ВІДГУК

офіційного опонента, доктора технічних наук, старшого наукового співробітника Кудіна Антона Михайловича

на дисертаційну роботу Євсеєва Сергія Петровича на тему:

“Методологія побудови системи безпеки банківських інформаційних ресурсів”

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

1. Актуальність теми дисертації

Зараз активно розвиваються інформаційні технології в банківському секторі, клієнтам банків надається значний та різноманітний набір послуг у вигляді електронних сервісів та онлайн-платежів, що безумовно призводить до фактичного об’єднання банківських інформаційних та комп’ютерних мереж до єдиного інформаційного та кібернетичного простору. Все це спонукає до створення автоматизованих банківських систем (АБС), які істотно розширюють спектр електронних послуг державних і комерційних банків світу та України. Як наслідок таких змін є суттєве трансформування й загроз такому національному інформаційному ресурсу держави, як банківський інформаційний ресурс (БІР). Загрози безпеці БІР набули ознак гібридності унаслідок одночасного впливу загроз інформаційній безпеці (ІБ), 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.

Дисертаційна робота присвячена вирішенню протиріччя між зростаючими на практиці вимогами до безпеки БІР при одночасному збільшенні кількості та технологічній складності загроз безпеці і набутті ними ознак гібридності та недосконалістю, а подекуди й відсутністю методології побудови системи безпеки БІР від таких загроз.

Прояви гібридних загроз безпеці БІР вже мали місце в Україні. Наприклад, почавшись з кібератаки за допомогою шкідливого програмного забезпечення “Petya” (2017 р.) було фактично скомпрометовано процес надання банківських послуг. Ланцюгова реакція після України поширилася на банківські сектори багатьох ін. держав світу. Таким чином, можна відзначити, що проблема забезпечення ІБ держави для інфраструктур критичного застосування (ІКЗ) стоїть дуже гостро. Відповідно кардинального перегляду потребують діючі методологічні засади побудови системи безпеки БІР як України, так й світу в цілому. Це безумовно вказує на те, що тема дисертаційного дослідження Євсеєва Сергія Петровича є актуальною.

2. Зв'язок роботи з науковими програмами, планами й темами

Наведені в дисертаційній роботі основні результати та рекомендації розроблено 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 визначених НДР здобувач брав участь як виконавець, відповідальний виконавець, а в останній НДР виступав науковим керівником.

3. Наукова новизна одержаних результатів

У дисертаційній роботі розроблено вперше концепцію побудови синергетичної моделі загроз безпеки банківських інформаційних ресурсів, базис якої становить трирівнева модель стратегічного управління безпекою банківських інформаційних технологій, а також 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. У дослідженні вперше розроблено та запропоновано 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. Автором вперше розроблено метод забезпечення автентичності банківських інформаційних ресурсів та вперше розроблено методологію побудови системи безпеки банківських інформаційних ресурсів.

Слід також відзначити, що у роботі 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. Також набув подальшого розвитку метод оцінювання безпеки банківських інформаційних ресурсів, який 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.

4. Практичне значення одержаних результатів.

Розроблено веб-застос*унок, 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. Автором розроблено: практичну методику для оцінювання рівня захищеності банківських інформаційних ресурсів та методику оцінювання безпеки банківських інформаційних ресурсів, поруч із цим запропоновані 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_K <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 $GF(q)$.

Розроблено програмні макети криптографічних засобів захисту інформації з використанням гібридних крипто-кодових конструкціях зі збитковими кодами, які дозволяють проводити експериментальні дослідження запропонованих крипто-кодових конструкцій, оцінювати їх властивості та стійкість. Результати дисертаційної роботи 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 Текнолоджіс" (акт впровадження від 30.11.2017).

Також 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.

Мова та стиль викладення дисертації та автореферату дозволяють зрозуміти суть розроблених наукових положень та одержаних практичних результатів. Дисертація та автореферат у цілому відповідають вимогам, які висуваються до його оформлення відповідно до "Порядку присудження наукових ступенів" затвердженого Постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами) та суттєво не відхиляються від вимог ДСТУ 3008-2015 "Інформація та документація. Звіти у сфері науки і техніки. Структура та правила оформлення" й "Вимог до оформлення дисертації" затверджених наказом Міністерства освіти і науки України від 12.01.2017 р. № 40.

Поряд з тим в тексті дисертації зустрічаються синтаксичні (наприклад, стор. 6, 126 та ін.) та русизми (наприклад, стор. 191 дисертації "флаг" – невірно, замість "прапор" – вірно).

У цілому зміст дисертації та автореферату викладено послідовно та логічно.

5. Ступінь обґрунтованості та достовірності наукових положень, висновків і рекомендацій, сформульованих у роботі

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

банківських системах.

Розроблено алгоритмічне забезпечення та програмні застосунки, що дозволило верифікувати запропоновані методи, моделі та методологію і підтвердити їх ефективність у контексті 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.

Сформульовані в дисертаційній роботі Євсеєва Сергія Петровича наукові положення, висновки та рекомендації є достатньо обґрунтованими, що підтверджується ретельною проробкою теоретичної частини роботи, обсягом експериментальних досліджень та впровадженням розроблених методик щодо діяльності банківської установи та сучасних компаній країни.

6. Повнота оприлюднення результатів дисертаційної роботи

Основні положення дисертації опубліковано у 120 наукових працях (54 основних з яких наведено у авторефераті), у тому числі: 3 монографії (у співавторстві), 4 розділи у колективних монографіях; 9 наукових статей у міжнародних рецензованих виданнях, що входять до баз даних *Scopus* та *Web of Science*; 16 наукових статей у закордонних, вітчизняних фахових наукових журналах, які входять до інших міжнародних наукометричних баз даних (*Index Copernicus*, *EBSCO*, *Inspec* тощо), та 12 статей у наукових журналах та збірниках наукових праць, що входять до переліку фахових видань України, а також 10 матеріалів і тез доповідей на міжнародних конференціях. Без співавторів – опубліковано 8 наукових статей. Основні положення дисертаційної роботи доповідалися та обговорювалися понад 20 наукових конференціях. Кількість публікацій відповідає вимогам наказу МОН України від 17.10.2012 № 1112 "Про опублікування результатів дисертацій на здобуття наукових ступенів доктора і кандидата наук".

Назва дисертації відповідає її змісту. Дисертація та автореферат оформлені згідно з вимогами МОН України. Науковий рівень дисертації відповідає вимогам "Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника", затвердженого постановою КМУ від 24.07.2013р. № 567, а зміст – паспорту спеціальності 21.05.01 – Інформаційна безпека держави.

7. Загальна характеристика структури та змісту дисертаційної роботи

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.

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.

Перший розділ присвячено виконанню аналізу 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.

Дотримуючись триєдиного правила щодо забезпечення безпеки БІР та ґрунтуючись на синергетичному підході до побудови відповідної системи безпеки в умовах дії загроз гібридного характеру, ідея, яка розвинута в дисертації, в загальному вигляді подана як 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 і в інтересах отримання в подальшому оцінювання величини ризику безпеці в роботі обґрунтовано та введено синергетичний показник безпеки БІР. 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 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.

Таким чином, у першому розділі на основі проведеного аналізу стану проблеми, обґрунтовано основні завдання дослідження, які потрібно вирішити для досягнення поставленої мети: створення науково обґрунтованої методології побудови системи безпеки банківських інформаційних ресурсів для підвищення рівня їх захищеності від загроз безпеці гібридного характеру.

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. На другому рівні формується корпоративна стратегія ІБ БІР. На третьому рівні проводиться деталізація функціональних стратегій другого рівня стратегічного набору, формується корпоративна стратегія безпеки інформації.

Запропонована концепція грунтується 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.

Запропонований 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 (“банківські інформаційні ресурси (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 (ГККК3К). На основі одержаних оцінок ефективності технічних засобів захисту інформації (ТЗЗІ) в АБС для забезпечення конфіденційності, цілісності БІР запропоновано нові механізми на основі ГККК3К, 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.

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 МЕС, ГККК3К були реалізовані відповідні програмні макети.

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 витрати коштів на її побудову в умовах впливу гібридних загроз ІБ, КБ та БІ.

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, вона враховує як технічні показники мережі (швидкість передачі даних, імовірність і час доставки пакета і ін.), показники безпеки технічних засобів захисту інформації, так і економічні параметри (вартість масштабування, обслуговування мережі, ефективність інвестицій в безпеку та ін.). Запропонована методика містить чотири етапи.

Перший етап передбачає визначення стійкості криптосистем методом експрес-аналізу на основі ентропійного методу оцінки випадковості вихідної послідовності, другий – у визначенні впливу загроз на складові безпеки (ІБ, КБ, БІ) з урахуванням їх гібридності і синергізму, третій – у визначенні комплексного показника ефективності інвестицій в забезпечення безпеки БІР при заданому рівні їх захищеності, четвертий – у визначенні ефективності обміну даними в АБС.

Аналіз результатів показав, що запропонована методика оцінки функціональної ефективності АБС дозволяє без значних часових і експертних витрат провести оцінку стану якості обслуговування користувачів АБС, використовувати результати оцінки для її масштабування, поліпшення технічних показників АБС, рівня захищеності БІР.

У п'ятому розділі дисертації розроблено методологію побудови системи безпеки БІР, приклад реалізації для ОБС України. Розроблена методологія побудови системи безпеки банківських інформаційних ресурсів. 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 одержувати 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 ГККК3К дозволить гарантувати послуги безпеки при заданих їх ймовірнісних показниках.

Загальні висновки дисертаційної роботи узгоджуються з метою і завданнями дослідження. За результатами дисертаційного дослідження зроблено дев'ять висновків, які повністю відповідають поставленим завданням. Отримані результати характеризуються науковою новизною та практичною цінністю, обґрунтовані теоретично та підтверджені експериментальними дослідженнями. В цілому дисертація Євсеєва Сергія Петровича є завершеним і повним дослідженням, яке містить теоретичні розробки високого рівня та відповідні їм експериментальні перевірки.

8. Ідентичність змісту автореферату та основних положень дисертації

Зміст автореферату є ідентичним до дисертаційної роботи та не містить інформації, яка відсутня у самій роботі. Текст автореферату повною мірою розкриває наукову та практичну цінність дисертації. Висновки в авторефераті збігаються з висновками по роботі.

9. Зауваження до дисертаційної роботи

1. У роботі недостатньо визначена особливість систем захисту банківських інформаційних ресурсів: зокрема нечітко визначено особливість нормативного регулювання захисту інформації та кіберзахисту в банківській системі України з боку Національного банку України, недостатньо розглянуті зміни в побудові інформаційно-телекомунікаційних систем Національного банку України та банківській системі, що відбулись останнім часом, нові програми забезпечення безпеки інформації в міжнародній системі SWIFT (зокрема, програма SWIFT CSP) та ін.

2. У науковій новизні треба було підкреслити саме відмінність та світову

значимість отриманих результатів, що потребує не простої констатації розробленої методології, а й визначення її відмінності від світових аналогів.

3. У постановочної частині роботи не досить чітко проводиться розділ між постановками задач забезпечення безпеки інформації, інформаційної безпеки та кібербезпеки.

4. У візуальному відбитті щодо класифікації кібератак на АБС з прив'язкою до моделі *OSI* (рис. 1.10) не зрозуміло яким чином рівні моделі *OSI* корелюють із рівнями кібератаки *NSL KDD*.

5. У сенсі огляду інструментів забезпечення безперервності бізнес-процесів слід було би розглянути модель рівнів зрілості *IT*-інфраструктури підприємства, наприклад, що була запропонована компанією *Microsoft* або моделі COBIT.

6. Не чітко визначена проблема забезпечення інформаційної безпеки БІР, її комплексність та глобальність, зокрема не розглянуті такі складові інформаційної безпеки як деструктивний інформаційний вплив, проблема достовірності інформації та ін. Це призводить до спрощеного, суто «технологічного» погляду на проблему забезпечення інформаційної безпеки.

7. Не досить коректним є посилання на широке використання в сучасних банківських інформаційно-телекомунікаційних системах «морально застарілих» криптографічних систем.

8. При визначені узагальнених показників рівня захищеності БІР на етапі 3, крок 3.1 автором неявно використовується безпеки з повним перекриттям, яка не може застосовуватись для багатьох сучасних (зокрема – хмарних) інформаційно-телекомунікаційних систем.

9. Не дуже коректним є визначення ентропії відкритого тексту та криптограм, а також «ймовірності криптозахисту» (таблиця 10, розділ 4). Зокрема не визначений характер відкритого тексту, довжина ключів криптосистеми RSA та ін.

10. Автору слід було звернути увагу на економічну складову отриманих результатів. У роботі не має їх вартісного аналізу, техніко-економічного обґрунтування вирішення практичних задач впровадження отриманої концепції як у банківській справі так і загалом у підвищенні інформаційної безпеки України.

Слід відзначити, що визначені зауваження не знижують загальної позитивної оцінки дисертаційної роботи.

10. Загальний висновок на дисертаційну роботу

За обсягом проведених досліджень, їх теоретичним рівнем, актуальністю розглянутої проблеми та значенням одержаних результатів для науки і практики дисертаційна робота Євсеєва Сергія Петровича "Методологія

побудови системи безпеки банківських інформаційних ресурсів" є завершеною науковою працею, в якій отримані нові науково обґрунтовані результати, які сприяють побудові ефективних систем безпеки банківських інформаційних ресурсів для підвищення рівня їх захищеності від загроз безпеці гібридного характеру.

Матеріали дисертації опубліковано у достатній мірі, висновки роботи відображають її результати.

Автореферат в достатній мірі відповідає зміст дисертаційної роботи, оформлення дисертації і автореферату в цілому відповідає нормативним вимогам. Дисертаційна робота повністю відповідає паспорту спеціальності 21.05.01 – Інформаційна безпека держави і вимогам, які висуваються до дисертацій на здобуття наукового ступеня доктора наук, а також пп. 9, 11, 12 "Порядку присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника", затвердженого постановою КМУ №567 від 24.07.2013 р., а її автор, Євсеєв Сергій Петрович, заслуговує присудження йому наукового ступеня доктора технічних наук за спеціальністю 21.05.01 – Інформаційна безпека держави.

Заступник директора департаменту безпеки –
начальник управління безпеки інформації
Національного банку України, доктор технічних наук,
старший науковий співробітник А.М. Кудін

А.М. Кудін

Підпис засвідчую
Кудіна А.М.

Начальник управління із супроводження та адміністрування персоналу Департаменту персоналу
В.В. Шульженко