ВІДГУК

офіційного опонента, доктора технічних наук, доцента Іванченка Сергія Олександровича на дисертаційну роботу Євсеєва Сергія Петровича "МЕТОДОЛОГІЯ ПОБУДОВИ СИСТЕМИ БЕЗПЕКИ БАНКІВСЬКИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ",

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

Актуальність теми дисертації. На сьогоднішній день у забезпеченні інформаційної безпеки банківського та інших секторів держави на усіх рівнях господарювання важливу роль відіграє використовуваність новітніх досягнень науки й техніки, де в основі управлінських рішень лежить ефективна методологічна база.

Революційні зміни, що відбуваються в банківському секторі держави протягом останніх років, істотно розширили спектр сервісів державних та комерційних банків та водночас призвели до суттєвої трансформації загроз безпеки банківських інформаційних ресурсів. Нові типи загроз набувають ознак гібридності та синергізму. У свою чергу негативні прояви таких загроз потребують кардинального перегляду та оновлення концепцій побудови діючих систем безпеки банківських інформаційних ресурсів. В такому разі є невирішеною проблема створення цілісної науково обґрунтованої методології побудови систем безпеки зазначених ресурсів, впровадження якої на практиці сприятиме підвищенню рівня інформаційної безпеки держави в банківському секторі.

Дисертаційна робота Євсеєва С.П. присвячена розв'язанню зазначених протиріч, а саме розробці такої цілісної методології з врахуванням нових умов та нових загроз, що на сьогоднішній день є надзвичайно важливим та актуальним.

Дисертаційну роботу виконано відповідно до планів науково-дослідних і прикладних робіт Міністерства освіти і науки України за темами: № 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.

Загальна оцінка змісту дисертаційної 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 інформаційної безпеки держави на сучасному етапі розвитку науки і техніки, зокрема роль й місце систем безпеки банківських інформаційних ресурсів при впливі на них нових видів загроз, які мають гібридний характер.

Проведений аналіз міжнародної та національної нормативно-правової бази, яка регламентує порядок побудови системи безпеки банківських інформаційних ресурсів, дав підстави виділити основні невирішені завдання щодо їх безпеки.

Встановлено, що відсутність на сьогодні ефективної та дієвої методології побудови системи безпеки 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 при одночасному зростанні їх технологічної складності. З іншого боку, в теорії відсутня цілісна науково обґрунтована методологія побудови на практиці системи безпеки в цілому, що обумовлено недосконалістю механізмів забезпечення її інформаційної безпеки, безпеки інформації та кібербезпеки зокрема. На основі проведеного аналізу стану проблеми, обґрунтовано основні завдання дослідження, які потрібно вирішити для досягнення поставленої мети.

Другий розділ присвячений розробці концептуальних засад забезпечення безпеки банківських інформаційних ресурсів. Запропоновано та розроблено концепцію побудови синергетичної моделі загроз, яка базується на трирівневій моделі стратегічного управління їх безпекою. Концепція ґрунтується на синергетичному підході до вибору найбільш ефективних напрямків досягнення поставлених цілей безпеки 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. У розділі також набули подальшого розвитку теоретичні положення щодо безпеки банківських інформаційних ресурсів, які полягають в уточненні та оновленні ряду відповідних означень та тверджень.

Третій розділ присвячено дослідженням, пов'язаним із забезпеченням конфіденційності, цілісності та автентичності банківських інформаційних ресурсів. Зокрема розроблено і експериментально досліджено методи гібридних крипто-кодових конструкцій на надлишкових кодах, які дозволяють будувати несиметричні криптосистеми на основі модифікованих несиметричних крипто-кодових систем Мак-Еліса з модифікованими еліптичними кодами – укороченими або подовженими, що забезпечують відповідний рівень безпеки та достовірності.

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

Для оцінки якості обслуговування об'єктів автоматизованої банківської системи щодо забезпечення безпеки запропонована методика оцінки функціональної ефективності обміну даними, що ґрунтується на простому багатофакторному аналізі, де враховано 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 і т.п.). Запропонована методика дозволяє без значних часових і експертних витрат провести оцінку стану якості обслуговування користувачів, використовувати результати оцінки для масштабування системи, поліпшення технічних показників та рівня захищеності інформаційних ресурсів.

У п'ятому розділі дисертації розроблено методологію побудови системи безпеки банківських інформаційних ресурсів та наведено приклад реалізації для організації банківського сектору України. Реалізація методології з урахуванням розроблених у дисертації методів і засобів дасть можливість забезпечити підвищення рівня захищеності банківських інформаційних ресурсів в умовах дії гібридних загроз, раціональну організацію системи забезпечення безпеки в умовах одночасної дії 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.

Наукова новизна. Обґрунтованість і достовірність одержаних наукових висновків і результатів дисертаційної роботи. Викладені в дисертаційній роботі положення та отримані автором теоретичні і практичні результати мають належний ступінь обґрунтованості, який було досягнуто завдяки використанню теоретично обґрунтованих та практично апробованих методів теорії множин, теорії криптографії та кодування, теорії скінчених полів Галуа, теорії ймовірностей і математичної статистики, експертного оцінювання, математичної логіки і теорії автоматів, системного аналізу, законів синергії. Зазначені моделі, алгоритми і програмні засоби, розроблені автором, базуються на відомих теоретичних положеннях та перевірені експериментально, що підтверджено актами впровадження отриманих результатів.

В дисертаційній роботі автором отримано наступні нові наукові результати:

– *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 можливості 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 систем 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, який на відміну від відомих, враховує комплексний показник ефективності інвестицій, що дозволяє оптимізувати витрати на її побудову в умовах впливу гібридних загроз при одночасному забезпеченні заданого рівня 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 та ефективний підхід до побудови діючих та перспективних систем безпеки банківських інформаційних ресурсів.

Практичне значення отриманих результатів. Отримані автором результати мають наступну **практичну цінність**:

1. Розроблено програмний додаток, який реалізує удосконалений класифікатор загроз для банківських інформаційних ресурсів, до якого є вільний доступ, що дозволяє легко 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, каналами зв'язку, інформаційними активами та загрозами для досягнення синергетичного ефекту та визначення рівня захищеності ресурсів.

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

4. Розроблено практичні алгоритми забезпечення конфіденційності, цілісності та автентичності банківських інформаційних ресурсів на основі інтеграції криптографічних перетворень і завадостійкого та збиткового кодування, що дає змогу забезпечити безпеку банківських інформаційних ресурсів (безпечний час – $T_б$ >200 р., стійкість до криптоаналізу $P_К$ <10^{25}–10^{35} групових операцій), достовірність передачі даних ($P_{пом}$ <10^{-9}) та зменшення енергетичних витрат на їх практичну реалізацію в 10 – 12 разів за рахунок зменшення порядку використаного поля Галуа.

5. Розроблено програмні прототипи криптографічних засобів захисту інформації з використанням гібридних крипто-кодових конструкцій зі збитковими кодами, які дозволяють проводити експериментальні дослідження та оцінювати їх властивості й стійкість.

6. Результати дисертаційної роботи впроваджено у діяльність ТОВ "Сайфер БІС", ТОВ "Тантаріум", Публічне акціонерне товариство "Мегабанк", ТОВ "Мікрокріпт Текнолоджіс", що підтверджується актами впровадження.

Рекомендації щодо використання наукових результатів. Подальший розвиток отриманих в дисертації результатів доцільно пов'язати з розробкою універсальної методології побудови систем безпеки на основі синергетичної моделі, з врахуванням гібридності загроз інформації в сучасних умовах, а також з максимально можливим використанням криптографічних систем на основі крипто-кодових конструкцій, аж до повної заміни асиметричних криптосистем, у зв'язку з їх нестійкістю в умовах постквантової криптографії.

Мова, стиль та оформлення дисертації й автореферату. Повний обсяг дисертації становить 471 сторінка, список використаних літературних джерел складається із 354 найменувань, у рукопису 102 рисунки, 67 таблиць, 90 сторінок додатків.

Дисертаційну роботу викладено на достатньо високому науковому рівні з використанням загальновизнаної наукової термінології.

Мова та стиль дисертаційної роботи повністю відповідають існуючим вимогам щодо викладення науково-технічної інформації, оформлення відповідає вимогам щодо докторських дисертацій.

Автореферат повністю відповідає змісту дисертації, повно відображає її основні наукові результати, оформлений з дотриманням вимог, встановлених Міністерством освіти і науки України.

Повнота викладення основних результатів у публікаціях.

За темою дисертаційної роботи, як зазначено у дисертації та авторефераті, здобувачем опубліковано 120 наукових праць, з яких 54 приведено, як основні в анотації та авторефераті. З них 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 та вітчизняних фахових наукових журналах, які входять до інших міжнародних наукометричних баз даних (*Index Copernicus, EBSCO, Inspec*, тощо), 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. Рівень і кількість публікацій та апробація матеріалів дисертації на конференціях повністю відповідають діючим вимогам.

Зауваження до дисертаційної роботи. До недоліків та зауважень дисертаційної роботи можна віднести наступне:

1. В дисертації не наведено повного обґрунтування щодо вибору крипто-кодових конструкцій для забезпечення конфіденційності та цілісності банківських інформаційних ресурсів (розділ 3, стор. 145, 147). Адже сьогодні існує ціла низка стандартних сертифікованих криптоалгоритмів, які виконують ті ж функції.

2. В роботі для оцінювання стійкості крипто-кодових схем використано лише статистичні тести за технологією NIST (розділ 3, стор. 225, автореферат стор. 20). А чи є це вичерпним засобом, залишилося без пояснень. Адже існує багато інших критеріїв для оцінювання стійкості шифрів.

3. Не наведено відомостей щодо обчислювальних потужностей, які були використаними для порівняння ефективності розроблених крипто-кодових конструкцій (підрозділ 3.2.3, стор. 218 – 224, автореферат стор.19 – 20). Адже виникає питання наскільки стійкими будуть розроблені крипто-кодові конструкції при використанні швидкодіючих квантових комп'ютерів – недалекого майбутнього обчислювальної техніки.

4. Не показано, як вплине на параметри системи безпеки банківських інформаційних ресурсів врахування гібридності та синергізму загроз, наскільки ускладниться розробка самої системи безпеки та зміниться її вартість, як зміниться стійкість системи безпеки по відношенню до стандартних вимог (розділ 2, стор. 107).

5. Не приведено кількісних оцінок ефекту від впровадження розробленої методології, а саме не показано на скільки це зменшить залежність експерта від помилок при використанні запропонованого класифікатора у побудові моделі загроз та моделі порушника (розділ 2, стор.106).

6. В роботі не здійснено прогнозування очікуваного економічного ефекту, який має бути від впровадження запропонованої методології побудови систем безпеки банківських інформаційних ресурсів з врахуванням її комплексності та синергізму (розділ 4, стор. 270, розділ 5, стор. 360 – 365).

7. В дисертації та авторефераті зустрічаються стилістичні неточності та русизми. Наприклад, вжите поняття "збиткових" кодів в контексті роботи українською мовою є "надлишковими" кодами, російською – "избыточными". "Збитковість" на російську мову перекладається як "убыточность" і т.п.

Однак вказані зауваження не занижують цінності та важливості результатів дисертаційної роботи Євсеєва С. П.

Висновки. На основі вивчення дисертації, автореферату дисертації та праць здобувача, що опубліковані за темою дисертації, встановлено:

дисертаційна робота Євсєєва С. П. відповідає вимогам Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (із змінами);

дисертаційна робота відповідає паспорту спеціальності 21.05.01 – інформаційна безпека держави;

зміст автореферату ідентичний основним положенням дисертації;

дисертація Євсеєва С. П. є завершеною кваліфікаційною науковою працею, яка є вирішенням важливої науково-прикладної проблеми зі створення нової методології побудови системи безпеки банківських інформаційних ресурсів та місить нові науково обґрунтовані результати, що отримані особисто здобувачем у проведених дослідженнях;

автор дисертації, Євсеєв Сергій Петрович, заслуговує присудження наукового ступеня доктора технічних наук за спеціальністю 21.05.01 – інформаційна безпека держави.

Офіційний опонент
професор спеціальної кафедри №1
Інституту спеціального зв'язку та захисту інформації
Національного технічного університету України
"Київський політехнічний інститут імені Ігоря Сікорського",
д.т.н., доцент С.О.Іванченко

Підпис д.т.н., доцента Іванченка Сергія Олександровича засвідчую.

Начальник відділу кадрової роботи
ІСЗЗІ КПІ ім. Ігоря Сікорського В.М.Грищук