267
03.02.02.03	0,268	0,268	0,268	0,268	0,241	0,222	0,241	0,268
…	…	…	…	…	…	…	…	…
03.03.02.03	0,267	0,267	0,267	0,267	0,2	0,112	0,2	0,267
01.01.03.05	0,133	0,133	0,133	0,133	0,114	0,101	0,114	0,133
03.03.02.04	0,332	0,332	0,332	0,332	0,199	0,116	0,199	0,332
03.01.03.02	0,267	0,267	0,267	0,267	0,182	0,094	0,182	0,267
01.01.03.04	0,332	0,332	0,332	0,332	0,299	0,189	0,299	0,332
3.01.01.01	0,2	0,2	0,2	0,2	0,186	0,086	0,186	0,2
03.01.04.01	0,132	0,132	0,132	0,132	0,132	0,066	0,132	0,132

Крок 2.6. Визначення зв'язку між джерелами загроз і елементами АБС, (рис. 9, табл. 6):

$$A^{DF} = \left\| a_{ij}^{DF} \right\|. \quad (12)$$

Етап 3. *Визначення узагальненого показника рівня захищеності БІР на основі удосконаленої моделі оцінювання рівня захищеності БІР.*

Визначення рівня захищеності АБС від загроз ІБ, КБ, БІ на БІР пропонується одержати на основі моделі [23]:

$$G_{OZ}^{ABS} = \begin{Bmatrix} \{I_A\}, \{O^{ABS}\}, \{DF^{ABS}\}, \{RR^{ABS}\}, \\ \{SZ^{ABS}\}, \{ROZ^{ABS}\}, \{UZ_r^{ABS}\} \end{Bmatrix}, \quad (13)$$

де $\{I_A\}$ – множина елементів інформаційних активів; $\{O^{ABS}\}$ – множина елементів ієрархії АБС; $\{DF^{ABS}\}$ – множина джерел загроз безпеці АБС; $\{RR^{ABS}\}$ – множина вимог регуляторів безпеки БІР; $\{SZ^{ABS}\}$ – множина можливих ТЗЗІ; $\{ROZ^{ABS}\}$ – дані обліку про результати оцінки захищеності АБС; $\{UZ_r^{ABS}\}$ – рівень захищеності АБС.

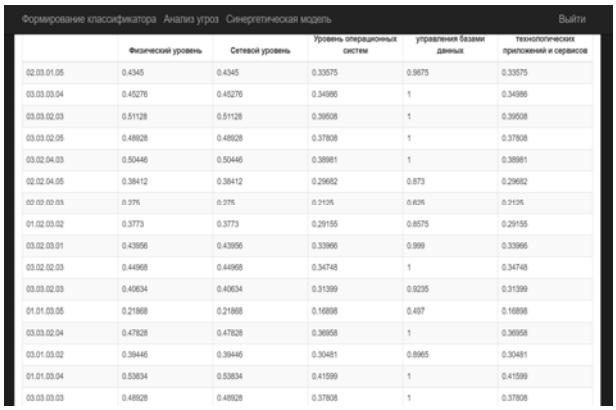

Рис. 9. Визначення зв'язку між джерелами загроз і елементами АБС

Таблиця 6

Визначення зв'язку між джерелами загроз і елементами АБС

ID загрози	Фізичний рівень	Мережевий рівень	Рівень ОС	Рівень СУБД	Рівень ПЗ
02.03.01.05	0,4345	0,4345	0,33575	0,9875	0,33575
03.03.03.04	0,45276	0,45276	0,34986	1	0,34986
03.03.02.03	0,51128	0,51128	0,39508	1	0,39508
03.03.02.05	0,48928	0,48928	0,37808	1	0,37808
03.02.04.03	0,50446	0,50446	0,38981	1	0,38981
…	…	…	…	…	…
03.01.01.01	0,32076	0,32076	0,24786	0,729	0,24786
03.01.04.01	0,2178	0,2178	0,1683	0,495	0,1683
03.01.04.05	0,42966	0,42966	0,33201	0,9765	0,33201
03.01.04.05	0,4158	0,4158	0,3213	0,945	0,3213
02.03.02.03	0,28512	0,28512	0,22032	0,648	0,22032
03.02.03.01	0,10098	0,10098	0,07803	0,2295	0,07803

Крок 3.1. Визначення зв'язку між загрозами і технічними засобами захисту інформації (рис. 10, табл. 7):

$$A^{DFSZ} = \left\| a_{ij}^{DFSZ} \right\|,$$

при цьому $\forall j \in \{I_A\}$, а $\forall i \in \{DF_i\}$.

Таблиця 7

Зв'язок між загрозами і ТЗЗІ

ID загрози	Фізичний рівень	Мережевий рівень	Рівень ОС	Рівень СУБД	Рівень ПЗ
02.03.01.05	MZ	MZ	MZ	MZ	MZ
03.03.03.04	MZ	MZ	MZ	MZ	MZ
03.03.02.03	MZ	MZ	MZ	MZ	MZ
03.03.02.05	MZ	MZ	MZ	MZ	MZ
03.02.04.03	MZ	MZ	MZ	MZ	MZ
…	…	…	…	…	…
03.01.01.01	MZ	MZ	MZ	MZ	MZ
03.01.04.01	MZ	MZ	MZ	MZ	MZ
03.01.04.05	MZ	MZ	MZ	MZ	MZ
03.01.04.05	MZ	MZ	MZ	MZ	MZ
02.03.02.03	MZ	MZ	MZ	MZ	MZ
03.02.03.01	MZ	MZ	MZ	MZ	MZ

У моделі використані такі типи зв'язку: MZ – є механізм захисту, що забезпечує протидію її деструктивному впливу $VH_i \in \{VH\}$; NMZ – немає механізму захисту для забезпечення протидії і-ї загрози.

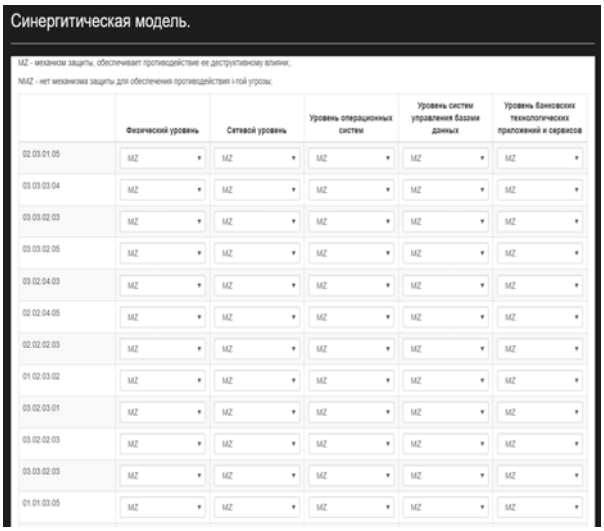

Рис. 10. Зв'язок між загрозами і ТЗЗІ

Якщо для всіх i=m $a_{mj}^{DFSZ} = NMZ$, то робиться висновок що ТЗЗІ АБС не здатні захистити БІР від певного деструктивного впливу, а тому для підвищення рівня захищеності АБС необхідно залучати додаткові кошти на механізми захисту.

Крок 3.2. Визначення вимог регуляторів $\{RR^{ABS}\}$, який включає вимоги до безпеки БІР – $\{R_{BBI}\}$, визначених у міжнародних і національних стандартах, множину оцінок ступеня виконання вимог безпеки $\{OV_{BBI}\}$ та множину підсумкового рівня відповідності безпеки БІР вимогам з множини $\{IU_{BBI}\}$ (рис. 11, 12):

$$\{RR^{ABS}\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}. \qquad (14)$$

Рис. 11. Визначення вимог регуляторів

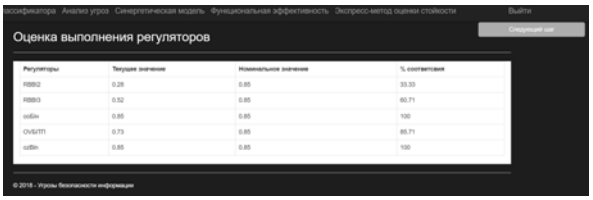

Рис. 12. Загальна оцінка вимог регуляторів

Припустимо що, цей показник виконується.

Крок 3.3. Визначення узагальненого показника рівня захищеності АБС, який дозволяє оцінити рівень відповідності ТЗЗІ вимогам регуляторів та визначається (рис. 13):

$$OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i, \qquad (15)$$

де k – кількість окремих показників безпеки, OPZ_i – окремий показник, що набуває значення з множини: OPZ_1 – відсутність неприпустимих ризиків, у разі якщо в ОБС при складанні моделі загроз / моделі зловмисника і оцінки ризиків виявлені неприпустимі за своїм рівнем ризики, то OPZ_1=0, в іншому випадку – OPZ_1=1; OPZ_2 – відсутність небезпечних загроз, незакритих механізмами ТЗЗІ, OPZ_2=0, в разі, якщо в ОБС при складанні моделі виявлені "незакриті" загрози – OPZ_2=1; OPZ_3 – рівень відповідності безпеки БІР вимогам регуляторів визнаний рекомендованим – OPZ_3=1, в разі, якщо визнано нерекомендованим – OPZ_3=0.

На основі результатів узагальненого показника рівня захищеності OPZ^{ABS}, узагальненої синергетичної загрози $W_{synerg}^{IB,KB,BI}$, множини активів БІР $I_{A_i} = (Type, A^C, A^D, A^A, A^K, C_Y)$ та запропонованих моделі оцінювання безпеки БІР на основі комплексного показника ефективності інвестицій в роботі [25] визначається ефективність інвестицій в забезпечення безпеки БІР.

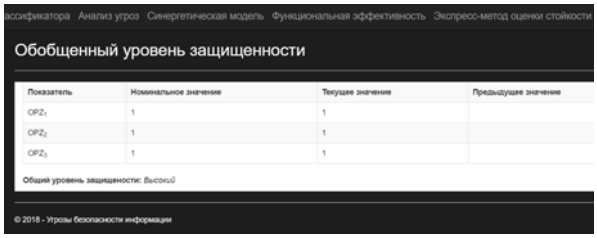

Рис. 13. Визначення узагальненого показника рівня захищеності БІР

Вихідними даними для проведення оцінки є основні показники на основі даних консолідованої фінансової звітності за Міжнародними стандартами фінансової звітності та звіту незалежного аудитора банку "ГРУПИ ПРИВАТ" за 2015, 2016 рр. (https://bank.gov.ua/control/uk/publish/article?art_id=34661442), які наведені у табл. 8. При розрахунках враховуємо, що на забезпечення ІБ в АБС банком витрачається до 4 % від річного прибутку, витрати на розробку ТЗЗІ складають до 2 % від річного прибутку, NPV_{zbtszi}^{ABS} – ймовірні витрати на усунення компрометації безпеки без застосування до 25 % від річного прибутку, NPV_{zbtszi}^{ABS} – ймовірні витрати на усунення компрометації безпеки, що становить до 2 % від річного прибутку, C_{sz} – вартість засобів захисту становить 30 % від загальної вартості БІР. Ставка дисконтування становить 13 %. (http://bank-ua.com/%D0%9E%D0%B1%D0%BB%D1%96%D0%BA%D0%BE%D0%B2%D0%B0_%D1%81%D1%82%D0%B0%D0%B2%D0%BA%D0%B0_%D0%9D%D0%91%D0%A3), табл. 9.

Таблиця 8

Вихідні дані, тис. грн.

Рік	$C_{приб}^{ABC}$	I_{nv}^{ABC}	N, (періоди)	r (%)
2015	7261000000	145220000	2	13
2016	2448000000	48960000	2	13

Таблиця 9

Вихідні дані за БІР, тис. грн.

Назва, I_{A_i} % від $C_{приб}^{ABC}$	u_j	NPV_{inv}^{ABS}	NPV_{zt}^{ABS}	ROI^{ABS}	C_{sz}
BT, (20%)	24480000	24480000	7344000	17136000	7344000
PID, (5%)	6120000	6120000	1836000	4284000	1836000
KrD, (30%)	36720000	36720000	11016000	25704000	11016000

Закінчення табл. 9

Назва, I_{A_i} % від $C_{прив}^{ABC}$	u_j	NPV_{inv}^{ABS}	NPV_{zt}^{ABS}	ROI^{ABS}	C_{sz}
KT, (20%)	24480000	24480000	734000	17136000	734000
StO, (3%)	3672000	3672000	1101600	2570400	1101600
Ol, (2%)	2448000	2448000	7344000	1713600	7344000
YI, (10%)	12240000	12240000	3672000	8568000	3672000
PD, (10%)	12240000	12240000	3672000	8568000	3672000

Оцінка безпеки БІР на основі комплексного показника ефективності інвестицій визначається за такими кроками [24]:

Крок 1. Оцінювання рівня прибутковості інвестицій в побудову системи безпеки БІР:

$$ROI^{ABS} = NPV_{inv}^{ABS} - NPV_{zt}^{ABS}, \quad (16)$$

де NPV_{inv}^{ABS} – прибуток від інвестицій в ТЗЗІ АБС; NPV_{zt}^{ABS} – витрати в ТЗЗІ АБС; ROI^{ABS} – прибутковість інвестицій в ТЗЗІ АБС.

Результати розрахунку наведені у табл. 9.

Крок 2. Оцінювання рентабельності інвестицій в ТЗЗІ:

$$ROSI^{ABS} = NPV_{zbtszi}^{ABS} - NPV_{zvtszi}^{ABS}, \quad (17)$$

де NPV_{zbtszi}^{ABS} – витрати на усунення компрометації безпеки без застосування ТЗЗІ; NPV_{zvtszi}^{ABS} – витрати на усунення компрометації безпеки з застосуванням ТЗЗІ.

Результати розрахунку наведені у табл. 10.

Таблиця 10

Результати оцінювання рентабельності інвестицій, тис. грн.

Назва, I_{A_i}	NPV_{zbtszi}^{ABS}	C_{sz}	ALE_i	NPV_{zvtszi}^{ABS}	$ROSI^{ABS}$
BT	122400000	7344000	16279200	34272000	88128000
PID	30600000	1836000	4069800	8568000	22032000
KrD	183600000	11016000	24418800	51408000	132192000
KT	122400000	734000	16279200	34272000	88128000
StO	18360000	1101600	1733184	5140800	13219200
Ol	12240000	7344000	682992	3427200	8812800
YI	61200000	3672000	5777280	17136000	44064000
PD	61200000	3672000	8139600	17136000	44064000

Крок 3. Оцінювання чистої зведеної вартості:

$$NPV_{zvtszi}^{ABS} = C_{sz} + \sum_{i=1}^{N} \frac{ALE_i}{(1+r)^i}, \quad (18)$$

де N – кількість інтервалів інвестування, ALE_i – очікувані витрати в і-му періоді, r – ставка дисконтування, C_{sz} – вартість засобів захисту. Результати наведені у табл. 10.

Крок 4. Оцінювання ризику БІР за методикою розрахунку *Annual loss expectancy – ALE*, тобто очікуваних втрат в кожен період оцінки:

$$ALE^{ABS} = \sum_{i=1}^{n} I\left(O_{DF}^{ABS}\right) F_i, \quad (19)$$

де $\left\{O_{DF}^{ABS}\right\}$ – множина загроз; $I\left(O_{DF}^{ABS}\right)$ – вартісні наслідки реалізації загрози; ALE^{ABS} – очікувана шкода від реалізації загрози; F_i – частота (можливість) реалізації загрози. Результати наведені у табл. 10.

Крок 5. Оцінювання потенційних збитків U^{ABS} інформаційного активу з урахуванням виразу (11) і табл. 5:

$$U^{ABS} = p_{rj} u_j, \quad (20)$$

де p_{rj} – ймовірність реалізації хоча б однієї загрози j-му активу; u_j – цінність j-го активу.

Результати наведені у табл. 11.

Таблиця 11

Результати оцінювання потенційних збитків U^{ABS}, тис. грн.

ID загрози	BT	PID	KrD	KT	StO	Ol	YI	PD
02.03.01.05	131212,8	32803,2	196819	131213	17699	7490,88	58997	65606
03.03.03.04	162547,2	40636,8	243821	162547	12191	3231,36	40637	81274
03.03.02.03	162547,2	243821	162547	18286,6	8127,36	8127,36	60955	81274
03.03.02.05	163036,8	40759,2	244555	163037	16377,1	5532,48	54590	81518
03.02.04.03	162547,2	40636,8	243821	162547	16303,7	9253,44	54346	81274
02.02.04.05	131212,8	131213	196819	131213	13219,2	2252,16	44064	65606

Закінчення табл. 11

ID загрози	BT	PID	KrD	KT	StO	Ol	YI	PD
03.02.02.03	131212,8	32803,2	196819	131213	17699	10869,12	58997	65606
…	…	…	…	…	…	…	…	…
03.03.02.03	130723,2	32680,8	196085	130723	14688	5483,52	48960	65362
01.01.03.05	65116,8	16279,2	97675,2	65116,8	8372,16	4944,96	27907	32558
03.03.02.04	162547,2	40636,8	243821	162547	14614,6	5679,36	48715	81274

Крок 6. Оцінювання загального очікуваного збитку:

$$OU^{ABS} = \sum_{j=1}^{n} U^{ABS}. \qquad (21)$$

Результати наведені у табл. 12.

Таблиця 12

Результати загального очікуваного збитку, наслідків виведення з ладу ТЗЗІ, тис. грн.

I_{A_i}	OU^{AI}	M^{ABS}	вагові коефіцієнти Фішберна				W_{ABS}^{effinv} за складовими послуг безпеки			
			w_i^C	w_i^I	w_i^A	w_i^{Au}	C	I	A	Au
BT	16279200	122400000	0,4	0,3	0,2	0,1	48960000	36720000	244800000	12240000
PID	4069800	30600000	0,4	0,3	0,2	0,1	12240000	9180000	55080000	36720000
KrD	24418800	183600000	0,4	0,3	0,2	0,1	73440000	55080000	36720000	183600000
KT	16279200	122400000	0,4	0,3	0,2	0,1	48960000	36720000	244800000	12240000
StO	1733184	18360000	0,4	0,3	0,2	0,1	7344000	5508000	3672000	18360000

Закінчення табл. 12

I_{A_i}	OU^{AI}	M^{ABS}	вагові коефіцієнти Фішберна				W_{ABS}^{effinv} за складовими послуг безпеки			
			w_i^C	w_i^I	w_i^A	w_i^{Au}	C	I	A	Au
Ol	682992	12240000	0,4	0,3	0,2	0,1	4896000	3672000	24480000	1224000
YI	5777280	61200000	0,4	0,3	0,2	0,1	24480000	18360000	12240000	6120000
PD	8139600	61200000	0,4	0,3	0,2	0,1	24480000	18360000	12240000	6120000

При цьому перший критерій (i = 1), розташований першим в строго упорядкованому за важливістю ранжируваному ряду критеріїв i = 1, 2, ..., n, є найбільш важливим і має найбільший ваговий коефіцієнт. Це правило задається виразом:

$$w_i = \frac{2(N-n+1)}{N(N+1)},$$

де w_i – ваговий коефіцієнт Фішберна; N – загальна кількість параметрів; n – порядковий номер параметра, i – кількість параметрів.

Відповідно до виразу Фішберна маємо:

$$w_1 = \frac{2\times N}{N(N+1)},\ w_N = \frac{2}{N(N+1)},\ \gamma = \frac{w_1}{w_N} = N,$$

де γ – кратність відмінності вагових коефіцієнтів один від одного.

Таким чином, $w_i^C = 0,4;\ \ w_i^I = 0,3;\ w_i^A = 0,2;$ $w_i^{Au} = 0,1.$

Для нормування отриманих значень показника W_{ABS}^{effinv} розділимо отримані результати на 10^8 та використаємо підхід формування загального показника $W_{synerg}^{IB,KB,BI}$ (результати наведені у табл. 13): $W_{ABS_{sar1_{A_i}}}^{effinv\ \ C} = \sum_{i=1}^{A_i} W_{ABS}^{effinvC}$ – загальний показник за послугою конфіденційність;

Крок 7. Оцінювання сукупної вартості витрат ліквідації наслідків реалізації загрози та інших причин виведення з ладу ТЗЗІ:

$$M^{ABS} = \sum_{i=1}^{m} C_i, \qquad (22)$$

де C_i – вартість і-го заходу; m – загальна кількість прийнятих заходів. Результати наведені у табл. 12.

Крок 8. Визначення комплексного показника ефективності інвестицій в забезпечення безпеки БІР:

$$W_{ABS}^{effinv} = \sum_{i=1}^{N} w_i M^{ABS}, \quad (23)$$

де $w_i \in [0;1]$, $W_{Ф}^{ABS} = \sum_{i=1}^{N} w_i$ – система вагових коефіцієнтів Фішберна, $i \in [1;N]$.

Таблиця 13

Результати загального показника ефективності

Назва, I_{A_i}	W_{ABS}^{effinv} за складовими послуг безпеки			
	C	I	A	Au
BT	0,04896	0,03672	0,02448	0,01224
PID	0,01224	0,00918	0,05508	0,00367
KrD	0,07344	0,05508	0,03672	0,01836
KT	0,04896	0,03672	0,02448	0,01224
StO	0,007344	0,005508	0,003672	0,001836
Ol	0,04896	0,03672	0,02448	0,01224
YI	0,02448	0,01836	0,01224	0,00612
PD	0,02448	0,01836	0,01224	0,00612
$W_{ABS_{sar}I_{A_i}}^{effinv}$	0,2448	0,1836	0,1224	0,0612
$W_{ABS_{sar}}^{effinv}$ =0,00034				

Кожному параметру присвоюються вагові категорії за правилом Фішберна [30], заснованому на тому, що зміна вагових коефіцієнтів критеріїв підкоряється спадній арифметичній прогресії.

$W_{ABS_{sar}I_{A_i}}^{effinv\ \ I} = \sum_{i=1}^{A_i} W_{ABS}^{effinv\,I}$ – загальний показник за послугою цілісність; $W_{ABS_{sar}I_{A_i}}^{effinv\ \ A} = \sum_{i=1}^{A_i} W_{ABS}^{effinv\,A}$ – загальний показник за послугою доступність; $W_{ABS_{sar}I_{A_i}}^{effinv\ \ Au} = \sum_{i=1}^{A_i} W_{ABS}^{effinv\,Au}$ – загальний показник за послугою автентичність.

Загальний показник визначається за виразом:

$$W_{ABS_{sar}}^{effinv} = W_{ABS_{sar}I_{A_i}}^{effinv\ \ C} \bigcap W_{ABS_{sar}I_{A_i}}^{effinv\ \ I} \bigcap$$
$$\bigcap W_{ABS_{sar}I_{A_i}}^{effinv\ \ A} \bigcap W_{ABS_{sar}I_{A_i}}^{effinv\ \ Au}.$$

Для оцінювання якості обслуговування об'єктів АБС щодо забезпечення безпеки БІР використаємо запропоновану методику оцінки функціональної ефективності обміну даними в мережі АБС, яка ґрунтується на простому багатофакторному аналізі, в якій враховуються як технічні показники мережі (швидкість передачі даних, імовірність і час доставки пакета і ін.), показники безпеки технічних засобів захисту інформації, так і економічні параметри (вартість масштабування, обслуговування мережі, ефективність інвестицій в безпеку і т.п.).

Методика містить 4 етапи: 1) визначення стійкості криптосистем методом експрес-аналізу на основі ентропійного методу оцінки випадковості вихідної послідовності; 2) визначення впливу загроз на складові безпеки (ІБ, КБ, БІ) з урахуванням їх гібридності і синергізму; 3) визначення інвестицій в безпеку БІР; 4) визначення ефективності обміну даними в АБС на основі комплексного показника.

1 етап. Визначення стійкості криптосистем методом експрес-аналізу на основі ентропійного методу оцінки випадковості вихідної послідовності запропонованого в роботі [25]. Результатом досліджень є таблиця максимального криптографічного захисту БІР (табл. 14).

2 етап. Визначення ступеня впливу загроз на складові безпеки (ІБ, КБ, БІ) з урахуванням їх гібридності і синергізму.

На основі класифікатора, з урахуванням виразів (2–6) визначається узагальнена синергетична ймовірність реалізації атаки на БІР $W_{synerg}^{IB,KB,BI}$.

Таблиця 14

Оцінка максимального криптографічного захисту інформації

№	Шифр	Ентропія відкр. тексту (H_M)	Ентропія криптограми (H_C)	різниця $H_{Cypher} = H_C - H_M$	Ймовірність криптозахисту, P_c
1.	Клітинні автомати, правило "60"	0,5023775	0,6820179	0,1796404	0,637079949
2.	генератор ПВП Secure Random	0,5023767	0,7999982	0,2976215	0,747287753
3.	DES	0,469276	0,812043	0,342767	0,812043
4.	3DES	0,469276	0,812043	0,342767	0,812043
5.	ГОСТ 28147-2009	0,469276	0,811348	0,342072	0,811348

Закінчення табл. 14

№	Шифр	Ентропія відкр. тексту (H_M)	Ентропія криптограми (H_C)	різниця $H_{Cypher} = H_C - H_M$	Ймовірність криптозахисту, P_c
6.	Калина-256	0,469276	0,954519	0,485243	0,954519
7.	AES-256	0,469276	0,95454	0,485264	0,95454
8	RSA	0,469276	1,000	0,530724	1,000
9	ГККЗК з МЕС (HCCDC)	0,469276	0,98764	0,518364	0,98764
10	Ідеальний шифр		1,000		1,000

Стійкість системи безпеки в АБС до можливих дій зловмисника визначається:

$$B = P_c \times W_{synerg}^{IB, KB, BI}, \quad (24)$$

де B – стійкість системи безпеки в АБС, P_c – ймовірність криптозахисту ТЗЗІ в АБС.

3 етап. *Визначення комплексного показника ефективності інвестицій в забезпечення безпеки БІР*. На основі виразів (15–23) і запропонованої методики визначається комплексний показник ефективності інвестицій в забезпечення безпеки БІР – W_{effinv}.

4. етап. *Визначення ефективності обміну даними в АБС на основі комплексного показника.*

Оцінка ефективності обміну даними здійснюється на основі комплексного показника за виразом:

$$W(u_i) = \frac{n^{(u_i)} - t^{(u_i)}}{n^{(u_i)}} \times B^{(u_i)} \times P_{пр.п}^{(u_i)} \times W_{effinv} \times W_{norm}, \quad (25)$$

де $W(u_i)$ – показник ефективності мережі для обраній стратегії (метод підвищення ймовірності) u_i; $n^{(ui)}$ – кількість інформаційних розрядів пакета для обраній стратегії u_i; $t^{(ui)}$ – час доставки пакета t для обраній стратегії u_i; $B^{(ui)}$ – стійкість системи безпеки в АБС; $P_{пр\ п}^{(ui)}$ – достовірність правильної доставки пакета для обраній стратегії; U – множина допустимих стратегій (методів підвищення ймовірності, використовуваних в мережі); $W_{eff}^{(ui)}$ – комплексний показник ефективності інвестицій в забезпечення безпеки банківських інформаційних ресурсів; W_{norm} – нормований багатофакторний показник ефективності. Вихідними даними мережі АБС є результати в умовних балах табл. 15 запропонованих в роботі [23] на основі опорних таблиць з параметрами систем передачі даних, які враховуються в інтегральному показнику функціональної ефективності IP-мережі АБС W_{norm}.

Таблиця 15

Узагальнена оцінка ефективності мереж передачі даних

Технологія	Умовні бали							
	група						Узагальнений індекс ефективності	Відносна ефективність,%
	1	2	3	4	5	6		
X.25	3	1	3	1	1	1	9	0,25
Frame Relay	3	2	1	5	3	3	270	7,37
Ethernet	3	1	2	4	3	3	216	5,89
Fast Ethernet	3	2	2	4	3	3	432	11,79
Gigabit Ethernet	2	3	4	4	3	3	864	23,59
10 Gb Ethernet	2	4	4	4	3	3	1152	31,45
40 Gb Ethernet	1	5	4	4	3	3	720	19,66
Всього:							3663	100

Група: 1 – вартість розгортання мережі;
2 – швидкість передачі даних;
3 – ймовірність доставки пакету;
4 – час доставки пакету;
5 – затримка пакету;
6 – продуктивність мережі.

На рис. 14 наведені результати досліджень функціональної ефективності передачі БІР в АБС.

Вихідними даними для проведення досліджень є: технології *Frame Relay*, 100 *Mbit Ethernet*, 10 *Gbit Ethernet*, 40 *Gbit Ethernet* з розв'язувальним зворотним зв'язком і *ARQ* "Повернення-на-N", $W_{synerg}^{IB,KB,BI}$ = =0,0022839; БСШ Gost – $t_{ш,\ рш}$=0,033 с; RSA – $t_{ш,\ рш}$= =0,2 с; ГККЗК з МЕС – $t_{ш,\ рш}$=0,0015 с; P_C^{Gost} = =0,95454; P_C^{HCCDC} =0,98764; P_C^{RSA} =1,0000; n=1518; C=36000; $P_{пр.п}$=0,9999; s=32; w=300000000.

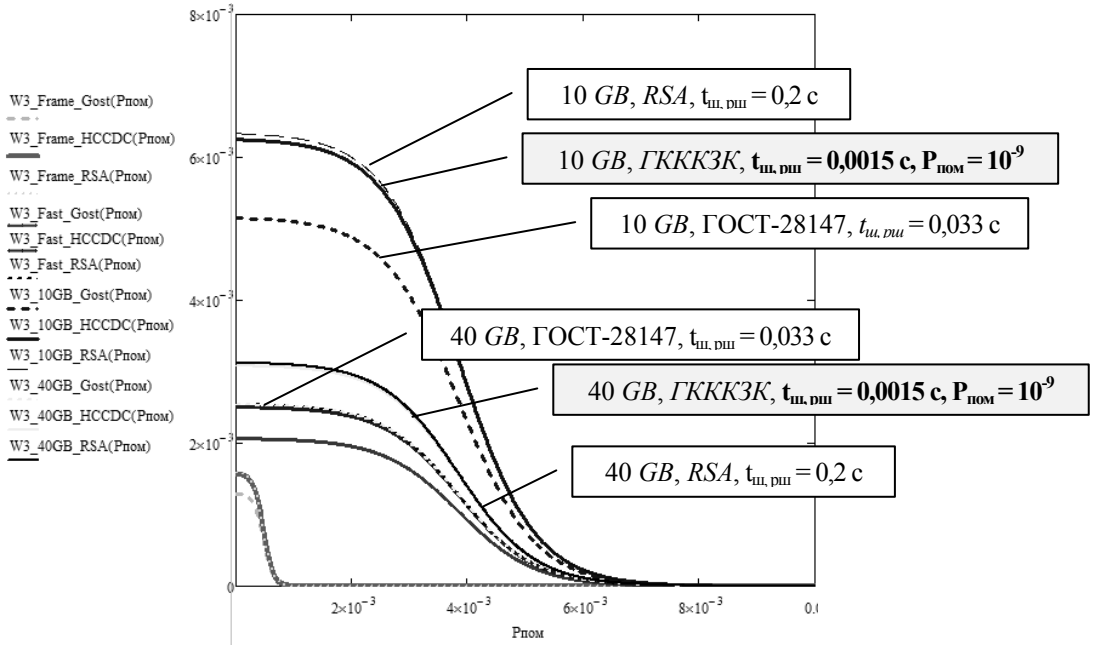

Рис. 14. Результати досліджень функціональної ефективності АБС з ARQ "Повернення-на-N"

Аналіз результатів рис. 14 показав, що запропонована методика оцінки функціональної ефективності АБС дозволяє без значних часових і експертних витрат провести оцінку стану якості обслуговування користувачів АБС, використовувати результати оцінки для її масштабування, поліпшення технічних показників АБС, рівня безпеки БІР.

Таким чином, усі сформульовані науково-прикладні висновки підтверджено результатами експерименту.

Висновки

Виконано верифікацію та дослідження адекватності запропонованих методу оцінювання безпеки банківських інформаційних ресурсів, який враховує комплексний показник ефективності інвестицій, які виділяються на забезпечення безпеки БІР, методики оцінювання функціональної ефективності передачі даних в АБС з урахуванням умов протидії гібридним загрозам ІБ, КБ, БІ на БІР.

Список літератури

1. МСЭ-Т Е.800 Определение терминов, относящихся к качеству обслуживания [Электронный ресурс]. – Режим доступа: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.800-200809.
2. Яновский Г.Г. Качество обслуживания в сетях IP [Электронный ресурс]. – Режим доступа: niits.ru/public/2008/2008-006.pdf.
3. Шриниваса Вегешны "Качество обслуживания в сетях IP" [Электронный ресурс]. – Режим доступа: http:// it-ebooks.ru/publ/cisco/cisco_ip_quality_of_service/11-1-0-293.
4. ISO 9000:2015(ru) Quality management systems – Fundamentals and vocabulary [Электронный ресурс]. – Режим доступа: http:// https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en.
5. Стандарт ГОСТ РВ 51987 «Информационная технология, комплекс стандартов на АС» [Электронный ресурс]. – Режим доступа: http://gearletitbit.weebly.com/blog/gost-rv-51987-2002.
6. Петриченко Г.С. Методика выбора средств защиты для корпоративной сети / Г.С. Петриченко, Н.Ю. Нарыжная, Л.М. Крицкая // Научный журнал КубГАУ, 2016. – № 121(07). – С. 1-10.
7. Quality of Service (QoS) in a network with software (SDN): an overview [Электронный ресурс]. – Режим доступа к ресурсу: https://doi.org/10.1016/j.jnca.2016.12.019.
8. A single quality of service (QoS) survey in OPS / OBS networks [Электронный ресурс]. – Режим доступа к ресурсу: https://doi.org/10.1016/j.yofte.2017.05.016.
9. Network function virtualization: Challenges and opportunities for innovations [Электронный ресурс]. – Режим доступа к ресурсу: 10.1109/MCOM.2015.7045396.

10. Modeling of network access protocols for network quality analysis [Электронный ресурс]. – Режим доступа к ресурсу: 10.1109 / ISORC.2015.47.

11. Бурячок В.Л. Політика інформаційної безпеки / В.Л. Бурячок, Р.В. Грищук, В.О. Хорошко, під заг. ред. проф. В.О. Хорошка. – К: ПВП «Задруга», 2014. – 222 с.

12. Основи захисту інформації: навч. пос. / Ю.Г. Даник, С.Г. Вдовенко, В.І. Шестаков, О.О. Писарчук, Р. В. Грищук, М.В. Куликівський, В.М. Ходаківський. – Житомир: ЖВІ ДУТ, 2015. – 220 с.

13. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення / О.К. Юдін. – К.: НАУ, 2011. – 640 с.

14. Грищук Р.В. Основи кібербезпеки / Р.В. Грищук, Ю.Г. Даник; за заг. ред. проф. Ю.Г. Даника. – Житомир: ЖНАЕУ, 2016. – 636 с.

15. Забезпечення інформаційної безпеки держави / І.С. Іванченко, В.О. Хорошко, Ю.Е.Хохлачова, Д.В. Чирков під заг. ред. проф. В.О. Хорошка. – К: ПВП "Задруга", 2013. – 170 с.

16. Оцінювання шкоди національній безпеці України у разі витоку державної таємниці: моногр. / О.Г. Корченко, О.Є. Архипов., Ю.О. Дрейс. – К: наук.-вид.центр НА СБУ України, 2014. – 332 с.

17. Банківська безпека: підручн. / А.О. Корченко, Л.М. Скачек, В.О. Хорошко, під заг. ред. проф. В.О. Хорошка. – К: ПВП "Задруга", 2014, – 185 с.

18. Евсеев С.П., "Анализ оценки рисков кибербезопасности банковской информации" / С.П. Евсеев, О.Г. Король, А.С. Сочнева // Сборник научных трудов НАУ "Защита информации". – 2016. – Вып. 23. – С. 109-129.

19. Грищук Р.В. The synergetic approach for providing bank information security: the problem formulation / Р.В. Грищук, С.П. Евсеев // Безпека інформації. – 2016. – № 22(1). – С. 64-74.

20. Малий Ю. Методические подходы к анализу угроз безопасности информации и рисков в банковской сфере / Ю. Малий // Вестник БУКЭП. – 2013. – № 1. – С. 135-140.

21. Васильченко З. Деякі аспекти методологічної основи моделювання фінансової безпеки банку / З. Васильченко // Економіка. – 2013. – № 6(147). – С. 15-19.

22. Маркова О. Совершенствование информационной безопасности электронных расчетов в коммерческих банках России / О. Маркова // Финансовая аналитика: проблемы и решения. – 2015. – № 31. – С. 38-49.

23. Євсеєв С.П. Оцінка обміну даними в глобальних обчислювальних мережах на основі комплексного показника якості обслуговування мережі / С.П. Євсеєв, С.Е. Остапов, Х.Н. Рзаєв, В.І. Ніколаєнко // Науковий журнал: Радіоелектроніка, інформатика, управління. – Запоріжжя. – 2017. – № 1(40). – С. 115-128.

24. Король О.Г. Оцінка якості обслуговування глобальної мережі на основі технологій Ethernet за допомогою комплексного показника / О.Г. Король // Системи обробки інформації. – 2017. – № 2(148). – С. 88-94.

25. Грищук Р.В. Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах / Р.В. Грищук, С.П. Евсеев // Науково-технічний журнал "Безпека інформації". – 2017. – Том 23, № 3. – С. 204-214.

26. Постников В. М. Методы выбора весовых коэффициентов локальных критериев / В.М. Постников, С.Б. Спиридонов // Издатель ФГБОУ ВПО "МГТУ им. Н.Э. Баумана". Эл, № ФС 77 – 48211. – 2016. – Вып. 3. – С. 267-287.

References

1. MSJe-T E.800 Opredelenie terminov, otnosjashhihsja k kachestvu obsluzhivanija [Online]. Available: https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.800-200809.

2. Janovskij, G.G. "*Kachestvo obsluzhivanija v setjah IP*", [*Quality of service in IP networks*] [Online]. Available: www.niits.ru/public/2008/2008-006.pdf. Accessed on December 1, 2017.

3. Shrinivasa Vegeshny (2017), "*Kachestvo obsluzhivanija v setjah IP*" [*Quality of service in IP networks*] [Online]. Available: http:// it-ebooks.ru/publ/cisco/cisco_ip_quality_of_service/11-1-0-293. Accessed on December 1.

4. (2017), ISO 9000:2015(ru) Quality management systems – Fundamentals and vocabulary [Online]. Available: http:// https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:en. Accessed on December 1.

5. Standart GOST RV 51987 «Informacionnaja tehnologija, kompleks standartov na AS» [Online]. Available: http://gearletitbit.weebly.com/blog/gost-rv-51987-2002. Accessed on December 1, 2017.

6. Petrichenko, G.S., Naryzhnaja, N.Ju. and Krickaja, L.M. (2016), "Metodika vybora sredstv zashhity dlja korporativnoj seti", [The method of selecting security solutions for the corporate network], *Nauchnyj zhurnal KubGAU*, No. 121(07), pp. 1-10/

7. Quality of Service (QoS) in a network with software (SDN): an overview (2016), [Online]. Available: https://doi.org/10.1016/j.jnca.2016.12.019. Accessed on December 1, 2017.

8. A single quality of service (QoS) survey in OPS / OBS networks (2017), [Online]. Available: https://doi.org/10.1016/j.yofte.2017.05.016. Accessed on December 1.

9. Network function virtualization: Challenges and opportunities for innovations (2015), [Online]. Available: 10.1109/MCOM.2015.7045396. Accessed on December 1, 2017.

10. Modeling of network access protocols for network quality analysis (2015), [Online]. Available: 10.1109 / ISORC.2015.47. Accessed on December 1, 2017.

11. Burjachok, V.L., Grishhuk, R.V. and Horoshko, V.O. (2014), "*Politika informacijnoї bezpeki*" [*Information Security Policy*], PVP «Zadruga», Kiev, 222 p.

12. Danik, Ju.G., Vdovenko, S.G., Shestakov, V.I., Pisarchuk, O.O., Grishhuk, R.V., Kulikivs'kij, M.V. and Hodakivs'kij, V.M. (2015), "*Osnovi zahistu informacii*" [*The basics of information protection*], ZhVI DUT, Zhitomir, 220 p.

13. Judin, O.K. (2011), "*Informacijna bezpeka. Normativno-pravove zabezpechennja*" [*Informational security. Regulatory and Legal Support*], NAU, Kiev, 640 p.

14. Grishhuk, R.V. and Danik, Ju.G. (2016), "*Osnovi kiberbezpeki*" [*Cybersecurity Basics*], ZhNAEU, Zhitomir, 636 p.

15. Ivanchenko, I.S., Horoshko, V.O., Hohlachova, Ju.E. and Chirkov, D.V. (2013), "*Zabezpechennja informacijnoї bezpeki derzhavi*" [*Providing information security of the state*], PVP "Zadruga", Kiev, 170 p.

16. Korchenko, O.G., Arhipov, O.Є. and Drejs, Ju.O. (2014), "*Ocinjuvannja shkodi nacional'nij bezpeci Ukraïni u razi vitoku derzhavnoï taємnici: monografija*" [*Assessment of harm to the national security of Ukraine in the event of a source of state secrets*], nauk.-vid.centr NA SBU Ukraïni, Kiev, 332 p.

17. Korchenko, A.O., Skachek, L.M. and Horoshko, V.O. (2014), "*Bankivs'ka bezpeka: pidruchnik*", [*Banking security*], PVP "Zadruga", Kiev, 185 p.

18. Evseev, S.P., Korol, O.G. and Sochneva, A.S. (2016), "Analiz ocenki riskov kiberbezopasnosti bankovskoj informacii" [Analysis of the assessment of cybersecurity risks of banking information], *Sbornik nauchnyh trudov NAU "Zashhita informacii"*, No. 23, pp. 109-129.

19. Grishhuk, R.V. and Evseev, S.P. (2016), The synergetic approach for providing bank information security: the problem formulation, *Bezpeka informacii*, No. 22(1), pp. 64-74.

20. Malij, Ju. (2013), "Metodicheskie podhody k analizu ugroz bezopasnosti informacii i riskov v bankovskoj sfere" [Methodical approaches to the analysis of threats to the security of information and risks in the banking sector], *Vestnik BUKJeP*, No. 1, pp. 135-140.

21. Vasil'chenko, Z. (2013), "*Dejaki aspekti metodologichnoï osnovi modeljuvannja finansovoï bezpeki banku*" [*Some aspects of the methodological basis of financial security modeling of the bank*], *Ekonomika*, No. 6(147), pp. 15-19.

22. Markova, O. (2015), "Sovershenstvovanie informacionnoj bezopasnosti jelektronnyh raschetov v kommercheskih bankah Rossii", [Perfection of information security of electronic settlements in commercial banks of Russia], *Finansovaja analitika: problemy i reshenija*, No. 31, pp. 38-49.

23. Єvseєv, S.P., Ostapov, S.E., Rzaєv, H.N. and Nikolaєnko, V.I. (2017), "Ocinka obminu danimi v global'nih obchisljuval'nih merezhah na osnovi kompleksnogo pokaznika jakosti obslugovuvannja merezhi" [Estimation of data exchange in global computer networks on the basis of a comprehensive indicator of network service quality], *Naukovij zhurnal Radioelektronika, informatika, upravlinnja*, Zaporizhzhja, No. 1(40), pp. 115-128.

24. Korol', O.G. (2017), "Ocinka jakosti obslugovuvannja global'noï merezhi na osnovi tehnologij Ethernet za dopomogoju kompleksnogo pokaznika"[Estimation of quality of service of the global network on the basis of Ethernet technologies with the help of complex index] . Sistemi obrobki informaciї. № 2(148). pp. 88 – 94.

25. Grishhuk, R.V. and Evseev, S.P. (2017). "Metodologija pobudovi sistemi zabezpechennja informacijnoï bezpeki bankivs'koï informaciї v avtomatizovanih bankivs'kih sistemah" [Methodology of building a system for providing information security of banking information in automated banking systems], *Bezpeka informacii*, tom 23, No. 3. pp. 204-214.

26. Postnikov, V.M. and Spiridonov, S.B. (2016), "Metody vybora vesovyh kojefficientov lokal'nyh kriteriev" [Methods of choosing weight coefficients of local criteria], *Izdatel' FGBOU VPO "MGTU im. N.Je. Baumana"*, No. 3, pp. 267-287.

Надійшла до редколегії 12.02.2018
Схвалена до друку 17.04.2018

Відомості про авторів:

Євсєєв Сергій Петрович
кандидат технічних наук
старший науковий співробітник
доцент кафедри Харківського національного
економічного університету,
Харків, Україна
https://orcid.org/0000-0003-1647-6444

Комишан Антон Сергійвич
магістр
Харківського національного
економічного університету,
Харків, Україна
https://orcid.org/0000-0002-3958-9698

Корольов Роман Володимирович
кандидат технічних наук
старший викладач кафедри
Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-7948-5914

Бонь Іван Васильович
магістр
Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0003-0352-5032

Information about the authors:

Serhii Yevseiev
PhD Senior Research
Senior Lecturer of Department
of Simon Kuznets Kharkiv National
University of Economics,
Kharkiv, Ukraine
https://orcid.org/0000-0003-1647-6444

Anton Komyshan
Master of Science
of Simon Kuznets Kharkiv National
University of Economics,
Kharkiv, Ukraine
https://orcid.org/0000-0002-3958-9698

Roman Korolev
PhD
Senior Instructor of Department
of Ivan Kozhedub Kharkiv National
Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0002-7948-5914

Ivan Bon
Master of Science
of Ivan Kozhedub Kharkiv National
Air Force University,
Kharkiv, Ukraine
https://orcid.org/0000-0003-0352-5032

Солоненко Сергій Геннадійович
магістр
Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-5161-1501

Serhii Solonenko
Master of Science
of Ivan Kozhedub Kharkiv National
Air Force University,
Kharkiv, Ukraine
https://orcid.org/ 0000-0002-5161-1501

Богульський Віктор Вікторович
магістр
Харківського національного університету
Повітряних Сил ім. І. Кожедуба,
Харків, Україна
https://orcid.org/0000-0002-2310-1993

Viktor Bohulskyi
Master of Science
of Ivan Kozhedub Kharkiv National
Air Force University,
Kharkiv, Ukraine
https://orcid.org/ 0000-0002-2310-1993

ВЕРИФИКАЦИЯ МЕТОДИКИ ОЦЕНКИ ФУНКЦИОНАЛЬНОЙ ЭФФЕКТИВНОСТИ ПЕРЕДАЧИ БАНКОВСКИХ ИНФОРМАЦИОННЫХ РЕСУРСОВ В АВТОМАТИЗИРОВАННЫХ БАНКОВСКИХ СИСТЕМАХ

С.П. Евсеев, Р.В. Королев, А.С. Комышан, И.В. Бонь, С.Г. Солоненко, В.В. Богульський

Рассматривается верификация методики оценки эмерджентных свойств функциональной эффективности АБС на основе комплексного показателя качества, который базируется на основных показателях безопасности и надежности, обеспечивающих противодействие гибридным угрозам на банковские информационные ресурсы и элементы инфраструктуры автоматизированных банковских систем. Для оценки комплексного показателя функциональной эффективности предложены опорные таблицы, позволяющие выделить диапазоны изменения необходимых параметров и определить их в условных баллах. Такой подход позволяет без значительных экономических, вычислительных и человеческих ресурсов учитывать не только технические, но и экономические параметры ТСЗИ АБС, что позволяет более точно оценивать ее функциональную эффективность, учитывать результаты исследований при масштабировании сети АБС, выборе ТСЗИ по построению и поддержанию КСЗИ, анализ противодействию угрозам на составляющие безопасности (ИБ, КБ, БИ) банковских информационных ресурсов, их гибридности и синергизм, минимизацию затрат и действенный контроль за программными средствами КСЗИ АБС.

Ключевые слова: *банковские информационные ресурсы, автоматизированная банковская система, методика функциональной эффективности передачи данных в АБС, гибридности, синергизм.*

VERIFICATION OF THE METHOD OF EVALUATING THE FUNCTIONAL EFFICIENCY OF THE TRANSFER OF BANKING INFORMATION RESOURCES IN AUTOMATED BANKING SYSTEMS

S. Yevseiev, R. Korolev, A. Komyshan, I. Bon, S. Solonenko, V. Bohulskyi

The verification of the method of estimating the emergent properties of the functional efficiency of automated banking systems on the basis of a complex quality index is considered. The comprehensive indicator is based on basic security and reliability, takes into account the counteraction to hybrid threats to banking information resources and elements of the infrastructure of automated banking systems. Reference tables are proposed for estimating the complex functional efficiency index. Tables define the ranges for changing the required parameters in conditional scores. This simple method allows obtaining adequate results of the evaluation and combine them with the results of accurate calculations for individual specific parameters. Such an approach allows, without significant economic, computational and human resources, to take into account not only technical but also economic parameters of technical means of information protection. This allows a more accurate assessment of its functional efficiency, taking into account the results of research in scaling automated banking networks. Provides a qualitative approach to the choice of technical means of information protection, the construction of a comprehensive information security system. It allows to take into account the results of analyzes of counteraction to threats to the components of security (information security, cybersecurity, security for information). Provides an assessment of the hybridity and synergy of modern threats, cost minimization and effective control over software tools for a comprehensive information security system. The proposed method for evaluating the functional efficiency of the transfer of banking information uses a complex indicator, which allows obtaining emergent properties. The synthesis of a complex indicator of the effectiveness of investments in the security of banking information resources, the results of assessing the hybridity and synergy of threats and elements of the ABS system, the results of the evaluation of the express method of stability and the effectiveness of the software (hardware and software) implementation of cryptographic algorithms provides a quantitative assessment of the functional efficiency of the transfer of banking information in automated banking systems.

Keywords: *banking information resources, automated banking system, method of functional efficiency of data transmission in ABS, hybridization, synergism.*