Голові спеціалізованої вченої ради
Д 26.062.17
Національного авіаційного університету

03680, м. Київ, пр. Космонавта Комарова, 1

ВІДГУК

офіційного опонента професора кафедри загальнонаукових та інженерних дисциплін Національної академії Державної прикордонної служби України імені Богдан Хмельницького, доктора технічних наук, професора Катеринчука Івана Степановича на докторську 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

1. Актуальність теми дисертації, зв'язок з науковими програмами, планами, темами. Дисертаційна робота БУЧИКА Сергія Степановича присвячена вирішенню важливої науково-прикладної проблеми: підвищенню 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). Мета роботи полягає у розробці методології побудови та підвищення ефективності захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів. Таким чином, тематика дисертаційного дослідження, а саме створення методології побудови та захисту українського сегмента дерева ідентифікаторів ДІР *є актуальною*.

Робота виконана 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.

Дисертант БУЧИК Сергій Степанович має практичний досвід з теми дослідження та в повній мірі ознайомлений з роботами провідних вчених у цій галузі, що надало йому можливості всебічно охопити теоретичні засади та розробити методологію побудови та підвищення ефективності захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів.

2. Ступінь обґрунтованості нових положень, висновків і рекомендацій, сформульованих у дисертації. Достовірність одержаних результатів.

Викладені у дисертаційній роботі основні положення, висновки та рекомендації обґрунтовані в повній мірі в доказовій формі. Обґрунтованість та достовірність наукових результатів, висновків і пропозицій, що розроблені й відображені у дисертаційному дослідженні, можна охарактеризувати як цілком достатні, що підтверджується,зокрема, використанням відповідної інформаційної бази: аналізу законодавчих та нормативних актів, аналізом наукових праць вітчизняних та зарубіжних вчених, монографій, дисертацій, публікацій у періодичних виданнях. Крім того, достовірність одержаних результатів підтверджується коректністю поставлених задач, використанням відомих та добре апробованих сучасних методів досліджень, застосуванням імітаційного моделювання, експертного оцінювання, опублікованими автором більше 50 науковими працями, актами про впровадження результатів дисертаційної роботи, свідоцтвами про реєстрацію авторського права на твір.

3. Новизна одержаних результатів:

вперше розроблено 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;

вперше 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»;

вперше розроблено 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;

удосконалено 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;

вперше розроблено 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;

вперше розроблено 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.

Сукупність нових наукових результатів, одержаних автором у ході дослідження, розв'язують актуальну науково-прикладну проблему – підвищення ефективності системи оперативного управління та захисту інформаційних ресурсів держави на основі організації системи мінімізації ризиків державних інформаційних ресурсів та формуванню динамічного комплексу функціональних профілів захищеності.

4. Практичне значення одержаних результатів полягає у наступному:

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 ІБ ДІР встановлено відповідність запропонованої системи їх класифікації до стандартів та вимог з урахування технологій кодифікації 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»;

вперше розроблено «Класифікатор загроз ДІР» на основі методу «подвійної трійки захисту», що дозволило сформувати методологічну основу для побудови та захисту ДІР України як на рівні нормативно-правового захисту, так і організаційному і інженерно-технічному рівні, та як наслідок виділити галузь захисту ДІР в окрему складову національної безпеки держави. Введена термінологія 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) є основою для формування нормативного документа в галузі захисту ДІР «Термінологія в галузі захисту державних інформаційних ресурсів»;

розроблена методологія побудови класифікатора загроз на основі організаційно-правового методу «подвійної трійки захисту» дозволила впровадити «Класифікатор загроз державних інформаційних ресурсів»; сформувати методологічну основу для побудови та захисту ДІР України на рівні нормативно-правового, організаційного та інженерно-технічного захисту; виділити галузь захисту ДІР в окрему складову національної безпеки держави. 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;

вдосконалено методологічні та технологічні основи побудови комплексної системи захисту ДІР, концептуальної моделі інформаційної безпеки ДІР на основі різних класів загроз, типової системи захисту ДІР. Запропонована класифікація типів систем захисту інформації, обґрунтована необхідність використання принципу комплексності захисту ДІР. Як наслідок цього розроблена загальна модель формування системи захисту ДІР на основі методології «подвійної трійки захисту» та визначення ДІР як складової національної безпеки. Це надало можливість розробити метод і модель визначення ефективності впроваджених методів та моделей на основі теорії ризиків та встановленої політики безпеки;

розроблено програмно-апаратний комплекс реалізації методів та моделей аналізу ризиків дерева ідентифікаторів ДІР, що дозволило здійснювати корегування та оптимізацію засобів захисту (необхідних контрзаходів) щодо визначених активів (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 ІТС;

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 в часі до 12 разів визначення функціонального профілю захищеності вузла ІТС на рівні адміністратора його безпеки шляхом з'ясування стандартного профілю або запропонованого нестандартного системою 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 інформаційно-комунікаційної системи об'єктів інформатизації державного призначення з умов проведення оцінки ефективності захисту ДІР та адекватності впровадженим методам.

В дисертації міститься чотири акти впровадження результатів досліджень дисертанта, які підтверджують практичне використання одержаних результатів.

5. Підтвердження повноти викладу основних результатів дисертації в наукових фахових виданнях. Основні наукові положення і результати дисертаційної роботи опубліковано у більше 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). В монографії, статтях, збірниках праць конференцій повністю висвітлено всі основні наукові результати досліджень. Кількість опублікованих результатів роботи та їх якість відповідає вимогам Міністерства освіти і науки України, що висуваються до докторських дисертацій.

6. Оцінка змісту дисертації, її завершеність у цілому, відповідність встановленим вимогам оформлення дисертації. Дисертаційна робота складається зі вступу, п'яти розділів, висновків та списку використаних джерел (234 найменування) на 30 сторінках, 8 додатків на 72 сторінках. Загальний обсяг дисертації становить 398 сторінок, у тому числі 262 сторінки основного тексту, ілюстрацій – 80 (з них 11 – на 11 окремих сторінках), таблиць – 35 (з них 9 – на 23 окремих сторінках).

Дисертація написана сучасною українською науково-технічною мовою, є логічно структурованою. Оформлення дисертації відповідає чинним вимогам, що пред'являються до дисертаційних робіт. Автореферат повністю

розкриває зміст дисертації. Стиль викладу матеріалів досліджень, наукових положень, висновків і рекомендацій забезпечує легкість і доступність їх сприйняття.

В цілому дисертація є закінченою науковою роботою, яка містить сукупність результатів досліджень й свідчить про вирішення науково-прикладної проблеми та особистий вклад автора в науку, відповідає паспорту спеціальності 21.05.01 – інформаційна безпека держави.

7. Відповідність змісту автореферату основним положенням дисертації. Автореферат дисертації БУЧИКА С. С. повністю відображає зміст дисертаційної роботи.

8. Дискусійні положення та зауваження:

1. В підрозділі 1.5 (стор. 62) дисертації автором стверджується, що "фактично місце аналізу ризиків інформаційної безпеки на державному рівні … майже не визначено", що на мій погляд є дискусійним.
2. При розгляді методів аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів матеріал, представлений в дисертації скоріш за все стосуються проблематики оброблення ризиків, точніше, одного з можливих аспектів цієї проблематики, а саме – економізації вартості рішень у сфері розробки систем захисту інформації на базі ризикового підходу, що на мій погляд знову ж є дискусійним питанням.
3. В зв'язку з тим, що автором за основу при постановці задачі аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів взято введений в дисертації куб Юдіна-Бучика, основою якого є трійка характеристик, було б доречним показати графік залежності витрат на захист від рівня захисту (рис. 4.14, стор. 221) також в тримірному вимірі.
4. Оцінку ефективності системи контрзаходів загрозам інформаційним ресурсам автор пропонує шляхом розв'язування задачі лінійного програмування розподілу способів та методів захисту від атак. У якості цільової функції обрано мультиплікативний функціонал (4.69, стор. 226), який необхідно спрямувати до 1. Проте, серед часткових критеріїв є такі (f_1, f_2), які необхідно максимізувати, а f_3 – мінімізувати одночасно. Вважаю, що цільова функція (4.69) записана некоректно, або необхідно було б розкрити процедуру оптимізації таї задачі.
5. В дисертаційній роботі таблиці оформлені не одноманітно. Так, наприклад в табл.1.1 на стор. 51 вказано про продовження таблиці і на стор. 52 про закінчення таблиці, на відміну від цього в табл.2.1 даний порядок не дотриманий. На відміну від дисертації, в авторефераті дисертанта

всі таблиці виконані одноманітно. На мій погляд, для більшої наочності необхідно було б збільшити деякі рисунки (наприклад рис. 4.6, стор. 202; рис. 5.1, стор. 244). В додатках (стор. 366) не вірно визначено літеру додатку, відповідно до змісту має бути Е, а не Д.

9. Висновок про дисертацію в цілому та відповідність її вимогам ВАК України. Зазначені недоліки й зауваження щодо дисертаційної роботи БУЧИКА С. С. не носять принципового характеру та не впливають на її позитивну оцінку. В цілому робота представляє самостійне, завершене наукове дослідження, а її основні положення є науково обґрунтованими, достовірними й корисними як у теоретичному, так і в практичному аспектах, які в сукупності вирішують важливу науково-прикладну проблему в галузі інформаційна безпека держави.

Дисертаційна робота за оформленням, науковим рівнем, актуальністю, науковою новизною та практичною цінністю відповідає чинним вимогам пп. 9, 10, 12 положення про „Порядок присудження наукових ступенів і присвоєння вченого звання старшого наукового співробітника" та паспорту спеціальності – 21.05.01 – інформаційна безпека держави.

Автор дисертації – БУЧИК Сергій Степанович заслуговує на присудження йому наукового ступеня доктора технічних наук за спеціальності – 21.05.01 – інформаційна безпека держави.

Офіційний опонент,
професор кафедри загальнонаукових та інженерних дисциплін
Національної академії Державної прикордонної служби України
імені Богдана Хмельницького
доктор технічних наук, професор,
заслужений працівник освіти України,
лауреат Державної премії України у галузі науки і техніки

І. С. Катеринчук

"30" вересня 2016 р.

Підпис професора Катеринчука І. С. засвідчую.
Начальник відділення контролю та документального забезпечення
Національної академії ДПС України

О. М. Олошинець

"30" вересня 2016 р.