2.3. Методологія синтезу та аналізу запропонованих моделей та методів забезпечення безпеки банківських інформаційних ресурсів

Аналіз останніх досліджень. У сучасних умовах, як показала практика, важлива роль у забезпеченні національної безпеки України та особливо її економічної складової належить процесам забезпечення інформаційної безпеки держави у банківському секторі. Ключову роль при побудові системи безпеки банківських інформаційних ресурсів (БІР), як складової національних інформаційних ресурсів держави, відіграє теорія та практика в якій науково-методологічна база є основою для прийняття обґрунтованих та ефективних управлінських рішень суб'єктами забезпечення інформаційної безпеки держави на усіх рівнях. Зміни останнього десятиліття, що відбулися в організацій банківського сектору (ОБС) призвели до об'єднання інформаційних та комп'ютерних мереж в єдиний інформаційний та кібернетичний простір. Інтеграційні процеси розвитку автоматизованих банківських систем (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 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.

Відомо, що методологічний базис в будь-якій галузі безпеки являє собою ключові компоненти самої теорії безпеки та ґрунтується на методах і моделях, необхідних і достатніх для дослідження проблеми безпеки та вирішення практичних задач відповідного призначення. Так, нині в галузі інформаційної безпеки існує достатньо велика кількість методологій [1].

Однак проаналізовані методології в роботі [1] не враховують синергізм та ознаки гібридності загроз на складові безпеки БІР, а саме: інформаційної безпеки, кібербезпеки, безпеки інформації. Тому усі вони потребують кардинального перегляду з погляду створення методологічного базису для побудови системи безпеки БІР як України зокрема, так і світу в цілому.

Виходячи з аналізу [**Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; **Ошибка! Источник ссылки не найден.**; 1; 3] можна стверджувати, що одним з пріоритетних напрямків підвищення рівня безпеки БІР зокрема та подальшої стабілізації ІБ держави в цілому є принципово нове вирішення проблеми безпеки організацій банківського сектору держави

шляхом створення сучасних методів і засобів захисту БІР від гібридного нападу на основі комплексування ознак загроз інформаційній безпеці (ІБ), кібербезпеці (КБ), безпеці інформації (БІ) на БІР, технічні об'єкти її інфраструктури. Так, вагомі наукові результати при вирішенні проблеми ІБ держави та розкриття окремих її складових в ОБС одержано в наукових працях [2 – 4] та ін., але незважаючи на це проблема залишається актуальною не тільки для України, а й для світової спільноти.

Виходячи з єдиних системних позицій [1, 4] та потреби реалізації комплексного підходу до побудови прогресивних систем безпеки БІР в умовах гібридизації та комплексування загроз ІБ, КБ, БІ нині існує об'єктивне протиріччя між високими вимогами практики до систем безпеки БІР та недосконалістю, а подекуди й відсутністю дієвих науково обґрунтованих методологічних засад її забезпечення.

Перспективним підходом забезпечення безпеки БІР є одночасне та раціональне поєднання організаційних заходів та технічних засобів, спрямованих на забезпечення ІБ, КБ та БІ, що зрештою позначається на інвестиціях банку, вкладених у безпеку. При цьому комплексування сил і засобів безпеки у кожному окремому випадку не є ефективним та таким, що не гарантує досягнення очікуваного безпекового синергетичного ефекту [1, 5].

Таким чином, як зрозуміло з вищевикладеного, на основі існуючого методологічного апарату досить проблематично, а в деяких випадках і неможливо досягнути поставленої мети дослідження.

Основні матеріали дослідження

Спираючись на відомий підхід до побудови методологій [1 – 4] на основі досліджень [1, 4, 5] пропонується принципово нова методологія побудови системи забезпечення БІР.

Вона містить п'ять етапів (рис. 1, 2): 1) визначення ймовірності впливу загроз ІБ, КБ, БІ на безпеку БІР; 2) визначення узагальненого показника рівня захищеності БІР; 3) оцінювання ефективності інвестицій в забезпечення безпеки БІР; 4) побудова інтегрованих механізмів забезпечення конфіденційності, цілісності, автентичності та достовірності БІР; 5) визначення стану та формування стратегій безпеки БІР. Реалізація методології, з урахуванням розроблених у дисертації методів і засобів, дасть можливість забезпечити підвищення рівня захищеності БІР в умовах дії гібридних загроз, раціональну організацію системи забезпечення безпеки БІР в умовах одночасної дії на систему загроз ІБ, КБ та БІ.

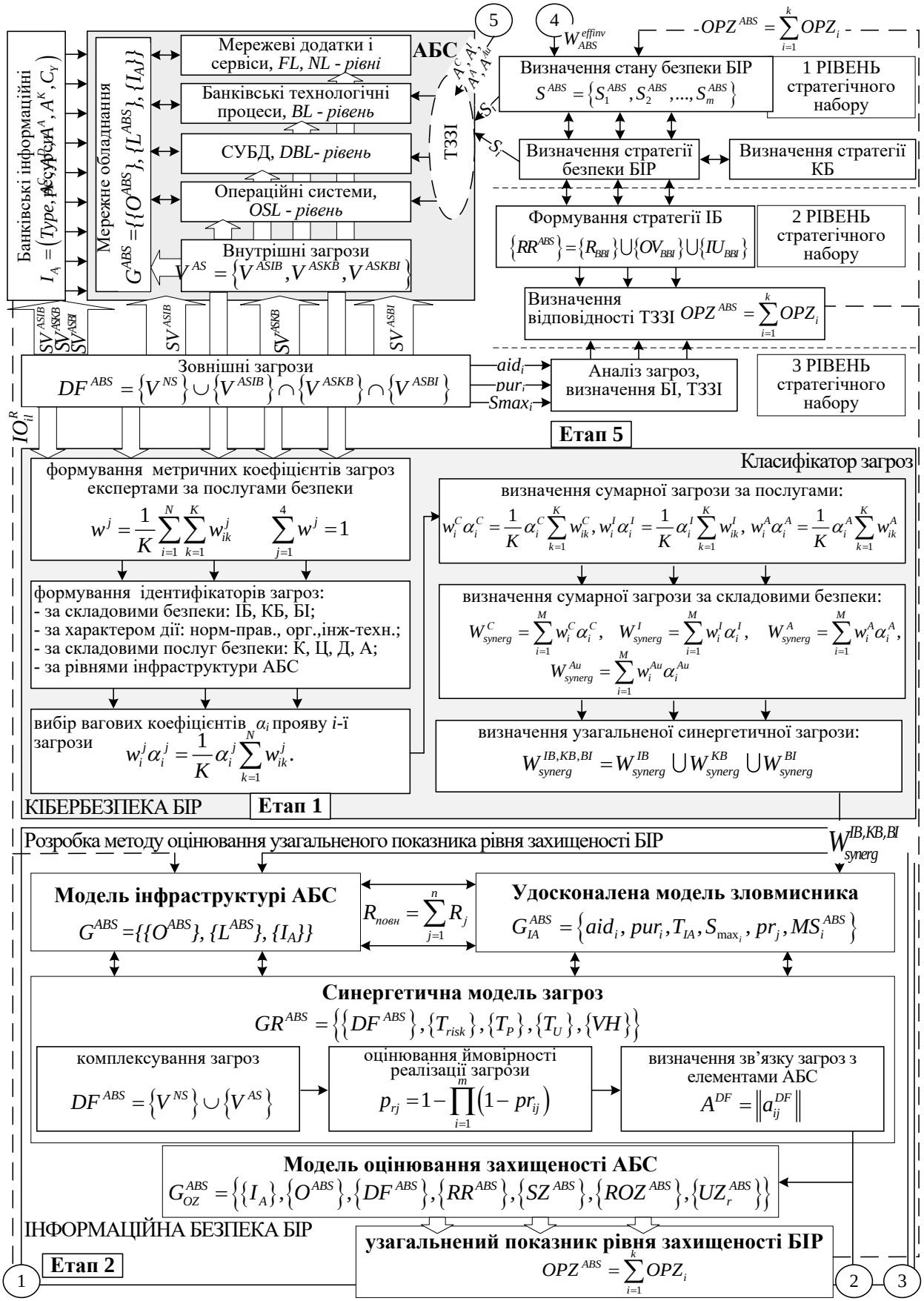

Рис. 1. Схема методології побудови системи безпеки банківських інформаційних ресурсів

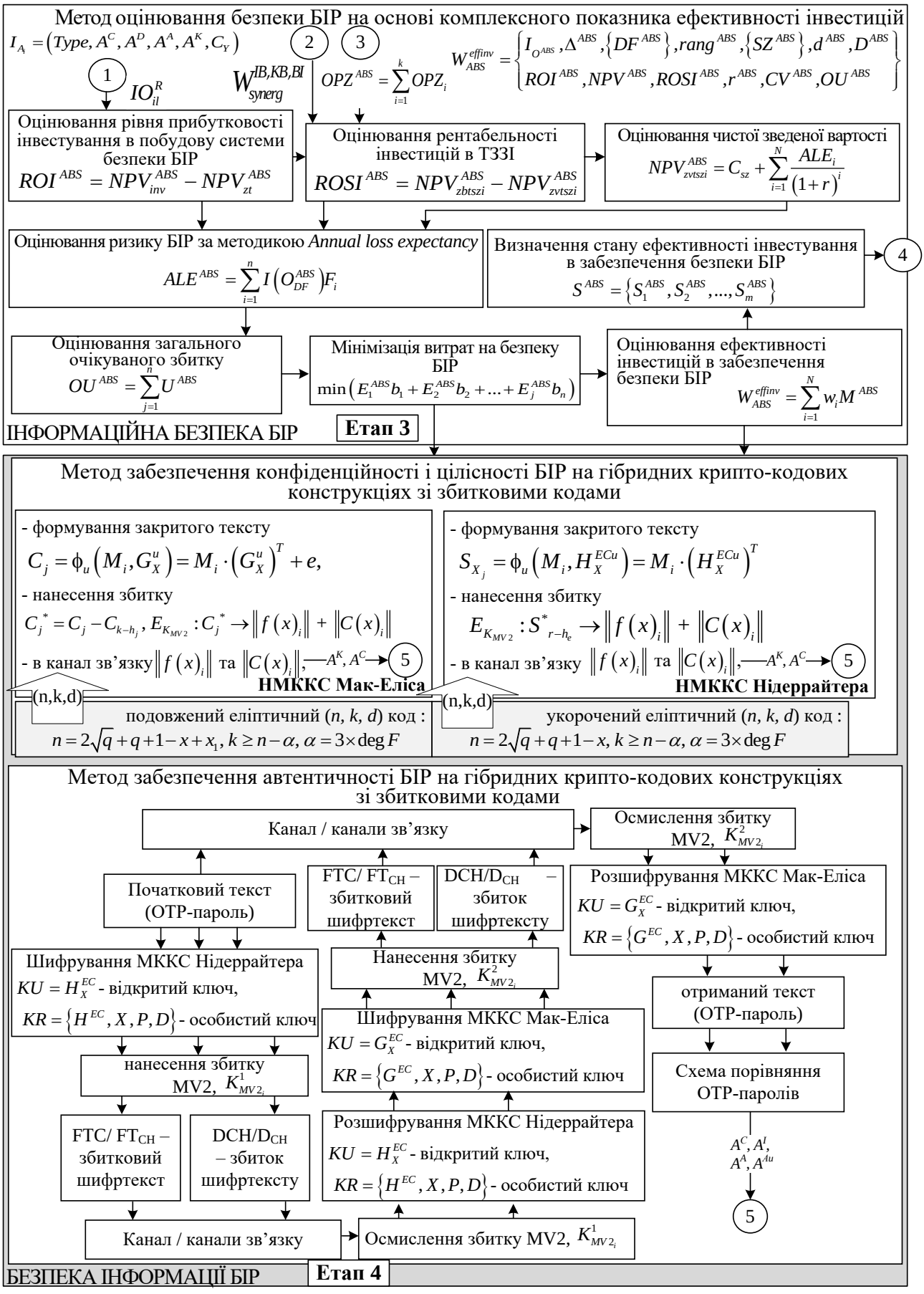

Рис. 2. Схема методології побудови системи безпеки банківських інформаційних ресурсів

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

На першому етапі, зважаючи на те, що загрози ІБ, КБ, БІ мають можливість впливати на різні послуги безпеки (конфіденційність, цілісність, доступність, автентичність) з різною інтенсивністю експертами з ІБ вирішується завдання щодо нормування метричних коефіцієнтів загроз за послугами безпеки та формування класифікації загроз на основі запропонованого класифікатора [5]. Складовими класифікатора є:

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

– 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). Множину загроз ІБ, КБ, БІ на БІР запропоновано використовувати з ресурсу http://bdu.fstec.ru/threat.

Для визначення вагових коефіцієнтів α_i, що визначають умови прояву *i*-ї загрози використовуються дані з табл. 1.

Таблиця 1

Вибір вагових коефіцієнтів α_i прояву *i*-ї загрози залежно від умови її 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

Визначення реалізації кожної *i*-ї загрози з урахуванням імовірності прояву атаки її виникнення здійснюється за виразом:

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

Для кожної послуги безпеки та *i*-ї загрози:

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

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

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

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

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 *i*-ї загрози.

Визначення реалізації виникнення декількох загроз на певну послугу безпеки визначається за виразами:

$$W_{synerg}^C = \sum_{i=1}^{M} w_i^C \alpha_i^C \text{ – послуга конфіденційність;}$$

$$W_{synerg}^I = \sum_{i=1}^{M} w_i^I \alpha_i^I \text{ – послуга цілісність;}$$

$$W_{synerg}^A = \sum_{i=1}^{M} w_i^A \alpha_i^A \text{ – послуга доступність;}$$

$$W_{synerg}^{Au} = \sum_{i=1}^{M} w_i^{Au} \alpha_i^{Au} \text{ – послуга автентичність,}$$

де M – кількість декількох загроз які вибрані експертом з ІБ банку з множини $\{i\}_i^M$, яка є підмножиною усієї множини загроз класифікатора, тобто $M \le N$.

Визначення сумарної загрози за складовими безпеки:

$$W_{synerg}^{IB} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) \alpha_i,$$

$$W_{synerg}^{KB} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) \alpha_i,$$

$$W_{synerg}^{BI} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) \alpha_i.$$

Визначення узагальненої синергетичної загрози проводиться згідно з виразом (рис. 1):

$$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \bigcup W_{synerg}^{KB} \bigcup W_{synerg}^{BI}.$$

Визначення узагальненої синергетичної загрози з урахуванням їх гібридності визначається: $W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^{C} \bigcap W_{synerg}^{\text{I}} \bigcap W_{synerg}^{A} \bigcap W_{synerg}^{Au}$.

Одержані за результатами аналізу комплексування загроз дані подаються на 3-й рівень моделі стратегічного управління банком для їх узагальнення при оцінюванні достатності технічних засобів захисту БІР. Результати досліджень загроз з максимальною частотою їх прояву на БІР наведені у табл. 2.

Таблиця 2

Результати оцінки загроз на основі синергетичного підходу

складові безпеки	послуги безпеки				
	C, W_{synerg}^{C}	I, W_{synerg}^{I}	A, W_{synerg}^{I}	Au, W_{synerg}^{Au}	Підсумок
IB, W_{synerg}^{IB}	0,023	0,223	0,193	0,207	0,0002
KB, W_{synerg}^{KB}	0,222	0,234	0,197	0,134	0,0014
BI, W_{synerg}^{BI}	0,226	0,109	0,152	0,189	0,0007
Підсумок	0,471	0,566	0,542	0,53	
$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \bigcup W_{synerg}^{KB} \bigcup W_{synerg}^{BI} =$ =0,0002+0,0014+0,0007=0,0223			$W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^{\text{C}} \bigcap W_{synerg}^{\text{I}} \bigcap W_{synerg}^{A} \bigcap W_{synerg}^{Au}$ = =0,471×0,566×0,542×0,53=0,0766		

Етап 2. визначення узагальненого показника рівня захищеності БІР.

На основі сформованої множини загроз ІБ, КБ, БІ на БІР та моделі ієрархії АБС – $G^{ABS} = \{\{O^{ABS}\}, \{L^{ABS}\}, \{I_A\}\}$ визначається залежність між інформаційними активами БІР і загрозами ІБ, КБ, БІ за такими діями:

– 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. A^C – конфіденційність, A^I – цілісність, A^A – доступність, A^{Au} – автентичність, *CY* – безперервність – це властивості інформації, які необхідно забезпечувати. Вони набувають значення 1 – якщо властивість необхідно, 0 – в іншому випадку;

– визначення зв'язку між інформаційними активами $\{I_A\}$ й об'єктами

середовища. 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 застосунків і сервісів. Для визначення типу зв'язку та існуючого відношення I^{OR} між інформаційними активами та об'єктами середовища використання використовується правило:

$$IO^R = \left\| IO_{il}^R \right\|,$$

де IO_{il}^R – відображає наявність і тип зв'язку між *i*-м інформаційним активом та *l*-м об'єктом середовища АБС.

На основі запропонованої синергетичної моделі загроз, маємо:

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

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, і узагальненої моделі зловмисника:

$$G_{IA}^{ABS} = \{aid_i, pur_i, T_{IA}, S_{\max_i}, pr_j, MS_i^{ABS}\} \; \forall i \in n, \forall j \in m,$$

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 технічними засобами захисту інформації (ТЗЗІ), здійснюється комплексування множини загроз вигляду:

$$DF^{ABS} = \{V^{NS}\} \cup \{V^{AS}\}, \text{ де } \{V^{AS}\} = \{V^{ASBI}\} \cap \{V^{ASIB}\} \cap \{V^{ASKB}\}.$$

Такий підхід дозволяє визначити зв'язок між джерелами загроз і елементами АБС $A^{DF} = \left\| a_{ij}^{DF} \right\|$, що захищаються.

Визначення ціни повного ризику всіх активів БІР:

$$R_{повн} = \sum_{j=1}^{n} R_j ,$$

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

Ймовірність реалізації хоча б однієї загрози для кожного активу БІР:

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

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

Визначення захищеності АБС від загроз ІБ, КБ, БІ на БІР пропонується здійснювати на основі удосконаленої моделі рівня захищеності банківських інформаційних ресурсів:

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

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 до забезпечення безпеки БІР; $\{SZ^{ABS}\}$ – множина можливих ТСЗІ; $\{ROZ^{ABS}\}$ – дані обліку про результати оцінки захищеності АБС; $\{UZ_r^{ABS}\}$ – рівень захищеності АБС.

На основі визначеного зв’язку між джерелами загроз та елементами АБС визначається зв’язок між загрозами і технічними засобами системи захисту інформації (ТЗСЗІ) – $A^{DFSZ} = \left\| a_{ij}^{DFSZ} \right\|$.

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 i-ї загрози.

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.

Визначення вимог регуляторів $\{RR^{ABS}\}$ включає вимоги до забезпечення безпеки БІР – $\{R_{BBI}\}$, що вказані у міжнародних і національних стандартах, множину оцінок ступеня виконання вимог безпеки $\{OV_{BBI}\}$ та множину підсумкового рівня відповідності безпеки БІР вимогам з множини $\{R_{BBI}\}$ – $\{IU_{BBI}\}$:

$$\{RR^{ABS}\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}.$$

Для оцінювання $\{RR^{ABS}\}$ використаємо вимоги з [1, 5], визначимо, що приватні показники поділяються на два типу:

перший – приватні показники, що відображають вимоги [5], виконання яких є обов'язковим в організації;

другий – приватні показники, що відображають положення [**Ошибка! Источник ссылки не найден.**], виконання яких рекомендується в організації БС.

Для часткових показників, виконання яких є обов'язковим (перший тип), встановлюється наступна шкала ступеня їх виконання:

"ні" – оцінці присвоюється значення, рівне нулю;

"частково" – оцінці присвоюється значення 0,25, 0,5 або 0,75;

"так" – оцінці присвоюється значення, рівне одиниці.

Якщо частковий показник призначений для оцінки вимог, які не належать до діяльності організації або на момент оцінки не є актуальними для організації, що зафіксовано документами організації, то даний частковий показник визначається як неоцінюваний (повинна бути заповнена графа "н/о" – немає оцінки) і не враховується у формуванні подальших результатів оцінки.

Для часткових показників, виконання яких рекомендується (другий тип), встановлюється наступна шкала ступеня їх виконання:

"так" – оцінці присвоюється значення, рівне одиниці;

"ні" – частковий показник визначається як неоцінюваний (повинна бути заповнена графа "н/о" – немає оцінки) і не враховується у формуванні подальших результатів оцінки. В табл. 3, 4 наведені рекомендовані критерії виставлення оцінок окремих показників ІБ за першим та другим типами часткових показників.

Таблиця 3

Рекомендовані критерії виставлення оцінок окремих показників ІБ, в яких оцінюється як ступінь документованості, так і ступінь виконання вимог ІБ

оцінка приватного показника ІБ	Критерій виставлення оцінки приватного показника ІБ
0	Вимоги приватного показника ІБ не встановлені (визначені) у внутрішніх документах аудиту
0,25	Вимоги приватного показника ІБ встановлені (визначені) у внутрішніх документах аудиту, але не виконуються
0,5	Вимоги приватного показника ІБ встановлені (визначені) у внутрішніх документах аудиту, але не виконуються
0,75	Вимоги приватного показника ІБ встановлені (визначені) у внутрішніх документах аудиту і виконуються майже в повному обсязі
1,0	Вимоги приватного показника ІБ встановлені (визначені) у внутрішніх документах аудиту і виконуються в повному обсязі

Таблиця 4

Рекомендовані критерії виставлення оцінок окремих показників ІБ, в яких оцінюється тільки ступінь документованості вимог ІБ

оцінка приватного показника ІБ	Критерій виставлення оцінки приватного показника ІБ
0	Вимоги приватного показника ІБ не встановлені у внутрішніх документах аудиту
1,0	Вимоги приватного показника ІБ повністю встановлені у внутрішніх документах аудиту

При проведенні оцінки часткових показників, для яких оцінюється тільки ступінь виконання (частковий показник категорії перевірки 3), використовується наступний загальний підхід (табл. 5):

Таблиця 5

Рекомендовані критерії виставлення оцінок окремих показників ІБ, в яких оцінюється тільки ступінь виконання вимог ІБ

оцінка приватного показника ІБ	Критерій виставлення оцінки приватного показника ІБ
0	Вимоги приватного показника ІБ не виконуються
0,5	Вимоги приватного показника ІБ виконуються в неповному обсязі
1,0	Вимоги приватного показника ІБ виконуються в повному обсязі

У випадках, якщо при проведенні оцінки приватного показника використовується обмежений набір об'єктів, що входять в область оцінювання відповідності ІБ (наприклад, обмежена вибірка АБС), і за результатами оцінювання приватного показника отримані результати, що вказують на повне виконання або повне невиконання / повну документованість або відсутність документованості відповідних вимог ІБ, рекомендується розширити набір зазначених об'єктів (вибірку) для підтвердження або корекції отриманих результатів [**Ошибка! Источник ссылки не найден.**]. В табл. 6 частково наведені відповідні групові та часткові показниками ІБ, призначеними для перевірки реалізації даних вимог.

Визначимо наступні групові показники:

R_{BBI_1} – оцінка ступеня виконання вимог за напрямом "поточний рівень ІБ організації";

R_{BBI_2} – оцінка ступеня виконання вимог за напрямом "менеджмент ІБ організації";

R_{BBI_3} – оцінка ступеня виконання вимог за напрямом "рівень усвідомлення ІБ організації";

OV_{ooIP} – оцінка ступеня виконання вимог, що регламентують обробку БІР;

$OV_{БІТП}$ – оцінка ступеня виконання вимог, що регламентують банківський інформаційний технологічний процес;

$OV_{БІТПП}$ – оцінка ступеня виконання вимог, що регламентують банківський платіжний технологічний процес;

OV_{ozIP} – оцінка ступеня захисту БІР з використанням криптографічних ЗЗІ;

OV_{IU_i} – оцінка ступеня виконання вимог для групового показника;

$OV_{IU_{ij}}$ – оцінка ступеня виконання вимог для приватного показника;

де i – номер групового показника, j – номер приватного показника;

Таблиця 6

Групові та часткові показниками ІБ, призначеними для перевірки реалізації даних вимог

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
R_{BBI_2} – оцінка ступеня виконання вимог за напрямом "менеджмент ІБ організації"									
$IU_{1.1}$	упровадження процесного підходу до діяльності банку	обов'язковий	категорія 2						
...	...	...	...						
$IU_{1.20}$	застосувати заходи безпеки для захисту від атак на відмову в обслуговуванні та/або розподілених атак на відмову в обслуговуванні (*DoS/DDoS*-атак) на зовнішньому периметрі мережі банку	обов'язковий	категорія 3						
R_{BBI_3} – оцінка ступеня виконання вимог за напрямом "рівень усвідомлення ІБ організації"									
$IU_{2.1}$	визначати підходи (методики) оцінювання та оброблення ризиків інформаційної безпеки	рекомендований	категорія 1						
...	...	...	...						

Продовження табл.6

Позначення ЧП	Частковий показник (ЧП)	Обов’язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$U_{2.25}$	визначити в посадових інструкціях працівників банку або організаційно-розпорядчих документах банку особисті функції та обов'язки з виявлення, класифікації, реагування і аналізу інцидентів безпеки інформації	обов’язковий	категорія 3						
OV_{ooIP} – оцінка ступеня виконання вимог, що регламентують обробку БІР									
$IU_{3.1}$	здійснити ідентифікацію змінних носіїв інформації за допомогою унікального ідентифікатора, який дозволить визначити тип носія та користувача змінного носія	обов’язковий	категорія 1						
…	…	…	…						

Продовження табл. 6

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{3.30}$	використовувати сертифікати відкритих ключів, отримані в акредитованих/зареєстрованих ЦСК для ідентифікації та автентифікації, забезпечення конфіденційності інформації під час інформаційного обміну між інформаційними системами банку та Національного банку	обов'язковий	категорія 2						
$OV_{БІТП}$ – оцінка ступеня виконання вимог, що регламентують банківський інформаційний технологічний процес									

Продовження табл. 6

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{4.1}$	забезпечується застосування багаторівневого (ешелонованого) підходу, за яким окремо за допомогою незалежних систем криптографічного захисту інформації захищається сеансовий рівень базової еталонної моделі взаємодії відкритих систем (*Open systems interconnection basic reference model, OSI/ISO*) та прикладний рівень моделі взаємодії відкритих систем інформаційних систем Національного банку	обов'язковий	категорія 2						
...	...	...	...						
$IU_{4.34}$	використовувати проміжний сервер для виконання функцій адміністрування чи супроводження інформаційних систем банку, мережевого обладнання та серверів	обов'язковий	категорія 2						
$OV_{БПТП}$ – оцінка ступеня виконання вимог, що регламентують банківський платіжний технологічний процес									

Кінець табл. 6

Позначення ЧП	Частковий показник (ЧП)	Обов'язковість виконання	Категорія перевірки	Оцінка часткового показника ІБ					
				0	0,25	0,5	0,75	1	н/о
$IU_{5.1}$	забезпечити дотримання принципу надання мінімального рівня повноважень під час надання доступу до інформаційних систем банку (уключаючи доступ привілейованих користувачів)	обов'язковий	категорія 2						
…	…	…	…						
$IU_{5.15}$	використовувати механізми багатофакторної автентифікації під час надання доступу до САБ	обов'язковий	категорія 2						
OV_{ozIP} – оцінка захисту БІР з використанням криптографічних ЗЗІ									
$IU_{6.1}$	використовувати механізми багатофакторної автентифікації під час надання доступу для виконання функцій адміністрування або супроводження САБ	обов'язковий	категорія 1						
…	…	…	…						
$IU_{6.20}$	використовувати стандарти, документи та настанови відкритого проекту захисту веб-додатків "*Open web application security project*" (*OWASP*)	обов'язковий	категорія 2						

IU_{ij} – позначення приватного показника;

Групові показники ІБ утворюють структуру напрямків оцінки, деталізуючи оцінки поточного рівня ІБ організації, менеджменту і рівня усвідомлення ІБ. Оцінки групових показників (OV_{IU_i}) використовуються для отримання оцінки за напрямами (R_{BBI_1}, R_{BBI_2} і R_{BBI_3}). Приватні показники ІБ входять до складу групових показників і представлені у вигляді питань, відповіді на які дають можливість визначити оцінки $\left(OV_{IU_{ij}}\right)$, які потім формують оцінки OV_{IU_i} групових показників.

Оцінка групового показника (OV_{IU_i}) обчислюється з оцінок, що входять до нього часткових показників $\left(OV_{IU_{ij}}\right)$:

$$OV_{IU_i} = \frac{\sum_j IU_{ij}}{j}.$$

Оцінка ступеня виконання вимог за напрямом R_{BBI_1} "поточний рівень ІБ організації" здійснюється за виразом:

$$R_{BBI_1} = \min\left(OV_{БІТП}, OV_{БІТТП}, OV_{ooIP}, OV_{ozIP}\right),$$

де OV_{ooIP} – оцінка ступеня виконання вимог, що регламентують обробку БІР; $OV_{БІТП}$ – оцінка ступеня виконання вимог, що регламентують банківський інформаційний технологічний процес; $OV_{БІТТП}$ – оцінка ступеня виконання вимог, що регламентують банківський платіжний технологічний процес; OV_{ozIP} – оцінка ступеня захисту БІР з використанням криптографічних ЗЗІ.

Оцінка ступеня виконання вимог за напрямом "менеджмент ІБ організації" визначається виразом:

$$R_{BBI_2} = k_{R_{BBI_2}} \frac{\sum_{j=1}^{m} IU_{1j}}{j},$$

де $k_{R_{BBI_2}}$ – коригуючий коефіцієнт, визначений у табл.7;

j – номер приватного показника, $j = \overline{1,...,m}$.

Оцінка ступеня виконання вимог за напрямом “рівень усвідомлення ІБ організації” визначається виразом:

$$R_{ВВІ_3} = k_{R_{ВВІ\,3}} \frac{\sum_{j=1}^{m} IU_{2j}}{j},$$

де $k_{R_{ВВІ\,3}}$ – коригуючий коефіцієнт, визначений у табл. 7;

j – номер приватного показника, $j = \overline{1,...,m}$.

Оцінка ступеня виконання вимог, що регламентують обробку БІР визначається виразом:

$$OV_{ooIP} = k_{ooIP} \frac{\sum_{j=1}^{m} IU_{3j}}{j},$$

де k_{ooIP} – коригуючий коефіцієнт, визначений у табл. 7;

j – номер приватного показника, $j = \overline{1,...,m}$.

Оцінка ступеня виконання вимог, що регламентують банківський інформаційний технологічний процес визначається виразом:

$$R_{OV_{БІТП}} = k_{OV_{БІТП}} \frac{\sum_{j=1}^{m} IU_{4j}}{j},$$

де $k_{OV_{БІТП}}$ – коригуючий коефіцієнт, визначений у табл. 7;

j – номер приватного показника, $j = \overline{1,...,m}$.

Оцінка ступеня виконання вимог, що регламентують банківський платіжний технологічний процес визначається виразом:

$$OV_{БІТП} = k_{БІТП} \frac{\sum_{j=1}^{m} IU_{5j}}{j},$$

де $k_{БІТП}$ – коригуючий коефіцієнт, визначений у табл. 7;

j – номер приватного показника, $j = \overline{1,...,m}$.

Оцінка ступеня захисту БІР з використанням криптографічних ЗЗІ визначається виразом:

$$OV_{ozIP} = k_{ozIP} \frac{\sum_{j=1}^{m} IU_{6j}}{j},$$

де k_{ozIP} – коригуючий коефіцієнт, визначений у табл. 7;

j – номер приватного показника, $j = \overline{1,...,m}$.

Правила визначення коригувальних коефіцієнтів наведені у табл. 7.

Таблиця 7

Правила визначення коригувальних коефіцієнтів

коригувальний коефіцієнт	Кількість часткових показників, оцінки яких дорівнюють нулю (Повністю не виконуються)		
$k_{R_{BBI_2}}$	0	1 – 15	більш 15
$k_{R_{BBI\,3}}$	0	1 –20	більш 20
k_{ooIP}	0	1 –25	більш 25
$k_{OV_{БІТП}}$	0	1 – 30	більш 30
$k_{БІТП}$	0	1 – 10	більш 10
k_{ozIP}	0	1 – 15	більш 15
Значення коригуючого коефіцієнта	1	0,85	0,7

Узагальний показник рівня захищеності АБС дозволяє оцінити рівень відповідності ТЗСЗІ вимогам регуляторів та визначається:

$$OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i,$$

де k – кількість часткових показників безпеки, OPZ_i – частковий 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 ТЗСЗІ, $OPZ_2 = 0$, 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 – $OPZ_3 = 0$.

Етап 3. оцінювання ефективності інвестицій в забезпечення безпеки БІР.

На основі результатів узагальненого показника рівня захищеності OPZ^{ABS}, узагальненої синергетичної загрози $W_{synerg}^{IB,KB,BI}$, множини активів БІР $I_{A_i} = \left(Type, A^C, A^I, A^A, A^{Au}, C_Y\right)$ та запропонованої моделі оцінювання безпеки банківських інформаційних ресурсів, яка враховує комплексний показник ефективності інвестицій, що виділяються на забезпечення безпеки БІР в умовах дії гібридних загроз визначається комплексний показник ефективності інвестицій в безпеку БІР ОБС. Формально модель оцінювання безпеки банківських інформаційних ресурсів, яка ґрунтується на комплексному показнику ефективності інвестицій, що виділяються на забезпечення безпеки БІР описується виразом:

$$W_{ABS}^{effinv} = \begin{Bmatrix} I_{O^{ABS}}, \Delta^{ABS}, \left\{DF^{ABS}\right\}, rang^{ABS}, \left\{SZ^{ABS}\right\}, d^{ABS}, D^{ABS} \\ ROI^{ABS}, NPV^{ABS}, ROSI^{ABS}, r^{ABS}, CV^{ABS}, OU^{ABS} \end{Bmatrix},$$

де $I_{O^{ABS}}$ – значення інформаційного активу; Δ^{ABS} – ознака ефективності витрат; $\left\{DF^{ABS}\right\}$ – множина джерел загроз безпеці БІР; $rang^{ABS}$ – вартість процесу розробки ТЗЗІ; $\left\{SZ^{ABS}\right\}$ – множина ТЗЗІ; d^{ABS} – зведена вартість грошового потоку; ROI^{ABS} – коефіцієнт повернення інвестицій; NPV^{ABS} – чиста зведена вартість; $ROSI^{ABS}$ – рентабельність інвестицій в ТЗЗІ; r^{ABS} – коефіцієнт рентабельності в безпеці БІР; CV^{ABS} – степінь ризику на одиницю середнього прибутку; D^{ABS} – прибуток від використання ТЗЗІ; OU^{ABS} – оцінка прибутку від використання ТЗЗІ.

Стан моделі ефективності інвестицій в безпеку БІР ОБС (рис. 2):

Крок 1. Оцінювання рівня прибутковості інвестицій в побудову системи безпеки банківських інформаційних ресурсів:

$$ROI^{ABS} = NPV_{inv}^{ABS} - NPV_{zt}^{ABS},$$

де NPV_{inv}^{ABS} – прибуток від інвестицій в ТЗЗІ АБС;

NPV_{zt}^{ABS} – витрати в ТЗЗІ АБС;

ROI^{ABS} – прибутковість інвестицій в ТЗЗІ АБС.

Крок 2. Оцінювання рентабельності інвестицій в ТЗЗІ:

$$ROSI^{ABS} = NPV_{zbtszi}^{ABS} - NPV_{zvtszi}^{ABS},$$

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

NPV_{zvtszi}^{ABS} – витрати на усунення компрометації безпеки з застосуванням ТЗЗІ.

Крок 3. Оцінювання чистої зведеної вартості:

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

де N – кількість інтервалів інвестування,

ALE_i – очікувані витрати в i-му періоді,

r – ставка дисконтування,

C_{sz} – вартість засобів захисту.

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

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

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.

Крок 5. Оцінювання потенційних збитків U^{ABS} інформаційного активу:

$$U^{ABS} = p_{rj} u_j ,$$

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

u_j – цінність j-го активу.

Крок 6. Оцінювання потенційних збитків U^{ABS} інформаційного активу БІР:

$$OU^{ABS} = \sum_{j=1}^{n} U^{ABS} .$$

Отримані дані надходять на 1-й рівень моделі стратегічного управління банком для прийняття рішення щодо стану безпеки БІР $S^{ABS} = \left\{ S_1^{ABS}, S_2^{ABS}, ..., S_m^{ABS} \right\}$

.

Етап 4. Побудова інтегрованих механізмів забезпечення конфіденційності, цілісності, автентичності та достовірності БІР. На основі оцінок ефективності ТЗЗІ в АБС для забезпечення конфіденційності, цілісності БІР запропоновані нові механізми на основі гібридних крипто-кодових конструкцій на збиткових кодах, які дозволяють будувати несиметричні криптосистеми на основі модифікованих крипто-кодових систем (МНККС) Мак-Еліса з модифікованими еліптичними кодами (*МЕС*) (укороченими або подовженими), що забезпечують відповідний рівень безпеки та достовірність БІР (рис. 2). Використання збиткових кодів дозволяє зменшити енергетичні затрати при практичній реалізації МНККС Мак-Еліса шляхом зменшення потужності алфавіту *GF(q)* без зменшення загальної стійкості криптосистеми в цілому та використовувати багатоканальну криптографію.

Для модифікації еліптичного коду, що не зменшує мінімальну кодову відстань, використовується скорочення його довжини шляхом скорочення інформаційних символів. $I=(I_1, I_2, ..., I_k)$ – інформаційний вектор (n, k, d) блокового коду, підмножина h інформаційних символів, $h=x$, $x \leq 1/2k$ визначає нульові символи. При кодуванні інформаційного вектора символи множини h не беруть участі (вони нульові) і їх можна відкинути, а отримане кодове слово буде коротше на x кодових символів. Другий спосіб модифікації використовує збільшення довжини шляхом формування вектора ініціалізації (визначення

символів скорочення) і заміни нульових символів символами інформаційного вектора.

Для нанесення збитку використовуємо універсальний механізм нанесення збитку C_m:

$$CFT / CH_{FT} = E_1\left(M, KU^{EC}\right),$$

$$CHD / CH_D = E_2\left(M, KU^{EC}\right),$$

$$M = E_{1,2}^{-1}(CFT / CH_{FT}, CHD / CH_D, KU^{EC}),$$

$$CFT / CH_{FT} = CFT / CH_{FT}^i, ..., CFT / CH_{FT}^m,$$

де $KU^{EC} = \varphi(K_D^i, ..., K_D^m, KU_1^{EC}, ..., KU_m^{EC},$

$$CHD / CH_D = CHD / CH_D^i, ..., CHD / CH_D^m$$

.

Таким чином, шифртекст вихідного повідомлення (*M*) в результаті має два шифртексти (збиток (*CHD*) і збитковий текст (*FTC*)), кожен з яких окремо не може відновити вихідний текст.

Основні властивості *MEC* наведені у табл. 8, основні параметри МНККС в табл. 9. Протоколи обміну БІР з застосуванням гібридних крипто-кодових конструкцій зі збитковими кодами (ГККККЗК) на укорочених та подовжених *MEC* наведені на рис. 3, 4 відповідно.

Таблиця 8

Основні *(n, k, d)* властивості *MEC*

Властивість	укорочені *MEC*	подовжені *MEC*
(n, k, d) параметри коду, який побудований через відображення виду $\varphi: X \to P^{k-1}$	$n = 2\sqrt{q} + q + 1 - x$, $k \geq \alpha - x$, $d \geq n - \alpha$, $\alpha = 3 \times degF$, $k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq \alpha - x + x_1$, $d \geq n - \alpha$, $\alpha = 3 \times degF$
n, k, d) параметри коду, який побудований через відображення виду $\varphi: X \to P^{r-1}$	$n = 2\sqrt{q} + q + 1 - x$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \times degF$, $k + d \geq n$	$n = 2\sqrt{q} + q + 1 - x + x_1$, $k \geq n - \alpha$, $d \geq \alpha$, $\alpha = 3 \times degF$

Таблиця 9

Основні параметри МНККС Мак-Еліса на *MEC*

Властивість	укорочені *MEC*	подовжені *MEC*
розмірність секретного ключа	$l_{K+} = x \times \left\lceil \log_2\left(2\sqrt{q} + q + 1\right) \right\rceil$	$l_{K+} = (x - x_1) \times \log_2\left(2\sqrt{q} + q + 1\right)$
розмірність інформаційного вектору	$l_I = (\alpha - x) \times m$	$l_I = (\alpha - x + x_1) \times m$
розмірність криптограми	$l_S = \left(2\sqrt{q} + q + 1 - x\right) \times m$	$l_S = \left(2\sqrt{q} + q + 1 - x + x_1\right) \times m$
відносна швидкість передачі	$R = (\alpha - x) / \left(2\sqrt{q} + q + 1 - x\right)$	$R = (\alpha - x + x_1) / \left(2\sqrt{q} + q + 1 - x + x_1\right)$

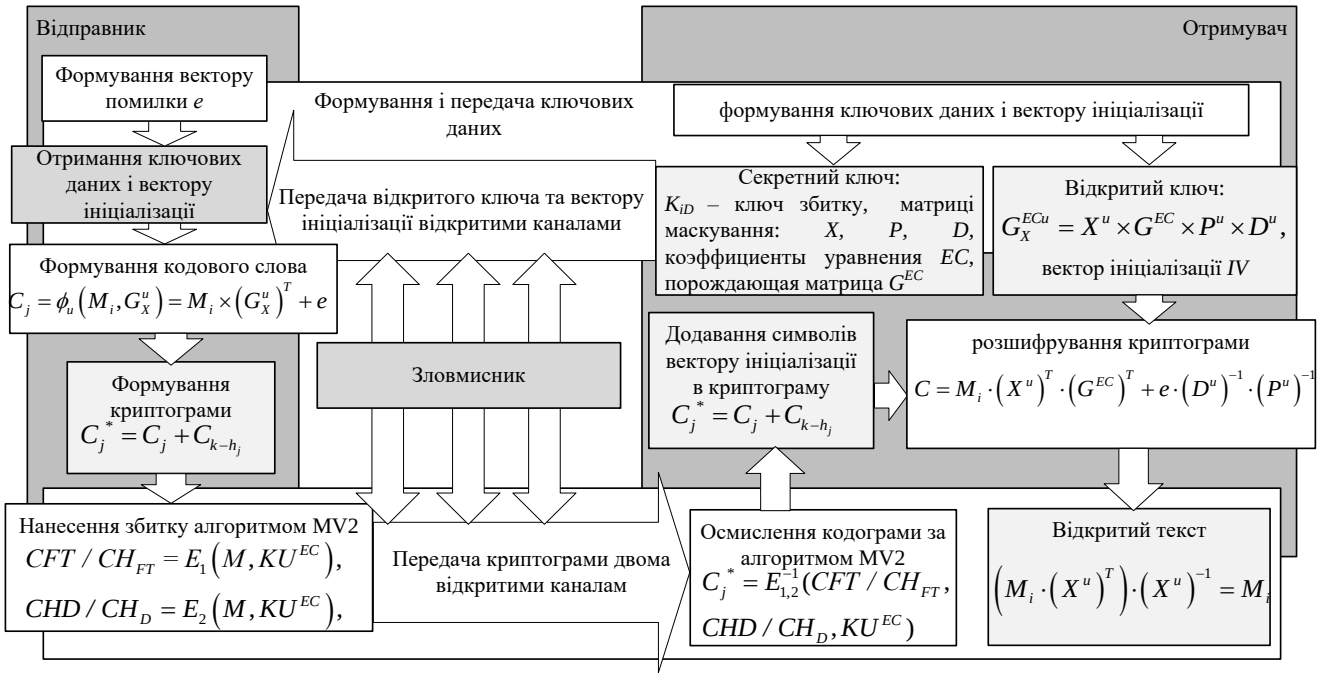

Рис. 3. Структурна схема протоколу забезпечення конфіденційності й цілісності БІР на основі ГКККЗК з укороченими *MEC*

Для забезпечення автентичності БІР пропонується використовувати модифіковану схему двофакторної автентифікації на основі *OTP*-паролів з використанням ГКККЗК на МНККС Мак-Еліса і Нідеррайтера.

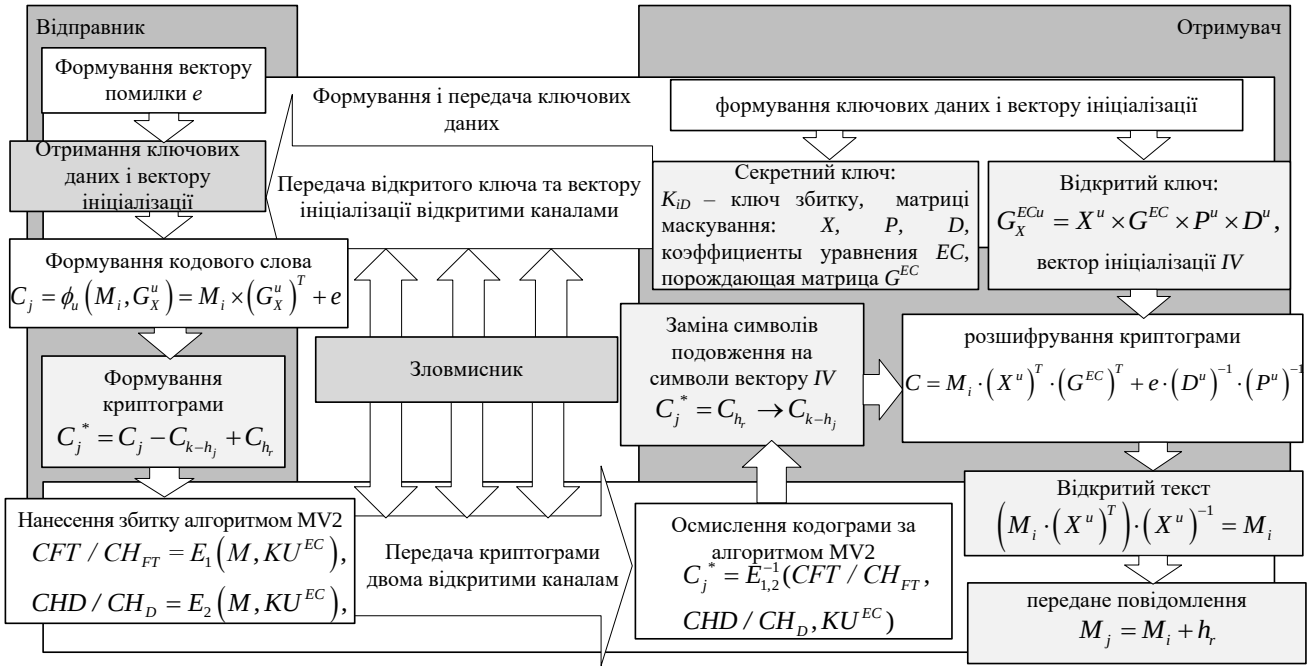

Рис. 4. Структурна схема протоколу забезпечення конфіденційності й цілісності БІР на основі ГККККЗК з подовженими *MEC*

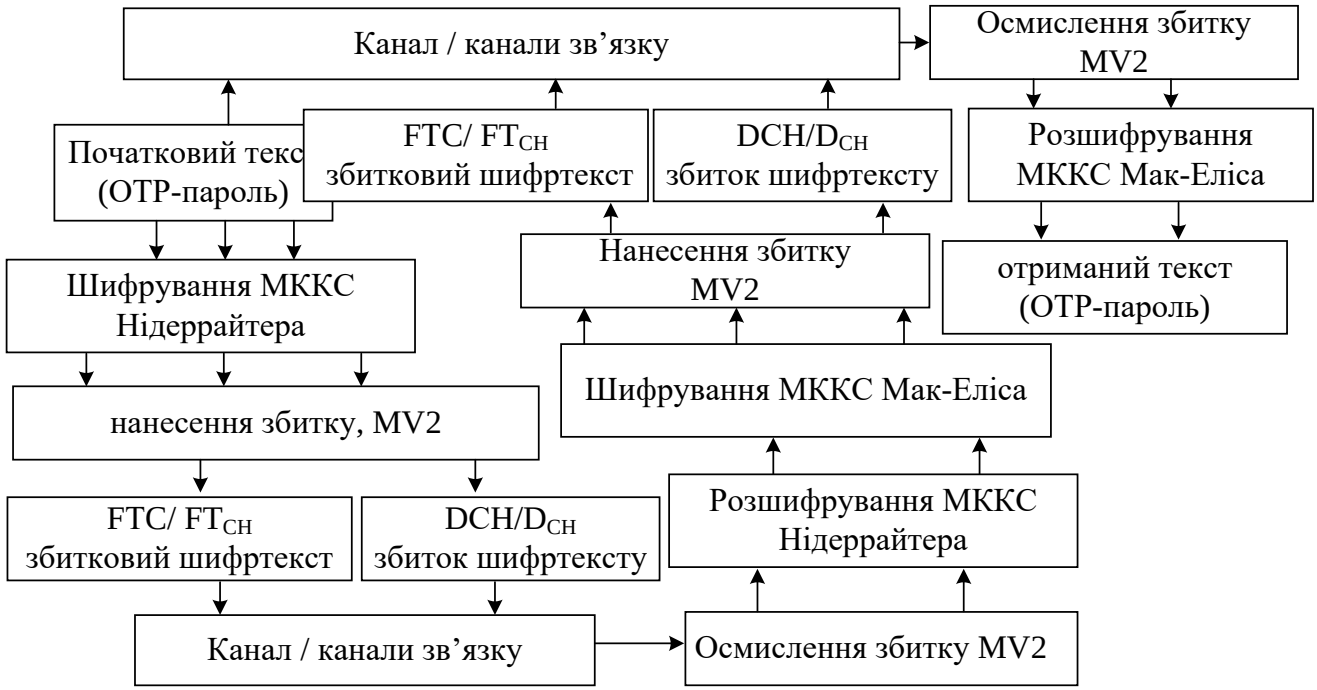

Рис. 5. Структурна схема протоколу вдосконаленого методу *OTP*-автентифікації на основі ГККККЗК

Структурна схема протоколу вдосконаленого методу *OTP*-автентифікації на основі ГККККЗК наведена на рис. 5 [1].

Використання гібридних крипто-кодових конструкцій на збиткових кодах дозволяє збільшувати кількість токенів автентифікатора, використовувати дві несиметричні крипто-кодові системи, два / чотири канали передачі збиткового тексту автентифікатора і збитку. Масштабованість програмного модуля шляхом зміни параметрів МНККС Нідеррайтера і / або Мак-Еліса залежно від висунутих вимог до комунікаційних каналах АБС, забезпечує його програмну реалізацію в мобільних гаджетах і сумісність з протоколами, що використовуються для передачі даних в Інтернет і мобільних мережах.

Етап 5. Визначення стану та формування стратегій безпеки БІР.

На заключному етапі реалізується трирівнева стратегія управління безпекою БІР (рис. 2).

Перший рівень описує загальну корпоративну стратегію банку та його функціональні стратегії. Корпоративна стратегія визначає перспективи розвитку та сприяє виконанню основної місії банку. На цьому рівні відповідно до синергетичного підходу розглядається загальна концепція забезпечення безпеки інформаційних технологій АБС і формуються цілі і завдання забезпечення КБ, а також визначається стан безпеки БІР $S^{ABS} = \left\{ S_1^{ABS}, S_2^{ABS}, ..., S_m^{ABS} \right\}$.

Функціональні стратегії одного рівня мають горизонтальні зв’язки і узгоджуються на рівні цілей з подальшою деталізацією на наступному рівні стратегічного набору.

На *другому рівні* формується корпоративна стратегія безпеки БІР – $\left\{ RR^{ABS} \right\} = \left\{ R_{BBI} \right\} \cup \left\{ OV_{BBI} \right\} \cup \left\{ IU_{BBI} \right\}$, визначаються цілі та завдання основних бізнес-процесів, пов’язаних із захистом персональних даних юридичних і фізичних клієнтів банку.

Корпоративна стратегія безпеки описує, яким чином слід керувати і координувати зусилля за різними аспектами безпеки. Вона розвивається у формі функціональних стратегій: фінансової, економічної, фізичної та ІБ.

На *третьому рівні* проводиться деталізація функціональних стратегій другого рівня стратегічного набору, формується корпоративна стратегія безпеки інформації. Серед основних напрямків щодо захисту доцільно виділити кадрову безпеку, фізичну безпеку, мережеву та БІ. На цьому рівні визначається

відповідність між застосованими ТЗСЗІ та загрозами ІБ, КБ, БІ на БІР – $OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i$.

Стратегія ІБ є важливою функцією керівництва банку в сфері безпеки і повинна формуватися і проводиться вищим керівництвом банку.

Концепція стратегічного управління безпекою ІТ АБС України на основі трирівневої моделі і синергетичної моделі загроз на відміну від відомих охоплює всі основні напрямки розвитку діяльності банку щодо безпеки БІР.

Запропонована концепція ґрунтується на синергетичному підході до вибору найбільш ефективних напрямків досягнення поставлених цілей безпеки БІР з урахуванням величини ризику на кожному рівні моделі стратегічного управління банком. Описаний підхід дозволяє комплексно проводити відбір альтернативних варіантів можливих стратегічних рішень з питань безпеки.

Запропонована методологія побудови системи безпеки БІР на відміну від відомих підходів реалізовує принципово нову концепцію протидії гібридним загрозам банківського сектору. Її сутність та зміст полягають в раціональній організації системи безпеки БІР в умовах одночасної дії на систему загроз інформаційній безпеці, кібербезпеці та безпеці інформації.

Методологія ґрунтується на вперше запропонованій трирівневій моделі стратегічного управління безпекою інформаційних технологій в АБС. Її основу складає вперше введена синергетична модель загроз безпеці БІР, що дозволила удосконалити відому модель зловмисника безпеки БІР.

На основі розробленої методології удосконалений класифікатор загроз безпеці в частині, що стосується одночасного урахування в ньому, крім загроз інформаційній безпеці, загроз кібербезпеці та загроз безпеці інформації БІР. Впровадження класифікатора дозволило зробити висновок про те, що для протидії гібридним загрозам БІР доцільно застосовувати нові інтегровані механізми забезпечення послуг на основі ГКККЗК, які також розробляються відповідно до запропонованої методології.

Запропоновані ГКККЗК ґрунтуються на криптографічних перетвореннях завадостійкого і збиткового кодування, що дозволило гарантувати послуги безпеки при заданих їх ймовірнісних показниках. Так, швидкість криптоперетворень забезпечено на рівні швидкості криптоперетворень БСШ, криптостійкість на рівні 10^{25}–10^{35} групових операцій, достовірність передачі БІР

відкритими каналами зв'язку не нижче $P_{пом}$ 10^{-9}–10^{-12}.

Висновок. Подана методологія є дієвим інструментом для розроблення практичних застосунків у вигляді програмних та програмно-апаратних засобів, що реалізують визначену системою безпеки БІР політику безпеки. Практичне зазначення методології підтверджено відповідними актами впровадження.

Таким чином, запропонована методологія дозволяє забезпечити підвищення рівня захищеності банківських інформаційних ресурсів, отримати максимальну кількість емерджентних властивостей в умовах протидії гібридним загрозам інформаційній безпеці, кібербезпеці та безпеці інформації а саме: оцінювання синергізму і гібридності загроз складових безпеки (інформаційній безпеці, кібербезпеці, безпеці інформації) на банківські інформаційні ресурси, мінімізація витрат на інвестування в забезпечення безпеки банківських інформаційних ресурсів, високої швидкості криптоперетворень та доказовий рівень стійкості в інтегрованих механізмах цілісності, конфіденційності, автентичності і достовірності банківських інформаційних ресурсів при використанні відкритих каналів зв'язку, оцінювання функціональної ефективності передачі банківських інформаційних ресурсів в автоматизованих банківських системах.

ЛІТЕРАТУРА

1. Р. Грищук, С. Євсеєв, "Методологія побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах", Науково-технічний журнал "Безпека інформації", том 23, № 3, с. 204 – 214, 2017.

2. О. К. Юдін, "*Інформаційна безпека. Нормативно-правове забезпечення*", К. : НАУ, 2011.

3. Р. В. Грищук, та Ю. Г. Даник; за заг. ред. проф. Ю. Г. Даника, *"Основи кібербезпеки"*, Житомир : ЖНАЕУ, 2016.

4. А. Корченко, С. Казмирчук, и Е. Иванченко, "Методология синтеза адаптивных систем оценивания рисков безопасности ресурсов информационных систем", Науково-практичний журнал *"Захист інформації"*, т. 19, № 3, с.198 – 204, 2017.

5. С. Евсеев, "Синергетическая модель оценки безопасности банковской информации", *Науково-технічний журнал "Інформаційна безпека"*, № 4 (24), с. 104 – 118, 2016.