КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (2), 2018
ISSN 2663 - 4023

УДК 004.056:336.71

Євсеєв Сергій Петрович
д.т.н., с.н.с., завідувач кафедри кібербезпеки та інформаційних технологій
Харківський національний економічний університет ім. С. Кузнеця, Харків, Україна
OrcID 0000-0003-1647-6444
Serhii.Yevseiev@hneu.net

Рзаєв Хазан Нураддін Огли
к.т.н., доцент, доцент кафедри комп'ютерних технологій і програмування
Азербайджанський державний університет нафти і промисловості, Баку, Азербайджан
OrcID 0000-0002-1934-4773
xazail49@mail.ru

Мамедова Таміла Абусаід
асистент кафедри комп'ютерних технологій і програмування
Азербайджанський державний університет нафти і промисловості, Баку, Азербайджан
OrcID 0000-0002-5176-1307
mammadova1965@gmail.com

Самедов Фируз Гюльмамедов огли
доцент кафедри комп'ютерних систем та мереж
Азербайджанський Технічний Університет, Баку, Азербайджан
OrcID 0000-0001-5668-0111
firuss@yahoo.com

Ромащенко Наталія Віталіївна
бакалавр
Національний технічний університет "Харківський політехнічний інститут"
OrcID 0000-0002-4500-4481
ronatavit@gmail.com

КЛАСИФІКАТОР КІБЕРЗАГРОЗ ІНФОРМАЦІЙНИХ РЕСУРСІВ АВТОМАТИЗОВАНИХ БАНКІВСЬКИХ СИСТЕМ

Анотація. Сучасний розвиток високих технологій та обчислювальної техніки значно посилив розвиток автоматизованих банківських систем (АБС) організацій банківського сектору (ОБС) та дозволив синтезувати інформаційні і комунікаційні технології щодо їх формування. Однак ера високих технологій поширила спектр загроз на банківські інформаційні ресурси (БІР), загрози набули ознак гібридності та синергізму. В цих умовах актуальним питанням при формуванні системи управління інформаційної безпекою (СУІБ) в організаціях банківського сектору є формування і аналіз сучасних загроз. З метою узагальнення підходу класифікації гібридних кіберзагроз на складові безпеки: інформаційну безпеку (ІБ), кібербезпеку (КБ), безпеку інформації (БІ) банківських інформаційних ресурсів в роботі пропонується удосконалений класифікатор загроз банківських інформаційних ресурсів з урахуванням рівнів моделі ISO\OSI в автоматизованих банківських системах, направленості загроз на послуги безпеки та їх критичності збитку. В статі проаналізовані сучасні міжнародні стандарти і нормативні документи Національного банку України з питань безпеки банківських інформаційних ресурсів. На основі проведеного аналізу пропонуються оцінки показників ступеня небезпеки зловмисників і ступеня реалізації захисних заходів в умовах дії сучасних гібридних кіберзагроз.

Ключові слова: банківські інформаційні ресурси; інформаційна безпека; гібридні кіберзагрози; автоматизовані банківські системи; класифікатор загроз

1. ВСТУП

У сучасних умовах масової доступності комп'ютерних систем і телекомунікацій, збільшення обігу електронного документообігу між банками і клієнтами, переходу на електронну комерцію проблеми безпеки БІР в силу природних і штучних чинників тільки загострюються. Як наслідок, збитки від порушення безпеки БІР стають все більш дорогим як для банків, так і для їх клієнтів [1; 2; 3]. Наприклад, найбільша кількість загроз безпеки ІТ АБС України, як і в інших державах, виходить з мережі Інтернет при передачі БІР відкритими каналами зв'язку [2; 4; 5; 6; 7; 8]. Недосконаліть стратегічного управління безпекою ІТ АБС України виливається для державного банківського сектору в ряд проблем, основними з яких є безсистемність в забезпеченні безпеки, неузгодженість механізмів забезпечення безпеки ІТ АБС, особливо в міжнародному двох- і багатосторонньому форматах і т.п. [6; 9; 10].

Аналіз основних міжнародних стандартів і стандартів України [5; 11; 12; 13; 14; 15; 16; 17; 18; 19; 20; 21; 22; 23; 24; 25; 26; 27] показав, що розглянуті окремі складові методології оцінювання безпеки інформаційних технологій, застосовуваних в банківському секторі, ґрунтуються на моделі безпеки – забезпечення цілісності, конфіденційності та доступності (моделі ЦКД), при цьому не враховується невід'ємна складова банківських транзакцій – послуга автентичності – стан БІР, при якому інформація забезпечує підтвердження автентичності джерела (авторизованого користувача і / або процесу) інформації. Відсутність синергетичного підходу до аналізу ризиків, єдиної методології оцінювання безпеки інформаційних технологій в стандартах банківського сектору не дозволяє своєчасно сформувати відповідні політики, нові підходи і заходи щодо забезпечення безпеки БІР, що обумовлено недосконалістю механізмів забезпечення її ІБ, КБ, БІ.

Постановка проблеми. Невід'ємною частиною побудови системи безпеки в АБС є формування системи управління ІБ на основі класифікації не тільки БІР, но і сучасних загроз. Невід'ємною частиною проблеми забезпечення безпеки БІР є проблема аналізу ризиків. Фактично ризик являє собою інтегральну оцінку того, наскільки ефективно існуючі засоби захисту здатні протистояти атакам на БІР [1; 2; 3; 5; 7; 8; 23; 28; 29; 30; 31]. Незважаючи на те, що нині розроблено множину механізмів і засобів захисту інформації, на сьогоднішній день одним з пріоритетних завдань залишається завдання оцінювання ефективності процесу забезпечення безпеки ІТ АБС на основі відповідних метрик. Наприклад, як показав аналіз [11; 12; 13; 14; 15; 16; 17; 18; 28], серед найпоширеніших метрик безпеки є їх такі таксономії: *Vaughn-Hennig-Siraj, NIST STS822, OCIPEP, OCTAVE, CISWG, Erkan Kahraman*. У результаті вивчення наведених метрик безпеки встановлено, що їх ефективне впровадження в банківський сектор України стримує: дефініційна невизначеність – в силу недосконалості національної законодавчої бази та її розбіжності з кращими світовими практиками в цій сфері; низька об'єктивність отриманих оцінок – зважаючи на відсутність міжнародного досвіду більшості банківського персоналу, який забезпечує безпеку БІР; методологічних проблем – з огляду на проблематичність отримання гармонізованих між собою кількісних і якісних оцінок тощо. [31; 32]. При цьому остання з наведених проблем носить системотвірний ключовий характер, а тому вимагає глибокого наукового та методичного опрацювання та подальшого дослідження.

Аналіз останніх досліджень і публікацій. Проведений аналіз показав, що основними документами, які внесли серйозний теоретичний і практичний внесок у вирішення завдань забезпечення інформаційної безпеки [28] є: Критерії оцінювання

захищеності комп'ютерних систем [11], що відомі як "Рожева книга"; Європейські критерії оцінювання безпеки ІТ [12]; Канадські критерії оцінювання безпеки надійних комп'ютерних систем [13]; Федеральні критерії США [14]; Міжнародний стандарт ISO/IEC 15408 – "Критерії оцінювання безпеки ІТ" [15; 16; 17]; Робочий проект стандарту СЕМ-97/017 – "Загальна методологія оцінювання безпеки ІТ" [24], ДСТУ ISO / IEC TR 13335 "Інформаційні технології. Настанови з управління безпекою інформаційних технологій", ч. 1 – 5 [33; 34; 35; 36; 37], Стандарт України ДСТУ СУІБ 2.0 / *ISO / IEC 27002*: 2010 "Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпеки" (*ISO / IEC 27002*: 2005, *MOD*) [38]. Аналіз цих документів підтверджує той факт, що для рішення завдань забезпечення ІБ, поряд з формальними методами моделювання процесів і оцінювання ефективності функціонування систем забезпечення безпеки, необхідно широко використовувати методи декомпозиції і структуризації компонентів систем і процесів, неформальні методи оцінювання ефективності функціонування та прийняття рішень. Це означає, що апарат системного аналізу необхідно використовувати на всіх етапах життєвого циклу систем захисту інформації [3; 31].

Особливе місце у розробці методології оцінювання безпеки інформаційних технологій в АБС посідає стандарт *ISO/IEC 15408* "Загальні критерії оцінювання захищеності ІТ", "Загальні критерії". Стандарт визначає загальні критерії, що є основою для оцінювання властивостей безпеки інформаційних продуктів і технологій [15; 16; 17]. Використовуючи стандарт можна вирішити конкретне прикладне завдання вибору відповідних вимог і показників безпеки ІТ [3; 28]. Крім цього, потенційні загрози безпеки з Єдиних критеріїв, а саме цілісності, доступності, конфіденційності в подальшому пропонується покласти як складові в нову синергетичну модель загроз безпеки. Стандарти Національного банку України [38; 39] базуються на міжнародних стандартах *ISO 27001* [40] і *ISO 27002* [41] з додаванням до них вимог захисту інформації [38,0], обумовлені конкретними потребами сфери банківської діяльності та правовими вимогами національного законодавства [19].

Мета статті. Метою статті є аналіз сучасних підходів формування безпеки банківських інформаційних ресурсів в умовах гібридних загроз, побудова з урахуванням аналізу удосконаленого класифікатора на основі синергетичного підходу та оцінки показників ступеня небезпеки зловмисників і ступеня реалізації захисних заходів.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Ключовим моментом керівних документів є те, що вони приписують принципи управління інформаційною безпекою банку, найбільш важливими з яких є оцінювання ризиків [13;19; 33; 34; 35; 36; 37; 39; 38;]. Практика показує, що сьогодні можна чітко виділити дві основні групи методів оцінювання ризиків безпеки [20; 21; 38; 40; 41]. Перша група методів дозволяє встановити рівень ризику шляхом оцінювання ступеня відповідності визначеному набору вимог до забезпечення інформаційної безпеки.

Джерелом таких вимог у банківському секторі України можуть виступати як міжнародні, так і національні керівні документи, систематизація яких у вигляді схеми наведена на рис. 1.

Друга група методів оцінювання ризиків безпеки БІР базується на визначенні ймовірності реалізації атак, а також рівня їх збитків. У такому разі значення ризику вираховується окремо для кожної загрози і в загальному випадку є добутком ймовірності реалізації загрози на величину потенційних збитків від цієї загрози.

Значення збитків визначається власником БІР, а ймовірність реалізації загрози вираховується групою експертів, які проводять процедуру аудиту.

Відмінною рисою методів першої і другої груп є застосування різноманітних 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.

Згідно з вимогами стандартів Національного банку України відповідно до запропонованої концепції стратегічного управління безпекою ІТ АБС України (рис.1) сферою застосування системи управління ІБ (СУІБ), яка повинна бути впроваджена, в цілому є банк.

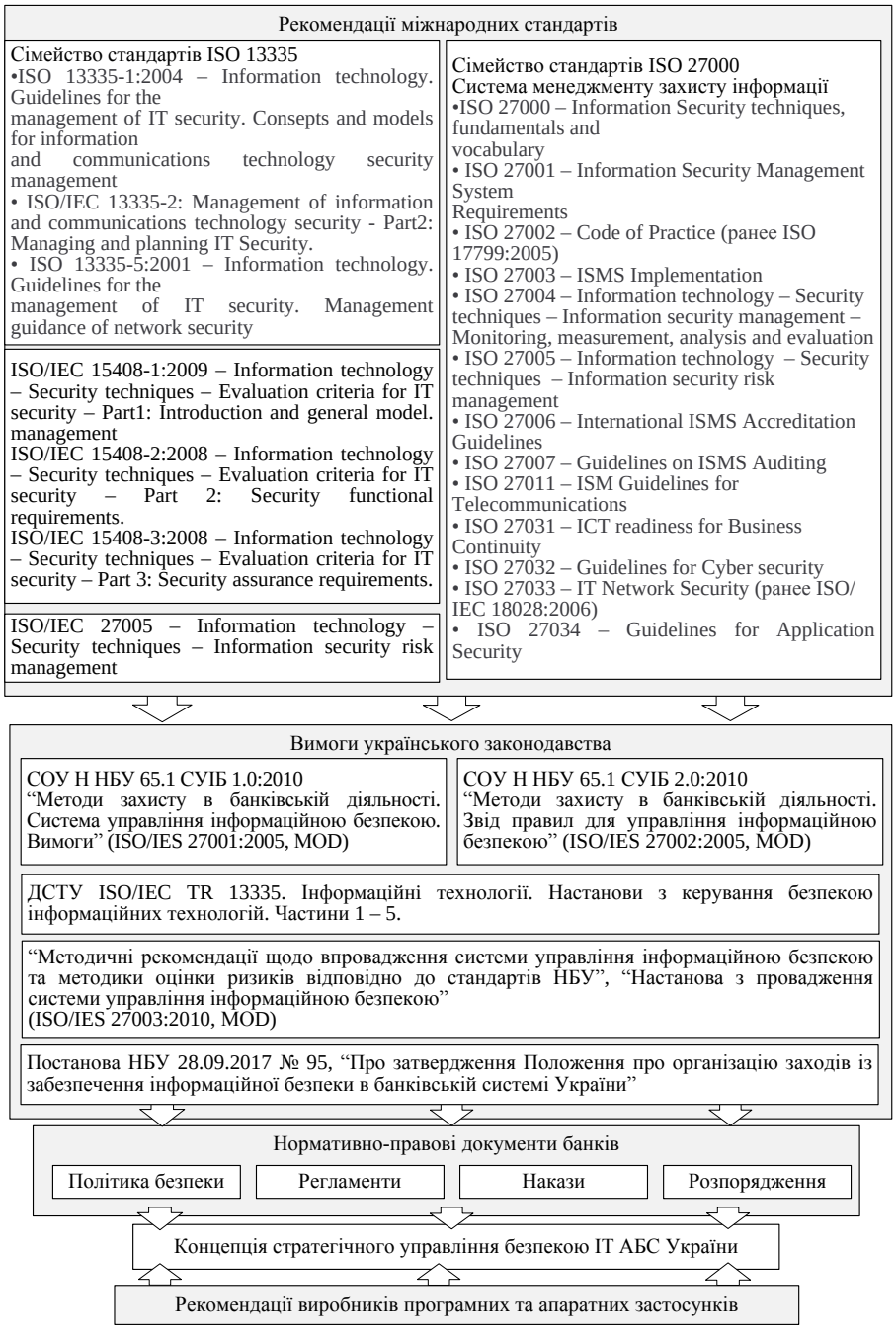

Рис.1. Систематизація джерел вимог до безпеки ІТ АБС України

Таким чином, весь комплекс питань, пов'язаних із забезпеченням безпеки БІР України, а саме – ІБ, КБ, БІ в АБС повинен вирішуватися в комплексі і нерозривно один від іншого, гармонійно доповнюючи і заповнюючи, в разі необхідності, один одного. Просте комплексування сил і засобів у кожному окремому випадку для забезпечення безпеки БІР є недоцільним як з практичної, так і наукової точок зору. Відсутність інших альтернативних підходів обумовлює нагальну потребу у вирішенні проблеми, що склалася – підвищення захищеності БІР на основі розробки нових підходів.

Враховуючи взаємозв'язок гібридності загроз ІБ, КБ, БІ на БІР, в подальшому пропонується провести синтезування БІР з типовими загрозами згідно синергетичної моделі загроз БІР [1] (рис. 2). Відмінною рисою запропонованого підходу (рис. 2) є закладання необхідної і достатньої умови розробки нового методологічного базису, спрямованого на досягнення синергетичного ефекту у сфері забезпечення складових безпеки (ІБ, КБ, БІ) БІР в умовах дії гібридних загроз не лише України, а й інших розвинених держав.

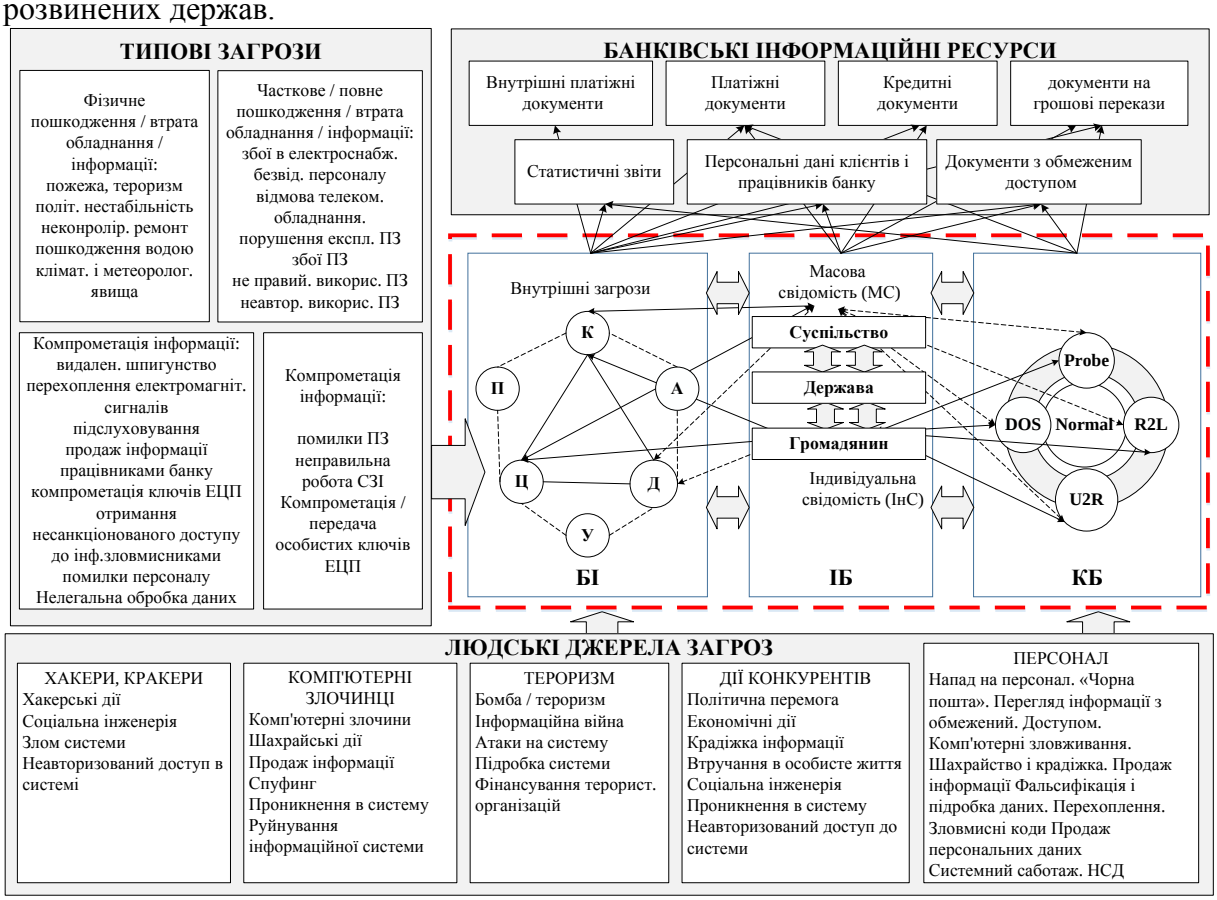

Рис. 2. Взаємозв'язок БІР з типовими джерелами загроз

Таким чином, в результаті уточнення вимог передових світових практик у питаннях методології оцінювання безпеки БІР встановлений взаємозв'язок між основними ризиками безпеки і БІР, які сьогодні і в найближчому майбутньому матимуть місце в АБС України. Спираючись на функціонал трирівневої моделі стратегічного набору типового підприємства [9] з метою розроблення концептуальних засад забезпечення безпеки БІР в роботі [42] запропонована концепція побудови

синергетичної моделі загроз безпеці БІР, яка базується на трирівневій стратегії управління безпекою БІР.

Реалізацію концепції на прикладі ОБС України подано на рис. 3. Розроблена на основі концепції модель за рахунок комплексування складових інформаційної безпеки, кібербезпеки та безпеки інформації відкриває новий напрямок у безпеці банківських інформаційних ресурсів на основі моделі стратегічного управління банком з урахуванням величини ризику на кожному рівні.

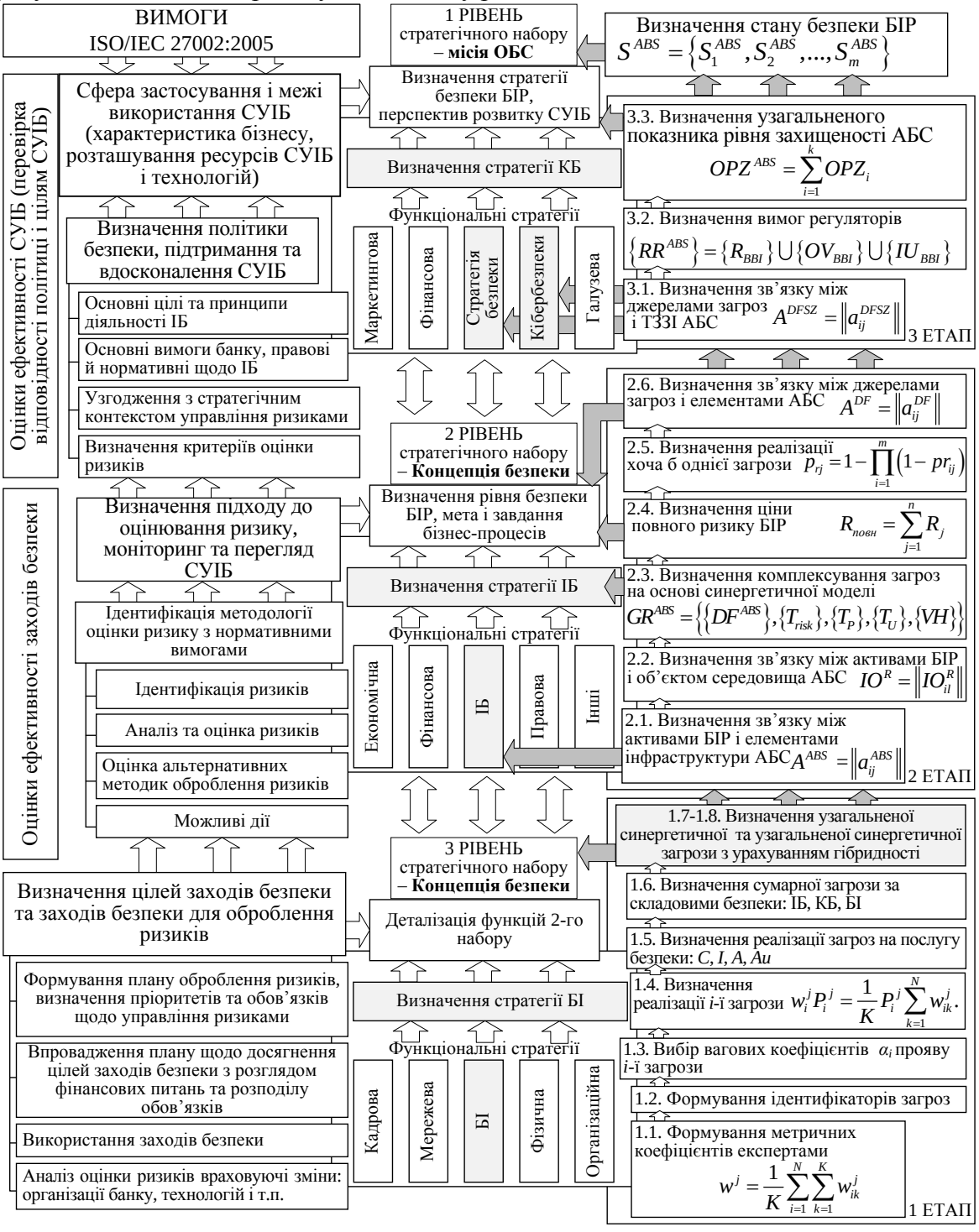

Рис. 3. Реалізація концепції на прикладі ОБС України

3. МЕТОДИКА ДОСЛІДЖЕННЯ

Для побудови метрик загроз на основі синергетичного підходу, запропонованого в роботі [31] скористаємося підходом побудови класифікатора загроз на основі інформаційно-аналітичної моделі методу подвійних трійок, запропонованого авторами в роботах [42; 43; 44; 45; 46]. На відміну від відомого при побудові класифікатора змістовна частина кожної з чотирьох платформ включає в себе відповідно ряд складових.

Перша платформа – класифікації загроз за складовими безпеки БІР ОБС: інформаційна безпека (ІБ) (01), безпека інформації (БІ) (02), кібербезпека (КБ) (03). Введемо такі дефініції.

Дефініція 1. *Безпека банківських інформаційних ресурсів (Б БІР)* – стан захищеності банківських інформаційних ресурсів, що характеризується здатністю користувачів, технічних засобів і інформаційних технологій забезпечити конфіденційність, цілісність автентичність і доступність банківських інформаційних ресурсів при їх обробці в АБС.

Дефініція 2. *Інформаційна безпека банківських інформаційних ресурсів (ІБ БІР)* – стан захищеності інформаційного середовища ОБС, що забезпечує її формування, використання і розвиток в інтересах громадян і ОБС.

Дефініція 3. *Кібербезпека банківських інформаційних ресурсів (КБ БІР)* – набір засобів, стратегій, принципів забезпечення безпеки, гарантій безпеки, підходів до управління ризиками, дій, професійної підготовки, страхування і технологій, які використовуються для захисту кіберсереди АБС, ресурсів і користувачів ОБС.

Друга платформа – класифікація загроз за характером напрямків: нормативно-правовий (01), організаційний (02), інженерно-технічний (03);

Третя платформа – класифікація загроз у відповідності з основними особливостями інформації: конфіденційність (01), цілісність (02), доступність (03), автентичність (04).

Четверта платформа – класифікація загроз за рівнями 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).

На рис. 4 наведено взаємозв'язок структурної схеми класифікатора загроз з АБС ОБС. Множину загроз інформаційній безпеці, кібербезпеці, безпеці інформації на банківські інформаційні ресурси запропоновано використовувати з електронного ресурсу (http://bdu.fstec.ru/vul).

Крок 1. Формування метричних коефіцієнтів загроз експертами за послугами безпеки. Нехай j – послуги безпеки БІР. Основними послугами безпеки БІР є C – конфіденційність; I – цілісність; A – доступність; Au – автентичність. Тоді класифікатор за чотирма послугами безпеки описується виразом вигляду $j = \{C, I, A, Au\}$.

Класифікатор містить N загроз. У складанні вагових коефіцієнтів прояву кожної загрози на послуги безпеки БІР брали участь K експертів.

Крім цього, для визначення можливого збитку кожну загрозу класифікують за критерієм критичності нанесення збитку організації банківського сектору.

Відповідно до стандарту *ISO/IEC 15408* експерти обирають якісний рівень збитку: критичний, високий, середній, низький. За допомогою методик оцінювання ризиків *CRAMM* або *FAIR* можливо оцінити якісний рівень в кількісних показниках.

Таким чином, на першому кроці формуються вагові коефіцієнті метрики сучасних гібридних кіберзагроз, що дозволяє їх використання в системах *SIEM* (*Security Information and Event Management*) з метою спрощення аудита та кореляції інформації з різних джерел.

Позначимо через i поточний номер загрози $(\{i\}_1^N)$, через k – поточний номер експерта, який виконував оцінку $(\{k\}_1^K)$.

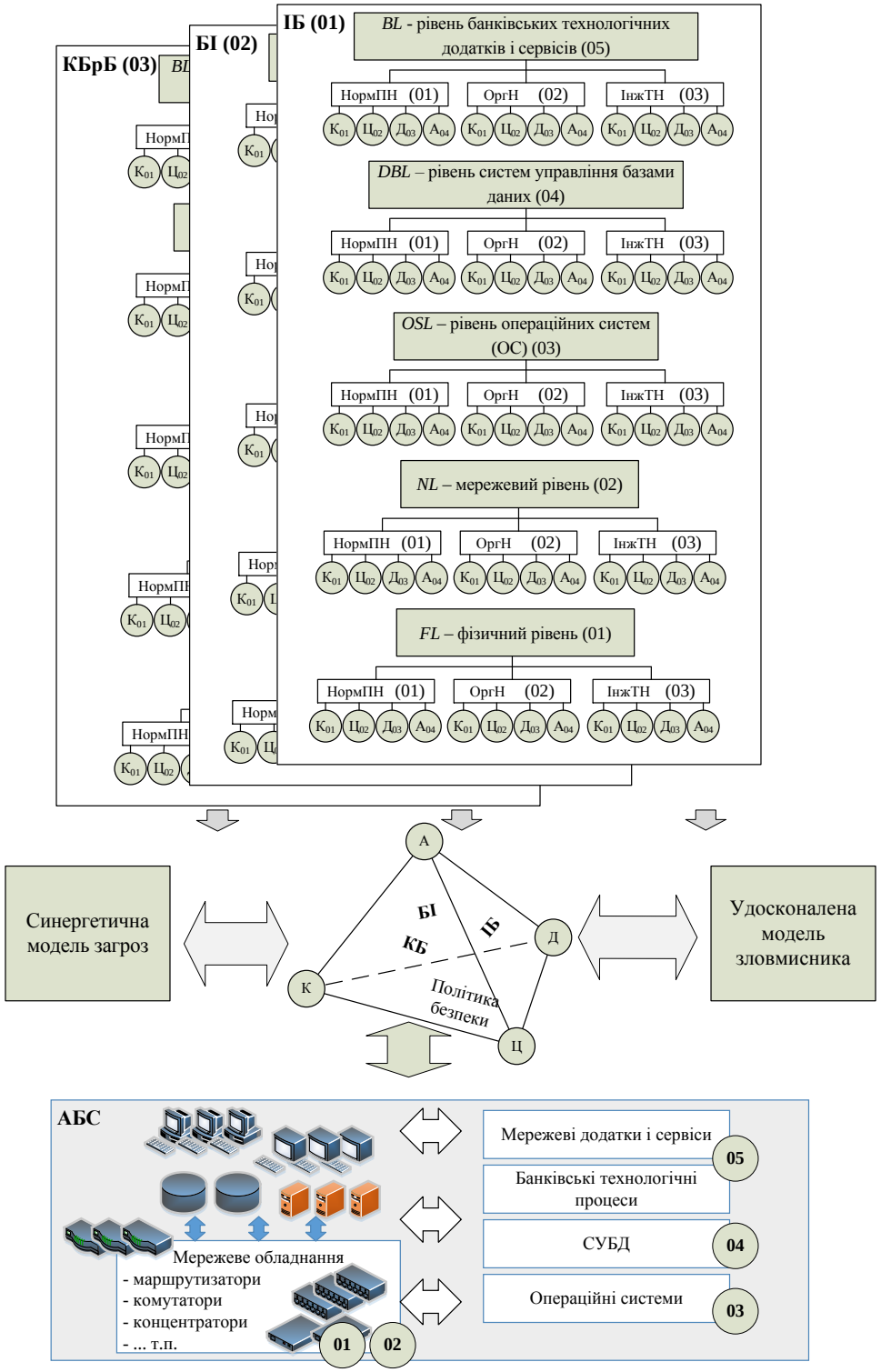

Рис. 4. Взаємозв'язок структурної схеми класифікатора загроз з АБС ОБС

Середнє значення оцінки експертів за всіма загрозами для певної послуги безпеки може бути записане:

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

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.

Крок 2. Формування ідентифікаторів загроз за складовими класифікатора. На цьому кроці експерти формують цифрове значення (код) ідентифікатора загрози за відповідними складовими класифікатора.

Крок 3. Вибір вагових коефіцієнтів α_i, що визначають умови прояву *i*-ї загрози (табл. 1) [47; 48].

Таблиця 1

Таблиця вибору 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 одного разу на 5 років
0,133	загроза проявляється не частіше одного разу на рік
0,2	загроза проявляється не частіше одного разу на місяць
0,267	загроза проявляється не частіше одного разу на тиждень
0,333	загроза проявляється щодня

Крок 4. Визначення реалізації кожної *i*-ї загрози з урахуванням імовірності прояву атаки (її виникнення) здійснюється за виразом:

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

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

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

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

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

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

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.

Крок 5. Визначення реалізації виникнення декількох загроз для обраної послуги

ISSN 2663 - 4023

розраховується з урахуванням виразу (2):

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

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

$$W_{synerg}^{A} = \sum_{i=1}^{M} w_i^A \alpha_i^A 2 \text{ – послуга доступність;}$$

$$W_{synerg}^{Au} = \sum_{i=1}^{M} w_i^{Au} \alpha_i^{Au} \text{ – послуга автентичність,} \quad (3)$$

де M – кількість декількох загроз, які вибрані експертом з ІБ банку з множини $\{i\}_i^M$, яка є підмножиною усієї множини загроз класифікатора, тобто $M \le N$. При визначенні реалізації виникнення декількох загроз для обраної послуги показник α_i береться найбільший серед усіх.

При формуванні метричних коефіцієнтів уважається, що отримані результати належать до незалежних загроз, у випадку їх залежності (збіг класифікатора загроз) необхідно скористатися виразом визначення повної ймовірності залежних подій:

$$P(AB) = P(A) + P(B) - P(AB).$$

Статистична обробка результатів оцінювання можливості впливу i-ї загрози на послугу безпеки в АБС експертами проводиться за методикою, описаної в роботі [49]. Підсумкова оцінка i-ї загрозі осереднюється за кількістю експертів відповідно до виразу:

$$x_i = \frac{\sum_{k=1}^{K} x_k \times k_k}{K}, \quad (4)$$

де x_k– оцінка k-го експерта впливу i-ї загрози;

k_k – рівень компетентності експерта;

K– кількість експертів.

Мірою погодженості думок експертів вважається дисперсія, що обчислюється за виразом:

$$\sigma_x^2 = \frac{1}{K} \sum_{k=1}^{K} k_k \left(x_k - x_i \right)^2. \quad (5)$$

Статистична значимість отриманих результатів з імовірністю 1 – α_i, становить: $\left[x_i - \Delta, x_i + \Delta \right]$, де величина x_i розподілена за нормальним законом із центром у x_i і дисперсією σ_x^2. Тоді Δ визначається за виразом:

$$\Delta = t\sqrt{\sigma_x^2 / N}, \quad (6)$$

де t – величина, що підкоряється розподілу Стьюдента для K – 1 ступенів свободи, K – кількість експертів.

Крок. 6. Визначення сумарної загрози за складовими безпеки з урахуванням виразу (3) розраховується:

ISSN 2663 - 4023

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

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

$$W_{synerg}^{BI} = \sum_{i=1}^{N} \left(w_i^C \cap w_i^I \cap w_i^A \cap w_i^{Au} \right) \alpha_i . \quad (7)$$

При визначенні реалізації виникнення декількох загроз для обраної послуги показник α_i береться найбільший серед усіх.

Крок. 7. Визначення узагальненої синергетичної загрози на БІР:

$$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \cup W_{synerg}^{KB} \cup W_{synerg}^{BI} . \quad (8)$$

Крок 1.8. Визначення узагальненої синергетичної загрози з урахуванням її гібридності розраховується:

$$W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^{C} \cap W_{synerg}^{\text{I}} \cap W_{synerg}^{A} \cap W_{synerg}^{Au} . \quad (9)$$

4. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

4.1. ВИЗНАЧЕННЯ ЙМОВІРНОСТІ ВПЛИВУ ЗАГРОЗ ІБ, КБ, БІ НА БЕЗПЕКУ БІР

Для оцінки ймовірності впливу сучасних кіберзагроз на складові безпеки в організаціях банківського сектору використаємо запропонований класифікатор загроз на основі синергетичного підходу.

Результати досліджень загроз з максимальною частотою їх прояву на банківських інформаційних ресурсів наведені у табл. 2

Таблиця 2

Результати оцінювання 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	
$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \cup W_{synerg}^{KB} \cup W_{synerg}^{BI} =$ =0,0002+0,0014+0,0007=**0,0223**		$W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^{\text{C}} \cap W_{synerg}^{\text{I}} \cap W_{synerg}^{A} \cap W_{synerg}^{Au} =$ =0,471×0,566×0,542×0,53=**0,0766**			

Результати наведені в табл. 2 свідчать, що гібридність сучасних кіберзагроз дозволяє практично в тричі збільшити ефективність синергетичного підходу і отримати несанкціонований доступ до конфіденційної інформації в АБС.

Тому необхідність оцінки показників небезпеки зловмисників та ступеня реалізації захисних заходів в організаціях банківського сектору дозволяє отримати додаткову інформацію про поточний стан безпеки БІР.

4.2. Оцінки показників ступеня небезпеки зловмисників і ступеня реалізації захисних заходів

Для оцінки показників ступеня небезпеки зловмисників і ступеня реалізації захисних заходів визначимо набори зважених метрик, які набувають значення в інтервалі [0; 1]. Кожна метрика характеризує ступінь відповідності певної ознаки зловмисника або захисний засіб заданому цільовому значенню.

Для оцінки ступеня небезпеки зловмисника будемо вважати, що він має такі характеристики (*Capabilities*) по відношенню до АБС: *C*={мотивація (*motivation, M*), оснащеність/наявне обладнання (*equipment, O*), технічна компетентність (*technical competence, K*), володіння інформацією про АБС і ТЗЗІ (*possession of information on the automated banking system and technical means of information protection, I*), доступні до реалізації загрози права доступу (*access rights, D*), час до моменту реагування ТЗЗІ на атаку (*response time to attack, T*)}. Таким чином, маємо таку множину характеристик зловмисника: *C* = {*M, O, K, I, D, T*}. Для опису множини характеристик використаємо індекс *h*: C_h, де $(\{h\}_1^C)$.

Нехай *j* – послуги безпеки БІР. Основними послугами безпеки БІР є *C* – конфіденційність; *I* – цілісність; *A* – доступність; *Au* – автентичність. Тоді класифікатор за чотирьома послугами безпеки описується виразом вигляду $j = \{C, I, A, Au\}$.

Позначимо через *i* поточний номер зловмисника $(\{i\}_1^L)$, через *k* – поточний номер експерта, який виконував оцінку $(\{k\}_1^K)$. Відповідно, ми будемо мати *L* зловмисників та *K* експертів. Позначимо також через w_{kih}^j – експертну оцінку *k*-го експерта для *h*-ї характеристики *i*-го зловмисника для *j*-ї послуги безпеки.

Тоді середнє значення оцінок усіх експертів за усією сукупністю характеристик усіх зловмисників для *j*-ї послуги безпеки буде мати вигляд:

$$w^j = \frac{1}{KLC}\sum_{k=1}^{K}\sum_{i=1}^{L}\sum_{h=1}^{C}\alpha_{kih}^j \times w_{kih}^j, \qquad (10)$$

де α_{kih}^j – ваговий коефіцієнт *h*-ї метрики *i*-го зловмисника для *j*-ї послуги. Вагові коефіцієнти підкоряються умові нормування, тобто $\sum_{k=1}^{K}\sum_{i=1}^{L}\sum_{h=1}^{C}=1$.

Аналогічним чином можна описати ступінь захищеності ТЗЗІ АБС. Для цього використаємо множину характеристик *B*= {*cryptographic resistance*, стійкість ТЗЗІ (C_r), обсяг ключових даних (*Key data amount*, S_c), складність виконання прямого і оберненого криптографічного перетворення (шифрування/розшифрування БІР) (*encryption/decryption of data*, O_E)}. Таким чином, маємо таку множину характеристик ТЗЗІ: $B = \{C_r, S_c, O_E\}$. Для опису множини характеристик використаємо індекс *g*: B_g, де $(\{g\}_1^B)$. Позначимо через w_{kg}^j – значення оцінки *g*-ї характеристики ТЗЗІ *k*-м експертом для *j*-ї послуги безпеки у випадку, коли ступінь захищеності системи та деструктивні дії зловмисників незалежні.

Тоді середнє значення оцінок усіх експертів ступені реалізації захисних заходів для *j*-ї послуги безпеки буде мати вигляд:

$$\psi^j = \frac{1}{KB}\sum_{k=1}^{K}\sum_{g=1}^{B}\left(\beta_{kg}^j \times w_{kg}^j\right), \qquad (11)$$

де β_{kg}^{j} – ваговий коефіцієнт *g*-ї метрики *j*-ї послуги безпеки для *k*-го експерта. Нормування вагових коефіцієнтів звичайне: $\sum_{k=1}^{K}\sum_{g=1}^{B}\beta_{kg}^{j}=1.$

Для кореляції між ступенем небезпеки зловмисника та характеристиками захисту системи, тобто між множинами *C* та *B*. використаємо матрицю *M* розміром [*C* × *B*], яку іноді називають матрицею парних порівнянь. Якщо *g*-а захисна характеристика B_g повністю блокує *h*-ту властивість зловмисника (або загрозу, яка реалізується цим зловмисником), то $M_{hg}=1$. в іншому випадку $M_{hg}=0$. Можливі також проміжні значення, коли загроза/характеристика зловмисника закривається не повністю. Таким чином, M_{hg} – матриця коефіцієнтів, які пов'язують між собою загрози/характеристики зловмисника із захисними заходами системи безпеки.

Тоді нові значення оцінок захисних заходів з використанням матриці *M* можна записати:

$$\left(w_{kg}^{j}\right)_{cor}=M_{hg}\times w_{kg}^{j}.$$

Тоді

$$\psi^{j}=\frac{1}{KB}\sum_{k=1}^{K}\sum_{g=1}^{B}\left(\beta_{kg}^{j}\times\left(w_{kg}^{j}\right)_{cor}\right).$$

Формування експертної групи (кількість експертів) обчислимо за формулою, яка запропонована в роботі [46; 50]:

$$K\geq 0,5\left(0,33/\beta+5\right), \qquad (12)$$

де β – помилка результату експертного аналізу або допустима ймовірність помилки.

Узгодженість отриманих оцінок визначається відповідно до [50;51]. Оцінюється індекс узгодженості оцінок експерта за виразом:

$$C_E=\frac{\lambda_{k_{\max}}-m}{m-1}, \qquad (13)$$

де $\lambda_{k_{\max}}$ – максимальна власна кількість матриці парних порівнянь *k*-го експерта;

m – розмірність матриці парних порівнянь.

Оцінки експерта вважаються узгодженими, якщо відношення узгодженості *CR* = C_E/CIS, де *CIS* – середнє значення індексу узгодженості, який визначається в діапазонах (табл. 3).

Таблиця 3

Значення *CIS* і *CR* від *m*

	3	4						0	1	2
IS	0,58	0,90	,12	,24	,32	,41	,45	,49	,51	,48
R	[0;0,05]	[0;0,08]	[0;0,1]							

Неприйнятні оцінки повинні бути скоректовані експертом, в іншому випадку їх не слід враховувати при розрахунку результуючого вектора пріоритетів. Узгодженість думок групи експертів визначається за правилом трьох сігм. Неузгоджені оцінки не враховуються при розрахунку результуючого вектора пріоритетів $\overline{B}=\left(\overline{b_1},\overline{b_2},...,\overline{b_m}\right)^T$,

$$\overline{b_i}=\sqrt[K]{\prod_{k=1}^{K}b_{ik}},$$

де $\overline{b_i}$ – результуючій пріоритет елементу x_i;

K – кількість експертів.

Думки експертів вважаються узгодженими, якщо все пріоритети b_{ik} лежать в інтервалі $\left(\overline{b_i}-3\sigma_{gi};\overline{b_i}+3\sigma_{gi}\right)$, де σ_{gi} – геометричне стандартне відхилення вагового коефіцієнта b_{ik}, яке визначається за виразом:

$$\sigma_{gi}=e^{\left(\sqrt{\frac{1}{K}\sum_{k=1}^{K}\ln\frac{b_{ik}}{b_i}}\right)^2}$$

Довірчий інтервал δ_i визначається за формулою:

$$\delta_i=t_{cm}\times\sigma_{gi}/\sqrt{K}, \qquad (14)$$

де t_{cm}=0,95 – критерій Стьюдента.

Запропоновані оцінки показників ступеня небезпеки зловмисників і ступеня реалізації захисних заходів

5. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Таким чином, на основі проведеного аналізу міжнародних стандартів та нормативних документів НБУ встановлено, що їх переважна більшість орієнтована на визначення загальних підходів до безпеки банківських інформаційних ресурсів, або використання засобів забезпечення на основі моделі *CIA*, що не повною мірою враховує сучасні вимоги й підходи до побудови системи безпеки банківських інформаційних ресурсів в умовах дії гібридних загроз з ознаками синергізму.

Запропоновано удосконалений класифікатор загроз безпеці банківських інформаційних ресурсів, який, на відміну від існуючих, ґрунтується на синергетичній моделі загроз, що дозволяє класифікувати загрози за складовими безпеки, видами послуг та рівнями ієрархії інфраструктури автоматизованих банківських систем, оцінювати синергію та гібридність загроз інформаційній безпеці, кібербезпеці, безпеці інформації, ймовірність їх впливу на безпеку банківських інформаційних ресурсів. Розроблено програмний засіб, що реалізує удосконалений класифікатор. Практична реалізація класифікатора дозволяє в он-лайн режимі формувати експертну оцінку рівня загроз банківських інформаційних ресурсів, аналізувати їх синергію та гібридність, оцінювати ймовірність впливу загроз інформаційній безпеці, кібербезпеці, безпеці

інформації на безпеку банківських інформаційних ресурсів без значних витрат інвестицій та людських ресурсів.

Використання результатів оцінки показників ступеня небезпеки зловмисників і ступеня реалізації захисних заходів дозволяє отримати додаткову інформацію щодо поточного стану безпеки банківських інформаційних ресурсів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1]. R. Hryshchuk, and S. Yevseiev, "The synergetic approach for providing bank information security: the problem formulation*", Науково-технічний журнал "Безпека інформації"*, № 22 (1), с. 64 – 74. 2016.

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

[3]. С. Евсеев, "Методология оценивания безопасности информационных технологий автоматизированных банковских систем Украины", Науково-технічний журнал "Захист інформації", том. 22, № 2, с. 297 – 309, 2016.

[4]. L. Sun, R. P. Srivastava, and T. J. Mock, "An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions", Journal of Management Information Systems, Vol. 22, p.3 – 28, 2006.

[5]. РС БР ИББС-2.2-2009. Методика оценки рисков нарушения информационной безопасности. [Електронний ресурс]. Доступно: http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf. Дата звернення: Груд. 7.2017.

[6]. І. С. Іванченко, В. О. Хорошко, Ю. Е.Хохлачова, та Д. В. Чирков під заг. ред. проф. В. О. Хорошка, "Забезпечення інформаційної безпеки держави", К: ПВП "Задруга", 2013.

[7]. А. О. Корченко, Л. М. Скачек, та В. О. Хорошко, під заг. ред. проф. В. О. Хорошка, "Банківська безпека" підручник, К: ПВП "Задруга", 2014.

[8]. В. И. Ярочкин, "Безопасность банковских систем", М.: Издательство: Ось-89, 416 с., 2012.

[9]. А. В. Потий, та Д. Ю. Пилипенко, "Концепция стратегического управления информационной безопасностью", Радіоелектронні і комп'ютерні системи, № 6 (47), с. 53 – 58, 2010.

[10]. О. К. Юдін "Інформаційна безпека. Нормативно-правове забезпечення", К. : НАУ, 2011.

[11]. Trusted Computer Systems Evaluation criteria, US DoD 5200.28-STD, 1985. [Online]. Available: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf. . Accessed on: Dec. 7.2017.

[12]. Information Technology Security Evaluation Criteria, v. 1.2. Office for Official publications of the European Communities, 1991. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile. Accessed on: Dec. 7.2017.

[13]. Canadian Trusted Computer Product Evaluation Criteria, v. 3.0. Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993. [Online]. Available: http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=&index=alt&srchtxt=CANADIAN%20TRUSTED%20COMPUTER%20PRODUCT%20EVALUATION%20CRITERIA. Accessed on: Dec. 7.2017.

[14]. Federal Criteria for Information Technology security. – NIST, NSA, US Government, 1993. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/ccpart1v2.3.pdf. Accessed on: Dec. 7.2017.

[15]. ISO/IEC 15408-1:1999 – Information technology – Security techniques – Evaluation criteria for IT security – Part1: Introduction and general model. [Online]. Available: https://www.iso.org/ru/standard/27632.html. Accessed on: Dec. 7.2017.

[16]. ISO/IEC 15408-2:2005– Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. [Online]. Available: https://www.iso.org/ru/standard/40613.html. Accessed on: Dec. 7.2017.

[17]. ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. [Online]. Available: https://www.iso.org/ru/standard/46413.html. Accessed on: Dec. 7.2017.

[18]. CEM-97/017. Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model.

[19]. Методичні рекомендації щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України: лист департаменту інформатизації Національного банку України банкам України від 03 березня 2011 р. № 24-112/365. – К.: Національний банк України, 2011.

[20]. ISO/IEC 27005 – Information technology – Security techniques – Information security risk management [Online]. Available: http://www.bank.gov.ua/doccatalog/document?id=72235https://exebit.files.wordpress.com/2013/11/iso-27005-2011-ru-v1.pdf. Accessed on: Des. 09, 2017.

[21]. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. ГОСТ Р ИСО/МЭК 15408-2-2008, [Електронний ресурс]. Доступно: http://primorsky.ru/authorities/executive-agencies/departments/information-security/Documents/doki-po-ib/. Дата звернення: Груд. 7.2017.

[22]. Руководящий документ. Безопасность информационных технологий. Общая методология оценки безопасности информационных технологий. Проект [Електронний ресурс]. Доступно: http://fstec.ru/component/attachments/download/293. Дата звернення: Груд. 7.2017.

[23]. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Методи захисту в банківській діяльності система управління інформаційною безпекою. Вимоги. (ISO/IEC 27001:2005, MOD). К: НБУ., 2010.

[24]. Постанова Правління Національного банку України від 18 червня 2003 року № 254 ‘‘ Про затвердження Положення про організацію операційної діяльності в банках України”, К: НБУ., 2003.

[25]. Доктрина інформаційної безпеки України, затверджено Указом Президента України від 25 лютого 2017 року № 47/2017. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/47/2017/paran2#n2. Дата звернення: Груд. 7.2017.

[26]. 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”. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/96/2016/paran11#n11. Дата звернення: Груд. 7.2017.

[27]. Указ Президента України від 12 лютого 2007 року № 105 “Про Стратегію національної безпеки України”. [Електронний ресурс]. Доступно: http://zakon3.rada.gov.ua/laws/show/105/2007. Дата звернення: Груд. 7.2017.

[28]. И. Д. Горбенко, А. В. Потий, и П. И. Терещенко, “Критерии и методология оценки безопасности информационных технологий”, [Електронний ресурс]. Доступно: http://www.bezpeka.com/ru/lib/spec/infsys/art108.html. Дата звернення: Груд. 7.2017.

[29]. С. Евсеев, “Модель нарушителя прав доступа в автоматизированной банковской системе на основе синергетического подхода”, Науково-технічний журнал “Інформаційна безпека”, № 2 (26), с. 110 – 120, 2017.

[30]. С. Евсеев, “Синергетическая модель оценки безопасности банковской информации”, Науково-технічний журнал “Інформаційна безпека”, № 4 (24), с. 104 – 118, 2016.

[31]. Р. Грищук, та 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.

[32]. А. В. Потий, та Д. Ю. Пилипенко, “Классификация показателей безопасности информации”, Системи обробки інформації, Вип. 3(84), с.53 –56. 2010.

[33]. ДСТУ ISO/IEC TR 13335-1:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 1. Концепції та моделі безпеки інформаційних технологій. [Электронный ресурс]. Доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11423.

[34]. ДСТУ ISO/IEC TR 13335-2:2003 Інформаційні технології. Частина 2. Настанови з керування безпекою інформаційних технологій. [Электронный ресурс]. Доступно: http://www.premier-hs.com.ua/ru/content/dstu-isoiec-tr-13335-22003-nastanovi-z-kieruvannia-biezpiekoiu-informatsiinikh-tiekhnologhii. Дата звернення: Груд. 7.2017.

[35]. ДСТУ ISO/IEC TR 13335-3:2003 Інформаційні технології. Настанови з керування безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій. [Электронный ресурс]. Доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11425. Дата звернення: Груд. 7.2017.

[36]. ДСТУ ISO/IEC TR 13335-4:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 4. Вибирання засобів захисту. [Электронный ресурс]. Доступно: http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005. Дата звернення: Груд. 7.2017.

[37]. ДСТУ ISO/IEC TR 13335-5:2005 Інформаційні технології. Настанови з управління безпекою інформаційних технологій. Частина 5. Настанова з управління мережною безпекою. [Электронный ресурс]. доступно: http://lindex.net.ua/ua/shop/bibl/500/doc/11427. Дата звернення: Груд. 7.2017.

[38]. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) [Электронный ресурс]. Доступно: http://s-byte.com/useful/27002.pdf. Дата звернення: Груд. 7.2017.

[39]. Стандарт України СОУ Н НБУ 65.1 СУІБ 1.0:2010. Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD). [Электронный ресурс]. Доступно: https://kyianyn.files.wordpress.com/2010/12/nbu-27001.pdf. Дата звернення: Груд. 7.2017.

[40]. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems –

Requirements. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534. Accessed on: Dec. 7.2017.

[41]. ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls. [[Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533. Accessed on: Dec. 7.2017.

[42]. О. К. Юдін, С. С. Бучик, Державні інформаційні ресурси. Методологія побудови класифікатора загроз, К.: НАУ, 2015.

[43]. О. К. Юдін, С. С. Бучик, А. В. Чунарьова, та О. І. Варченко, "Методологія побудови класифікатора загроз державним інформаційним ресурсам", Наукоємні технології, № 2 (22), с. 200 – 210, 2014.

[44]. О. К. Юдін, та С. С. Бучик, "Класифікація загроз державним інформаційним ресурсам нормативно-правового спрямування. Методологія побудови класифікатора", Захист інформації, Том 17 (2), с. 108 – 116, 2015.

[45]. С. С. Бучик, "Теоретичні основи аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів", Наукоємні технології, № 1 (29), с. 70 – 77. 2016.

[46]. С. С. Бучик, "Методологія аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів", Захист інформації, №1 (18 , с. 81 – 89, 2016.

[47]. Д. Домарєв, В. Домарєв та С. Прокопенко, "Методика оцінювання захищеності інформаційних систем за допомогою СУІБ "Матриця", Захист інформації, том 15, №1, с. 80 – 86, 2013.

[48]. С. В. Павленко, "Метод оцінки захищеності інформаційних систем", Системи озброєння і військова техніка, № 4(20), с. 149 – 154, 2009.

[49]. С. С. Бучик, "Методика експертного оцінювання функціональних профілів загроз державних інформаційних ресурсів", Открытые информационные и компьютерные интегрированные технологии, № 70, с. 271 – 280, 2015.

[50]. Р. А. Нурдинов, и Т. Н. Батова, "Подходы и методы обоснования целесообразности выбора средств защиты информации", Современные проблемы науки и образования. [Электронный ресурс]. Доступно: http://elibrary.ru/item.asp?id=21285749. Дата обращения: Дек. 7, 2017.

[51]. ISO/IEC 18045:2014 Information technology – Security techniques – Guidelines for cybersecurity [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46412. Accessed on: Des. 09, 2017.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (2), 2018
ISSN 2663 - 4023

Serhii. Yevseiev
Doctor of Technical Science, Senior Research
Department of Cyber Security and Information Technology
Simon Kuznets Kharkiv National University of Economics, Kharkiv, Ukraine
OrcID 0000-0003-1647-6444
serhii.yevseiev@hneu.net

Khazail Rzayev
PhD, Associate Professor,
Department of Computer Technology and Programming
Azerbaijan State University of Oil and Industry identify the organization, Baku, Azerbaijan
OrcID 0000-0002-1934-4773
xazail49@mail.ru

Tamilla Mammadova
Assistant Department of Computer Technology and Programming
Azerbaijan State University of Oil and Industry identify the organization, Baku, Azerbaijan
OrcID 0000-0002-5176-1307
mammadova1965@gmail.com

Firuz Samedov
Associate Professor, Department of Computer Technology and Programming
Azerbaijan Technical University, Baku, Azerbaijan
OrcID 0000-0001-5668-0111
firuss@yahoo.com

Nataliia Romashchenko
Bachelor
National Technical University "Kharkiv Polytechnic Institute", Kharkiv, Ukraine
OrcID 0000-0002-4500-4481
ronatavit@gmail.com

CLASSIFICATION OF CYBER CRUISE OF INFORMATIONAL RESOURCES OF AUTOMATED BANKING SYSTEMS

Abstract. The modern development of high technologies and computer technology greatly enhanced the development of automated banking systems of banking sector organizations and allowed the synthesis of information and communication technologies for their formation. However, the era of high technology has increased the range of threats to banking information resources; threats have gained signs of hybridity and synergy. In these conditions, the current issue in shaping the information security management system in banking sector organizations is the formation and analysis of modern threats. In order to generalize the approach of classification of hybrid cyber threats to the components of security: information security, cybersecurity, security of information banking information resources in the work proposed an advanced classification of threats to banking information resources. The classifier takes into account ISO / OSI model levels in automated banking systems, the targeting of threats to security services and their criticality of damage. The article analyzes contemporary international standards and normative documents of the National Bank of Ukraine on security issues of banking information resources. On the basis of this analysis, we propose estimates of the level of danger to intruders and the degree of implementation of protective measures under the conditions of modern hybrid cyber threats.

Keywords: banking information resources; information security; hybrid cyber threats; automated banking systems; threat classifier.

REFERENCES

[1]. R. Hryshchuk, ta S. Yevseiev, "The synergetic approach for providing bank information security: the problem formulation", Ukrainian scientific journal of information security, vol. 1, no. 22, pp. 64 – 74, 2016. (in English)

[2]. R. V. Grishhuk, ta Ju. G. Danik; za zag. red. prof. Ju. G. Danika, Osnovi kiberbezpeki, Zhitomir, Ukraina: ZhNAEU, 2016. (in Ukrainian)
[3]. S. Yevseiev, "Methodology for information technologies security evaluation for automated banking systems of Ukraine", Naukovo-tehnichnij zhurnal "Zahist informacii, vol. 22, issue 3, pp. 297-309, 2016. (in Russian)
[4]. L. Sun, R. P. Srivastava, and T. J. Mock, "An Information Systems Security Risk Assessment Model under Dempster-Shafer Theory of Belief Functions", Journal of Management Information Systems, vol. 22, pp. 3 – 28, 2006. (in English)
[5]. RS BR IBBS-2.2-2009. Metodika ocenki riskov narushenija informacionnoj bezopasnosti, 2009. [Online]. Available: http://www.cbr.ru/credit/gubzi_docs/st22_09.pdf. Accessed on: Des., 07.2017. (in Russian)
[6]. I. S. Ivanchenko, V. O. Horoshko, Ju. E.Hohlachova, ta D. V. Chyrkov pid zag. red. prof. V. O. Horoshka, Zabezpechennja informacijnoi' bezpeky derzhavy, Kyi'v, Ukraina: PVP "Zadruga", 2013. (in Ukrainian)
[7]. A. O. Korchenko, L. M. Skachek, ta V. O. Horoshko, pid zag. red. prof. V. O. Horoshka, Bankivs'ka bezpeka, Kyi'v, Ukraina: PVP "Zadruga", 2014. (in Ukrainian)
[8]. В. И. Ярочкин, "Безопасность банковских систем", М.: Издательство: Ось-89, 416 с., 2012. V. I. Jarochkin, Bezopasnost' bankovskih sistem, Moskva, Rossija: Os'-89, 2012. (in Russian)
[9]. A. V. Potij, ta D. Ju. Pilipenko, "The concept of information security strategic management", Radioelektronni i komp'juterni sistemi, vol. 47, no. 6, pp. 53 – 58, 2010. (in Russian)
[10]. O. K. Judin, Informacijna bezpeka. Normativno-pravove zabezpechennja, Kyi'v, Ukraina: NAU, 2011. (in Ukrainian)
[11]. Trusted Computer Systems Evaluation criteria, US DoD 5200.28-STD, 1985. [Online]. Available: https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf. . Accessed on: Dec. 7.2017. (in English)
[12]. Information Technology Security Evaluation Criteria, v. 1.2. Office for Official publications of the European Communities, 1991. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/ITSicherheitskriterien/itsec-en_pdf.pdf?__blob=publicationFile. Accessed on: Dec. 7.2017. (in English)
[13]. Canadian Trusted Computer Product Evaluation Criteria, v. 3.0. Canadian System Security Centre, Communications Security Establishment, Government of Canada, 1993. [Online]. Available: http://www.btb.termiumplus.gc.ca/tpv2alpha/alpha-eng.html?lang=eng&i=&index=alt&srchtxt=CANADIAN%20TRUSTED%20COMPUTER%20PRODUCT%20EVALUATION%20CRITERIA. Accessed on: Dec. 7.2017. (in English)
[14]. Federal Criteria for Information Technology security. – NIST, NSA, US Government, 1993. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/ccpart1v2.3.pdf. Accessed on: Dec. 7.2017. (in English)
[15]. ISO/IEC 15408-1:1999 – Information technology – Security techniques – Evaluation criteria for IT security – Part1: Introduction and general model. [Online]. Available: https://www.iso.org/ru/standard/27632.html. Accessed on: Dec. 7.2017. (in English)
[16]. ISO/IEC 15408-2:2005– Information technology – Security techniques – Evaluation criteria for IT security – Part 2: Security functional requirements. [Online]. Available: https://www.iso.org/ru/standard/40613.html. Accessed on: Dec. 7.2017. (in English)
[17].ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements. [Online]. Available: https://www.iso.org/ru/standard/46413.html. Accessed on: Dec. 7.2017. (in Eglish)
[18]. CEM-97/017. Common Evaluation Methodology for Information Technology Security – Part 1: Introduction and general model. (in English)
[19]. Metodychni rekomendacii' shhodo vprovadzhennja systemy upravlinnja informacijnoju bezpekoju ta metodyky ocinky ryzykiv vidpovidno do standartiv Nacional'nogo banku Ukrai'ny: lyst departamentu informatyzacii' Nacional'nogo banku Ukrai'ny bankam Ukrai'ny vid 03 bereznja 2011 r. № 24-112/365. – K.: Nacional'nyj bank Ukrai'ny, 2011. (in Ukrainian)
[20]. ISO/IEC 27005 – Information technology – Security techniques – Information security risk management. [Online]. Available: http://www.bank.gov.ua/doccatalog/document?id=72235https://exebit.files.wordpress.com/2013/11/iso-27005-2011-ru-v1.pdf. Accessed on: Dec. 09, 2017. (in English)
[21]. Rukovodjashhij dokument. Bezopasnost' informacionnyh tehnologij. Kriterii ocenki bezopasnosti informacionnyh tehnologij. GOST R ISO/MJeK 15408-2-2008, 2008. [Online]. Available: http://primorsky.ru/authorities/executive-agencies/departments/information-security/Documents/doki-po-ib/. Accessed on: Dec., 07.2017. (in Russian)

[22]. Rukovodjashhij dokument. Bezopasnost' informacionnyh tehnologij. Obshhaja metodologija ocenki bezopasnosti informacionnyh tehnologij. Proekt. [Online]. Available: http://fstec.ru/component/attachments/download/293. Accessed on: Dec., 07.2017. (in Russian)

[23]. Standart Ukrai'ny SOU N NBU 65.1 SUIB 1.0:2010. Metody zahystu v bankivs'kij dijal'nosti systema upravlinnja informacijnoju bezpekoju. Vymogy. (ISO/IEC 27001:2005, MOD). K: NBU., 2010. (in Ukrainian)

[24]. Postanova Pravlinnja Nacional'nogo banku Ukrai'ny vid 18 chervnja 2003 roku № 254 " Pro zatverdzhennja Polozhennja pro organizaciju operacijnoi' dijal'nosti v bankah Ukrai'ny", K: NBU., 2003. (in Ukrainian)

[25]. Doktrina informacijnoi' bezpeki Ukrai'ni, zatverdzheno Ukazom Prezidenta Ukrai'ni vid 25 ljutogo 2017 roku № 47/2017, 2017. [Online]. Available: http://zakon3.rada.gov.ua/laws/show/47/2017/paran2#n2. Accessed on: Dec., 07.2017. (in Ukrainian)

[26]. Ukaz Prezydenta Ukrai'ny vid 15 bereznja 2016 roku № 96 "Pro rishennja Rady nacional'noi' bezpeky i oborony Ukrai'ny vid 27 sichnja 2016 roku "Pro Strategiju kiberbezpeky. [Online]. Available: http://zakon3.rada.gov.ua/laws/show/96/2016/paran11#n11. Accessed on: Dec., 07.2017. (in Ukrainian)

[27]. Ukaz Prezydenta Ukrai'ny vid 12 ljutogo 2007 roku № 105 "Pro Strategiju nacional'noi' bezpeky Ukrai'ny", 2007. [Online]. Available: http://zakon3.rada.gov.ua/laws/show/105/2007 Accessed on: Dec., 07.2017. (in Ukrainian)

[28]. D. Gorbenko, A. V. Potij, i P. I. Tereshhenko, "Kriterii i metodologija ocenki bezopasnosti informacionnyh tehnologij", [Online]. Available: http://www.bezpeka.com/ru/lib/spec/infsys/art108.html. Accessed on: Dec., 07.2017. (in Ukrainian)

[29]. S. Yevseiev, "The model of access rights violator in an automated banking system based on a synergistic approach ", Naukovo-tehnichnij zhurnal "Informacijna bezpeka", vol. 26, no. 2, pp.110-120, 2017. (in Russian)

[30]. S. Yevseiev, "The synergetic approach for bank systems' security assesment", Naukovo-tehnichnij zhurnal "Informacijna bezpeka", vol. 24, no. 4, pp. 104-108, 2016. (in Russian)

[31]. R. Hryshchuk, ta S. Yevseiev, "Methodology of building a system for providing information security of bank information in automated banking systems", Naukovo-tehnichnij zhurnal "Informacijna bezpeka", vol. 3, no. 23, pp. 204-214, 2017. (in Ukrainian)

[32]. A.V. Potiy, D.J. Pilipenko, "Security metrics classification", Sistemi obrobki informacii, vol. 84, no. 3, pp. 53-56, 2010. (in Russian)

[33]. DSTU ISO/IEC TR 13335-1:2003 Informacijni tehnologii'. Nastanovy z keruvannja bezpekoju informacijnyh tehnologij. Chastyna 1. Koncepcii' ta modeli bezpeky informacijnyh tehnologij, 2003. [Online]. Available: http://lindex.net.ua/ua/shop/bibl/500/doc/11423. Accessed on: Dec., 07.2017. (in Ukrainian)

[34]. DSTU ISO/IEC TR 13335-2:2003 Informacijni tehnologii'. Chastyna 2. Nastanovy z keruvannja bezpekoju informacijnyh tehnologij, 2003. [Online]. Available: http://www.premier-hs.com.ua/ru/content/dstu-isoiec-tr-13335-22003-nastanovi-z-kieruvannia-biezpiekoiu informatsiinikh-tiekhnologhii. Accessed on: Dec., 07.2017. (in Ukrainian)

[35]. DSTU ISO/IEC TR 13335-3:2003 Informacijni tehnologii'. Nastanovy z keruvannja bezpekoju informacijnyh tehnologij. Chastyna 3. Metody keruvannja zahystom informacijnyh tehnologij, 2003. [Online]. Available: http://lindex.net.ua/ua/shop/bibl/500/doc/11425. Accessed on: Dec., 07.2017. (in Ukrainian)

[36]. DSTU ISO/IEC TR 13335-4:2005 Informacijni tehnologii'. Nastanovy z upravlinnja bezpekoju informacijnyh tehnologij. Chastyna 4. Vybyrannja zasobiv zahystu, 2005. [Online]. Available: http://metrology.com.ua/download/iso-iec-ohsas-i-dr/61-iso/290-dstu-iso-iec-tr-13335-4-2005. Accessed on: Dec., 07.2017. (in Ukrainian)

[37]. DSTU ISO/IEC TR 13335-5:2005 Informacijni tehnologii'. Nastanovy z upravlinnja bezpekoju informacijnyh tehnologij. Chastyna 5. Nastanova z upravlinnja merezhnoju bezpekoju, 2005. [Online]. Available: http://lindex.net.ua/ua/shop/bibl/500/doc/11427. Accessed on: Dec., 07.2017. (in Ukrainian)

[38]. Standart Ukrai'ny SOU N NBU 65.1 SUIB 1.0:2010. Informacijni tehnologii'. Metody zahystu. Zvid pravyl dlja upravlinnja informacijnoju bezpekoju (ISO/IEC 27002:2005, MOD), 2010[Online]. Available: http://s-byte.com/useful/27002.pdf. Accessed on: Dec., 07.2017. (in Ukrainian)

[39]. Standart Ukrai'ny SOU N NBU 65.1 SUIB 1.0:2010. Metody zahystu v bankivs'kij dijal'nosti. Systema upravlinnja informacijnoju bezpekoju. Vymogy (ISO/IEC 27001:2005, MOD), 2005. [Online]. Available: https://kyianyn.files.wordpress.com/2010/12/nbu-27001.pdf. Accessed on: Dec. 7.2017. (in Ukrainian)

[40]. ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Req. [Online]. Available:

http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534. Accessed on: Dec. 7.2017.

[41]. ISO/IEC 27002:2013 – Information technology – Security techniques – Code of practice for information security controls. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533. Accessed on: Dec. 7.2017. (in English)

[42]. O. K. Judin, S. S. Buchik, Derzhavni informacijni resursy. Metodologija pobudovy klasyfikatora zagroz. Kyi'v, Ukraina: NAU, 2015. (in Ukrainian)

[43]. O. K. Judin, S. S. Buchik, A. V. Chunar'ova, ta O. I. Varchenko, "Technique of constructing a classification of threats to state information resources", Naukojemni tehnologii, vol, 22, no. 2, pp. 200-210, 2014. (in Ukrainian)

[44]. O. K. Judin, S. S. Buchik, "Classification of threats to state informative resources of normatively-legal aspiration. methodology of construction of classifier", Zahyst informacii', vol. 17, no. 2, pp. 108-116, 2015. (in Ukrainian)

[45]. S. S. Buchik, "Theoretical basis of the analysis of the risks of the tree of identifiers of state information resources", Naukojemni tehnologii', vol. 29, no. 1, pp. 70-77, 2016. (in Ukrainian)

[46]. S. S. Buchik, " Methodology of risk analysis of the tree of identifiers of state information resources", Zahyst informacii', vol. 18, no. 1, pp. 81 – 89, 2016. (in Ukrainian)

[47]. D. Domarjev, V. Domarjev ta S. Prokopenko, "Method of information system's security level estimation using ISMS "Matrix", Zahyst informacii', vol. 15, no. №1, pp. 80 – 86, 2013. (in Ukrainian)

[48]. S. V. Pavlenko, "Method of estimation of protected of informative systems", Systemy ozbrojennja i vijs'kova tehnika, vol. 4, no. 20, pp. 149-154, 2009. (in Ukrainian)

[49]. S. S. Buchyk, "Estimation of functional types of threats to state informative resources", Otkrytye informacionnye i komp'juternye integrirovannye tehnologii, no. 70, pp. 271-280, 2015. (in Ukrainian)

[50]. R. A. Nurdinov, T. N. Batova, "Approaches and methods of rationale choosing of information protection facilities", Sovremennye problemy nauki i obrazovanija, no. 2, 2013. [Online]. Available: http://elibrary.ru/item.asp?id=21285749. Accessed on: Des. 07, 2017. (in Russian)

[51]. ISO/IEC 18045:2014 Information technology – Security techniques – Guidelines for cybersecurity. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=46412. Accessed on: Des. 09, 2017. (in English)