© Hryshchuk R., Yevseiev S. Methodology of building a system for providing information security of bank information in automated banking systems // Ukrainian Scientific Journal of Information Security, 2017, vol. 23, issue 3, p.204-214.

УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ / INFORMATION SECURITY MANAGEMENT

DOI: 10.18372/2225-5036.23.12095

МЕТОДОЛОГІЯ ПОБУДОВИ СИСТЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКІВСЬКОЇ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ БАНКІВСЬКИХ СИСТЕМАХ

Руслан Грищук[1], Сергій Євсеєв[2]

[1]Житомирський військовий інститут радіоелектроніки ім. С. П. Корольова, Україна
[2]Харківський національний економічний університет ім. С. Кузнеця, Україна

ГРИЩУК Руслан Валентинович, д.т.н.

Дата та місце народження: 1981, Пішаниця, Житомирська область, Україна.
Освіта: Житомирський військовий інститут радіоелектроніки ім. С.П. Корольова, 2003.
Посада: начальник науково-дослідного відділу інформаційної та кібернетичної безпеки наукового центру з 2015 року.
Наукові інтереси: інформаційна та кібернетична безпека держави.
Публікації: більше 200 наукових публікацій, включаючи монографії, підручники, статті та патенти.
E-mail: Dr.Hry@i.ua

ЄВСЕЄВ Сергій Петрович, к.т.н.

Дата і місце народження: 1969, Харцизьк, Донецька обл., Україна.
Освіта: Харківський воєнний університет, 2002.
Посада: доцент кафедри інформаційних систем з 2007 року.
Наукові інтереси: безпека банківської інформації в автоматизованих банківських системах.
Публікації: більше 180 наукових публікацій, включаючи монографії, книги, статті та патенти.
E-mail: serhii.yevseiev@hneu.net

Анотація. *У статті подано методологію побудови системи забезпечення інформаційної безпеки банківської інформації у автоматизованих банківських системах. Методологія з єдиних системних позицій дозволяє здійснювати побудову системи забезпечення інформаційної безпеки банківської інформації. В основу методології покладено запропоновану концепцію побудови синергетичної моделі загроз інформаційній безпеці банківської інформації в автоматизованих банківських системах. Показано, що базис синергетичної моделі становить трирівнева модель стратегічного управління безпекою банківських інформаційних технологій, яка забезпечує одержання синергетичного ефекту в умовах одночасної дії загроз інформаційної безпеки, кібербезпеки та безпеки інформації. На відміну від відомих такий підхід забезпечує визначення якісно нових і невідомих до цього емерджентних властивостей системи безпеки банківської інформації з урахуванням коштів які використані на її створення. Застосування методології на практиці за рахунок розроблення та впровадження нових рішень забезпечення послуг безпеки дозволяє підвищувати рівень інформаційної безпеки банківської інформації в автоматизованих банківських системах. Запропоновані механізми послуг безпеки інформації будуються на гібридних криптосистемах на основі крипто-кодових конструкцій з збитковими кодами. Результати методології відображаються як у кількісній, так і якісній формі, що не суперечать основним положенням теорій захисту інформації та складних систем.*

Ключові слова: *автоматизована банківська система, банківська інформація, інформаційна безпека, кібербезпека, безпека інформації, синергетична модель загроз безпеки банківської інформації, класифікатор загроз інформаційній безпеці банківській інформації, система забезпечення інформаційної безпеки.*

Постановка проблеми

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 та систе-

моутворюючу роль при побудові системи забезпечення інформаційної безпеки банківської інформації, 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.

Революційні зміни останнього десятиліття, що відбулися в банківському секторі призвели до об'єднання інформаційних та комп'ютерних мереж в єдиний інформаційний та кібернетичний простір. Інтеграційні процеси обумовили створення автоматизованих банківських систем (АБС), які істотно розширили спектр електронних послуг державних і комерційних банків світу та України. Як наслідок, суттєво трансформувалися і загрози у такому національному інформаційному ресурсі держави, як банківська інформація (БІн). Загрози набули ознак гібридності. Від суто загроз інформаційної, кібернетичної безпеки та безпеки інформації БІн прояви ознак гібридності почали мати місце унаслідок одночасного впливу на об'єкт захисту – БІн в АБС, за рахунок виникнення явища синергізму.

Аналіз останніх досліджень і публікацій

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. Зокрема проведено аналіз методологій, які пов'язані з розробленням наукового базису для синтезу наступних систем безпеки [1–11]: синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси [1], оцінки рівня захищеності державних ресурсів від соціотехнічних атак [2]; оцінювання шкоди національній безпеці у сфері охорони державної таємниці [3], побудови та застосування безпечних бездротових сенсорних мереж з випадковими параметрами мережі [4], захисту державних інформаційних ресурсів [5], аналізу стану комплексу технічного захисту інформації [6], аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів [7], побудови систем виявлення аномалій породжених кібератаками [8], систем аналізу та оцінки ризиків втрат інформаційних ресурсів [9], комплексного захисту людини та соціальних груп від негативного інформаційно-психологічного впливу [10], адаптивних систем оцінювання ризиків безпеки ресурсів інформаційних систем [11] та ін. Однак проаналізовані методології не враховують синергізм та ознаки гібридності загроз на складові безпеки БІн в АБС, а саме [12-14]: інформаційної безпеки (ІБ), кібербезпеки (КБрБ), безпеки інформації (БІ). Тому усі вони потребують кардинального перегляду в частині, що стосується створення методологічного базису для побудови системи забезпечення інформаційної безпеки БІн в АБС як України в цілому, так і світу зокрема.

Виходячи з аналізу [15-19] можна стверджувати, що одним з пріоритетних напрямків підвищення рівня ІБ БІн в АБС зокрема, та подальшої стабілізації ІБ держави в цілому є принципово нове вирішення проблеми ІБ організацій банківського сектору держави (ОБС) шляхом створення сучасних методів і засобів захисту БІн від гібридного нападу на основі комплексування ознак загроз ІБ, КБрБ, БІ на БІн в АБС, 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 [16, 17, 19–23] та ін., але незважаючи на це проблема залишається актуальною не тільки для України, а й для світовій спільноти.

Виходячи з єдиних системних позицій [19, 21–23] та потреби реалізації комплексного підходу до побудови прогресивних систем забезпечення ІБ БІн в АБС в умовах гібридизації та комплексування загроз ІБ, КБрБ, БІ нині існує об'єктивне протиріччя між високими вимогами практики до забезпечення ІБ БІн в АБС та недосконалістю, а подекуди й відсутністю дієвих науково обґрунтованих методологічних засад її забезпечення.

У зв'язку з цим, метою статі є розроблення відповідної методології побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах.

Основні матеріали дослідження

Проведений аналіз керівних документів з організації побудови системи забезпечення ІБ БІн в АБС в [12–14, 24–28] показав, що до сьогодні розглянуті лише окремі складові методології оцінювання рівня безпеки інформаційних технологій, застосовуваних в ОБС. Усі вони ґрунтуються на моделях безпеки – забезпечення конфіденційності, цілісності та доступності (моделі КЦД). Застосування моделі КЦД не враховує невід'ємну складову банківських транзакцій – послугу автентичності – стан БІн, при якому інформація забезпечує підтвердження автентичності джерела (авторизованого користувача і / або процесу) інформації. Крім цього, відсутність синергетичного підходу до аналізу ризиків, єдиної методології оцінювання безпеки інформаційних технологій в стандартах банківського сектору не дозволяє своєчасно виробляти відповідні політики, нові підходи і заходи щодо забезпечення ІБ БІн. Відомо, що своєчасне виявлення і аналіз ризиків є невід'ємною частиною проблеми забезпечення ІБ БІн. Фактично ризик являє собою інтегральну оцінку того, наскільки ефективно існуючі засоби захисту інформації (ЗЗІ) здатні протистояти атакам на БІн в АБС. На практиці існує дві основні групи методів оцінювання ризиків безпеки [29–31]. Перша група дозволяє встановити рівень ризику шляхом оцінювання ступеня відповідності визначеному набору вимог щодо забезпечення ІБ. Друга базується на визначенні ймовірності реалізації атак, а також рівнів їх збитку. Але обидві групи методів також не враховують гібридності сучасних атак на ОБС, тому не дозволяють своєчасно реагувати на їх прояви.

Перспективним підходом забезпечення ІБ БІн в АБС є одночасне та раціональне поєднання органі-

заційних заходів та технічних засобів, спрямованих на забезпечення ІБ, КБрБ та БІ, що у кінцевому рахунку відображаються 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 [32].

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

Спираючись на відомий підхід до побудови методологій [1-11] в статті на основі досліджень [32–51] пропонується принципово нова методологія побудови системи забезпечення ІБ БІн в АБС. Вона містить п'ять етапів (рис. 1, 2): 1) визначення ймовірності впливу загроз ІБ, КБрБ, БІ на інформаційну безпеку БІн, 2) визначення узагальненого показника рівня ІБ БІн в АБС, 3) оцінювання ефективності інвестицій в ІБ БІн в АБС, 4) побудова інтегрованих механізмів забезпечення конфіденційності, цілісності, автентичності та вірогідності БІн в АБС, 5) визначення стану та формування стратегій ІБ БІн в АБС.

1. Визначення ймовірності впливу загроз ІБ, КБрБ, БІ на інформаційну безпеку БІн. На першому етапі, виходячи з того міркування, що загрози ІБ, КБрБ, БІ мають можливість впливати на різні послуги безпеки (конфіденційність, цілісність, доступність, автентичність) з різною інтенсивністю експертами з ІБ вирішується завдання щодо нормування вагових коефіцієнтів та формування класифікації загроз на основі запропонованого класифікатора [33].

Складовими класифікатора є:

- складова забезпечення безпеки БІн в АБС ОБС: ІБ (01), БІ (02), КБрБ (03);
- характер напрямків: нормативно-правове (01), організаційне (02), інженерно-технічне (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 додатків і сервісів (05). Множину загроз ІБ, КБрБ, БІ на БІн в АБС запропоновано використовувати з ресурсу [52].

Для визначення ймовірності P_i виникнення i-тої загрози використовуються дані з табл. 1.

Визначення реалізації кожної i-тої загрози з урахуванням частоти її виникнення здійснюється згідно виразу:

$$w_i = w_i^C P_i + w_i^I P_i + w_i^A P_i + w_i^{Au}, \quad P_i = 1,$$

Визначення ймовірностей виникнення декількох загроз на визначену послугу безпеки здійснюється як:

$$W^C = \sum_{i=1}^{N} w_i^C P_{i,} \text{ – для конфіденційності;}$$

$$W^I = \sum_{i=1}^{N} w_i^I P_{i,} \text{ – для цілісності;}$$

$$W^A = \sum_{i=1}^{N} w_i^A P_{i,} \text{ – для доступності;}$$

$$W^{Au} = \sum_{i=1}^{N} w_i^I P_{i,} \text{ – для автентичності.}$$

Таблиця визначення ймовірності виникнення загроз, залежно від частоти їх прояву Таблиця 1

P_i	**Частота виникнення 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 сумарної загрози за складовими безпеки набуває вигляду:

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

$$W_{synerg}^{KBrB} = \sum_{i=1}^{N} \left(w_i^C \times w_i^I \times w_i^A \times w_i^{Au} \right) P_i,$$

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

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

$$W_{synerg}^{IB,KBrB,BI} = \sum W_{synerg}^{IB} + W_{synerg}^{KBrB} + W_{synerg}^{BI}.$$

Одержані за результатами аналізу комплексування загроз дані поступають на 3-й рівень моделі стратегічного управління банком для їх узагальнення при оцінюванні достатності технічних засобів захисту БІн.

2. Визначення узагальненого показника рівня ІБ БІн в АБС. На основі сформованої множини загроз ІБ, КБрБ, БІ на БІн в АБС та моделі ієрархії АБС – $G^{ABS} = \{\{O^{ABS}\}, \{L^{ABS}\}, \{I_A\}\}$ визначається залежність між інформаційними активами і загрозами ІБ, КБрБ, БІ за наступними діями: визначення зв'язку між інформаційними активами БІн $\{I_A\}$ та елементами інфраструктури АБС $A^{ABS} = \left\| a_{ij}^{ABS} \right\|$; визначення зв'язку між інформаційними активами $\{I_A\}$ й об'єктами середовища $O_l = \left\{ Y^{ABS}, TO \right\}$: $IO^R = \left\| IO_{il}^R \right\|$.

На основі запропонованої синергетичної моделі загроз $GR^{ABS} = \left\{ \{DF^{ABS}\}, \{T_{risk}\}, \{T_P\}, \{T_U\}, \{VH\} \right\}$, і узагальненої моделі порушника:

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

здійснюється комплексування множини загроз вигляду: $DF^{ABS} = \left\{ V^{NS} \right\} \cup \left\{ V^{AS} \right\}$, де $\left\{ V^{AS} \right\} = \left\{ V^{ASBI} \right\} \cap \left\{ V^{ASIB} \right\} \cap \left\{ V^{ASKBr} \right\}$. 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 БІн: $R_{повн} = \sum_{j=1}^{n} R_j$, 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 БІн – $p_{rj} = 1 - \prod_{i=1}^{m}(1 - pr_{ij})$, де pr_{ij} – ймовірність реалізації *i*-тої загрози *j*-му активу.

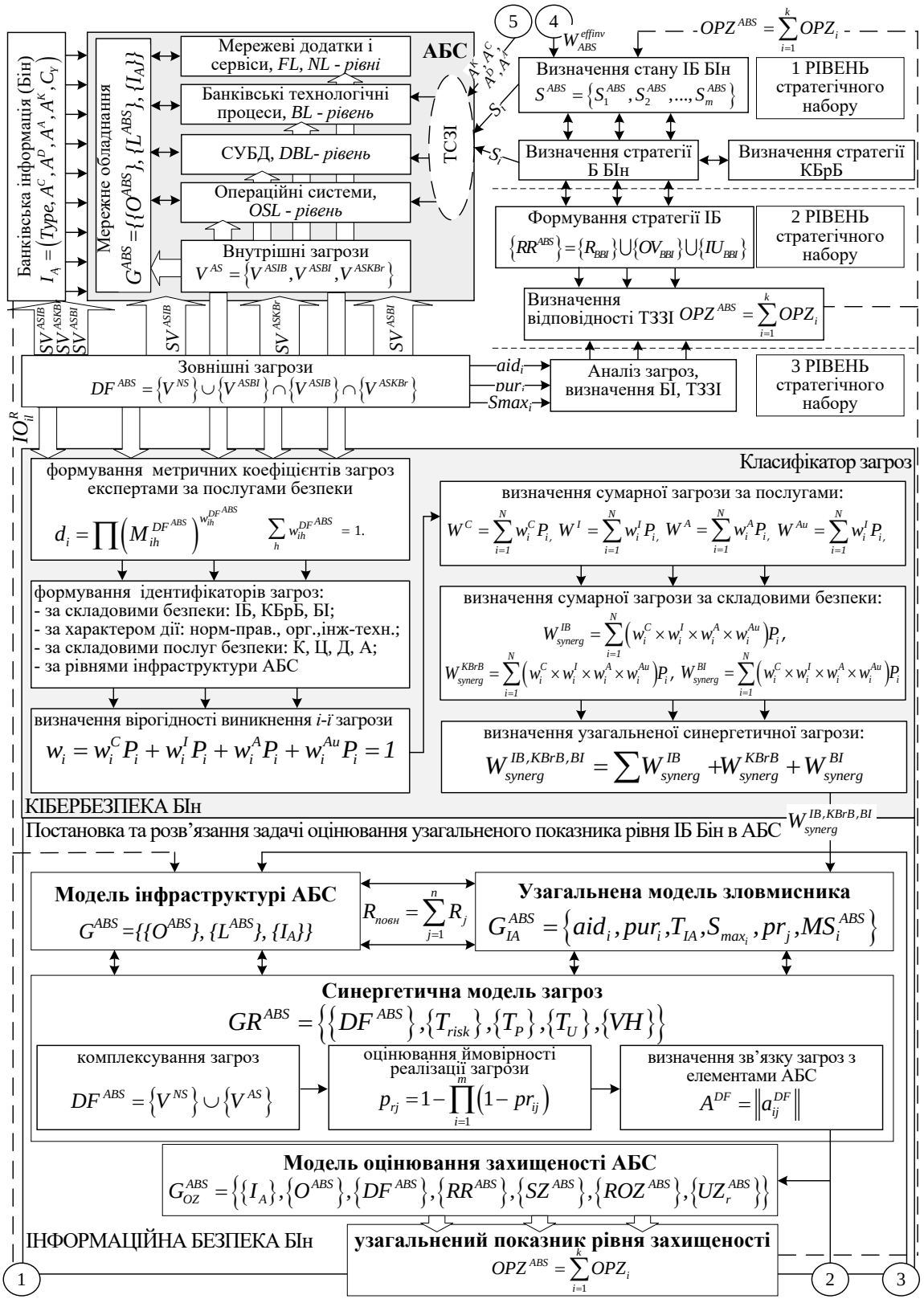

Рис. 1. Схема методології побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах

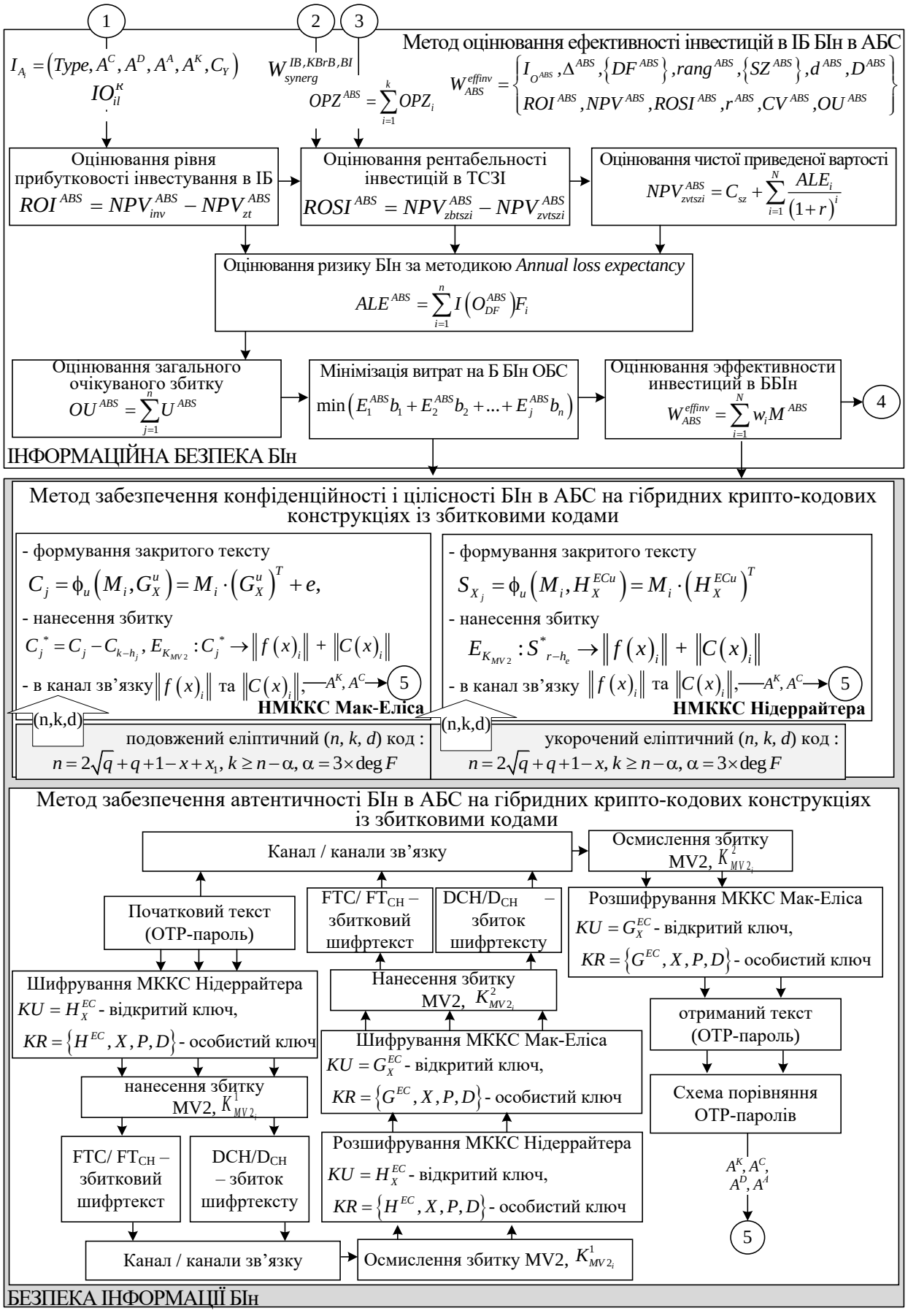

Рис. 2. Схема методології побудови системи забезпечення інформаційної безпеки банківської інформації в автоматизованих банківських системах

Визначення захищеності АБС від загроз ІБ, КБрБ, БІ на БІн в АБС пропонується одержати на основі моделі:

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

де $\{I_A\}$ – множина елементів інформаційних активів; $\{O^{ABS}\}$ – множина елементів ієрархії АБС; $\{DF^{ABS}\}$ – множина джерел загроз безпеки АБС; $\{RR^{ABS}\}$ – множина вимог регуляторів до забезпечення безпеки БІн; $\{SZ^{ABS}\}$ – 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) – $A^{DFSZ} = \|a_{ij}^{DFSZ}\|$. У моделі використані наступні 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*-тої загрози.

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

Визначення вимог регуляторів $\{RR^{ABS}\}$ включає в себе вимоги до забезпечення безпеки БІн – $\{R_{BBI}\}$, визначених у міжнародних і національних стандартах, множину оцінок ступеня виконання вимог безпеки $\{OV_{BBI}\}$ та множину підсумкового рівня відповідності безпеки БІн вимогам з множини: $\{R_{BBI}\}$ – $\{IU_{BBI}\} : \{RR^{ABS}\} = \{R_{BBI}\} \cup \{OV_{BBI}\} \cup \{IU_{BBI}\}$.

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 приватних показників безпеки, OPZ_i – приватний показник приймає значення з множини: OPZ_1 – відсутність неприпустимих ризиків, у разі якщо в ОБС при складанні моделі загроз / моделі порушника 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 БІн вимогам регуляторів визнаний рекомендованим – $OPZ_3 = 1$, в разі, якщо визнано нерекомендованим – $OPZ_3 = 0$.

3. Оцінювання ефективності інвестицій в ІБ БІн в АБС. На основі результатів узагальненого показника рівня захищеності OPZ^{ABS}, узагальненої синергетичної загрози $W_{synerg}^{IB,KBrB,BI}$, множини активів БІн $I_{A_i} = (Type, A^C, A^D, A^A, A^K, C_Y)$ та запропонованої моделі оцінки інвестицій в ІБ БІн в АБС визначається стан моделі ефективності інвестицій в ІБ БІн ОБС за наступними кроками (див. рис. 2).

Крок 1. Оцінювання рівня прибутковості інвестицій в ІБ – $ROI^{ABS} = NPV_{inv}^{ABS} - NPV_{zt}^{ABS}$, де NPV_{inv}^{ABS} – прибуток від інвестицій в СЗІ АБС; NPV_{zt}^{ABS} – затрати в СЗІ АБС; ROI^{ABS} – доходність інвестицій в СЗІ АБС.

Крок 2. Оцінювання рентабельності інвестицій в ТЗСЗІ – $ROSI^{ABS} = NPV_{zbtszi}^{ABS} - NPV_{zvtszi}^{ABS}$, де NPV_{zbtszi}^{ABS} – затрати на усунення компрометації безпеки без застосування технічних засобів захисту інформації (ТЗЗІ); NPV_{zvtszi}^{ABS} – затрати на усунення компрометації безпеки з застосуванням ТЗЗІ.

Крок 3. Оцінювання чистої приведеної вартості $NPV_{zvtszi}^{ABS} = C_{sz} + \sum_{i=1}^{N} \frac{ALE_i}{(1+r)^i}$, де N – кількість інтервалів інвестування, ALE_i – очікувані затрати в *i*-му періоді, r – ставка дисконтування, C_{sz} – вартість засобів захисту.

Крок 4. Оцінювання ризику БІн за методикою розрахунку *Annual loss expectancy* – *ALE*, тобто очікуваних втрат в кожен період оцінки – $ALE^{ABS} = \sum_{i=1}^{n} I(O_{DF}^{ABS}) F_i$, де $\{O_{DF}^{ABS}\}$ – множина загроз; $I(O_{DF}^{ABS})$ – 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 загального очікуваного збитку збитку: $OU^{ABS} = \sum_{j=1}^{n} U^{ABS}$. Отримані данні поступають на 1-й рівень моделі стратегічного управління банком для прийнятя рішення щодо стану ІБ БІн: $S^{ABS} = \{S_1^{ABS}, S_2^{ABS}, ..., S_m^{ABS}\}$.

4. Побудова інтегрованих механізмів забезпечення конфіденційності, цілісності, автентичності та вірогідності БІн в АБС. На основі оцінок ефективності ТЗЗІ в АБС для забезпечення конфіденційності, цілісності БІн запропоновані нові механізми на основі гібридних крипто-кодових конструкцій на збиткових кодах (ГККК3К), які дозволяють будувати несиметричні криптосистеми на основі модифікованих несиметричних крипто-кодових систем (МНККС) Мак-Еліса з модифікованими еліптичними кодами ((МЕС) – укороченими або подовженими), що забезпечують відповідний рівень безпеки та вірогідності БІн (див. 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 побудови МЕС використовують наступні (*n, k,d*) параметри еліптичного коду (ЕС-коду): для укорочених МЕС:

$$n = 2\sqrt{q} + q + 1 - x,\ k \geq n - \alpha,\ \alpha = 3 \times \deg F,$$

де α –кількість точок в перетині $\varphi(X)$ з гіперплощиною кривої *X*, *k* – кількість інформаційних символів в криптограмі, *n* – довжина криптограми, *x* – кількість символів скорочення криптограми; для подовжених МЕС: $n = 2\sqrt{q} + q + 1 - x + x_1,\ k \geq n - \alpha,\ \alpha = 3 \times \deg F$, де x_1 – кількість символів подовження криптограми.

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 шифртекста (збиток (*CHD*) і збитковий текст (*FTC*)), кожен з яких окремо не може відновити вихідний текст.

Визначимо несиметричну крипто-кодову систему Мак-Еліса з ЕС [23–25, 28, 29]: відкритий ключ – матриця $G_X^{EC} = X \cdot G^{EC} \cdot P \cdot D$; особистий (закритий) ключ – матриці *X, P, D*.

Криптограма (кодограма) – вектор довжини *n*: $c_X^* = i \cdot G_X^{EC} + e$, де вектор $c_X = i \cdot G_X^{EC}$ належить ЕС *(n, k, d)*-коду з породжувальною матрицею G_X^{EC}, *i* – *k*-розрядний інформаційний вектор, вектор *e* – секретний вектор похибки ваги $\leq t$ (сеансовий ключ криптосистеми).

Протоколи обміну БІн з застосуванням ГККККЗК на укорочених та подовжених МЕС кодах наведені на рис. 3, 4 відповідно.

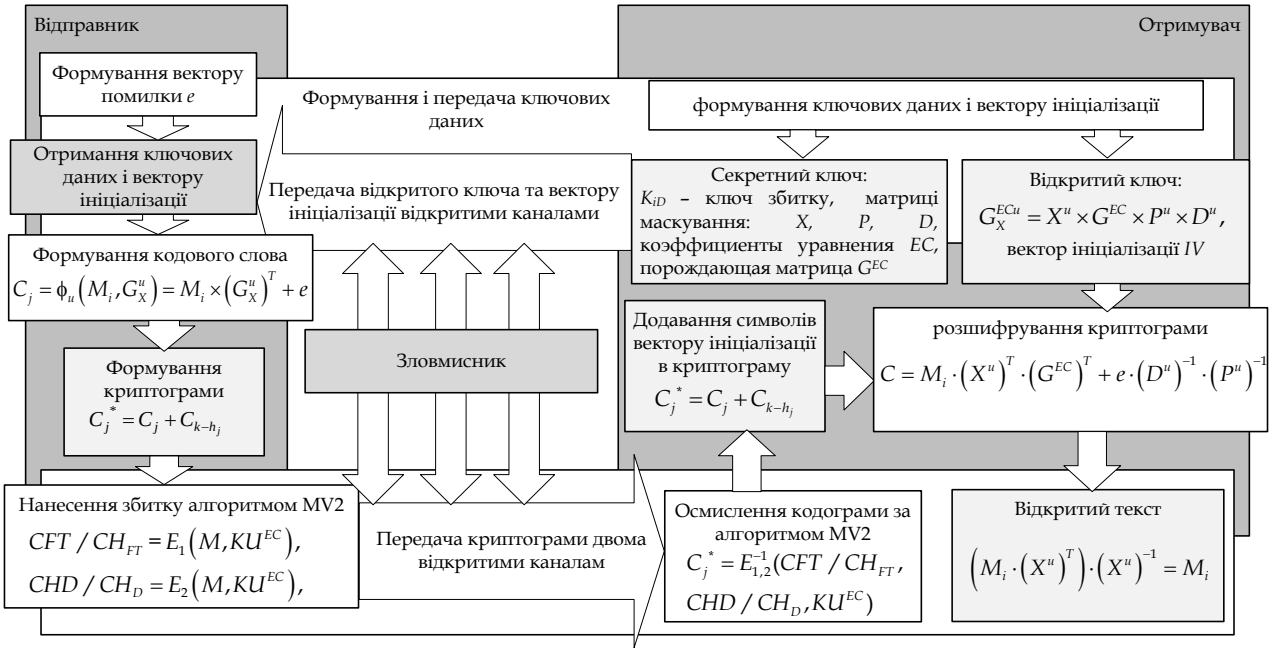

Рис. 3. Схема протоколу обміну БІн з застосуванням запропонованих ГККККЗК на МНККС Мак-Еліса на укорочених МЕС

Для забезпечення автентичності БІн в АБС пропонується використовувати модифіковану схему двофакторної автентифікації на основі ОТР-паролів з використанням ГККККЗК на МНККС Мак-Еліса і Нідеррайтера.

Визначимо несиметричну крипто-кодову систему Нідеррайтера з ЕС: відкритий ключ – матриця $H_X^{EC} = X \cdot H^{EC} \cdot P \cdot D$; особистий (закритий) ключ – матриці *X, P, D*.

Криптограма (кодограма) – $S_X = e \cdot \left(H_X^{EC}\right)^T$, де вектор *e* – вектор довжини *n* та ваги $\leq t$, який несе конфіденційну інформацію. Структурна схема протоколу вдосконаленого методу ОТР-автентифікації на основі ГККККЗК наведена на рис. 5 [51].

Використання гібридних крипто-кодових конструкцій на збиткових кодах дозволяє збільшувати кількість токенів автентифікатору, використовувати дві несиметричні крипто-кодові системи, два / чотири канали передачі збиткового тексту автентифікатору і збитку. Масштабованість програмного модуля шляхом зміни параметрів МНККС Нідеррайтера і / або Мак-Еліса, в залежності 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.

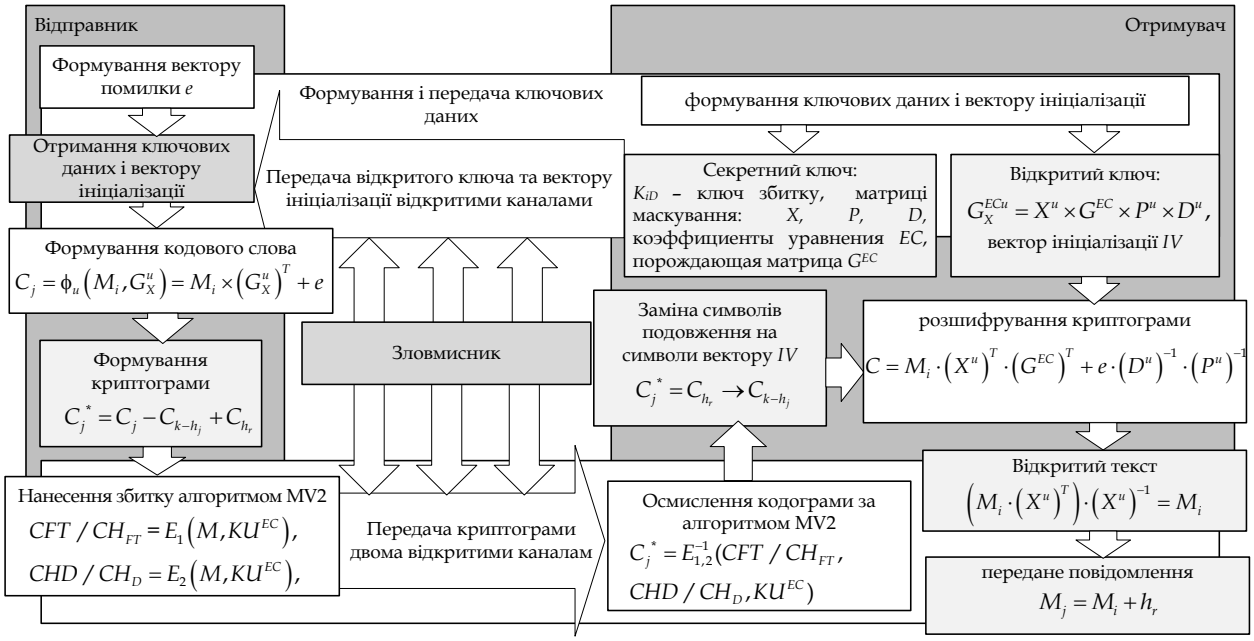

Рис. 4. Схема протоколу обміну БІн з застосуванням запропонованих ГКККЗК на МНККС Мак-Еліса на подовжених МЕС

Рис. 5. Структурна схема протоколу вдосконаленого методу ОТР-автентифікації на основі ГКККЗК

5. Визначення стану та формування стратегій ІБ БІн в АБС. На заключному етапі реалізується трирівнева стратегія управління безпекою БІн в АБС (див. 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 даному рівні відповідно до синергетичного підходу розглядається загальна концепція забезпечення безпеки інформаційних технологій АБС і формуються цілі і завдання забезпечення КБрБ. На цьому рівні визначається стан ІБ БІн в АБС $S^{ABS} = \left\{S_1^{ABS}, S_2^{ABS}, ..., S_m^{ABS}\right\}$. 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 ІБ БІн в АБС – $\left\{RR^{ABS}\right\} = \left\{R_{BBI}\right\} \cup \left\{OV_{BBI}\right\} \cup \left\{IU_{BBI}\right\}$, 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 функціональними стратегіями: 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, КБрБ, БІ на БІн в АБС – $OPZ^{ABS} = \sum_{i=1}^{k} OPZ_i$.

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 забезпечення ІБ. Запропонована концепція ґрунтується на синергетичному підході до вибору найбільш ефективних напрямків досягнення поставлених цілей ІБ БІн в АБС 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.

Висновки

Запропонована методологія побудови системи забезпечення ІБ БІн в АБС на відміну від відомих підходів реалізовує принципово нову концепцію протидії гібридним загрозам банківському сектору. Її сутність та зміст полягають в раціональній організації системи забезпечення ІБ БІн в АБС в умовах одночасної дії на систему загроз інформаційній безпеці, кібербезпеці та безпеці інформації. Такий підхід дозволяє одержувати повноцінну та адекватну оцінку рівня ІБ БІн в АБС, що суттєво впливає на величину інвестицій в безпеку банківського сектору та відкриває шляхи до прийняття обґрунтованих управлінських рішень з питань забезпечення безпеки.

Методологія ґрунтується на вперше запропонованій трирівневої моделі стратегічного управління безпекою інформаційних технологій в АБС. Її основу складає вперше введена синергетична модель загроз інформаційній безпеці банківської інформації, що дозволила узагальнити відому модель порушника безпеки банківської інформації. На основі розробленої методології набув подальшого розвитку класифікатор загроз інформаційній безпеці в частині, що стосується одночасного урахування в ньому крім загроз інформаційній безпеці загроз кібербезпеці та загроз безпеці інформації банківської інформації в АБС. Впровадження класифікатора дозволило зробити висновок про те, що для протидії гібридним загрозам банківської інформації в АБС доцільно застосовувати нові інтегровані механізми забезпечення послуг на основі ГККККЗК, які також розробляються відповідно до запропонованої методології.

Запропоновані ГККККЗК ґрунтуються на криптографічних перетвореннях перешкодостійкого і збиткового кодування, що дозволило гарантувати послуги безпеки при заданих їх ймовірнісних показниках. Так швидкість криптоперетворень забезпечено на рівні БСШ, криптостійкість на рівні 10^{25}–10^{35} групових операцій, вірогідність передачі банківської інформації в АБС відкритими каналами зв'язку не нижче $P_{пом}$ 10^{-9}–10^{-12}.

Новизна розробленої методології підтверджена патентами на винаходи та корисні моделі. Подана методологія є дієвим інструментом для розроблення практичних застосунків у вигляді програмних та програмно-апаратних засобів, що реалізують визначену системою забезпечення ІБ БІн в АБС політику безпеки. Практичне зазначення методології підтверджено відповідними актами впровадження в провідні банківські установи України.

Література

[1] Р. Грищук., О. Корченко, «Методологія синтезу та аналізу диференціально-ігрових моделей та методів моделювання процесів кібернападу на державні інформаційні ресурси», *«Захист інформації»*, № 3, с.115-122, 2012.

[2] Г. Баранов, М. Захарова, Д. Горніцька, «Методологія синтезу систем оцінки рівня захищеності державних інформаційних ресурсів від соціотехнічних атак», *«Захист інформації»*, № 3, с.98-103, 2012.

[3]. О. Корченко, М. Луцький, М. Захарова, Ю. Дрейс, «Методологія синтезу та програмна реалізація системи оцінювання шкоди національній безпеці у сфері охорони державної таємниці», *Захист інформації,* Т. 15, №1, С. 14-20, 2013.

[4] S. Rajba, M. Karpinski, O. Korchenko, «Generalized models, construction methodology and the application of secure wireless sensor networks with random network parameters», *Інформаційна безпека*, № 2(20), с. 120-125, 2014.

[5] О. Юдін, С. Бучик, «Методологія захисту державних інформаційних ресурсів. порівняльний аналіз основних термінів та визначень», *«Захист інформації»*, т. 17, № 3, с.218-225, 2015.

[6] Б. Журиленко, «Методология построения и анализа состояния комплекса технической защиты информации с вероятностной надежностью и учетом временных попыток взлома», *«Захист інформації»,* т. 17, № 3, с.196-204, 2015.

[7] С. Бучик, «Методологія аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів», *Науково-практичний журнал «Захист інформації»*, т. 18, № 1, с.81-89, 2016.

[8] А. Корченко, В. Щербина, Н. Вишневская, «Методология построения систем выявления аномлий порожденных кибератаками», *Захист інформації,* Т. 18, №1, С. 30-38, 2016.

[9] Е. Иванченко, С. Казмирчук, А. Гололобов, «Методология синтеза систем анализа и оценки рисков потерь информационных ресурсов», *Захист інформації*, Т. 14, №2, С. 24-28, 2012.

[10]. А. Шиян, «Методологія комплексного захисту людини та соціальних груп від негативного інфор-

маційно-психологічного впливу», *Інформаційна безпека*, № 1(22), с. 94-98, 2016.

[11] А. Корченко, С. Казмирчук, Е. Иванченко, «Методология синтеза адаптивных систем оценивания рисков безопасности ресурсов информационных систем», *«Захист інформації»*, т. 19, № 3, с.198-204, 2017.

[12] Доктрина інформаційної безпеки України, затверджено Указом Президента України від 25 лютого 2017 року № 47/2017, Электроний ресурс, Режим доступу : http://zakon3.rada.gov.ua/laws/show/47/2017/paran2#n2.

[13] Указ Президента України від 15 березня 2016 року № 96 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України», Электроний ресурс, Режим доступу : http://zakon3.rada.gov.ua/laws/show/96/2016/paran11#n11.

[14] Указ Президента України від 12 лютого 2007 року № 105 «Про Стратегію національної безпеки України», Электроний ресурс, Режим доступу : http://zakon3.rada.gov.ua/laws/show/105/2007.

[15] Р. Грищук, Ю. Даник, Синергія інформаційних та кібернетичних дій, *Труди університету. НУОУ*, № 6 (127), с. 132–143. 2014.

[16] В. Бурячок, Р. Грищук, В. Хорошко, під заг. ред. проф. В. Хорошка, «Політика інформаційної безпеки», ПВП «Задруга»,. 222 с. 2014

[17] Ю. Даник, С. Вдовенко, В. Шестаков, О. Писарчук, Р. Грищук, М. Куликівський, В. Ходаківський, «Основи захисту інформації», *навч. пос.*, Житомир : ЖВІ ДУТ, 220 с., 2015.

[18] О. Юдін, «Інформаційна безпека. Нормативно-правове забезпечення», К. : НАУ, 640 с., 2011.

[19] Р. Грищук, Ю. Даник, за заг. ред. проф.Ю. Даника, «Основи кібербезпеки», Житомир : ЖНАЕУ, 636 с., 2016.

[20] І. Іванченко, В. Хорошко, Ю. Хохлачова, Д. Чирков, під заг. ред. проф. В. Хорошка В., «Забезпечення інформаційної безпеки держави», К: ПВП «Задруга», 170 с., 2013.

[21] А. Корченко, О. Архипов, Ю. Дрейс, «Оцінювання шкоди національній безпеці України у разі витоку державної таємниці», *монографія*, К: наук.-вид.центр НА СБУ України, 332 с., 2014.

[22] А. Корченко, Л. Скачек, В. Хорошко, під заг. ред. проф. В. Хорошка, «Банківська безпека», підручник, К: ПВП «Задруга», 185 с., 2014.

[23] В. Ярочкин, «Безопасность банковских систем», М.: Издательство: Ось-89, 416 с., 2012.

[24] А. Потий, Д. Пилипенко, «Концепция стратегического управления информационной безопасностью», *Радіоелектронні і комп'ютерні системи*, № 6 (47). С. 53 – 58. 2010.

[25] М. Барилюк, «Методичний підхід до формування організаційно-економічного забезпечення управління фінансовою безпекою комерційного банку», *Бізнесінформ*, № 6, с.191-200, 2017.

[26] С. Евсеев, «Анализ защиты в национальной системе масовых электронных платежей», *Інформаційна безпека*, № 3(15), № 4 (16), с. 15-28, 2014.

[27] С. Евсеев, О. Король, Г. Коц, «Анализ законодательной базы к системе управления информационной безопасностью НСМЭП», *Восточно-европейский журнал передовых технологий*, вып. 5/3(77), с. 48-59, 2015.

[28] С. Евсеев, «Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины», *«Захист інформації»*, том. 22, № 2, с. 297-309, 2016.

[29] A. Briones, P. Chamoso, A. Barriuso, «Review of the Main Security Problems with Multi-Agent Systems used in E-commerce Applications», *ADCAIJ*, Regular Issue, Vol. 5, N. 3, pp. 55-61, 2016.

[30] W. Simpson, «Securing Information Systems in an Uncertain World Enterprise Level Security», Systemics, *Cybernetics and Informatics,* Vol. 14, № 2, pp. 83-90, 2016.

[31] С. Евсеев, О. Король, А. Сочнева, «Анализ оценки рисков кибербезопасности банковской информации», *Сборник научных трудов НАУ «Защита информации»*, вып 23, с. 109-129, 2016.

[32] Р. Грищук, С. Евсеев, «The synergetic approach for providing bank information security: the problem formulation», *Безпека інформації*, № 22(1), с. 64-74, 2016.

[33] С. Евсеев, «Модель нарушителя прав доступа в автоматизированной банковской системе на основе синергетического подхода», *«Інформаційна безпека»*, № 2 (26), с. 110-120, 2017.

[34] Ю. Малий, «Методические подходы к анализу угроз безопасности информации и рисков в банковской сфере», *Вестник БУКЭП*, № 1, с. 135-140, 2013.

[35] З. Васильченко, «Деякі аспекти методологічної основи моделювання фінансової безпеки банку», *Економіка,* № 6(147), с.15-19, 2013.

[36] С. Евсеев, «Синергетическая модель оценки безопасности банковской информации», *«Інформаційна безпека»*, № 4 (24), с. 104-118, 2016.

[37] С. Евсеев, «Оценка эффективности инвестиций в безопасность организаций банковского сектора на основе синергетической модели угроз», *Системи обробки інформації*, № 2(148), с. 88-94, 2017.

[38] О. Маркова, «Совершенствование информационной безопасности электронных расчетов в коммерческих банках России», *Финансовая аналитика: проблемы и решения*, 31, с. 38–49, 2015.

[39] С. Евсеев, С. Остапов, Х. Рзаев, Николаенко В., «Оцінка обміну даними в глобальних обчислювальних мережах на основі комплексного показника якості обслуговування мережі», *Радіоелектроніка, інформатика, управління*, № 1(40), с. 115-128, 2017.

[40] С. Евсеев, О. Король, Х. Рзаев, З. Иманова, «Разработка модифицированной несимметричной крипто-кодовой системы Мак-Элиса на укороченных эллиптических кодах», *Восточно-европейский журнал передовых технологий*, том 4. 9(82), с. 18-26, 2016.

[41] С. Евсеев, Х. Рзаев, А. Цыганенко, «Анализ программной реализации прямого и обратного преобразования по методу недвоичного равновесного кодирования», *«Безпека інформації»*, том.22, № 2, с. 196 – 203, 2016.

[42] С. Евсеев, О. Король, Г. Коц, «Construction of hybrid security systems based on the crypto-code structures and flawed codes», *Восточно-европейский журнал передовых технологий*, 4/9(88), с. 4-21, 2017.

[43] С. Евсеев, «Использование ущербных кодов в крипто-кодовых системах», *Системи обробки інформації*, № 5 (151) , с. , 2017.

[44] С. Евсеев, А. Андрощук, В. Федорченко, «Побудова систем безпеки інформаційно-телекомунікаційних систем на основі комплексного криптографічного підходу», *Збірник наукових праць Нац. академії Держ. прикор. служби України ім. Богдана Хмельницького. Серія : військові та технічні науки / [гол. ред. Олексієнко Б. М.]*, № 2(72), с. 172-178, 2017.

[45] C. Scheau, A. Arsene, G. Dinca, «Phishing and e-commerce: an information security management problem», *Journal of Defence Resources Management*, vol.7, № 1 (12), pp. 129-140, 2016.

[46] A. Alhothaily, A. Alrawais, T. Song, B. Lin, X. Cheng, «QuickCash: Secure Transfer Payment Systems», *Sensors,* № 17, 1376, pp.1-20, 2017.

[47] О. Юсупова, «Безопасность транзакций при использовании интернет-банкинга», *Финансовая аналитика: проблемы и решения*, № 35, с. 26–40, 2016.

[48] С. Евсеев, О. Король, «Исследование методов двухфакторной аутентификации», *Системи обробки інформації,* № 2(118), с. 81– 87, 2014.

[49] С. Евсеев, В. Абдулаев, «Алгоритм мониторинга метода двухфакторной аутентификации на основе системы Passwindow», *Восточно-европейский журнал передовых технологий*, вып. 2/2(74), с. 9-15, 2015.

[50] С. Евсеев, Г. Коц, Е. Лекарев, «Developing of multi-factor authentication method based on Niederreiter-McEliece modified crypto-code system», *Восточно-европейский журнал передовых технологий*, 6/4(84), с. 11-23, 2016.

[51] С. Евсеев, О. Король, Г. Коц, Минухин С., Холодкова А., «The development of the method of multifactor authentication based on hybrid crypto-code constructions on defective codes», *Восточно-европейский журнал передовых технологий*, 5/9(89), с. 19-36, 2017.

[52] «Банк данных угроз безопасности информации», Электроний ресурс, Режим доступу: http://bdu.fstec.ru/vul.

УДК 336.71:004.056 (045)

Грищук Р. В., Евсеев С. П. Методология построения системы обеспечения информационной безопасности банковской информации в автоматизированных банковских системах

Аннотация. *В статье представлена методология построения системы обеспечения информационной безопасности банковской информации в автоматизированных банковских системах. Созданная методология с единых системных позиций позволяет осуществлять построение системы обеспечения информационной безопасности банковской информации. В основу методологии положена предложенная концепция построения синергетической модели угроз информационной безопасности банковской информации в автоматизированных банковских системах. Базис синергетической модели составляет трехуровневая модель стратегического управления безопасностью банковских информационных технологий, что обеспечивает получение синергетического эффекта в условиях одновременного действия угроз информационной безопасности, кибербезопасности и безопасности информации. Такой подход способствует определению качественно новых и неизвестных до этого эмерджентных свойств системы безопасности банковской информации с учетом средств использованных на ее построение. Применение методологии позволяет на основе комплексированого подхода оценки состояния системы обеспечения информационной безопасности банковской информации повысить ее уровень за счет разработки и внедрения новых решений обеспечения услуг безопасности. Предложенные механизмы услуг безопасности строятся на гибридных криптосистемах на основе крипто-кодовых конструкций с ущербными кодами. Результаты методологии отражаются, как в количественной, так и качественной форме, не противоречат основным положениям теории защиты информации и сложных систем.*

Ключевые слова: *информационная безопасность банковской информации, автоматизированная банковская система, синергетическая модель угроз безопасности банковской информации, классификатор угроз информационной безопасности банковской информации, кибербезопасность, безопасность банковской информации.*

Hryshchuk R., Yevseiev S. Methodology of building a system for providing information security of bank information in automated banking systems

Abstract. *The article presents a methodology for building an information security system for banking information in automated banking systems. The created methodology from unified system positions allows to implement the construction of a system for ensuring information security of banking information. The basis of the methodology is the proposed concept of building a synergistic model of threats to information security of banking information in automated banking systems. The basis of the synergetic model is the three-level model of the strategic management of security of banking information technologies, which ensures a synergistic effect in the conditions of simultaneous action of threats to information security, cybersecurity and information security. Such an approach contributes to the definition of qualitatively new and unknown to this emergent features of the security of banking information, taking into account the means used for its construction. The application of the methodology allows, based on a complex approach, to assess the state of the information security system of banking information to increase its level by developing and implementing new solutions for providing security services. The proposed security mechanisms are based on hybrid cryptosystems based on crypto-code designs with defective codes. The results of the methodology are reflected in both quantitative and qualitative form; do not contradict the basic provisions of the theory of information protection and complex systems.*

Key words: *information security of banking information, automated banking system, synergistic model of threats to the security of banking information, information security threat classifier of banking information, cybersecurity, security of banking information.*

Отримано 8 *жовтня 2017 року,* затверджено редколегією 29 *жовтня 2017 року*