МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

ЄВСЕЄВ Сергій Петрович

УДК 004.056:336.71

МЕТОДОЛОГІЯ ПОБУДОВИ СИСТЕМИ БЕЗПЕКИ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

21.05.01 – Інформаційна безпека держави

Автореферат
дисертації на здобуття наукового ступеня
доктора технічних наук

Київ – 2018

Дисертацією є рукопис.

Робота виконана на кафедрі інформаційних систем Харківського національного економічного університету імені Семена Кузнеця.

Науковий консультант: доктор технічних наук, старший науковий співробітник
Грищук Руслан Валентинович,
Житомирський військовий інститут
імені С. П. Корольова,
начальник науково-дослідного відділу
інформаційної та кібернетичної безпеки наукового центру.

Офіційні опоненти: доктор технічних наук, професор
Хорошко Володимир Олексійович,
Національний авіаційний університет,
професор кафедри безпеки інформаційних технологій;

доктор технічних наук, старший науковий співробітник
Кудін Антон Михайлович,
Національний банк України,
керівник проектів і програм Департаменту безпеки;

доктор технічних наук, доцент
Іванченко Сергій Олександрович,
Інститут спеціального зв'язку та захисту інформації
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря
Сікорського", професор спеціальної кафедри №1.

Захист відбудеться "27" квітня 2018 р. о 13^{00} на засіданні спеціалізованої вченої ради Д 26.062.17 при Національному авіаційному університеті за адресою: 03058, м. Київ, пр. Космонавта Комарова 1, корпус 11, ауд. 111.

З дисертацією можна ознайомитись у Науково-технічній бібліотеці Національного авіаційного університету за адресою: 03058, м. Київ, пр. Космонавта Комарова 1.

Автореферат розісланий "26" березня 2018 р.

Учений секретар
спеціалізованої вченої ради С.О. Гнатюк

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. У сучасних умовах, як показала практика, важлива роль у забезпеченні національної безпеки України та особливо її економічної складової належить процесам забезпечення інформаційної безпеки (ІБ) держави в банківському секторі (БнС). Ключову роль при побудові систем безпеки банківських інформаційних ресурсів (БІР) як складових 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 ІБ держави на усіх рівнях.

Революційні зміни останнього десятиліття, що відбулися в банківському секторі, зумовили до об'єднання інформаційних та комп'ютерних мереж в єдиний інформаційний та кібернетичний простір, що спонукало до створення автоматизованих банківських систем (АБС), які істотно розширили спектр електронних послуг державних і комерційних банків світу та України. Як наслідок, суттєво трансформувалися і загрози такому національному інформаційному ресурсу держави, як БІР під якими в роботі розуміється банківська інформація (БІн). Загрози безпеці БІР набули ознак гібридності. Прояви ознак гібридності внаслідок одночасного впливу загроз інформаційній безпеці, кібернетичній безпеці (КБ) та безпеці інформації (БІ) на БІР призвели до виникнення явища синергізму, негативні прояви якого потребують кардинального перегляду концепцій побудови діючих систем безпеки. Як показує світовий досвід, прояви гібридних загроз безпеці БІР мали місце, наприклад, під час блокування роботи АБС БнС в США (вересень, 2011 р.), що призвело виникнення масової акції непокори під назвою "Захопи Уолл-Стрітт", яка ланцюговою реакцією поширилася на найбільші міста згаданої держави та ряду найбільш економічно розвинених держав Європейського Союзу та зрештою спровокувала світовий економічний колапс. Прояви гібридних загроз безпеці БІР мали місце і в Україні. Наприклад, розпочавшись з кібератаки за допомогою шкідливого програмного забезпечення "Petya.A", "Petya.B" (червень–липень, 2017 р.) було скомпрометовано процес надання банківських послуг, що викликало невдоволення клієнтів банків – громадян, які є суб'єктами ІБ держави. Ланцюгова реакція після України поширилася на банківські сектори Італії, Ізраїлю, Сербії, Румунії, Угорщини, Аргентини, Чехії, Німеччини та інших розвинених держав світу. Таким чином, проблема забезпечення ІБ держави для інфраструктур критичного застосування (ІКЗ), до яких належить і банківський сектор, стоїть дуже гостро. Отже, стає зрозуміло, що потребують кардинального перегляду діючі методологічні засади побудови системи безпеки БІР як України зокрема, так і світу в цілому.

Відомо, що вирішенню проблеми ІБ держави в цілому та безпеки БІР зокрема присвячено праці відомих вітчизняних і закордонних вчених та їх наукових шкіл: І. Горбенка, В. Задіраки, О. Кузнецова, С. Ленкова, О. Молдовяна, В. Мохора, В. Сідельникова, С. Тімофєєва, Б. Шнайера, В. Шокала, В. Ярочкина, А. Калашнікова та багатьох ін. Разом з тим встановлено, що невирішеними аспектами загальної проблеми забезпечення ІБ держави залишається **проблема** створення цілісної науково обґрунтованої методології побудови системи безпеки БІР, впровадження якої на практиці сприятиме стійкому та стабільному розвитку банківського сектору держави.

Отже, на сьогодні ***склалося об'єктивне протиріччя*** між зростаючими на практиці вимогами до безпеки БІР при одночасному збільшенні кількості та технологічній складності загроз безпеці і набутті ними ознак гібридності з одного боку та недосконалістю, а подекуди й відсутністю методології побудови системи безпеки БІР від таких загроз з іншого. Наявність цього протиріччя ***обумовлює актуальність теми дисертації***, а тому вирішення поставленої науково-прикладної проблеми має важливе наукове та практичне значення.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційні дослідження проведено згідно з Доктриною інформаційної безпеки України, затвердженою указом Президента України від 25.02.2017 р. № 47/2017 та Стратегією кібербезпеки України, затвердженою указом Президента України від 15.03.2016 р. № 96/2016 у рамках НДР: № 36Б115 "Розробка методів синтезу тестових моделей поведінки програмних об'єктів, підвищення оперативності передачі та захисту інформації у телекомунікаційних системах" (д.р. № 0115U003103) – виконувалася у Кіровоградському національному технічному університеті; "Розроблення алгоритмів несиметричного шифрування для мобільних засобів зв'язку" (д.р. № 0116U005696), "Розробка методу підвищення конфіденційності і ймовірності банківської інформації в автоматизованих банківських системах" (д.р. №. 0117U000136), № 15/2016-2017 "Методологія побудови системи забезпечення безпеки банківської інформації: аналіз проблеми та синтез нових рішень" (д.р. №. 0117U001628) – виконувалися в Харківському національному економічному університеті ім. С. Кузнеця. У згаданих НДР здобувач брав участь як виконавець, відповідальний виконавець, а в останній НДР виступав науковим керівником.

Мета і завдання дослідження. Метою дисертаційної роботи є створення науково обґрунтованої методології побудови системи безпеки банківських інформаційних ресурсів для підвищення рівня їх захищеності від загроз безпеці гібридного характеру.

Для досягнення поставленої мети **необхідно розв'язати такі основні завдання**:

– провести аналіз сутності та змісту проблеми інформаційної безпеки держави на сучасному етапі розвитку науки і техніки та дослідити роль й місце систем безпеки банківських інформаційних ресурсів при впливі на них нових загроз, які мають гібридний характер. Оцінити сучасний стан нормативно-правової бази, яка регламентує порядок побудови системи безпеки банківських інформаційних ресурсів, а також встановлює вимоги до їх захищеності;

– розробити концепцію побудови синергетичної моделі загроз безпеки банківських інформаційних ресурсів для обґрунтування та вибору найбільш ефективних напрямків досягнення цілей безпеки банківських інформаційних ресурсів на кожному з рівнів моделі управління стратегічним управлінням безпекою банківських інформаційних технологій з урахуванням величини ризику на кожному рівні та забезпеченням дієвого контролю за виконанням функцій системи управління інформаційною безпекою організацій банківського сектору;

– удосконалити класифікатор загроз безпеці банківських інформаційних ресурсів для формування експертної оцінки рівня загроз банківських інформаційних ресурсів за складовими безпеки, видами послуг та рівнями ієрархії інфраструктури

автоматизованих банківських систем, аналізу їх синергії та гібридності, оцінювання ймовірності впливу загроз інформаційній безпеці, кібербезпеці та безпеці інформації на безпеку банківських інформаційних ресурсів;

– розробити метод оцінювання узагальненого показника рівня захищеності банківських інформаційних ресурсів з урахуванням розробленої синергетичної моделі загроз та удосконаленого класифікатора для встановлення взаємозв'язків між елементами структури автоматизованих банківських систем, каналами зв'язку, активами банківських інформаційних ресурсів, та загрозами інформаційній безпеці, кібербезпеці, безпеці інформації, а також визначення рівня захищеності банківських інформаційних ресурсів;

– розробити метод забезпечення конфіденційності та цілісності банківських інформаційних ресурсів при одночасній дії на них загроз інформаційній безпеці, кібербезпеці та безпеці інформації для підвищення рівня їх інформаційної прихованості та достовірності банківських інформаційних ресурсів;

– розробити метод забезпечення автентичності банківських інформаційних ресурсів при одночасній дії на них загроз інформаційній безпеці, кібербезпеці та безпеці інформації для підвищення рівня їх інформаційної прихованості та достовірності *OTP*-паролів в протоколі двофакторної автентифікації;

– розробити метод оцінювання безпеки банківських інформаційних ресурсів, що повинен враховувати комплексний показник ефективності інвестицій, які виділяються на забезпечення безпеки банківських інформаційних ресурсів, для оптимізації витрати коштів на її побудову в умовах впливу гібридних загроз при одночасному забезпеченні заданого рівня їх безпеки;

– розробити методологію побудови системи безпеки банківських інформаційних ресурсів, яка забезпечує одержання максимальної кількості емерджентних властивостей системи безпеки банківських інформаційних ресурсів при мінімальних ресурсних витратах на її створення та функціонування в умовах впливу гібридності загроз.

Об'єктом дослідження є процеси забезпечення інформаційної безпеки держави в банківському секторі.

Предметом дослідження є методологія побудови системи безпеки банківських інформаційних ресурсів.

Методи дослідження. Проведені дослідження ґрунтуються на теоретично обґрунтованих та практично апробованих методах теорії множин (формалізовано загрози безпеки банківських інформаційних ресурсів, здійснено їх класифікацію, визначено вимоги і повноту забезпечення безпеки банківських інформаційних ресурсів), теорії криптографії, теорії кодування та теорії скінчених полів Галуа (використано при розробці гібридних крипто-кодових конструкцій на збиткових кодах (ГККЗК) та обґрунтуванні їх стійкості), теорії ймовірностей і математичної статистики (використано для розроблення методу експрес-аналізу стійкості і дослідження властивостей гібридних крипто-кодових конструкцій на збиткових кодах), експертного оцінювання (для визначення вагових коефіцієнтів загроз для формування класифікатора загроз), математичної логіки і теорії автоматів (для оцінювання енергетичних затрат при практичній реалізації гібридних крипто-кодових конструкцій на збиткових кодах), системного аналізу (для ієрархічного

подання автоматизованих банківських систем), законах синергії (для побудови моделі загроз, дослідження її впливу на систему безпеки банківських інформаційних ресурсів).

Наукова новизна одержаних результатів:

– *вперше розроблено* концепцію побудови синергетичної моделі загроз безпеки банківських інформаційних ресурсів, базис якої становить трирівнева модель стратегічного управління безпекою банківських інформаційних технологій. Розроблена на основі концепції модель за рахунок комплексування складових інформаційної безпеки, кібербезпеки та безпеки інформації відкриває новий напрямок у забезпеченні безпеки банківських інформаційних ресурсів на основі моделі стратегічного управління банком з урахуванням величини ризику на кожному рівні та дієвого контролю за виконанням функцій системи управління інформаційною безпекою організацій банківського сектору;

– *удосконалено* класифікатор загроз безпеці банківських інформаційних ресурсів, який, на відміну від відомих, 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;

– *вперше розроблено* метод оцінювання узагальненого показника рівня захищеності банківських інформаційних ресурсів на основі синергетичної моделі загроз, удосконалених класифікатора та моделі зловмисника, моделі оцінки захищеності банківських інформаційних ресурсів, та моделі інфраструктури автоматизованої банківської системи, що надає можливість встановлення взаємозв'язків між елементами ієрархічної структури автоматизованої банківської системи, каналами зв'язку, інформаційними активами банківських інформаційних ресурсів та загрозами інформаційній безпеці, кібербезпеці, безпеці інформації для досягнення синергетичного ефекту та визначення рівня захищеності банківських інформаційних ресурсів;

– *вперше розроблено* метод забезпечення конфіденційності та цілісності банківських інформаційних ресурсів, який ґрунтується на гібридних крипто-кодових конструкціях зі збитковими кодами на основі модифікованої крипто-кодової системи Мак-Еліса на модифікованих алгеброгеометричних кодах, що дозволяє підвищити рівень інформаційної прихованості та достовірності банківських інформаційних ресурсів в умовах дії гібридних загроз;

– *вперше розроблено* метод забезпечення автентичності банківських інформаційних ресурсів, який ґрунтується на гібридних крипто-кодових конструкціях зі збитковими кодами на основі модифікованих несиметричних крипто-кодових системах Мак-Еліса і Нідеррайтера на модифікованих алгеброгеометричних кодах, що дозволяє підвищити рівень інформаційної прихованості та достовірності *OTP*-паролів в протоколі двофакторної автентифікації;

– *набув подальшого розвитку* метод оцінювання безпеки банківських інформаційних ресурсів, що, на відміну від відомих, враховує комплексний показник ефективності інвестицій, які виділяються на забезпечення безпеки банківських інформаційних ресурсів, що дозволяє оптимізувати витрати коштів на її побудову в

умовах впливу гібридних загроз при одночасному забезпеченні заданого рівня їх безпеки;

– *вперше розроблено* методологію побудови системи безпеки банківських інформаційних ресурсів, в основу якої покладено концепцію побудови синергетичної моделі загроз, удосконалений класифікатор загроз, методи забезпечення конфіденційності, цілісності та автентичності банківських інформаційних ресурсів на гібридних крипто-кодових конструкціях зі збитковими кодами та удосконалений метод оцінювання безпеки банківських інформаційних ресурсів на основі комплексного показника ефективності інвестицій, що дозволяє відкрити новий (емерджентний) з позицій безпеки та ефективний з позицій витрачених коштів підхід до побудови діючих та перспективних систем безпеки банківських інформаційних ресурсів.

Практичне значення одержаних результатів у сукупності складає підґрунтя для практичної побудови дієвої та ефективної системи безпеки БІР.

Практична цінність одержаних результатів:

1. Розроблено програмний застосунок, який реалізує удосконалений класифікатор загроз інформаційній безпеці, кібербезпеці та безпеці інформації банківських інформаційних ресурсів (електронний доступ: *http://skl.hneu.edu.ua/*), що дозволяє в он-лайн режимі здійснити класифікацію та оцінювання ймовірності впливу зазначених загроз інформаційній безпеці, кібербезпеці та безпеці інформації на безпеку банківських інформаційних ресурсів, їх синергію та гібридність.

2. Розроблено практичну методику для оцінювання рівня захищеності банківських інформаційних ресурсів на основі синергетичної моделі загроз, удосконалених класифікатора загроз та моделі зловмисника, моделі оцінки захищеності банківських інформаційних ресурсів та моделі інфраструктури автоматизованих банківських систем, що дозволяє встановити взаємозв'язки між елементами ієрархічної структури автоматизованої банківської системи, каналами зв'язку, інформаційними активами банківських інформаційних ресурсів та загрозами інформаційній безпеці, кібербезпеці, безпеці інформації для досягнення синергетичного ефекту та визначення рівня захищеності банківських інформаційних ресурсів.

3. Розроблено методику оцінювання безпеки банківських інформаційних ресурсів на основі комплексного показника ефективності інвестицій, які виділяються на забезпечення безпеки банківських інформаційних ресурсів для оптимізації витрати коштів на її побудову в умовах впливу гібридних загроз при одночасному забезпеченні заданого рівня їх безпеки.

4. Розроблені практичні алгоритми забезпечення конфіденційності, цілісності та автентичності банківських інформаційних ресурсів на основі інтеграції криптографічних перетворень і завадостійкого та збиткового кодування, що дозволяє інтегровано (одним механізмом) забезпечувати безпеку банківських інформаційних ресурсів (безпечний час – $T_Б > 200$ р., стійкість до криптоаналізу $P_К < 10^{25}$–10^{35} групових операцій), достовірність передачі банківських інформаційних ресурсів ($P_{пом} < 10^{-9}$) та зменшення енергетичних витрат на їх практичну реалізацію в 10 – 12 разів (шифрування, розшифрування) за рахунок зменшення порядку *GF (q)*.

5. Розроблено програмні макети криптографічних засобів захисту інформації з використанням гібридних крипто-кодових конструкцій зі збитковими кодами, які

дозволяють проводити експериментальні дослідження запропонованих крипто-кодових конструкцій, оцінювати їх властивості та стійкість.

6. Результати впроваджено у діяльність ТОВ “Сайфер БІС” (акт впровадження від 18.05.2017), ТОВ “ТАНТАРІУМ” (акт впровадження від 14.06.2017), “МЕГАБАНК” Публічне акціонерне товариство (акт впровадження від 9.06.2017), ТОВ “Мікрокріпт Технолоджіс” (акт впровадження від 30.11.2017).

Особистий внесок здобувача. Основні положення і результати дисертаційної роботи, що виносяться на захист, отримані автором самостійно. У роботах, написаних у співавторстві, автору належать: [21, 37, 38] – дослідження сучасних механізмів забезпечення ІБ в інтернет-платіжних, внутрішньо-платіжних системах; [3, 4, 17, 33, 36] – дослідження методів побудови та властивості універсальних класів геш-функцій; [8, 34, 39, 42] – розробка моделей атак на АБС, дослідження загроз на БІР, механізмів надання послуг безпеки; [1, 2, 18, 27, 35] – розробка методів побудови несиметричних крипто-кодових систем (НККС) на основі теоретико-кодових схем (ТКС) Мак-Еліса та Нідеррайтера на еліптичних кодах (*EC*), дослідження їх властивості; [22] – розроблення вимог оцінки методу каскадного формування *MAC*-коду на основі модулярних перетворень; [5, 9, 12, 15, 24, 42] – дослідження методів 2*FA*, розробка методу моніторингу системи *PassWindow*, розробка методу 2*FA* на основі *OTP*-паролів з використанням модифікованих крипто-кодових систем Мак-Еліса і Нідеррайтера, методу 2*FA* на основі ГКККЗК; [10, 23, 47] – порівняльний аналіз законодавчої бази забезпечення безпеки БІР в національної системі масових електронних платежів; [6, 7, 25, 26, 29, 40, 48] – розробка концепції та розробка синергетичної моделі оцінки загроз; [19, 28, 45] – дослідження ризиків КБ БІР та методів їх виявлення, розробка моделі оцінки складових безпеки БІР на основі синергетичного підходу оцінки загроз; [11, 46, 51, 52] – розроблено метод побудови модифікованої крипто-кодової конструкції на модифікованих еліптичних кодах (*MEC*); [29, 50] – розробка удосконаленого класифікатора загроз безпеці БІР; [13, 16] – розробка методики оцінки функціональної ефективності комп’ютерних систем; [43, 44] – розробка методики оцінки безперервності бізнес-процесів в організаціях банківського сектору; [14, 41, 52, 53, 54] – розробка методів побудови ГКККЗК; [31] – дослідження адекватності використання міні-версій блоково-симетричних шифрів (БСШ) для оцінки їх криптостійкості, [30, 49] – методика оцінки ефективності інвестицій в безпеку ОБС на основі синергетичної моделі загроз, [20] – удосконалення методу формування *MAC*-коду на основі модулярних перетворень, [32] – методологія побудови системи безпеки БІР.

Апробація результатів дисертації. Основні положення дисертаційної роботи доповідалися та обговорювалися на понад 20 наукових конференціях серед яких: “Securitatea informaţională 2008”, conf. intern. (2008; Chişinău), “Інформаційна безпека” (Київ, 2009, 2015–2016 рр.), “Проблеми й перспективи розвитку ІТ-індустрії” (Харків, 2010–2017рр.), “Сучасні проблеми і досягнення в галузі радіотехніки, телекомунікацій та інформаційних технологій” (Запоріжжя, 2014 р.), “Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі” (Харків, 2016–2017 рр.), “Інформаційно-комп’ютерні технології – 2016” (Житомир, 2016 р.), “Методи та засоби кодування, захисту й ущільнення інформації” (Вінниця, 2016 р.), “Захист інформації і безпека інформаційних систем” (Львів, 2016–2017 рр.), “Економічний розвиток і спадщина Семена Кузнеця” (Харків, 2016 р.), “Застосування інформаційних технологій у

підготовці та діяльності сил охорони правопорядку" (Харків, 2017 р.), "Інформація, комунікація, суспільство 2017" (Славське, 2017 р.), "ITSEC: Безпека інформаційних технологій" (Київ, 2017 р.), "Інформаційні технології та комп'ютерне моделювання" (Івано-Франківськ, 2017 р.), "Проблеми інформатизації" (Черкаси, 2017 р.), "Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України" (Хмельницький, 2017 р.).

Публікації. Основні положення дисертації опубліковано у 120 наукових працях (54 основних з яких наведено у авторефераті), у тому числі: 3 монографії (у співавторстві) [1 – 3], 4 розділи у колективних монографіях [4 – 7]; 9 наукових статей у міжнародних рецензованих виданнях, що входять до баз даних *Scopus* та *Web of Science* [8 – 16]; 16 наукових статей у закордонних [17 – 20], вітчизняних фахових наукових журналах, які входять до інших міжнародних наукометричних баз даних (*Index Copernicus, EBSCO , Inspec* тощо) [21 –32], та 12 статей у наукових журналах та збірниках наукових праць [33 – 44], що входять до переліку фахових видань України, а також 10 матеріалів і тез доповідей на міжнародних конференціях [45 – 54]. Без співавторів – опубліковано 8 наукових статей [23, 25, 28 – 30, 33, 38, 40].

Структура роботи та її обсяг. Дисертація складається з анотації, змісту, переліку умовних позначень, вступу, п'яти розділів, загальних висновків, додатків, списку використаних джерел в кінці кожного розділу основної частини дисертації і має 289 сторінки основного тексту, 102 рисунки, 67 таблиць, 90 сторінок додатків. Список використаних джерел містить 279 найменувань і займає 41 сторінку. Загальний обсяг дисертації – 471 сторінка.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** подано загальну характеристику роботи, обґрунтовано актуальність, сформульовано мету і завдання досліджень, відображено наукову новизну і практичну цінність отриманих результатів, наведено дані щодо їх апробації та впровадження.

У першому розділі проведено аналіз сутності та змісту проблеми ІБ держави на сучасному етапі розвитку науки і техніки, зокрема роль й місце систем безпеки БІР при впливі на них нових видів загроз, які мають гібридний характер. З огляду на зазначене уточнено категорію *банківські інформаційні ресурси* (банківська інформація). Для коректного її опису запропоновано ознакову класифікацію (рис. 1).

Проведений аналіз міжнародної та національної нормативно-правової бази, яка регламентує порядок побудови системи безпеки БІР, дав підстави виділити основні невирішені завдання щодо безпеки БІР: до сьогодні з питань побудови систем безпеки БІР розглянуті лише окремі складові методології оцінювання рівня захищеності інформаційних технологій, застосовуваних в ОБС; 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 безпеки БІР; неврахування в моделі ІБ (модель CIA) невід'ємної складової банківських транзакцій – послуги автентичності; відсутні механізми оцінювання рівня захищеності БІР від загроз гібридного характеру на основі комплексування ознак загроз ІБ, КБ, БІ на БІР, технічні об'єкти її інфраструктури; для

забезпечення цілісності й конфіденційності в АБС застосовуються “морально застарілі” симетричні БСШ – ГОСТ-28147, 3*DES* та несиметричні криптосистеми *RSA, Diffie-Hellman*. У перших механізмах проблемним є питання розподілу ключів

Рис. 1. Ознакова класифікація банківських інформаційних ресурсів

шифрування, у других низька – швидкість шифрування (на 3–5 порядків нижче, ніж у БСШ), проте використання інтегрованих механізмів дає змогу забезпечити швидкість криптоперетворень, безпеку та достовірність БІР.

Таким чином, дотримуючись триєдиного правила щодо забезпечення безпеки БІР та ґрунтуючись на синергетичному підході до побудови відповідної системи безпеки в умовах дії загроз гібридного характеру, запропоновано ідею, яка розвинута в дисертації. Її загальний вигляд подано на рис. 2.

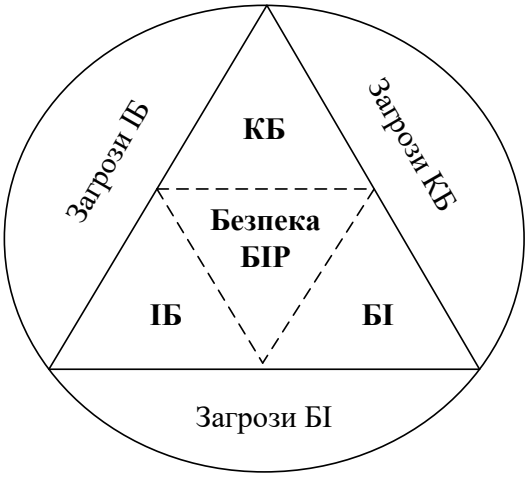


Рис. 2. Сутність синергетичного підходу до побудови системи безпеки банківських інформаційних ресурсів в умовах дії загроз гібридного характеру

З огляду на різну природу загроз для обраних профілів безпеки БІР (рис. 2) та в інтересах отримання в подальшому оцінювання величини ризику загрози безпеці в роботі обґрунтовано та введено синергетичний показник безпеки БІР (рис. 3).

Встановлено, що відсутність на сьогодні ефективної та дієвої методології побудови системи безпеки БІР також обумовлена наявністю протиріччя, яке визначається тим, що з одного боку практика вимагає від теорії пошуку нових підходів

Рис. 3. Роль і місце синергетичного показника безпеки БІР

до забезпечення безпеки БІР в умовах зростання кількості загроз її складових: ІБ, КБ, БІ при одночасному зростанні їх технологічної складності. З іншого боку, в теорії відсутня цілісна науково обґрунтована методологія побудови на практиці системи безпеки БІР в цілому, що обумовлено недосконалістю механізмів забезпечення її інформаційної безпеки, безпеки інформації та кібербезпеки зокрема.

У формалізованому вигляді науково-прикладну проблему описано виразом:

$$Emerdg = \max\left\{\prod\nolimits_{synerg}{}^{M}_{N}\right\},$$

де $\prod_{synerg}{}^{M}_{N}$ – максимальна кількість емерджентних властивостей системи безпеки БІР в цілому, що досягається при виникненні синергетичного ефекту в результаті взаємодії обраних профілів безпеки (M), N – кількість станів системи безпеки БІР або кількість її емерджентних властивостей; $M \le N$. При цьому максимальну кількість емерджентних властивостей системи безпеки БІР в цілому можна досягти при виконанні умови $\prod_{synerg}{}^{M}_{N} = \sum_{m=1}^{M} C_N^m$.

Таким чином, у першому розділі на основі проведеного аналізу стану проблеми, обґрунтовано основні завдання дослідження, які потрібно вирішити для досягнення поставленої мети.

Другий розділ присвячений розробленню концептуальних засад забезпечення безпеки БІР. Запропоновано та розроблено концепцію побудови синергетичної моделі загроз безпеці БІР, яка базується на трирівневій моделі стратегічного управління їх безпекою.

Перший рівень описує загальну корпоративну стратегію банку та його функціональні стратегії. Корпоративна стратегія визначає перспективи розвитку та сприяє виконанню основної місії банку. На цьому рівні відповідно до синергетичного підходу розглядається загальна концепція безпеки інформаційних

технологій АБС і формуються цілі і завдання забезпечення КБ, а також визначається стан безпеки БІР $S^{ABS} = \left\{ S_1^{ABS}, S_2^{ABS}, ..., S_m^{ABS} \right\}$, де $S_i^{ABS} \in \left\{ S^{ABS} \right\}, (i = \overline{1,\mathrm{m}})$ – стан безпеки БІР. 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 БІР:

$$\left\{ RR^{ABS} \right\} = \left\{ R_{BBI} \right\} \cup \left\{ OV_{BBI} \right\} \cup \left\{ IU_{BBI} \right\},$$

де $\left\{ RR^{ABS} \right\}$ – множина вимог регуляторів, яка включає вимоги до безпеки БІР – $\left\{ R_{BBI} \right\}$, що визначені у міжнародних і національних стандартах; множина оцінок ступеня виконання вимог безпеки $\left\{ OV_{BBI} \right\}$ та множина підсумкового рівня відповідності безпеки БІР. Також визначаються цілі та завдання основних бізнес-процесів, пов'язаних із захистом персональних даних юридичних і фізичних клієнтів банку. Корпоративна стратегія безпеки описує, яким чином слід керувати і координувати зусилля за різними аспектами безпеки. Вона розвивається у формі функціональних стратегій: фінансової економічної, фізичної та ІБ.

На *третьому рівні* проводиться деталізація функціональних стратегій другого рівня стратегічного набору, формується корпоративна стратегія безпеки інформації. Серед основних напрямків захисту доцільно виділити кадрову безпеку, фізичну безпеку, мережеву та БІ. На цьому рівні визначається відповідність між застосованими технічними засобами захисту інформації (ТЗЗІ) та загрозами ІБ, КБ, БІ на безпеку БІР:

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

де OPZ_i – узагальнений показник рівня захищеності АБС, що дозволяє оцінити рівень відповідності ТЗЗІ вимогам регуляторів; k – кількість окремих показників безпеки. Стратегія безпеки БІР є важливою функцією керівництва банку і повинна формуватися його керівництвом на основі методів експертних оцінок.

Запропонована концепція ґрунтується на синергетичному підході до вибору найбільш ефективних напрямків досягнення поставлених цілей безпеки БІР з урахуванням величини ризику на кожному рівні моделі стратегічного управління банком. Описаний підхід дозволяє комплексно проводити відбір альтернативних варіантів можливих стратегічних рішень з питань безпеки та розробити методику оцінювання узагальненого показника рівня захищеності БІР, яка містить три етапи.

Перший етап передбачає визначення ймовірності впливу загроз ІБ, КБ, БІ на безпеку БІР, другий – визначення залежностей між елементами інфраструктури АБС, інформаційними активами БІР, загрозами ІБ, КБ, БІ та ТЗЗІ на основі удосконаленої моделі інфраструктури АБС, синергетичної моделі загроз, удосконалених класифікатора загроз та моделі зловмисника.

Третій, заключний етап, присвячений визначенню узагальненого показника рівня захищеності БІР на основі удосконаленої моделі оцінювання рівня захищеності БІР. Реалізацію концепції на прикладі ОБС України подано на рис. 4.

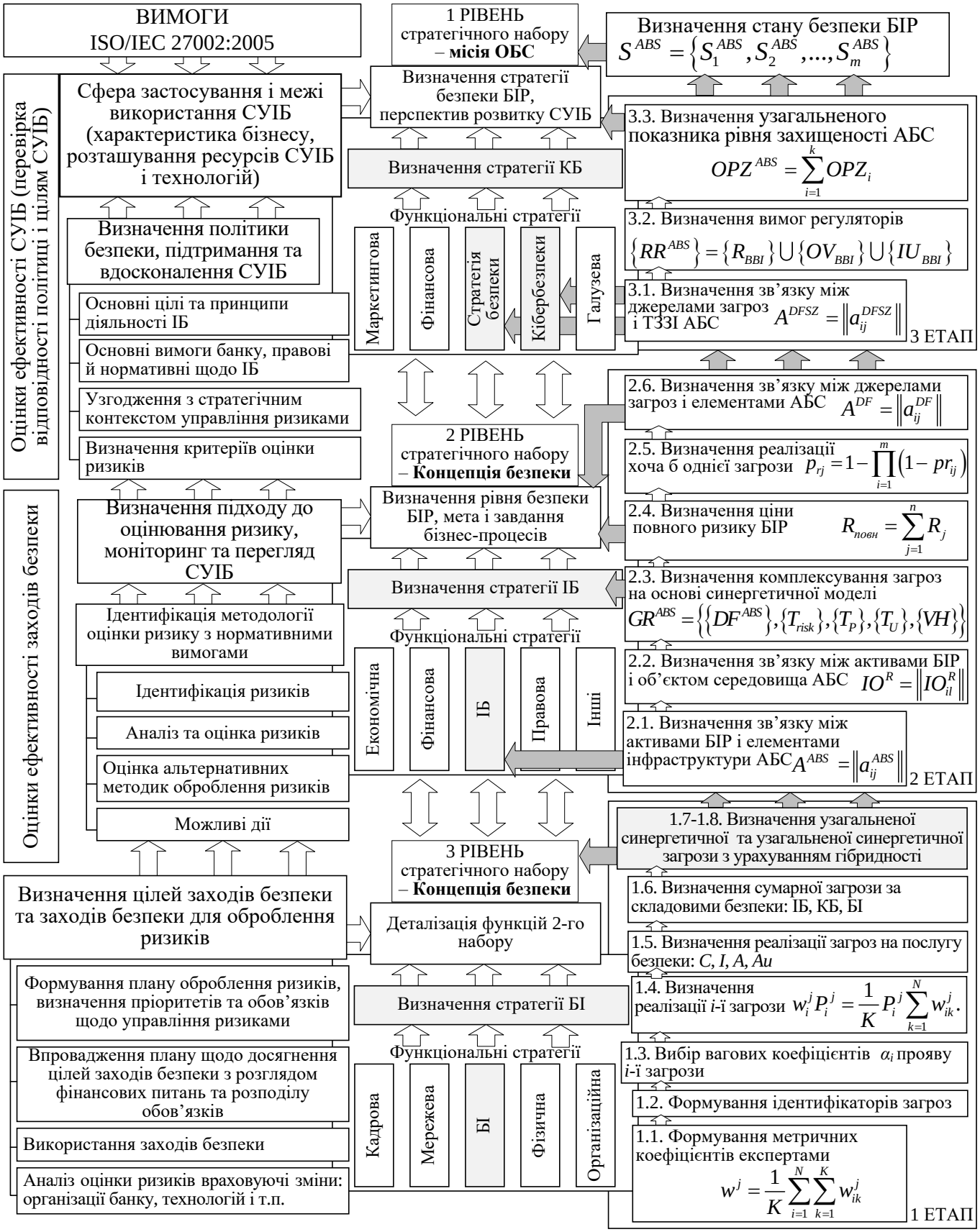


Рис. 4. Реалізація концепції на прикладі ОБС України

Етап 1. Визначення ймовірності впливу загроз ІБ, КБ, БІ на безпеку БІР реалізується на основі запропонованого класифікатора. Складовими класифікатора є:

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

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

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

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

Крок 1.1. 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.

Позначимо через *i* поточний номер загрози ($\{i\}_1^N$), через *k* – поточний номер експерта, який виконував оцінку ($\{k\}_1^K$). Середнє значення оцінки експертів за всіма загрозами для певної послуги безпеки може бути записане:

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

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

Крок 1.3. Вибір вагових коефіцієнтів α_i, що визначають умови прояву *i*-ї загрози (табл. 1).

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

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

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

$w_i^C \alpha_i^C = \frac{1}{K} \alpha_i^C \sum_{k=1}^{K} w_{ik}^C$ – послуга конфіденційність; $w_i^I \alpha_i^I = \frac{1}{K} \alpha_i^I \sum_{k=1}^{K} w_{ik}^I$ – послуга цілісність; $w_i^A \alpha_i^A = \frac{1}{K} \alpha_i^A \sum_{k=1}^{K} w_{ik}^A$ – послуга доступність; $w_i^{Au} \alpha_i^{Au} = \frac{1}{K} \alpha_i^{Au} \sum_{k=1}^{K} w_{ik}^{Au}$ – послуга автентичність, де $w_{ik}{}^C$, $w_{ik}{}^I$, $w_{ik}{}^A$, $w_{ik}{}^{Au}$ – експертні вагові коефіцієнти послуг безпеки: конфіденційності, цілісності, доступності, автентичності; α_i^C , α_i^I , α_i^A , α_i^{Au} – ваговий коефіцієнт послуги безпеки: конфіденційності, цілісності, доступності, автентичності прояву атаки *i*-ї загрози.

Крок 1.5. Визначення реалізації виникнення декількох загроз для обраної послуги розраховується з урахуванням виразу (1):

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

$$W_{synerg}^A = \sum_{i=1}^{M} w_i^A \alpha_i^A \text{ – послуга доступність; } W_{synerg}^{Au} = \sum_{i=1}^{M} w_i^{Au} \alpha_i^{Au} \text{ – послуга автентичність,} \quad (2)$$

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

Крок 1.6. Визначення сумарної загрози за складовими безпеки з урахуванням виразу (2) розраховується:

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

$$W_{synerg}^{BI} = \sum_{i=1}^{N} \left(w_i^C \bigcap w_i^I \bigcap w_i^A \bigcap w_i^{Au} \right) \alpha_i. \quad (3)$$

Крок 1.7. Визначення узагальненої синергетичної загрози на БІР:

$$W_{synerg}^{IB,KB,BI} = W_{synerg}^{IB} \bigcup W_{synerg}^{KB} \bigcup W_{synerg}^{BI}. \quad (4)$$

Крок 1.8. Визначення узагальненої синергетичної загрози з урахуванням її гібридності розраховується: $W_{synerg}^{\text{hybrid } C,I,A,Au} = W_{synerg}^C \bigcap W_{synerg}^{\text{I}} \bigcap W_{synerg}^A \bigcap W_{synerg}^{Au}$. (5)

Результати досліджень загроз з максимальною частотою їх прояву на БІР наведені у табл. 2.

Таблиця 2

Результати оцінки загроз на основі синергетичного підходу

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

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

На основі сформованої множини загроз ІБ, КБ, БІ на БІР та моделі ієрархії АБС – G^{ABS} ={{O^{ABS}}, {L^{ABS}}, {I_A}}, де {O^{ABS}} – множина об'єктів середовища АБС, що описують елементи АБС та їх приналежність до рівнів ієрархії АБС, визначається {L^{ABS}} – множина зв'язків між елементами АБС та {I_A} – множина інформаційних активів.

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

Крок 2.2. Визначення типу зв'язку між інформаційними активами БІР $\{I_A\}$ й об'єктами середовища АБС. Кожен елемент $O_l \in \{O^{ABS}\}$ описується вектором $O_l = \{Y^{ABS}, IO\}$, де Y^{ABS} – рівень ієрархії інформаційної структури, яка визначається множиною Y^{ABS} = {*FL, NL, OSL, DBL, BL*}, де *FL* – фізичний рівень; *NL* – мережевий рівень; *OSL* – рівень операційних систем (ОС); *DBL* – рівень систем управління базами даних; *BL* – рівень банківських технологічних застосунків і сервісів. Для визначення типу зв'язку та існуючого співвідношення I^{OR} між інформаційними активами БІР і об'єктами АБС використовується правило:

$$IO^R = \left\| IO_{il}^R \right\|, \tag{6}$$

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

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

Синергетична модель загроз формально описується виразом:

$$GR^{ABS} = \left\{ \left\{ DF^{ABS} \right\}, \{T_{risk}\}, \{T_P\}, \{T_U\}, \{VH\} \right\}, \tag{7}$$

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

Узагальнена модель визначається п'ятьма категоріями зловмисника та формально описується виразом: $G_{IA}^{ABS} = \left\{ aid_i, pur_i, T_{IA}, S_{\max_i}, pr_j, MS_i^{ABS} \right\} \forall i \in n, \forall j \in m$, (8)

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

На основі запропонованих моделей здійснюється комплексування множини загроз: $DF^{ABS} = \{V^{NS}\} \cup \{V^{AS}\}$, де $\{V^{AS}\} = \{V^{ASIB}\} \cap \{V^{ASKB}\} \cap \{V^{ASBI}\}$, де $\{V^{NS}\}$ – клас природних джерел загроз; $\{V^{AS}\}$ – клас антропогенних загроз, де $\{V^{ASIB}\}$ – множина загроз ІБ; $\{V^{ASKB}\}$ – множина загроз КБ; $\{V^{ASBI}\}$ – множина загроз БІ.

Крок 2.4. Визначення ціни повного ризику всіх активів БІР:

$$R_{повн} = \sum_{j=1}^{n} R_j , \tag{9}$$

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

Крок 2.5. Визначення ймовірності реалізації хоча б однієї загрози для кожного активу БІР:

$$p_{rj} = 1 - \prod_{i=1}^{m} (1 - pr_{ij}), \tag{10}$$

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

Крок 2.6. Визначення зв'язку між джерелами загроз і елементами АБС:

$$A^{DF} = \left\| a_{ij}^{DF} \right\|. \tag{11}$$

Етап 3. Визначення узагальненого показника рівня захищеності БІР на основі удосконаленої моделі. Визначення захищеності АБС від загроз ІБ, КБ, БІ на БІР пропонується одержати на основі моделі:

$$G_{OZ}^{ABS} = \begin{Bmatrix} \{I_A\}, \{O^{ABS}\}, \{DF^{ABS}\}, \{RR^{ABS}\}, \\ \{SZ^{ABS}\}, \{ROZ^{ABS}\}, \{UZ_r^{ABS}\} \end{Bmatrix}, \tag{12}$$

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

Крок 3.1. Визначення зв'язку між загрозами і технічними засобами системи захисту інформації:

$$A^{DFSZ} = \left\| a_{ij}^{DFSZ} \right\|, \tag{13}$$

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

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

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

Крок 3.2. Визначення множини вимог регуляторів $\{RR^{ABS}\}$, яка складається з вимог до забезпечення безпеки БІР – $\{R_{BBI}\}$, зазначених у міжнародних і національних стандартах, множини оцінок ступеня виконання вимог безпеки $\{OV_{BBI}\}$ та множини підсумкового рівня відповідності безпеки БІР вимогам з множини $\{IU_{BBI}\}$:

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

Крок 3.3. Визначення узагальненого показника рівня захищеності АБС, який дозволяє оцінити рівень відповідності ТЗЗІ вимогам регуляторів та розраховується:

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

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

Таким чином, запропонована концепція ґрунтується на синергетичному підході до вибору найбільш ефективних напрямків досягнення поставлених цілей безпеки БІР з урахуванням величини ризику на кожному рівні моделі стратегічного управління банком. Описаний підхід дозволяє комплексно проводити відбір альтернативних варіантів можливих стратегічних рішень з питань безпеки. У цьому розділі також набули подальшого розвитку *теоретичні положення* щодо безпеки БІР, які полягають у формулюванні відповідних дефініцій ("банківська інформація", "конфіденційність БІР", "конфіденційність АБС", "цілісність БІР", "цілісність АБС", "доступність БІР", "доступність АБС", "автентичність БІР", "автентичність АБС", "безперервність бізнес-процесів", "безпека БІР", "інформаційна безпека БІР", "кібербезпека БІР", "безпека інформації БІР", "синергетичний показник безпеки БІР", "рівень захищеності БІР", "гібридність загроз ІБ, КБ, БІ", "синергізм загроз ІБ, КБ, БІ".

У **третьому розділі** наведено результати досліджень, пов'язаних із забезпеченням конфіденційності, цілісності та автентичності БІР. Зокрема розроблено і експериментально досліджено методи гібридних крипто-кодових конструкцій на збиткових кодах (ГККЗК). На основі одержаних оцінок ефективності ТЗЗІ в АБС для забезпечення конфіденційності, цілісності БІР запропоновано нові механізми на основі

ГККЗК, які дозволяють будувати несиметричні криптосистеми на основі модифікованих несиметричних крипто-кодових систем (МНККС) Мак-Еліса з модифікованими еліптичними кодами ((*MEC*) – укороченими або подовженими), що забезпечують відповідний рівень безпеки та достовірності. Відомо, що НККС Мак-Еліса забезпечують швидкість криптоперетворень на рівні швидкості криптоперетворень у БСШ, криптостійкість за рахунок *NP*-задачі – декодування випадкового коду, достовірність за рахунок використання завадостійких алгебраїчних кодів.

Для модифікації еліптичного коду, що не зменшує мінімальну кодову відстань, запропоновано скоротити кількість інформаційних символів. $I=(I_1, I_2, \ldots, I_k)$ – інформаційний вектор *(n, k, d)* блокового коду, підмножина *h* інформаційних символів, $h=x$, $x \le 1/2k$ визначає нульові символи. При кодуванні інформаційного вектора символи множини *h* не застосовуються (вони нульові) і їх можна відкинути, а отримане кодове слово буде коротше на *x* кодових символів. Другий спосіб модифікації використовує збільшення довжини шляхом формування вектора ініціалізації (визначення символів скорочення) і заміни нульових символів символами інформаційного вектора. Вектор ініціалізації (*IV*) є додатковим секретним параметром системи. Основні властивості *MEC* наведені у табл. 3, основні параметри МНККС в табл. 4.

Таблиця 3

Основні *(n, k, d)* властивості *MEC*

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

Таблиця 4

Основні параметри МНККС Мак-Еліса на *MEC*

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

Для нанесення збитку використовується універсальний механізм C_m за алгоритмом *MV*2(збиткові коди, *DC*):

$$CFT / CH_{FT} = E_1\left(M, KU^{EC}\right), \quad CHD / CH_D = E_2\left(M, KU^{EC}\right),$$
$$M = E_{1,2}^{-1}(CFT / CH_{FT}, CHD / CH_D, KU^{EC}), \tag{16}$$

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

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

Таким чином, шифртекст вихідного повідомлення (M) в результаті має два шифртексти (збиток (CHD) і збитковий текст (FTC)), кожен з яких окремо не може відновити вихідний текст. Для забезпечення автентичності БІР пропонується використовувати модифіковану схему двофакторної автентифікації на основі *OTP*-паролів з використанням ГККККЗК на МНККС Мак-Еліса і Нідеррайтера.

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

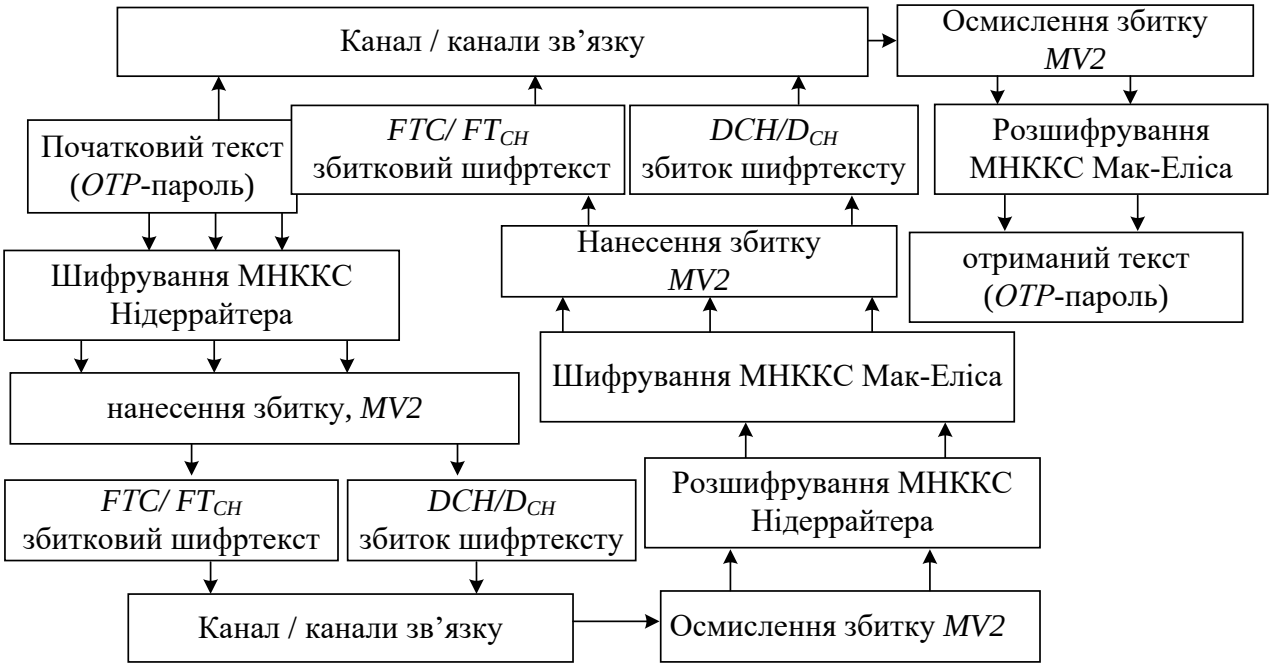


Рис. 5. Структурна схема двофакторної автентифікації на ГККККЗК

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

Для експериментального дослідження запропонованих МНККС на *MEC*, ГККККЗК були реалізовані відповідні програмні макети. Результати порівняльних досліджень НККС Мак-Еліса, МНККС Мак-Еліса на *MEC*, ГККККЗК наведені в табл. 5, 6. У табл. 5, 6 були використані умовні скорочення (префікси): ukh / udh – гібридні КККЗК з укороченими *MEC* / гібридні КККЗК з подовженими *MEC*; uk –

МНККС з укороченими *MEC*; ud – МНККС з подовженими *MEC*. При розрахунках параметрів криптосистем були використані поля Галуа: для НККС Мак-Еліса – *GF* (2^{10}); для МНККС з укороченими/подовженими *MEC* – *GF* (2^6); для гібридних КККЗК – *GF* (2^4).

Складність процесу декодування для НТКС на ЕС задається виразами:

– для НТКС на *EC*: $O_{K+} = N_{покр} \times n \times r$,

де $N_{покр} \geq \frac{C_n^{\rho \cdot t}}{C_{n-k}^{\rho \cdot t}} = \frac{n(n-1)...(n-\rho \cdot t-1)}{(n-k)(n-k-1)...(n-k-\rho \cdot t-1)}$, $t = \lfloor (d-1)/2 \rfloor$,

– для МНККС на укорочених кодах: $O_{K+} = N_{покр} \times \left(2\sqrt{q} + q + 1 - 1/2k\right) \times r$;

– для МНККС на подовжених кодах: $O_{K+} = N_{покр} \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times r$.

Складність процесу декодування для ГККЗК на укорочених МЕС має вигляд:

– для ГККЗК на укорочених *MEC*: $O_{K+} = N_{покр} \times \left(2\sqrt{q} + q + 1 - 1/2k\right) \times r + N_{F\ \text{або}}\left(N_K\right)$,

де $N_F \approx \frac{K_C^{\ z}}{2^{1-K_C^{\ z+1}}} \times |F|$; K_C=97/128; $|F|$ – сумарна довжина вихідних прапорів (збитків) (бітів) – при відомому зловмисникові залишку (збитковому тексті) і заданих прапорах (збитках), при невідомому ключі: $N_K \approx 2^{1190 \times z}$; z = 16;

– для ГККЗК на подовжених *MEC*: $O_{K+} = N_{покр} \times \left(2\sqrt{q} + q + 1 - 1/2k + 1/2k\right) \times r + N_{F\ \text{або}}\left(N_K\right)$.

Таблиця 5

Результати аналізу складності злому і складності кодування для різних швидкостей *EC (MEC)*

$lg(l_s)$	Відносна швидкість кодування, R					
	0.5	0.75	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)
1	4.75	12.1	15.6	18.23	19.12	19.82
2	10.52	21.76	32.47	35.67	38.63	39.18
3	18.22	33.17	43.75	51.61	56.88	58.03
4	21.42	51.75	59.43	72.81	78.92	80.52
5	38.77	61.09	68.26	87.32	94.91	104.56
6	54.13	78.37	**101.72**	**112.46**	**120.83**	**128.79**
7	82.14	83.72	156.75	164.72	182.39	189.74
8	165.84	179.13	223.64	231.57	276.27	287.33
9	358.33	371.09	421.97	428.63	459.81	476.52
10	**672.37**	**684.94**	716.41	722.26	783.46	794.28

Таблиця 6

Результати аналізу складності злому і складності кодування для різних швидкостей *MEC(MEC+DC)*

$lg(l_s)$	Відносна швидкість кодування, R							
	0.5(ud)	0.75(ud)	0.5(uk)	0.75(uk)	0.5(udh)	0.75(udh)	0.5(ukh)	0.75(ukh)
1	15.6	18.23	19.12	19.82	7.21	9.17	12.54	14.56
2	32.47	35.67	38.63	39.18	21.46	23.72	27.48	29.82
3	43.75	51.61	56.88	58.03	31.68	33.83	37.38	38.43
4	59.43	72.81	78.92	80.52	**41.72**	**42.27**	**47.48**	**58.23**
5	68.26	87.32	94.91	104.56	56.63	58.91	62.86	66.53
6	**101.72**	**112.46**	**120.83**	**128.79**	72.32	74.79	89.5	97.71

Аналіз табл. 5, 6 підтверджує, що використання збиткових кодів і подальше зменшення потужності поля Галуа призводить до значного зменшення складності формування (≈ в 12 разів) і розкодування криптограми (≈в 20 разів).

У табл. 7, 8 наведені результати досліджень залежності ємнісної характеристики від потужності поля Галуа для програмної реалізації.

Таблиця 7

Залежність швидкості програмної реалізації від потужності поля (кількість групових операцій)

Криптосистеми	$GF(q^m)$					
	2^5	2^6	2^7	2^8	2^9	2^{10}
НККС *MacElis* на *ЕС*	10018042	18048068	32847145	47489784	63215578	**82467897**
МНККС *MacElis* на укорочених *МЕС*	10007947	**17787431**	28595014	44079433	61974253	79554764
МНККС *MacElis* на подовжених *МЕС*	11156138	**18561228**	33210708	48297112	65171690	84051337

Таблиця 8

Залежність швидкості програмної реалізації від потужності поля (кількість групових операцій)

Криптосистеми	$GF(q^m)$						
	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}
МНККС *MacElis* на укорочених *МЕС*	8293075	10007947	**17787431**	28595014	44079433	61974253	79554764
МНККС *MacElis* на подовжених *МЕС*	8506422	11156138	**18561228**	33210708	48297112	65171690	84051337
ГККК3К подовжених *МЕС*	**5612316**	7900315	14892945	25565274	42279183	58963778	76564173
ГККК3К укорочених *МЕС*	**5942627**	7905257	14682411	25595014	42116327	58468143	75474764

У табл. 9 наведені результати досліджень статистичних властивостей запропонованих методів на основі пакета *NIST STS* 822.

Таблиця 9

Результати дослідження статистичної безпеки

Криптосистеми	Кількість тестів, в яких тестування пройшли більше 99% послідовностей	Кількість тестів, в яких тестування пройшли більше 96% послідовностей	Кількість тестів, в яких тестування пройшли менше 96% послідовностей
НККС *MacElis*	149 (78,83%)	189 (100%)	0 (0%)
МНККС *MacElis* на укорочених *МЕС*	151 (79,89%)	189 (100%)	0 (0%)
МНККС *MacElis* на подовжених *МЕС*	152 (80,42%)	189 (100%)	0 (0%)
ГККК3К на подовжених *МЕС*	**153 (80,95%)**	189 (100%)	0 (0%)
ГККК3К на укорочених *МЕС*	**155 (82 %)**	189 (100%)	0 (0%)

Табл. 9 продемонструвала, що не зважаючи на зменшення потужності поля Галуа до $GF(2^6)$ для МНККС і $GF(2^4)$ для ГКККЗК, статистичні характеристики таких крипто-кодових конструкцій виявилися, як мінімум, не гірше традиційних НККС Мак-Еліса на $GF(2^{10})$. Всі криптосистеми пройшли 100% тестів, причому найкращий результат показала ГКККЗК на укорочених *MEC*: 155 з 189 тестів пройдено на рівні 0,99, що становить 82% від усієї кількості тестів. При цьому традиційна НККС Мак-Еліса на $GF(2^{10})$ показала 149 тестів на рівні 0,99. Таким, чином запропоновані методи забезпечують основні послуги безпеки, необхідний рівень стійкості та достовірності БІР.

У четвертому розділі наведено результати досліджень, одержаних на основі удосконаленого методу оцінювання безпеки БІР, який, на відміну від відомих, враховує комплексний показник ефективності інвестицій, що виділяються на забезпечення безпеки БІР, для оптимізації витрат на її побудову в умовах впливу гібридних загроз ІБ, КБ та БІ.

У формалізованому вигляді модель оцінювання безпеки БІР на основі комплексного показника ефективності інвестицій пропонується описати виразом:

$$W_{ABS}^{effinv} = \begin{Bmatrix} I_{O^{ABS}}, \Delta^{ABS}, \{DF^{ABS}\}, rang^{ABS}, \{SZ^{ABS}\}, d^{ABS}, D^{ABS} \\ ROI^{ABS}, NPV^{ABS}, ROSI^{ABS}, r^{ABS}, CV^{ABS}, OU^{ABS} \end{Bmatrix}, \quad (17)$$

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

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

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

$$ROI^{ABS} = NPV_{inv}^{ABS} - NPV_{zt}^{ABS}, \quad (18)$$

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

Крок 2. Оцінювання рентабельності інвестицій в ТЗЗІ:

$$ROSI^{ABS} = NPV_{zbtszi}^{ABS} - NPV_{zvtszi}^{ABS}, \quad (19)$$

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

Крок 3. Оцінювання чистої зведеної вартості:

$$NPV_{zvtszi}^{ABS} = C_{sz} + \sum_{i=1}^{N} \frac{ALE_i}{(1+r)^i}, \tag{20}$$

де N – кількість інтервалів інвестування; ALE_i – очікувані витрати в i-му періоді; r – ставка дисконтування; C_{sz} – вартість засобів захисту.

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

$$ALE^{ABS} = \sum_{i=1}^{n} I\left(O_{DF}^{ABS}\right) F_i, \tag{21}$$

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

Крок 5. Оцінювання потенційних збитків U^{ABS} інформаційного активу БІР з урахуванням виразу (10):

$$U^{ABS} = p_{rj} u_j, \tag{22}$$

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

Крок 6. Оцінювання загального очікуваного збитку:

$$OU^{ABS} = \sum_{j=1}^{n} U^{ABS}. \tag{23}$$

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

$$M^{ABS} = \sum_{i=1}^{m} C_i, \tag{24}$$

де C_i – вартість i-го заходу; m – загальна кількість вжитих заходів.

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

$$W_{ABS}^{effinv} = \sum_{i=1}^{N} w_i M^{ABS}, \tag{25}$$

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

Запропонований метод, на відміну від відомих, дозволяє оптимізувати витрати коштів на побудову системи безпеки БІР в умовах впливу гібридних загроз при одночасному забезпеченні заданого рівня їх безпеки.

Для оцінювання якості обслуговування об’єктів АБС щодо забезпечення безпеки БІР запропонована методика оцінки функціональної ефективності обміну даними в мережі АБС, що ґрунтується на простому багатофакторному аналізі, у ній враховуються як технічні показники мережі (швидкість передачі даних, імовірність і

час доставки пакета та ін.), показники безпеки технічних засобів захисту інформації, так і економічні параметри (вартість масштабування, обслуговування мережі, ефективність інвестицій в безпеку і т.п.). Методика містить чотири етапи. Перший етап передбачає визначення стійкості криптосистем методом експрес-аналізу на основі ентропійного методу оцінки випадковості вихідної послідовності, другий – визначення впливу загроз на складові безпеки (ІБ, КБ, БІ) з урахуванням їх гібридності і синергізму, третій – визначення комплексного показника ефективності інвестицій в забезпечення безпеки БІР при заданому рівні їх захищеності, четвертий – визначення ефективності обміну даними в АБС.

1 етап. Визначення стійкості криптосистем методом експрес-аналізу на основі ентропійного методу оцінки випадковості вихідної послідовності. Результатом досліджень є таблиця оцінки максимального рівня криптографічного захисту БІР (табл. 10).

Таблиця 10

Оцінка максимального криптографічного захисту інформації

№	Шифр	Ентропія відкр. тексту (H_M)	Ентропія криптограми (H_C)	Різниця $H_{Cypher} = H_C - H_M$	Ймовірність криптозахисту, P_c
1.	Клітинні автомати, правило “60”	0,5023775 (5,023775)	0,6820179 (6,820179)	0,1796404 (1,796404)	0,637079949
2.	генератор ПВП Secure *Random*	0,5023767 (5,023767)	0,7999982 (7,999982)	0,2976215 (2,976215)	0,747287753
3.	*DES*	0,469276	0,812043	0,342767	0,812043
4.	3*DES*	0,469276	0,812043	0,342767	0,812043
5.	ГОСТ 28147-2009	0,469276	0,811348	0,342072	0,811348
6.	Калина-256	0,469276	0,954519	0,485243	0,954519
7.	*AES*-256	0,469276	0,95454	0,485264	0,95454
8	*RSA*	0,469276	1,000	0,530724	1,000
9	ГККЗК з *MEC (HCCDC)*	0,469276	0,98764	0,518364	0,98764
10	Ідеальний шифр		1,000		1,000

2 етап. Визначення ступеня впливу загроз на складові безпеки (ІБ, КБ, БІ) з урахуванням їх гібридності і синергізму. На основі класифікатора, з урахуванням виразів (1)–(5) визначається узагальнена синергетична ймовірність реалізації атаки на БІР $W_{synerg}^{IB,KB,BI}$. Стійкість системи безпеки в АБС до можливих дій зловмисника визначається таким чином:

$$B = P_C \times W_{synerg}^{IB,KB,BI}, \tag{26}$$

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

3 етап. Визначення комплексного показника ефективності інвестицій в забезпечення безпеки БІР. На основі виразів (17)–(23) і запропонованої методики

визначається комплексний показник ефективності інвестицій в забезпечення безпеки БІР – W_{effinv}.

4 етап. Визначення ефективності обміну даними в АБС на основі комплексного показника. Оцінка ефективності обміну даними здійснюється на основі комплексного показника за виразом:

$$W(u_i) = \frac{n^{(u_i)} - t^{(u_i)}}{n^{(u_i)}} \times B^{(u_i)} \times P_{np.n}{}^{(u_i)} \times W_{effinv} \times W_{norm}, \qquad (27)$$

де $W(u_i)$ – показник ефективності мережі для обраної стратегії u_i; $n^{(ui)}$ – кількість інформаційних розрядів пакета для обраної стратегії u_i; $t^{(ui)}$ – час доставки пакета t для обраної стратегії u_i; $B^{(ui)}$ – стійкість системи безпеки в АБС; $P_{np\,n}{}^{(ui)}$ – достовірність правильної доставки пакета для обраної стратегії; U – множина допустимих стратегій (методів підвищення достовірності доставки пакетів); $W_{eff}{}^{(ui)}$ – комплексний показник ефективності інвестицій в забезпечення безпеки банківських інформаційних ресурсів; W_{norm} – нормований багатофакторний показник ефективності.

На рис. 6 наведені результати досліджень $W(u_i)$. Вихідними даними для проведення досліджень є: технології *Frame Relay*, 100 *Mbit Ethernet*, 10 *Gbit Ethernet*, 40 *Gbit Ethernet* з розв'язувальним зворотним зв'язком і *ARQ* "Повернення-на-*N*", $W_{synerg}^{IB,KB,BI}$ = 0.0022839, БСШ *Gost* – $t_{ш,\,рш}$ = 0,033 с, *RSA* – $t_{ш,\,рш}$ = 0,2 с, ГККЗК з *MEC* – $t_{ш,\,рш}$ = 0,0015 с, P_C^{Gost} = 0,95454, P_C^{HCCDC} = 0,98764, P_C^{RSA} = 1,0000, n = 1518, C = 36000, $P_{np.n}$ = 0,9999, s = 32, w = 300000000.

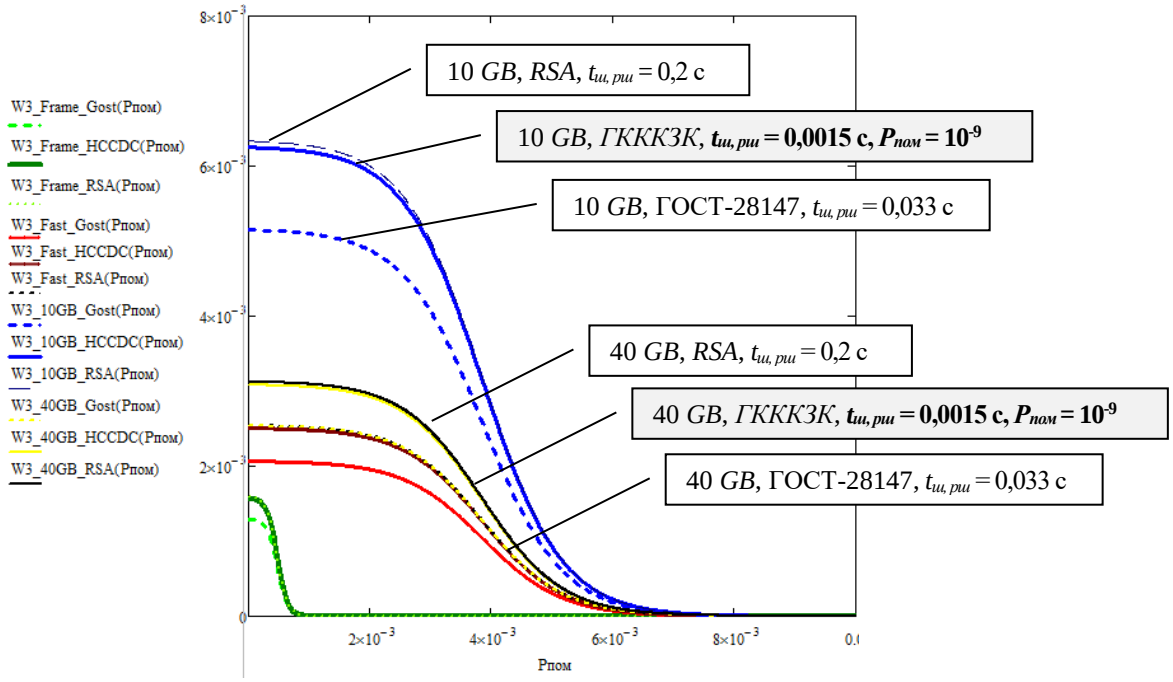


Рис. 6. Результати досліджень функціональної ефективності АБС з протоколом *ARQ* "Повернення-на-*N*"

Аналіз результатів рис. 6 показав, що запропонована методика оцінювання функціональної ефективності АБС дозволяє без значних часових і експертних витрат дослідити стан якості обслуговування користувачів АБС, використовувати результати оцінки для її масштабування, поліпшення технічних показників АБС та рівня захищеності БІР.

У **заключному розділі** дисертації розроблено методологію побудови системи безпеки БІР, приклад реалізації для ОБС України наведено на рис. 7.

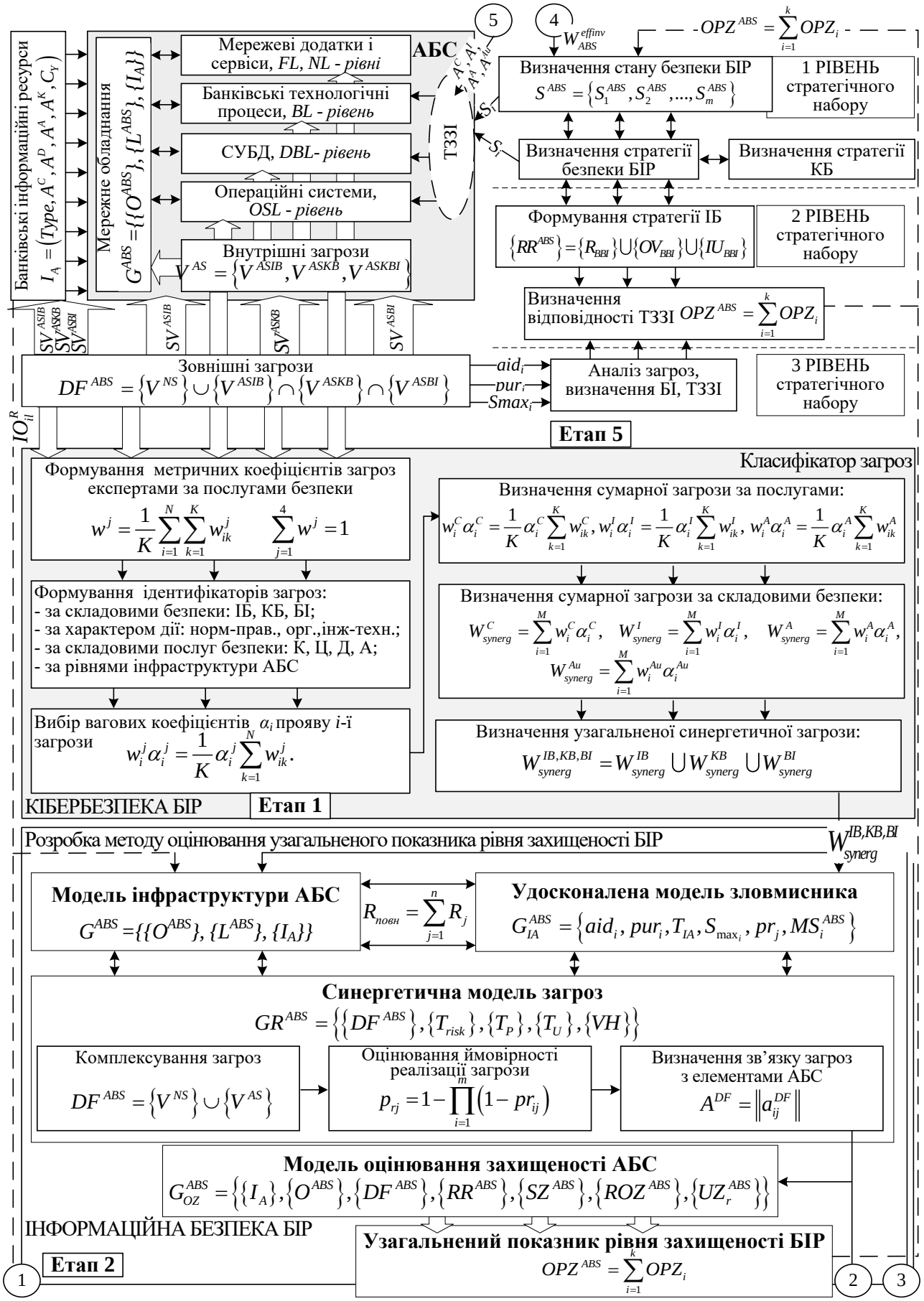
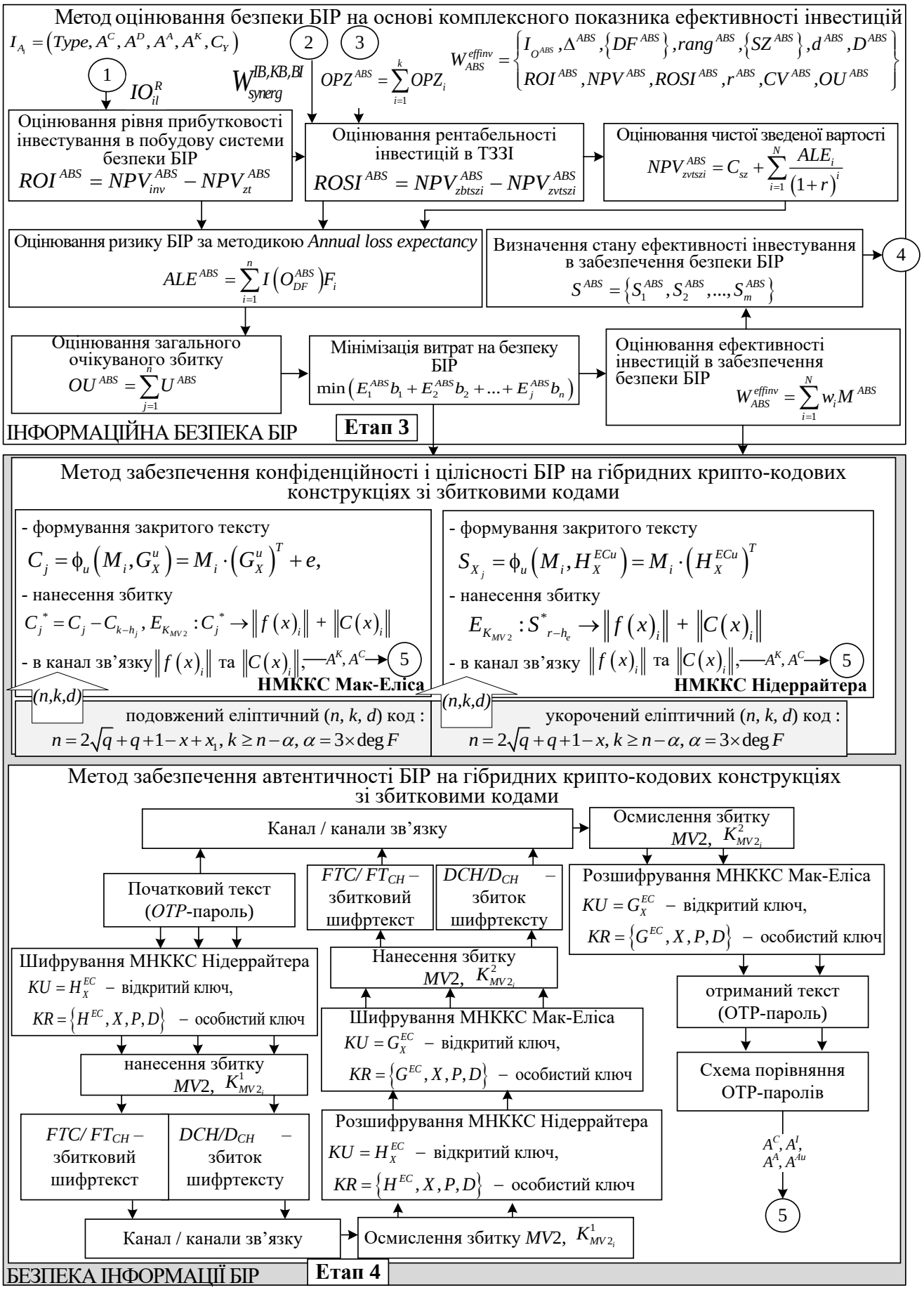


Рис. 7. Схема методології побудови системи безпеки банківських інформаційних ресурсів



Продовження рис. 7. Схема методології побудови системи безпеки банківських інформаційних ресурсів

Розроблена методологія (рис. 7) реалізується за такими базовими етапами: 1) визначення ймовірності впливу загроз ІБ, КБ, БІ на безпеку БІР за виразами (1) – (5) і табл. 1, 2; 2) визначення узагальненого показника рівня захищеності БІР згідно з (6) – (15); 3) оцінювання ефективності інвестицій у забезпечення безпеки БІР згідно з вимогами (17) – (25) та табл. 10; 4) побудова інтегрованих механізмів забезпечення конфіденційності, цілісності, автентичності та достовірності БІР, відповідно до (16) та табл. 3 – 9; 5) визначення стану та формування стратегій безпеки БІР відповідно до вимог (14), (15).

Реалізація методології, з урахуванням розроблених у дисертації методів і засобів, дасть можливість забезпечити підвищення рівня захищеності БІР в умовах дії гібридних загроз, раціональну організацію системи забезпечення безпеки БІР в умовах одночасної дії на систему загроз інформаційній безпеці, кібербезпеці та безпеці інформації. Такий підхід дозволяє одержати повноцінну та адекватну оцінку рівня безпеки БІР, що суттєво впливає на величину інвестицій в безпеку банківського сектору та відкриває шляхи до прийняття обґрунтованих управлінських рішень з питань забезпечення безпеки. Крім того, використання ГККЗК дозволить гарантувати послуги безпеки при заданих їх ймовірнісних показниках – швидкість криптоперетворень на рівні швидкості криптоперетворень у БСШ, криптостійкість на рівні 10^{25}–10^{35} групових операцій, достовірність передачі БІР відкритими каналами зв’язку не нижче $P_{пом}$ 10^{-9}–10^{-12}.

ВИСНОВКИ

У дисертації вирішена актуальна науково-прикладна проблема створення методології побудови системи безпеки банківських інформаційних ресурсів для підвищення рівня їх захищеності від загроз безпеці гібридного характеру, що має важливе значення для подальшого розвитку галузі інформаційної безпеки держави.

У процесі виконання дисертаційної роботи отримані такі основні результати:

1. Проведено аналіз сучасних моделей, методів та систем безпеки банківських інформаційних ресурсів організацій банківського сектору як складової систем з критичною кібернетичною інфраструктурою держави. Встановлено, що переважна більшість відомих досліджень орієнтована на розробку або загальних підходів до безпеки банківських інформаційних ресурсів, або створення методів, моделей та засобів забезпечення на основі моделі *CIA*, що не повною мірою враховує сучасні вимоги й підходи до побудови системи безпеки банківських інформаційних ресурсів. Невирішеними аспектами загальної проблеми захисту банківських інформаційних ресурсів залишаються питання розробки цілісної науково-обґрунтованої методології побудови на практиці системи безпеки банківських інформаційних ресурсів, розробка та впровадження в комплексну систему захисту інформації інтегрованих механізмів *CIA* із забезпеченням вимог до швидкодії та достовірності циркуляції банківських інформаційних ресурсів в автоматизованих банківських системах. Результати проведеного аналізу дали можливість чітко визначити завдання дисертаційного дослідження щодо розробки методології побудови системи безпеки банківських інформаційних ресурсів.

2. Вперше розроблено концепцію побудови синергетичної моделі загроз безпеки банківських інформаційних ресурсів, базис якої становить трирівнева модель

стратегічного управління безпекою банківських інформаційних технологій. Концепція охоплює всі основні напрямки розвитку діяльності банку щодо безпеки банківських інформаційних ресурсів, ґрунтується на синергетичному підході до вибору найбільш ефективних напрямків досягнення цілей безпеки банківських інформаційних ресурсів на кожному з рівнів моделі управління стратегічним управлінням безпеки банківських інформаційних технологій з урахуванням величини ризику на кожному рівні та забезпеченням дієвого контролю за виконанням функцій системи управління інформаційною безпекою організацій банківського сектору.

3. Удосконалено 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 (електронний доступ до ресурсу: http://skl.hneu.edu.ua/).

4. Вперше розроблено метод оцінювання узагальненого показника рівня захищеності банківських інформаційних ресурсів. Розроблено практичну методику для оцінювання рівня захищеності банківських інформаційних ресурсів на основі синергетичної моделі загроз, удосконалених класифікатора загроз та моделі зловмисника, моделі оцінки захищеності банківських інформаційних ресурсів та моделі інфраструктури автоматизованих банківських систем, що дозволяє оптимізувати витрати коштів на побудову системи безпеки банківських інформаційних ресурсів. Практична значимість полягає у можливості своєчасного оцінювання взаємозв'язків між активами банківських інформаційних ресурсів, елементами інфраструктури, технічними засобами захисту автоматизованих банківських систем і можливими проявами загроз інформаційній безпеці, кібербезпеці та безпеці інформації, що дозволяє своєчасно корегувати керівні документи банку з інформаційної безпеки, планувати інвестування в технічні засоби захисту інформації, формувати превентивні заходи для недопущення реалізації загроз.

5. Вперше розроблено метод забезпечення конфіденційності та цілісності банківських інформаційних ресурсів на гібридних крипто-кодових конструкціях зі збитковими кодами. Метод базується на модифікованій крипто-кодовій системі Мак-Еліса на модифікованих алгеброгеометричних кодах, що інтегровано (одним механізмом) забезпечує безпеку банківських інформаційних ресурсів (безпечний час – $T_Б$> 200 р., стійкість до криптоаналізу P_K <10^{25}–10^{35} групових операцій), достовірність передачі банківських інформаційних ресурсів в автоматизованих банківських системах ($P_{пом}$ <10^{-9}) та зменшення енергетичних витрат на їх практичну реалізацію в 10 – 12 разів (шифрування, розшифрування) за рахунок зменшення порядку *GF (q)*. Впровадження запропонованого методу дозволяє підвищити рівень захищеності

банківських інформаційних ресурсів та забезпечити своєчасне реагування на вимоги міжнародних і національних регуляторів безпеки банківських інформаційних ресурсів за рахунок зміни окремих параметрів та модифікації застосування модифікованих крипто-кодових систем Мак-Еліса і Нідеррайтера з системами багатоканальної криптографії на збиткових кодах.

6. Вперше розроблено метод двофакторної автентифікації на гібридних крипто-кодових конструкціях зі збитковими кодами на основі модифікованих крипто-кодових систем Мак-Еліса і Нідеррайтера з *MEC*, що дозволяє забезпечити рівень стійкості *OTP*-паролів при передачі відкритими каналами зв'язку та зберегти можливість подальшого використання протоколу двофакторної автентифікації на основі *SMS*-повідомлень. Не зважаючи на зменшення потужності поля Галуа до $GF(2^6)$ для модифікованих крипто-кодових систем і $GF(2^4)$ для гібридних крипто-кодових конструкцій на збиткових кодах, статистичні характеристики таких крипто-кодових конструкцій виявилися, як мінімум, не гірше традиційних схем Мак-Еліса над $GF(2^{10})$. Всі криптосистеми пройшли 100% тестів, причому найкращий результат показала гібридна крипто-кодова конструкція на укорочених *MEC*: 155 з 189 тестів пройдено на рівні 0,99, що становить 82% від усієї кількості тестів. При цьому традиційна схема Мак-Еліса на $GF(2^{10})$ показала 149 тестів на рівні 0,99.

7. Набув подальшого розвитку метод оцінювання безпеки банківських інформаційних ресурсів, що на, відміну від відомих, враховує комплексний показник ефективності інвестицій, які виділяються на забезпечення безпеки банківських інформаційних ресурсів, що дозволяє оптимізувати витрати коштів на її побудову в умовах впливу гібридних загроз при одночасному забезпеченні заданого рівня їх безпеки. Практична реалізація методу дозволяє комплексно оцінювати основні показники інвестування в забезпечення безпеки банківських інформаційних ресурсів з урахуванням синергетичного оцінювання загроз інформаційній безпеці, кібербезпеці та безпеці інформації.

8. Вперше розроблено методологію побудови системи безпеки банківських інформаційних ресурсів, яка, на відміну від відомих підходів, реалізує принципово нову концепцію протидії гібридним загрозам банківському сектору держави. Її сутність та зміст полягають в раціональній організації системи безпеки банківських інформаційних ресурсів в умовах одночасної дії на систему загроз інформаційній безпеці, кібербезпеці та безпеці інформації. Такий підхід дозволяє одержати повноцінну та адекватну оцінку рівня захищеності банківських інформаційних ресурсів, що суттєво впливає на величину інвестицій в забезпечення безпеки банківського сектору та відкриває шляхи до прийняття обґрунтованих управлінських рішень з питань забезпечення безпеки банківських інформаційних ресурсів. Практичне використання методології дозволяє забезпечити виконання всього функціоналу системи управління інформаційною безпекою банку на принципово новому підході до оцінювання ймовірності впливу загроз інформаційній безпеці, кібербезпеці та безпеці інформації на безпеку банківських інформаційних ресурсів, без значних часових та експертних витрат на проведення їх оцінювання і аналіз, забезпечити раціональне інвестування в інформаційну безпеку організацій банківського сектору.

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

9. Розроблено алгоритмічне забезпечення та програмні застосунки, що дозволило верифікувати запропоновані методи, моделі та методологію і підтвердити їх ефективність у контексті безпеки банківських інформаційних ресурсів. Результати дисертації впроваджено в діяльність ТОВ "Сайфер БІС" – реалізовані програмні бібліотеки криптографічних перетворень інформації на основі модифікованих крипто-кодових систем Нідеррайтера – Мак-Еліса на еліптичних кодах з відкритим ключем на основі збиткових кодів. Розроблені програмні бібліотеки криптографічних перетворень інформації використано у підсистемі автентифікації Інтернет-банкінгу "*ELPay*" (Акт від 18.05.2017), "Мікрокріпт Текнолоджіс" – розроблені бібліотеки криптографічних перетворень інформації використано у програмному комплексі захисту миттєвих повідомлень "*Crypto-IM+*" (акт впровадження від 30.11.2017), планується використання в банківській установі у складі перспективного протоколу 2*FA* спільно з ТОВ "ТАНТАРІУМ" (Акт від 14.06.2017), та "МЕГАБАНК" Публічне акціонерне товариство (Акт від 9.06.2017). Результати дисертаційної роботи використовуються у навчальному процесі Харківського національного економічного університету ім. С. Кузнеця, Харківського національного університету "ХПІ", Чернівецького національного університету ім. Ю. Федьковича для підвищення рівня ефективності підготовки фахівців з інформаційної безпеки, безпеки інформації.

ОСНОВНІ ПУБЛІКАЦІЇ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. О. О. Кузнецов, С. П. Євсеєв, С. В. Кавун, та О. Г. Король, *Сигнали і коди. Алгебраїчні методи синтезу*. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.

2. О. О. Кузнецов, С. П. Євсеєв, та С. В. Кавун, *Захист інформації та економічна безпека підприємства*. Монографія. Харків, Україна: Вид. ХНЕУ, 2009.

3. С. П. Євсеєв, О. Ю. Йохов, та О. Г. Король *Гешування даних в інформаційних системах*. Монографія. Харків, Україна: Вид. ХНЕУ, 2013.

4. С. П. Евсеев, и О. Г. Король, "Исследование коллизионных свойств кодов аутентификации сообщений UMAC", *Информационные технологии и системы в управлении, образовании, науке*. Коллективная монография [под. редакцией В. С. Пономаренко]. Харків, Україна: Цифрова друкарня, с. 25 – 38, 2013.

5. С. П. Евсеев, и Т. А. Свердло, “Исследование угроз методов двухфакторной аутентификации”, *Информационные технологии и защита информации в информационно-коммуникационных системах*: Коллективная монография [под. редакцией В. С. Пономаренка]. Харків, Україна: Вид-во ТОВ “Щедра садиба плюс”, с. 141 – 154, 2015.

6. С. П. Евсеев, та О. Г. Король, “Синергетические модели оценки безопасности в автоматизированных банковских системах”, *Інформаційні технології: проблеми та перспективи*. Колективна монографія [за заг. ред. В. С. Пономаренка]. Харків, Україна: Вид. Рожко С. Г., с. 203 – 221, 2017.

7. С. П. Евсеев, Г. П. Коц, и И. П. Отенко, “Методология построения модифицированной системы электронного документооборота в университете на основе электронной цифровой подписи стандарта X.509”, *Моделирование процессов управления в информационной экономике*. Колективна монографія [Под ред. докт. экон. наук, проф. В. С. Пономаренка, докт. экон. наук, проф. Т. С. Клебановой] – Бердянск, Україна: видавник Ткачук А. В., с. 264 – 295, 2017.

8. С. Евсеев, и А. Дорохов, “Информационные угрозы и безопасность в банковских платежных системах Украины”, *Криминологический журнал БГУЭП*, вип. 2, с. 68 – 75, 2011. *(Scopus)*

9. С. Евсеев, и В. Абдулаев, “Алгоритм мониторинга метода двухфакторной аутентификации на основе системы Passwindow”, *Восточно-европейский журнал передовых технологий*, вып. 2/2(74), с. 9 – 15, 2015. *(Scopus)*

10. С. Евсеев, О. Король, и Г. Коц, “Анализ законодательной базы к системе управления информационной безопасностью НСМЭП”, *Восточно-европейский журнал передовых технологий*, вып. 5/3(77), с. 48 – 59, 2015. *(Scopus)*

11. С. Евсеев, О. Король, Х. Рзаев, и 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. *(Scopus)*

12. S. Yevseiev, H. Kots, and Y. Liekariev, “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 *(Scopus)*

13. С. Євсеєв, С. Остапов, Х. Рзаєв, та В. Ніколаєнко, “Оцінка обміну даними в глобальних обчислювальних мережах на основі комплексного показника якості обслуговування мережі”, *Науковий журнал Радіоелектроніка, інформатика, управління*, № 1(40), с. 115 – 128, 2017. *(Web of Science)*

14. S. Yevseiev, O. Korol, and H. Kots, “Construction of hybrid security systems based on the crypto-code structures and flawed codes”, *Восточно-европейский журнал передовых технологий*, 4/9(88), с. 4 – 20, 2017. *(Scopus)*

15. S. Yevseiev, H. Kots, S. Minukhin, O. Korol, and A. Kholodkova, “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 – 35, 2017. *(Scopus)*

16. S. Yevseiev, V. Ponomarenko, and O. Rayevnyeva, “Assessment of functional effectiveness of the corporate scientific-educational network based on comprehensive

indicators of service quality", *Восточно-европейский журнал передовых технологий*, 6/2 (90), с. 4 – 15, 2017. *(Scopus)*

17. С. Евсеев, и О. Король, "Результаты статистического тестирования безопасности и продуктивности хеш-алгоритмов-претендентов конкурса по отбору стандартного алгоритма SHA-3", *Известия Высших технических учебных заведений Азербайджана*. том.14, № 2 (78), с. 73 – 78, 2012.

18. S. Yevseiev, T. Sverdlo, and O. Korol, "Mécanismes intégrés de sécurité et de fiabilité des données dans les systèmes d'information basés sur la théorie des codes correcteurs d'erreurs", *French Journal of Science and Education*, № 2(12), p. 358 – 368, 2014.

19. С. Евсеев, А. Сочнева, О. Король, и В. Абдулаев, "Анализ методик оценки рисков нарушения безопасности банковской информации", *Известия Высших технических учебных заведений Азербайджана*. том.19, № 2 (106), с. 77 – 86, 2017.

20. С. Евсеев, и О. Король, "Метод каскадного формирования МАС-кодов на основе модулярных преобразований", *Известия Высших технических учебных заведений Азербайджана*, № 1 (89), с. 71 – 78, 2014.

21. С. Евсеев, О. Король, и А. Жученко, "Защита информации в интернет-платежных системах", *Восточно-европейский журнал передовых технологий*, 5/2(35), с. 34 – 37. 2008.

22. С. Евсеев, О. Король, и Л. Пархуць, "Разработка модели и метода каскадного формирования МАС с использованием модулярных преобразований" *Захист інформації: науково-технічний журнал*, том 15, № 3, с. 186 – 196, 2013.

23. S. Evseev, "International legislation on personal data protection", *Системи обробки інформації*, № 9(107), с. 140 – 144, 2012.

24. S. Evseev, and B. Tomashevsky, "Two-factor authentication methods threats analysis", *Радіоелектроніка, інформатика, управління*, вип. 1(32), с. 52 – 59, 2015.

25. С. Евсеев, "Синергетический подход к оценке безопасности банковских систем", *Системи обробки інформації*, № 4(141), с. 90 – 103, 2016.

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

27. С. Евсеев, Х. Рзаев, и А. Цыганенко, "Анализ программной реализации прямого и обратного преобразования по методу недвоичного равновесного кодирования", *Науково-технічний журнал "Безпека інформації"*, том 22, № 2, с. 196 – 203, 2016.

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

29. С. Евсеев, "Модель нарушителя прав доступа в автоматизированной банковской системе на основе синергетического подхода", *Науково-технічний журнал "Інформаційна безпека"*, № 2 (26), с. 110 – 119, 2017.

30. С. Евсеев, "Оценка эффективности инвестиций в безопасность организаций банковского сектора на основе синергетической модели угроз", *Системи обробки інформації*, № 2 (148), с. 88 – 94, 2017.

31. С. Євсеєв, С. Остапов, та Р. Королев, “Використання міні-версій для оцінки стійкості блоково-симетричних шифрів”, *Науково-технічний журнал “Безпека інформації”,* том 23, № 2, с. 100 – 108, 2017.

32. 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.

33. С. Євсеєв, “Анализ методов построения универсальных классов хеш-функций”, *Вісник Державного університету інформаційно-комунікаційних технологій*, том 7 (№ 4), с. 337 – 345, 2009.

34. С. Евсеев, О. Король, и А. Гончарова, “Построение моделей атак на внутриплатежные банковские системы”, *Радіоелектроніка, інформатика, управління*, вип. 1(22), с. 56 – 66, 2010.

35. С. Евсеев, и Б. Томашевский, “Исследование теоретико-кодовых схем для комплексного обеспечения безопасности и достоверности данных в информационных системах”, *Науковий вісник Чернівецького університету. Серія: Комп’ютерні системи та компоненти*, том 2, вип.1, с. 6 – 14, 2011.

36. А. Кузнецов, О. Король и С. Евсеев, “Исследование коллизионных свойств кодов аутентификации сообщений UMAC”, *Прикладная радиоэлектроника*, том 11, № 2, с. 171 – 183, 2012.

37. С. Евсеев, О. Король, и Н. Суханова, “Анализ угроз и механизмов защиты во внутриплатежных системах коммерческого банка”, *Науково-практичний журнал “Сучасна спеціальна техніка”*, 1(24), с. 49 – 60, 2011.

38. С. Евсеев, “Анализ защиты в национальной системе массовых электронных платежей”, *Інформаційна безпека*, № 3(15), с. 15 – 28, 2014.

39. С. Евсеев, О. Король, и А. Сочнева, “Анализ оценки рисков кибербезопасности банковской информации”, *Сборник научных трудов НАУ “Защита информации”*, вып. 23, с. 109 – 128, 2016.

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

41. С. Євсеєв, О. Андрощук, та В. Федорченко, “Побудова систем безпеки інформаційно-телекомунікаційних систем на основі комплексного крипто-графічного 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. 258 – 268, 2017.

42. С. Євсеєв, та О. Король, “Дослідження загроз методів двофакторної автентифікації”, *Вісник національного університету “Львівська політехніка”*, № 806, с. 62 – 71, 2014.

43. С. Евсеев, Ю. Хохлачева, и О. Король, “Оценка обеспечения непрерывности бизнес-процессов в организациях банковского сектора на основе синергетического подхода, ч.1”, *Сучасна спеціальна техніка. Науково-практичний журнал*, № 1(48), с. 17 – 25. 2017.

44. С. Евсеев, Ю. Хохлачева, и О. Король, “Оценка обеспечения непрерывности бизнес-процессов в организациях банковского сектора на основе

синергетического подхода, ч. 2", *Сучасна спеціальна техніка. Науково-практичний журнал*, № 2(49), с. 10 – 17, 2017.

45. С. Евсеев, Р. Грищук, и О. Король, "Анализ современных методов выявления кибератак на ресурсы коммуникационных систем", *Науково-практична конференція "Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі"*, Харків, 2016, с. 9.

46. С. Евсеев, и И. Белодед, "Крипто-кодовая система на модифицированных кодах", *V Міжнародна науково-технічна конференція "Методи та засоби кодування, захисту й ущільнення інформації"*, Вінниця, 2016, с. 47 – 50.

47. С. Евсеев, "Методология оценивания безопасности информационных технологий автоматизированных банковских систем", *III Міжнародна науково-практична конференція "Актуальні питання забезпечення кібербезпеки та захисту інформації"*, Київ, 2017, с. 75 – 76.

48. С. Евсеев, и О. Король, "Модель нарушителя прав доступа в автоматизированной банковской системе на основе синергетического подхода", *Друга Міжнародна науково-практична конференція "Проблеми науково-технічного та правового забезпечення кібербезпеки у сучасному світі"*, Харків, 2017, с. 23.

49. С. Євсеєв, та О. Король, "Комплексний показник ефективності інвестицій в безпеку банківської інформації на основі синергетичної моделі загроз", *VI Міжнародна наукова конференція "Інформація, комунікація, суспільство 2017"*, Славське, 2017, с. 18 – 19.

50. С. Евсеев, и О. Король, "Классификатор угроз на основе синергетического подхода", *VII міжнародна науково-технічна конференція "ITSEC: Безпека інформаційних технологій"*, Київ, 2017, с. 83 – 84.

51. С. Євсеєв, "Математичні моделі модифікованої несиметричної крипто-кодової системи Мак-Еліса на модифікованих еліптичних кодах", *Міжнародна науково-практична конференція "Інформаційні технології та комп'ютерне моделювання"*, Івано-Франківськ, 2017, с. 192 – 196.

52. С. Евсеев, и О. Король, "Математическая модель протокола обмена данными на основе модифицированных несимметричных крипто-кодовых систем Мак-Элиса и Нидеррайтера на ущербных кодах", *VII міжнародна науково-технічна конференція "Захист інформації і безпека інформаційних систем"*, Львів, 2017, с. 89 – 90.

53. С. Євсеєв, та І. Білодід, "Використання збиткових кодів в гібридних крипто-кодових конструкціях", *П'ята міжнародна науково-технічна конференція "Проблеми інформатизації"*, Черкаси – Баку – Бельсько-Бяла – Полтава, 2017, с. 11.

54. С. Євсеєв, та О. Андрощук, "Система безпеки інформаційно-телекомунікаційних систем на основі комплексного криптографічного підходу", *X Всеукраїнська науково-практична конференція "Освітньо-наукове забезпечення діяльності складових сектору безпеки і оборони України",* Хмельницький, 2017, с. 268 – 269.

АНОТАЦІЯ

Євсеєв С. П. Методологія побудови системи безпеки банківських інформаційних ресурсів. – Рукопис.

Дисертація на здобуття наукового ступеня доктора технічних наук за спеціальністю 21.05.01 – "Інформаційна безпека держави". – Національний авіаційний університет, Київ, 2018.

У роботі запропоновано концепцію побудови синергетичної моделі загроз безпеці БІР, базис якої складає трирівнева модель стратегічного управління безпекою інформаційних технологій в АБС. Розроблена синергетична модель загроз безпеки БІР, що дозволила удосконалити відому модель зловмисника безпеки БІР та надало можливості встановлення взаємозв'язків між елементами інфраструктури АБС, комунікаційними каналами, БІР та загрозами й досягти синергетичного ефекту. Розроблено класифікатор загроз безпеці БІР, який ґрунтується на синергетичній моделі загроз, що дозволить класифікувати загрози за складовими безпеки, видами послуг та рівнями ієрархії інфраструктури АБС. Для протидії гібридним загрозам БІР доцільно застосовувати нові інтегровані механізми забезпечення послуг на основі ГКККЗК, що дозволило гарантувати послуги безпеки й достовірність при заданих їх ймовірнісних показниках. Удосконалений метод двофакторної автентифікації на основі ГКККЗК дозволяє гарантувати безпеку і достовірність передачі *OTP*-паролів. Розроблено метод оцінювання безпеки БІР, який враховує комплексний показник ефективності інвестицій, що дозволяє оптимізувати витрати коштів на забезпечення безпеки БІР. Розроблена методика оцінювання функціональної ефективності АБС враховує технічні показники мережі, показники безпеки ТЗЗІ та економічні параметри. Розроблено методологію побудови системи безпеки БІР, яка дозволяє в умовах зростання гібридних загроз відкрити новий з позицій безпеки та ефективний з позицій витрачених коштів підхід до побудови системи безпеки критичної інформаційної інфраструктури держави.

Ключові слова: безпека банківських інформаційних ресурсів, автоматизована банківська система, синергетична модель загроз безпеці БІР, класифікатор загроз безпеці БІР, інформаційна безпека, кібербезпека, безпека інформації, інвестиції, емерджентні властивості, синергетичний ефект, гібридні крипто-кодові конструкції на збиткових кодах, модифіковані еліптичні коди, методологія.

АННОТАЦИЯ

Евсеев С. П. Методология построения системи безопасности банковских информационных ресурсов. – Рукопись.

Диссертация на соискание ученой степени доктора технических наук по специальности 21.05.01 – "Информационная безопасность государства". – Национальный авиационный университет, Киев, 2018.

Диссертационная работа посвящена решению актуальной научно-практической проблемы создания методологии построения системы безопасности банковских информационных ресурсов на основе разработанных теоретических основ, методов, моделей и средств защиты критических информационных систем банковского сектора государства.

В работе предложена концепция построения синергетической модели угроз безопасности банковских информационных ресурсов, базис которой составляет трехуровневая модель стратегического управления безопасностью информационных технологий в автоматизированных банковских системах, что позволяет рационально организовать построение системы безопасности банковских информационных ресурсов в условиях одновременного воздействия на систему угроз информационной безопасности, кибербезопасности и безопасности информации.

Разработана синергетическая модель угроз безопасности банковских информационных ресурсов, которая позволяет усовершенствовать известную модель злоумышленника безопасности банковских информационных ресурсов, и установить взаимосвязи между элементами и коммуникационными каналами иерархической структуры автоматизированной банковской системы, информационными активами банковских информационных ресурсов с угрозами информационной безопасности, кибербезопасности и безопасности информации, а также достичь синергетического эффекта.

Разработан классификатор угроз безопасности банковских информационных ресурсов, который, в отличие от известных, основывается на синергетической модели угроз, что позволяет классифицировать угрозы по составляющим безопасности, видам услуг и уровням иерархии инфраструктуры автоматизированных банковских систем. Внедрение классификатора позволяет сделать вывод о том, что для противодействия гибридным угрозам на безопасность банковских информационных ресурсов целесообразно применять новые интегрированные механизмы обеспечения конфиденциальности и целостности – гибридные крипто-кодовые конструкции с ущербными кодами на основе модифицированной крипто-кодовой системы Мак-Элиса на модифицированных алгеброгеометрических кодах, что позволяет повысить уровень информационной скрытности и достоверности банковских информационных ресурсов в условиях действия гибридных угроз. Кроме того, усовершенствованный метод обеспечения аутентификации на гибридных крипто-кодовых конструкциях с ущербными кодами на основе модифицированных несимметричных крипто-кодовых систем Мак-Элиса и Нидеррайтера с модифицированными алгеброгеометрическими кодами позволяет повысить уровень информационной скрытности и достоверности *OTP*-паролей в протоколе двухфакторной аутентификации. Разработан метод оценки безопасности банковских информационных ресурсов, который учитывает комплексный показатель эффективности инвестиций, выделяемых на обеспечение безопасности банковских информационных ресурсов, и позволяет оптимизировать затраты средств на ее создание в условиях воздействия гибридных угроз при одновременном обеспечении заданного уровня их безопасности. Также разработана методика оценки функциональной эффективности автоматизированных банковских систем, которая основывается на простом многофакторном анализе, и учитывает как технические показатели сети (скорость передачи данных, вероятность и время доставки пакета и др.), показатели безопасности технических средств защиты информации, так и экономические параметры (стоимость масштабирования, обслуживание сети, эффективность инвестиций в обеспечение безопасности банковских информационных ресурсов и т.п.). Разработана методология построения

системы безопасности банковских информационных ресурсов, которая позволяет, в условиях роста гибридных угроз, открыть новый, с позиций безопасности, и эффективный, с точки зрения затраченных средств, подход к созданию системы безопасности критической информационной инфраструктуры государства.

Реализация методологии, на основе разработанных в диссертации методов и средств, позволяет обеспечить повышение уровня защищенности банковских информационных ресурсов в условиях действия гибридных угроз на организации банковского сектора, рациональную организацию системы обеспечения безопасности банковских информационных ресурсов, в условиях одновременного действия на систему угроз информационной безопасности, кибербезопасности и безопасности информации.

Такой подход позволяет получить полноценную и адекватную оценку уровня защищенности банковских информационных ресурсов, что существенно влияет на величину инвестиций в обеспечение безопасности банковских информационных ресурсов и открывает пути к принятию обоснованных управленческих решений в вопросах обеспечения безопасности банковских информационных ресурсов. Кроме того, использование гибридных крипто-кодовых конструкций на ущербных кодах позволяет гарантировать услуги безопасности при заданных их вероятностных показателях – скорость криптопреобразования на уровне криптопреобразований в блочно-симметричных шифрах, криптостойкость на уровне $10^{25} – 10^{35}$ групповых операций, достоверность передачи банковских информационных ресурсов открытыми каналами связи с $P_{ош}$ не ниже $10^{-9} – 10^{-12}$.

Ключевые слова: безопасность банковских информационных ресурсов, автоматизированная банковская система, синергетическая модель угроз безопасности банковских информационных ресурсов, классификатор угроз безопасности банковских информационных ресурсов, информационная безопасность, кибербезопасность, безопасность информации, инвестиции, эмерджентные свойства, синергетический эффект, гибридные крипто-кодовые конструкции на ущербных кодах, модифицированные эллиптические коды, методология.

ABSTRACT

Yevseiev S. Methodology for building a security system for banking information resources. – Manuscript.

Thesis for a Doctor of Technical Sciences degree in specialty 21.05.01 – “Information Security of the State”. – National Aviation University, Kyiv, 2018.

The paper proposes the concept of constructing a synergetic model of threats to the security of banking information resources, the basis of which is a three-level model of strategic management of information technology security in automated banking systems. A synergetic model of threats to the security of banking information resources has been developed, which has made it possible to generalize a known model of a cybercriminal and allows to establish interrelations between elements, communication channels, banking information resources and achieve a synergistic effect. A classifier of threats to the security of banking information resources was developed, based on a synergetic threat model, which allowed to classify threats by security components, types of services and

levels of the hierarchy of the ABS infrastructure. To counter the hybrid threats of banking information resources, it is advisable to apply new integrated service provision mechanisms based on hybrid crypto-code constructions on the defective codes. This approach allows us to provide security services and reliability for given probabilistic indicators. The advanced method of two-factor authentication based on hybrid crypto-code constructions on the defective codes makes it possible to ensure the security and reliability of OTP password transmission. The developed method of assessing investments in building the security system of banking information resources allows to optimize the costs of funds for the formation of a security system for banking information resources. A methodology for evaluating the functional efficiency of automated banking systems is developed, taking into account the technical indicators of the network, the safety indicators of technical means of information protection, and economic parameters. A methodology for building a security system for banking information resources was developed. The methodology allows, in conditions of growth of hybrid threats, to open a new effective approach to building the security system of the critical information infrastructure of the state.

Keywords: security of banking information resources, automated banking system, a synergetic model of threats to the security of banking information resources, a classifier of threats to the security of banking information resources, information security, cybersecurity, security to information, investments, emergent properties, synergistic effect, hybrid crypto codes on damaged codes, elliptic codes, methodology.