ВІДГУК

офіційного опонента
на дисертацію БУЧИКА Сергія Степановича
"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

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

Дисертаційна робота Бучика Сергія Степановича присвячена вирішенню важливої науково-прикладної проблеми підвищення ефективності системи оперативного управління та захисту інформаційних ресурсів держави на основі організації системи мінімізації ризиків державних інформаційних ресурсів (ДІР) та формуванню динамічного комплексу функціональних профілів захищеності (ФПЗ). Автором дисертаційної роботи визначено протиріччя між наявними ДІР і нормативно-правовими, організаційними та інженерно-технічними напрямками їх захисту, та як наслідок цього, наявність недосконалої системи оперативного управління та захисту інформаційних ресурсів держави. Тому тематика дисертаційного дослідження, а саме створення методології побудови та захисту українського сегмента дерева ідентифікаторів ДІР *є актуальною*.

Автор дисертаційної роботи проводив свої дослідження у відповідності з планами наукової та науково-технічної діяльності кафедри комп'ютеризованих систем захисту інформації навчально-наукового Інституту комп'ютерних інформаційних технологій Національного авіаційного університету з тем 876-ДБ13 (№ 0113U000893), № 12/09.01.09/13, № 27/09.01.09/14, № 64/09.01.09/15.

Ступінь обґрунтованості нових положень, висновків і рекомендацій, сформульованих у дисертації.

Сформульовані у дисертаційній роботі основні положення, висновки та рекомендації достатньо повно обґрунтовані, викладені в доказовій формі. Обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації, підтверджується використанням відомого математичного апарату, припущень і обмежень, що не суперечать фізичним основам і відомим рішенням.

Достовірність одержаних результатів також підтверджується коректністю поставлених задач, використанням відомих та добре апробованих сучасних методів досліджень, врахуванням специфіки об'єкта моделювання, застосуванням імітаційного моделювання, експертного оцінювання, а також опублікованими науковими працями, актами впровадження результатів дисертаційної роботи, свідоцтвами про реєстрацію авторського права на твір (комп'ютерні програми).

Наукова новизна одержаних в дисертації результатів полягає, на мій погляд, в наступному:

- розроблено новий організаційно-правовий метод «подвійної трійки захисту» інформаційних ресурсів держави нормативно-правового, організаційного та інженерно-технічного спрямування на базі введеної класифікації та кодифікації загроз різних класів та їх нормативно-правової і професійної семантики;
- розроблена методологія 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»;
- розроблено нову 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;
- удосконалено метод визначення стандартних функціональних профілів захищеності інформаційно-комунікаційних систем (ІКС) від несанкціонованого доступу, вперше введеного поняття моделі «Куб захисту Юдіна-Бучика», що дало можливість впровадити запропоновану систему аналізу ризиків вузлів ІКС дерева ідентифікаторів ДІР та нові підходи для удосконалення методології оцінки ризиків безпеки ІКС у відповідності до міжнародних стандартів;
- запропоновано комплексний підхід до аналізу ризиків дерева ідентифікаторів ДІР українського сегмента, 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;

- розроблено технологію побудови та захисту українського сегмента дерева ідентифікаторів ДІР, сформовано профілі захищеності дерева ідентифікаторів ДІР, що дозволило здійснювати корегування та оптимізацію засобів захисту визначених інформаційних ресурсів.

Практичне значення одержаних в дисертації результатів:

- на основі визначених правових аспектів формування системи ДІР, введеного класифікатора ДІР, аналізу світового дерева ідентифікаторі об'єктів та місця українського сегмента в ньому, розроблених моделей та принципів інформаційної безпеки ДІР встановлено відповідність запропонованої системи їх класифікації до стандартів та вимог згідно світового дерева ідентифікаторів інформаційних ресурсів, що дозволило розробити та ввести сучасну нормативно-правову термінологію класифікації та визначень в галузі захисту ДІР, яка є основою для формування нормативного документа «Термінологія в галузі захисту державних інформаційних ресурсів»;
- розроблений «Класифікатор загроз державних інформаційних ресурсів» дозволив сформувати методологічну основу для побудови та захисту ДІР України як на рівні нормативно-правового захисту, так і на організаційному та інженерно-технічному рівні, виділити галузь захисту ДІР в окрему складову національної безпеки держави. Введена термінологія в галузі захисту ДІР (кількість термінів складає 26, з них 23 введені вперше, 3 уточнені та доповнені) є основою для формування нормативного документа «Термінологія в галузі захисту державних інформаційних ресурсів»;
- розроблена методологія побудови класифікатора загроз на основі організаційно-правового методу «подвійної трійки захисту» дозволила сформувати методологічну основу для побудови та захисту ДІР України на рівні нормативно-правового, організаційного та інженерно-технічного захисту; це підвищило ефективність системи управління інформаційною безпекою ДІР за рахунок введеної деталізації загроз та як наслідок зменшило час (до 8 разів) на формування моделей загроз;
- розроблено програмно-апаратний комплекс реалізації методів та моделей аналізу ризиків дерева ідентифікаторів ДІР, що дозволило здійснювати корегування та оптимізацію засобів захисту щодо визначених ресурсів; впровадження розробленої технології надало змогу 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 ІКС;

- впровадження методу визначення функціональних профілів захищеності вузлів дерева ідентифікаторів ДІР, якій базується на існуючий в Україні нормативно-правовій базі в галузі технічного захисту інформації, дозволило прискорити до 12 разів визначення функціонального профілю захищеності вузла ІКС на рівні адміністратора його безпеки шляхом застосування стандартного профілю або запропонованого системою нестандартного профілю;
- на основі розроблених методології, технології, методів, моделей впроваджено програмно-апаратний комплекс системи захисту та аналізу ризиків ДІР, а також впроваджено систему формування профілів захищеності вузлів ідентифікаторів ІКС.

Дисертація містить 4 акти впровадження результатів досліджень автора, що підтверджують практичне використання одержаних результатів.

Підтвердження повноти викладу основних результатів дисертації в наукових фахових виданнях.

За напрямком досліджень опубліковано більше 50 наукових праць, 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). В монографії, статтях, збірниках праць конференцій повністю висвітлені основні наукові результати досліджень. Таким чином, кількість опублікованих результатів роботи та їх якість відповідає вимогам МОН України до докторських дисертацій.

Оцінка змісту дисертації, її завершеність у цілому, відповідність встановленим вимогам оформлення дисертації.

Дисертація Бучика С.С. написана грамотно, стиль викладення матеріалів досліджень, наукових положень та висновків забезпечує доступність їх сприйняття спеціалістами, а науковий рівень дисертації відповідає існуючим вимогам до докторських дисертацій.

Робота являє собою завершену кваліфікаційну наукову працю, яка містить сукупність результатів досліджень, спрямованих на створення методології побудови та підвищення ефективності захисту українського

сегмента дерева ідентифікаторів державних інформаційних ресурсів й свідчить про вирішення науково-прикладної проблеми та особистий вклад автора в науку.

Відповідність змісту автореферату основним положенням дисертації.

Зміст автореферату достатньо повно відображає основні положення, що викладені у докторській дисертаційній роботі Бучика С.С.

Відповідність дисертаційної роботи заявленої спеціальності.

Дисертаційна робота відповідає паспорту спеціальності 21.05.01 – інформаційна безпека держави, оскільки вона спрямована на розв'язання науково-прикладної проблеми підвищенні ефективності системи оперативного управління та захисту державних інформаційних ресурсів на основі організації системи мінімізації ризиків державних інформаційних ресурсів та формування динамічного комплексу функціональних профілів захищеності.

Об’єкт дослідження – процеси захисту, класифікації, збору, висвітлення, кодифікації державних інформаційних ресурсів, мета дослідження – розроблення методології побудови та підвищення ефективності захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів, відповідають паспорту спеціальності 21.05.01 – інформаційна безпека держави.

Зауваження щодо дисертаційної роботи:

1. На мій погляд в дисертації було б доречним провести аналіз методів та інструментальних засобів управління ризиками (OCTAV, GRAMM, RiskWatch та інш.), хоча автор посилається на праці, де ці методи та інструментальні засоби достатньо повно описані.
2. При розробці класифікатора загроз державним інформаційним ресурсам автором не достатньо обґрунтовано, чому саме здійснено розподіл за двома рівнями загроз, а саме стратегічні та тактичні. Можливо, доречно було б ввести ще додаткові рівні.
3. По тексту дисертації є деякі повтори тлумачень термінів.
4. Коефіцієнти компетентності експертів (табл. 2.8) на мій погляд недостатньо обґрунтовані.
5. Деякий матеріал в дисертації (наприклад, табл. 2.1, 2.2) можна б було винести в додатки. Автореферат дисертації дещо перевантажений рисунками, що в деякій мірі ускладнює процес сприйняття основного матеріалу роботи.
6. У дисертації розроблено метод «подвійної трійки захисту» та етапи реалізації даного методу. Доцільно було б даний матеріал повніше

представити в авторефераті, так як автор представив в авторефераті тільки інформаційно-аналітичну модель методу «подвійної трійки захисту», як основу формування методології.

7. В дисертації проведено аналіз основних підходів до створення класифікатора загроз державним інформаційним ресурсам, що не відображено в матеріалах автореферату.

Загальний висновок про дисертацію та її відповідність вимогам МОН України щодо докторських дисертацій.

Беручи до уваги актуальність теми, наукову новизну та практичну цінність одержаних результатів можна вважати, що дисертаційна робота Бучика С.С. відповідає вимогам «Порядку присудження наукових ступенів», які висуваються до докторської дисертації, як кваліфікаційної наукової праці, а автор дисертаційної роботи – Бучик Сергій Степанович заслуговує на присудження йому наукового ступеня доктора технічних наук за спеціальністю 21.05.01 – інформаційна безпека держави.

Офіційний опонент,
директор навчально-наукового інституту
Радіо, телебачення та інформаційної безпеки
Одеської національної академії зв'язку ім. О. С. Попова,

доктор технічних наук, професор Є.В. Василіу

Підпис завіряю:
Вчений секретар
ОНАЗ ім. О.С. Попова
Руда Г.В.