Прим. № ___

Голові спеціалізованої вченої ради Д 26.062.17
03680, м. Київ, просп. Космонавта Комарова, 1

ВІДГУК
офіційного опонента

завідуючого кафедрою інформаційної та кібернетичної безпеки Навчально-наукового інституту захисту інформації Державного університету телекомунікацій, доктора технічних наук, професора *БУРЯЧКА Володимира Леонідовича*
на дисертаційну роботу *БУЧИКА Сергія Степановича* за темою «Методологія побудови та захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів», подану на здобуття наукового ступеня доктора технічних наук за спеціальністю 21.05.01 – інформаційна безпека держави

1. Актуальність теми дисертації, зв'язок з науковими програмами, планами, темами.

Інтенсивний розвиток інформаційних технологій та їх інтеграція практично у всі сфери життєдіяльності суспільства і держави відкриває можливості масового доступу користувачів до інформації. Це сприяє збільшенню кількості критично важливого інформаційного ресурсу (ІР), який циркулює, накопичується та обробляється в інформаційно-телекомунікаційних системах (ІТС) й призводить до підвищення ступеня залежності більшості важливих рішень, що приймаються на різних рівнях, від якості інформації та оперативності її обробки. Зважаючи на проблемну ситуацію, яка склалася, саме здатність суспільства та його інститутів збирати, накопичувати й використовувати ІР, забезпечувати своєчасний доступ до нього та свободу інформаційного обміну, а також захищати критично важливу інформацію від внутрішніх і зовнішніх загроз, стає нині важливим чинником забезпечення національної безпеки й виступає запорукою як для соціального та технологічного прогресу, так й для швидкого економічного зростання об'єктів і суб'єктів державної та позадержавної власності.

Такий стан справ призводить до того, що нині, в умовах фактичного проведення країнами світу одна проти одної інформаційних та кібервоєн, прикладом чому є потерпаюча від неприкритої гібридної війни та російської збройної агресії Україна, надзвичайно актуальним стає завдання щодо забезпечення захисту передусім державних інформаційних ресурсів (ДІР). Його вирішення має ґрунтуватися на ефективній інформаційній політиці країн світу та їх комплексному підході до побудови власних систем захисту. В умовах України це, за рахунок мінімізації ризиків ДІР та формування динамічного комплексу функціональних профілів захищеності (ФПЗ), дозволить підвищити ефективність захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів. Саме цьому й присвячена дисертаційна робота *Бучика Сергія Степановича.* Зважаючи на те,

що в умовах сьогодення існують протиріччя між наявними ДІР і нормативно-правовими, організаційними та інженерно-технічними напрямками їх захисту, а система оперативного управління та захисту інформаційних ресурсів держави є недосконалою – тематика дисертаційної роботи *Бучика С.С.* є актуальною.

2. Аналіз основного змісту, наукової новизни та практичної значимості, оцінка достовірності та обґрунтованості результатів

Дисертація складається зі вступу, п'яти розділів, висновків, вісьмох додатків та списку використаних джерел, що містить 234 найменування. Загальний обсяг дисертації становить 398 аркушів, з яких основний зміст роботи розкрито на 262 аркушах.

Зміст роботи відповідає поставленому науковому завданню та сформульованим задачам. Їх рішення є суттю та змістом виконаних досліджень, які відповідають паспорту спеціальності 21.05.01 – інформаційна безпека держави й спрямовані на розробку методології побудови системи захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів.

При цьому ***у вступі*** автором обґрунтовано актуальність досліджуваної проблеми та висвітлено її поточний стан, чітко сформульовано мету, котра корелює з темою роботи, та деталізується у задачах, визначено об'єкт та предмет дослідження. Визначено систему використаних в роботі дослідницьких методів та інструментів.

У ***першому розділі*** автором проведено аналіз світового простору ідентифікаторів об'єктів та уразливостей ДІР, а також нормативно-правового забезпечення (НПЗ) захисту ДІР в ІТС, досліджено ступінь посилань на поняття ДІР в основних нормативно-правових актах (НПА), а також ступінь впровадження міжнародних стандартів та технологій, методологій, методів і моделей щодо створення системи управління інформаційною безпекою в ІТС. На основі проведеного аналізу розроблено загальну систему основного НПЗ захисту ДІР, загальну систему класифікації загроз безпеці інформації ДІР, а також сформульовано загальну концепцію проведення дослідження.

У ***другому розділі*** на основі організаційно-правового методу «подвійної трійки захисту» державних інформаційних ресурсів нормативно-правового, організаційного та інженерно-технічного спрямування автором удосконалено технологію побудови класифікатора загроз ДІР в ІТС.

У ***третьому розділі*** автором вперше розроблено концептуальну модель інформаційної безпеки ДІР та загальну модель формування системи їх захисту, визначено принципи побудови комплексної системи захисту ДІР, розроблено типову систему захисту інформації ДІР, проведено аналіз класифікацій типів систем захисту інформації, запропоновано узагальнену багаторівневу структурну схему системи захисту ДІР та схему її формалізованого опису.

У ***четвертому розділі*** автором визначено місце українського сегмента в світовому просторі ідентифікаторів об'єктів. Вперше розроблено структурно-логічну модель організації ієрархічної гілки кодів-вузлів українського сегмента ідентифікаторів об'єктів державних органів на основі стандартизованої системи світового простору IP різних класів та світового дерева ідентифікаторів

інформаційних об'єктів. Розроблено методи та моделі реалізації системи управління інформаційної безпеки ДІР, які відповідають розробленій в третьому розділі загальній моделі формування системи захисту ДІР. Вперше введено поняття «Куб Юдіна-Бучика». Розроблено комплексний підхід до аналізу ризиків вузлів ІТС дерева ідентифікаторів ДІР українського сегмента.

П'ятий розділ дисертаційної роботи присвячено удосконаленню методу визначення функціональних профілів захищеності ІТС від НСД до ДІР. На основі розробленого комплексного підходу до аналізу ризиків вузлів ІТС дерева ідентифікаторів ДІР українського сегмента автором вперше представлено технологію побудови та захисту вузлів ІТС дерева ідентифікаторів ДІР. Здійснено оцінку ефективності та адекватності представлених методів, моделей та технології.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації, переконливо окреслена використанням сучасних методів, моделей та положень системного аналізу, складності систем, експертного оцінювання, методів та засобів захисту інформаційних ресурсів, методів аналізу інформаційного ризику тощо.

Отримані автором наукові результати у відповідності до поставлених задач досліджень є логічними, не суперечать фундаментальним фізичним і математичним закономірностям та підтверджуються достатньою апробацією основних положень і висновків як на міжнародних, так і всеукраїнських науково-технічних конференціях та семінарах.

Достовірність отриманих в роботі положень і наукових результатів підтверджується результатами проведених досліджень, коректністю застосування математичного апарату, можливих припущень та формулюванням умов досліджень при створенні українського сегмента дерева ідентифікаторів об'єктів, та розробці і впровадженні нової технології побудови системи захисту вузлів ІТС дерева ідентифікаторів ДІР на основі засад ризик-менеджменту.

Додатково достовірність отриманих результатів експериментально підтверджується проведенням автором досліджень на науково-дослідній базі Державної служби спеціального зв'язку та захисту інформації, Житомирського військового інституту імені С.П.Корольова, а також апробацією в апеляційному суді Житомирської області, що підтверджено відповідними актами впровадження.

До основних нових наукових результатів, які отримані в дисертаційній роботі, можна віднести:

1. Вперше розроблений організаційно-правовий метод «подвійної трійки захисту» інформаційних ресурсів держави нормативно-правового, організаційного та інженерно-технічного спрямування, на базі вперше введеної класифікації та кодифікації загроз різних класів та їх нормативно-правової і професійної семантики, що дозволило підвищити ефективність системи управління інформаційною безпекою ДІР.

2. Удосконалену методологію побудови класифікатора загроз ДІР в інформаційно-телекомунікаційних системах на основі організаційно-правового методу «подвійної трійки захисту» з урахуванням сформованої класифікації

інформаційних об'єктів. Розроблено методи та моделі реалізації системи управління інформаційної безпеки ДІР, які відповідають розробленій в третьому розділі загальній моделі формування системи захисту ДІР. Вперше введено поняття «Куб Юдіна-Бучика». Розроблено комплексний підхід до аналізу ризиків вузлів ІТС дерева ідентифікаторів ДІР українського сегмента.

П'ятий розділ дисертаційної роботи присвячено удосконаленню методу визначення функціональних профілів захищеності ІТС від НСД до ДІР. На основі розробленого комплексного підходу до аналізу ризиків вузлів ІТС дерева ідентифікаторів ДІР українського сегмента автором вперше представлено технологію побудови та захисту вузлів ІТС дерева ідентифікаторів ДІР. Здійснено оцінку ефективності та адекватності представлених методів, моделей та технології.

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих в дисертації, переконливо окреслена використанням сучасних методів, моделей та положень системного аналізу, складності систем, експертного оцінювання, методів та засобів захисту інформаційних ресурсів, методів аналізу інформаційного ризику тощо.

Отримані автором наукові результати у відповідності до поставлених задач досліджень є логічними, не суперечать фундаментальним фізичним і математичним закономірностям та підтверджуються достатньою апробацією основних положень і висновків як на міжнародних, так і всеукраїнських науково-технічних конференціях та семінарах.

Достовірність отриманих в роботі положень і наукових результатів підтверджується результатами проведених досліджень, коректністю застосування математичного апарату, можливих припущень та формулюванням умов досліджень при створенні українського сегмента дерева ідентифікаторів об'єктів, та розробці і впровадженні нової технології побудови системи захисту вузлів ІТС дерева ідентифікаторів ДІР на основі засад ризик-менеджменту.

Додатково достовірність отриманих результатів експериментально підтверджується проведенням автором досліджень на науково-дослідній базі Державної служби спеціального зв'язку та захисту інформації, Житомирського військового інституту імені С.П.Корольова, а також апробацією в апеляційному суді Житомирської області, що підтверджено відповідними актами впровадження.

До основних нових наукових результатів, які отримані в дисертаційній роботі, можна віднести:

1. Вперше розроблений організаційно-правовий метод «подвійної трійки захисту» інформаційних ресурсів держави нормативно-правового, організаційного та інженерно-технічного спрямування, на базі вперше введеної класифікації та кодифікації загроз різних класів та їх нормативно-правової і професійної семантики, що дозволило підвищити ефективність системи управління інформаційною безпекою ДІР.

2. Удосконалену методологію побудови класифікатора загроз ДІР в інформаційно-телекомунікаційних системах на основі організаційно-правового методу «подвійної трійки захисту» з урахуванням сформованої класифікації

загроз інформаційним ресурсам, що дозволило вперше розробити та впровадити «Класифікатор загроз державних інформаційних ресурсів».

3. Вперше розроблену структурно-логічну модель організації ієрархічної гілки кодів-вузлів українського сегмента ідентифікаторів, на основі стандартизованої системи світового простору інформаційних ресурсів різних класів та світового дерева ідентифікаторів інформаційних об'єктів, що дозволило визначити місце українського сегмента та створити кодифікації класів загроз ДІР. Дана модель стає організаційно-правовим та організаційно-технічним підґрунтям формування дієздатного реєстру електронних інформаційних ресурсів країни, яка не суперечить міжнародним стандартам.

4. Удосконалений метод визначення стандартних функціональних профілів захищеності ІТС від несанкціонованого доступу до ДІР, на основі структурно-логічної схеми захисту ДІР та стандартизованого опису підсистеми захисту ресурсів, а також вперше введеного поняття моделі «Куб захисту Юдіна-Бучика», що дало можливість впровадити запропоновану систему аналізу ризиків вузлів ІТС дерева ідентифікаторів ДІР та нові підходи для удосконалення методології оцінки ризиків безпеки ІТС у відповідності до міжнародних стандартів.

5. Вперше розроблений комплексний підхід до аналізу ризиків дерева ідентифікаторів ДІР українського сегмента, на базі розробленого методу «подвійної трійки захисту» ДІР та методу визначення рівнів ризику застосування контрзаходів протидії інформаційним атакам та кластеризації ризиків з метою транзитивного замикання бінарного відношення активів. Даний підхід дозволив шляхом розбиття за відповідними альфа-рівнями отримати кластери ДІР різних класів, які згруповані за рівнями ризику та підлягають першочерговим організаційно-технічним діям з формування профілів захищеності.

6. Вперше розроблену технологію побудови та захисту українського сегмента дерева ідентифікаторів ДІР, на базі представлених методів та моделей аналізу ефективності і мінімізації системи ризиків вузлів інформаційно-телекомунікаційної мережі, сформовано профілі захищеності дерева ідентифікаторів державних інформаційних ресурсів, що дозволило здійснювати корегування та оптимізацію засобів захисту (необхідних контрзаходів) визначених інформаційних активів (ресурсів) та провести практичну оцінку ефективності процесу групування активів у кластери для їх подальшого аналізу та корегування в умовах процесів захисту.

Теоретична і наукова цінність та практичне значення одержаних автором наукових результатів. Як показав аналіз, дисертаційна робота Бучика С.С. виконувалась в рамках завдань кафедри комп'ютеризованих систем захисту інформації навчально-наукового Інституту комп'ютерних інформаційних технологій Національного авіаційного університету (тема 876-ДБ13 за № 0113U000893, № 12/09.01.09/13, № 27/09.01.09/14 та № 64/09.01.09/15).

Теоретична та наукова цінність отриманих автором результатів полягає в тому, що вони сприяють формуванню методологічного і технологічного підґрунтя для створення власного стандарту захисту ДІР в Україні. Зазначений

стандартизований підхід може стати системним фактором національної безпеки та оборони країни, базовою практичною моделлю реалізації системи захисту ДІР.

Практичне значення отриманих результатів полягає у тому, що впровадження методології побудови та підвищення ефективності системи захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів дозволило:

сформувати підґрунтя для розробки нових, або удосконалення існуючих нормативних документів в сфері захисту ДІР на кшталт «Термінології в сфері захисту ДІР» та виокремлення сфери захисту державних інформаційних ресурсів в окрему складову національної безпеки держави;

в 1,5 – 2 рази знизити інформаційний ризик вузла інформаційних об'єктів ДІР згідно визначеного ідентифікатора та до 50% зменшити ризик несанкціонованого доступу до повідомлень, які передаються між вузлами ІТС;

прискорити в часі до 12 разів визначення функціонального профілю захищеності вузла ІТС на рівні адміністратора його безпеки шляхом з'ясування стандартного профілю або нестандартного, запропонованого системою.

Оцінка мови та стилю викладання дисертації та автореферату. Дисертація та автореферат написані грамотно, а стиль викладення в них матеріалів досліджень, наукових положень, висновків і рекомендацій відповідає вимогам стандарту ДСТУ 3008-95 «Документація. Звіти у сфері науки і техніки» й у цілому забезпечує доступність їх сприйняття.

Зміст автореферату відображає основні результати роботи, які приведені в дисертації. Дисертація по тематиці і результатам відповідає паспорту спеціальності 21.05.01 – інформаційна безпека держави.

Повнота викладення наукових результатів дисертації в опублікованих роботах. Основні положення та висновки дисертаційної роботи опубліковано в 50 наукових працях. Серед них 1 монографія, 28 статей у фахових наукових виданнях (з них 5 одноосібних), 30 у збірниках праць конференцій (з них 9 одноосібних), 19 статей опубліковано у виданнях, які включені до міжнародних наукометричних баз, отримано два авторських свідоцтва на твір (комп'ютерну програму).

Зазначені публікації повною мірою висвітлюють основні наукові положення дисертації. Стиль викладення автореферату в цілому забезпечує його доступність та сприйняття. В ньому чітко і лаконічно викладені наукові завдання дослідження та шляхи їх вирішення. З тексту зрозуміла наукова і практична значущість роботи, особистий внесок здобувача.

Дискусійні положення та зауваження щодо дисертаційного дослідження.

1) Мета роботи сформульована некоректно. Виходячи з наданих матеріалів метою дисертаційного дослідження має бути, наприклад, підвищення ефективності системи захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів за рахунок мінімізації ризиків ДІР та формування динамічного комплексу ФПЗ.

2) Мають місце розбіжності у кількості задач дослідження (всього їх 8) та отриманих автором наукових результатів (всього їх 6). Доцільніше було б об'єднати 6, 7 і 8 задачі та під номером 6 (новим) озвучити їх, наприклад, так:

«Розробити програмний комплекс оцінки ефективності та адекватності впроваджених методів і моделей».

3) Формулювання задачі під номером 5 «Розробити *метод і модель* визначення ефективності впроваджених *методів та моделей* на основі теорії ризиків та встановленої політики безпеки» в якому двічі повторюється словосполучення «метод і модель» потребує, зважаючи на тавтологію, певного коригування.

4) Не зрозуміло, що саме дозволяє автору вважати запропоновану ним «… сучасну нормативно-правову термінологію класифікації та визначень в галузі захисту ДІР …», а також введену ним « …. термінологію в галузі захисту ДІР (кількість термінів введених у розрізі розробленої методології захисту ДІР сягає 26, з них 23 введені вперше, 3 здійснено уточнення та доповнення) …» (стор. 5 автореферату, стор., 17-18 дисертації) - основою для формування нормативного документа «Термінологія в галузі захисту державних інформаційних ресурсів».

5) Не зрозуміло, якими фактами оперує автор вважаючи, що розроблена ним «…методологія побудови класифікатора загроз на основі організаційно-правового методу «подвійної трійки захисту» …» (стор. 5-6 автореферату, стор., 17-18 дисертації) - дозволила впровадити «Класифікатор загроз державних інформаційних ресурсів». Заява автора стосовно його першості щодо розробки та впровадження «Класифікатора загроз державних інформаційних ресурсів» взагалі провокує на певну дискусію.

6) В дисертації та авторефераті бажано б було вказати про документальне підтвердження (наприклад актами впровадження) кожної практичної цінності, а не представляти це підтвердження в узагальненому вигляді після їх перерахування. Більший акцент необхідно було б зробити на практичні цінності починаючи з п'ятого пункту практичного значення отриманих результатів.

Зазначені недоліки не є визначальними. Вони суттєво не впливають на загальне позитивне враження від роботи, не зменшують її наукової цінності та практичної значимості.

3. Відповідність дисертаційної роботи встановленим вимогам та загальний висновок

Дисертаційна робота *БУЧИКА Сергія Степановича* за темою «Методологія побудови та захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів» є завершеною, одноосібно написаною кваліфікаційною науковою працею, що:

1) являє собою системне дослідження, проведене з певною метою;

2) має внутрішню єдність і свідчить про особистий внесок автора в науку;

3) розв'язує актуальну задачу, яка має важливу наукову і практичну спрямованість й результати вирішення якої за рахунок організації системи мінімізації ризиків ДІР та формування динамічного комплексу ФПЗ істотно впливають на підвищення ефективності системи оперативного управління та захисту інформаційних ресурсів держави.

За актуальністю, ступенем новизни, обґрунтованістю, науковою та практичною значимістю одержаних результатів дисертаційна робота Бучика С.С. відповідає паспорту спеціальності 21.05.01 – «інформаційна безпека держави», а також вимогам «Порядку присудження наукових ступенів і присвоєння вчених звань старшого наукового співробітника», а її автор *БУЧИК Сергій Степанович* заслуговує присудження йому наукового ступеня доктора технічних наук за спеціальністю 21.05.01 – «інформаційна безпека держави».

Офіційний опонент
доктор технічних наук, професор,
завідуючий кафедрою інформаційної та кібернетичної безпеки
Навчально-наукового інституту захисту інформації
Державного університету телекомунікацій В. Л. Бурячок

Підпис д.т.н., професора Бурячка В.Л. засвідчую

Начальник відділу кадрів
Державного університету телекомунікацій С.М.Львовський