ВІДГУК

офіційного опонента - професора кафедри безпеки інформаційних технологій,
Навчально-наукового інституту інформаційно-діагностичних систем,
Національного авіаційного університету,
доктора технічних наук, професора Хорошка Володимира Олексійовича
на дисертаційну роботу Євсеєва Сергія Петровича

"Методологія побудови системи безпеки банківських інформаційних ресурсів",

подану на здобуття наукового ступеня доктора технічних наук за спеціальністю 21.05.01 – інформаційна безпека держави

Актуальність теми. У сучасних умовах 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. Загрози безпеці БІР набули ознак гібридності. Прояви ознак гібридності унаслідок одночасного впливу загроз інформаційній безпеці, кібернетичній безпеці (КБ) та безпеці інформації (БІ) на БІР призвели до виникнення явища синергізму, негативні прояви від якого потребують кардинального перегляду концепцій побудови діючих систем безпеки. Прояви гібридних загроз безпеці БІР вже мали місце в Україні, у зв'язку з чим проблема забезпечення ІБ держави для інфраструктур критичного застосування (ІКЗ), до яких відносять і банківський сектор, стоїть дуже гостро. Таким чином, діючі методологічні засади побудови системи безпеки БІР як України зокрема, так і світу в цілому, потребують кардинального перегляду.

Слід зазначити, що невирішеними аспектами загальної проблеми забезпечення ІБ нашої держави залишається проблема створення цілісної науково обґрунтованої методології побудови системи безпеки БІР, впровадження якої на практиці сприятиме стійкому та стабільному розвитку банківського сектору.

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.

Достовірність і обґрунтованість результатів роботи підтверджується результатами експериментів, впровадженнями і експлуатацією результатів дисертаційної роботи. Результати наукових досліджень оприлюднено на понад 20-ох наукових конференціях різного рівня.

Основні наукові результати досліджень. Наукова цінність основних положень дисертації полягає у розробленні принципово нової методології створення системи безпеки банківських інформаційних ресурсів, в основу якої покладено запропоновану концепцію побудови синергетичної моделі загроз безпеці банківських інформаційних ресурсів, базис якої становить трирівнева модель стратегічного управління безпекою банківських інформаційних технологій, що забезпечує одержання синергетичного ефекту в умовах одночасної дії загроз інформаційної безпеки, КБ та БІ і, як наслідок, сприяє визначенню якісно нових і невідомих до цього емерджентних властивостей системи безпеки банківських інформаційних ресурсів з урахуванням коштів, витрачених на її створення.

Для досягнення мети, визначеної в роботі як створення науково обґрунтованої методології побудови системи безпеки банківських інформаційних ресурсів для підвищення рівня їх захищеності від загроз безпеці гібридного характеру, поставлено і вирішено такі задачі:

1. Проведено аналіз сутності та змісту проблеми інформаційної безпеки держави на сучасному етапі розвитку науки і техніки та досліджено роль й місце систем безпеки банківських інформаційних ресурсів при впливі на них нових загроз, які мають гібридний характер.

2. Розроблено 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.

3. Удосконалено 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.

4. Розроблено 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.

5. Розроблено 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.

6. Розроблено метод забезпечення автентичності банківських інформаційних ресур-

сів при одночасній дії на них загроз інформаційній безпеці для підвищення рівня їх інформаційної прихованості та достовірності *OTP*-паролів в протоколі двофакторної автентифікації.

7. Розроблено 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.

8. Розроблено 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.

Наукова новизна та практичне значення дисертаційної роботи

Наукова новизна одержаних особисто здобувачем результатів на мою думку полягає у наступному:

Уперше

– *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, КБ та БІ відкриває новий напрямок у забезпеченні безпеки банківських інформаційних ресурсів;

– *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;

– *розроблено* метод забезпечення конфіденційності та цілісності банківських інформаційних ресурсів, який грунтується 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.

Удосконалено

– класифікатор загроз безпеці банківських інформаційних ресурсів, який, на відміну від відомих, грунтується 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, КБ, БІ, ймовірність їх впливу на безпеку банківських інформаційних ресурсів.

Новизна результатів роботи підтверджується наявністю у автора багатьох наукових праць.

Практичне значення отриманих результатів полягає в тому, що розроблено класифікатор загроз безпеки банківських інформаційних ресурсів, який дозволяє в он-лайн режимі здійснювати класифікацію та оцінювати ймовірності впливу загроз інформаційної безпеці, КБ, БІ на банківські інформаційні ресурси, а також визначати рівень безпеки банківських інформаційних ресурсів на основі синергетичної моделі загроз, удосконалених моделі зловмисника та моделі інфраструктури автоматизованої банківської системи, моделі оцінки захищеності банківських інформаційних ресурсів, оптимізації витрати коштів на побудову системи безпеки банківських інформаційних ресурсів. Впровадження розроблених методів забезпечення конфіденційності, цілісності та автентичності банківських інформаційних ресурсів на гібридних крипто-кодових конструкціях забезпечує зменшення в 2 – 3 рази енергетичних витрат при використанні у складі автоматизованих банківських систем відкритих каналів зв'язку й передачі даних при одночасному забезпеченні заданих показників безпеки.

Як зазначається у роботі, дослідження, що провів автор, виконувалися в Харківському національному економічному університеті імені С. Кузнеця в 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). У згаданих НДР здобувач брав участь як виконавець, відповідальний виконавець, а в останній НДР виступав науковим керівником.

Цінність теоретичних та практичних результатів роботи підтверджується актами впровадження.

Зміст дисертаційної роботи досить повно відображений в опублікованих відкритим друком наукових працях. Робота написана зрозуміло і грамотно, науково-технічна термінологія використовується логічно та коректно. Стиль викладу матеріалів дисертації логічний. Зміст автореферату повністю відповідає основним положенням та висновкам, зробленим у дисертації.

Недоліки та зауваження. До основних недоліків та зауважень дисертації можна віднести такі:

1. Не зрозуміло, що мається на увазі під терміном банківський інформаційний ресурс, оскільки на стор. 49 наведено визначення, згідно з яким банківський інформаційний ресурс «сукупність відомостей, пов'язаних зі Статутними документами та Керівництвом банківської установи, організаційно-правовою формою банківської установи, нинішнім виглядом банківської установи та її службовців, видами і формами банківського обслуговування, кількістю і складом клієнтів, операціями з рахунками клієнтів, наявністю кореспондентських стосунків і технічним забезпеченням банку». Зазначимо, що також застосовується і поняття «банківська інформація». Виникає питання: якщо БІР не має матеріаль-

ної форми, тоді чим він відрізняється від інформації. А якщо він має матеріальну форму, тоді не зрозуміло, як він «циркулює».

2. В тексті дисертації автором не розкрито чому формула (2.1, яка описує середнє значення оцінки експертів за всіма загрозами для певної послуги безпеки) була повторно використана у розділі 5 (формула 5.7, стор. 343). Аналогічний недолік властивий формулам (2.14), (2.21), (3.7) та (3.11). На мій погляд повторне застосування при проведені експерименту у розділі 5 є нераціональним. Вважається доцільним використання посилань на відповідні формули. Поряд з тим відмічаю, що вказані недоліки в авторефераті відсутні.

3. На стор. 112 наведено рис. 2.7, який названо "Узагальнений підхід формування синергетичної моделі безпеки БІР". Але не зрозуміло, що слід мати на увазі під словосполученням «Узагальнений підхід» взагалі. Наведений рисунок більше відповідає певній спробі ілюстрації очевидного факту, що кожний з відомих загальних підходів дає можливість отримувати різні типи оцінок (кількісні, якісні і кількісно-якісні) в залежності від застосовуваних методів (моделей). Далі стверджується, що на підставі цього підходу сформульовані дефініції основних компонент концептуальної синергетичної моделі безпеки БІР, (стор. 116). Ця теза не одержує подальшого розвитку, і не зрозуміло, чи слід розглядати формулювання згаданих "компонент" як науковий результат.

4. Для підвищення рівня безпеки БІР здобувачем пропонується використовувати крипто-кодові конструкції Мак-Еліса і Нідеррайтера на збиткових кодах, але не зрозуміло чому саме їх необхідно використовувати для забезпечення основних послуг: конфіденційності, цілісності, автентичності. Також в дисертації відсутні результати дослідження їх використання в автоматизованих банківських системах, які на сьогодні використовуються в організаціях банківського сектору.

5. В четвертому розділі запропонований удосконаленого методу оцінювання безпеки БІР, який, на відміну від відомих, враховує комплексний показник ефективності інвестицій, що виділяються на забезпечення безпеки БІР, але підтвердження його переваг над діючими методиками оцінювання безпеки БІР (рис. 4.5, стор. 285) в дисертації не наведено.

6. У табл. 4.1. (стор. 278) та табл. 10 автореферату (стор. 23) наведені результати досліджень стійкості криптоалгоритмів експрес-методом на основі ентропійного методу оцінювання випадковості криптограми алгоритму шифрування, в яких зазначено, що RSA-алгоритм має стовідсоткову ймовірність криптозахисту, що не відповідає дійсності. Крім того, ентропійний метод має велику похибку, тому не зовсім зрозуміло чому здобувач використовує саме цей метод.

7. У частині, що стосується аналізу, на мою думку, недостатньо відображено недоліки існуючих моделей, методів захисту інформації, значна увага приділена висвітленню синергетичного підходу.

Висновок щодо відповідності встановленим вимогам.

Робота має достатньо високий теоретичний рівень, дослідження виконані на сучасному рівні. Наведені вище недоліки не зменшують теоретичну та практичну цінність дисертаційної роботи, яка є завершеним науковим дослідженням, що присвячено отриманню нових рішень актуальних науково-практичних завдань, пов'язаних з розробкою систем безпеки банківських інформаційних ресурсів.

Вважаю, що за актуальністю обраної тематики, новизною досліджень, їх обгрунтованістю та науково-практичною значимістю отриманих результатів, дисертаційна робота Євсеєва Сергія Петровича задовольняє вимогам пунктів 9, 10, 12, 13, 14 "Порядку присудження наукових ступенів" (постанова КМУ № 567 від 24 липня 2013 р.) до докторських дисертацій, а її автор заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 21.05.01 – Інформаційна безпека держави.

Офіційний опонент
Професор кафедри безпеки інформаційних технологій,
Навчально-наукового інституту інформаційно-діагностичних систем,
Національного авіаційного університету,
доктор технічних наук, професор В.О. Хорошко

Підпис професора Хорошка В.О. засвідчую,
Вчений секретар НАУ Г.Г. Єнчева