УДК 004.056.5:35.078.3(02)

С. С. Бучик — д-р техн. наук, доц.
Житомирський військовий інститут імені С. П. Корольова
orcid.org/0000-0003-0892-3494
e-mail: s_stbu@ukr.net;

О. К. Юдін — д-р техн. наук, проф.
Національний авіаційний університет
orcid.org/0000-0001-5098-7796
e-mail: kszi@ukr.net

ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ АСПЕКТИ ПОБУДОВИ ТА ЗАХИСТУ УКРАЇНСЬКОГО СЕГМЕНТА ДЕРЕВА ІДЕНТИФІКАТОРІВ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Актуальність дослідження

Рівень інформаційного суспільства провідної держави світу характеризується показниками розвитку сучасних наукоємних технологій, а також роллю, що відіграють інформаційно-телекомунікаційні системи (ІТС) в інтеграції державних інформаційних ресурсів (ДІР) у сферу життєдіяльності країни та суспільства. Розвиток сучасних комунікаційних відносин в інформаційному просторі держави, сукупність політичних, економічних, військових і соціальних рішень у країні залежить від взаємодії та спільного використання інформаційних потоків загального й спеціального призначення.

Подальший розвиток національної безпеки і оборони держави, досягнення стратегічних цілей можливо реалізувати тільки на основі сучасних розвинених інфраструктур між різними відомчими і міжрегіональними рівнями, об'єднаними у єдиний інформаційно-телекомунікаційний простір з динамічним розподілом функцій управління. Зазначений простір повинен забезпечити інформаційну й функціональну взаємодію окремих державних структур, міністерств, відомств між собою в інтегрованому процесі зберігання, впровадження, використання та висвітлення інформаційних ресурсів держави.

Гостра необхідність інформатизації системи управління, створення баз даних та знань ДІР зумовлена сьогодні, насамперед, проведенням в державі нової економічної політики, зростанням кількості техногенних катастроф, загостренням військової агресії з боку інших держав, тощо. Зазначимо, що інформаційна війна як соціально-технічний інструмент, стала важливою частиною військово-політичного втручання інших держав у життєві процеси України.

Значну роль у протидії інформаційній війні слід приділяти захисту ДІР на основі сформованої інформаційної політики країни та впровадженню комплексного підходу до побудови системи захисту. Нормативно-правові акти (НПА) та питання створення політики безпеки, моделі загроз, моделі порушника, профілів захищеності ДІР в Україні несуть загальний характер, або не сформовані взагалі. Загрози інформаційній безпеці (ІБ) держави відіграють базову роль у формуванні політики та самої системи захисту ресурсів країни.

Закони України та НПА повинні чітко визначати стратегію і концептуальні кроки в забезпеченні національної безпеки України, а саме такі як: забезпечення інформаційного суверенітету; вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових передумов для розвитку національної інформаційної інфраструктури та її ресурсів; визначення методів та заходів протидії актуальним загрозам ІБ країни; актуалізація загроз кібербезпеки і безпеки ДІР (уразливість об'єктів критичної інфраструктури, ДІР до кібератак) тощо.

Для реалізації вказаних основних напрямів національної безпеки та протидії різним класам загроз інформаційним ресурсам виникає необхідність розроблення науково-обґрунтованої методології побудови та захисту ДІР, як складової національної безпеки держави. Виникає гостра потреба в необхідності володіти відповідним науково-методологічним апаратом побудови моделей політики безпеки, загроз, порушника, оцінки ризиків, вибору функціонального профілю захищеності (ФПЗ) та методів оцінки ефективності системи захисту ДІР. Звідси виникає *актуальне науково-практичне завдання* — підвищення ефективності захисту ДІР в сучасних умовах інформаційного протиборства та зовнішньої агресії, а також об'єктивна необхідність в створенні дієвої системи управління ІБ ДІР.

Основні загрози ІБ, які впливають на ДІР, характеризуються політичною, економічною, соціальною нестабільністю та дестабілізацією сус-

пільних факторів та відносин на платформі реалізації великого спектра напрямів ведення інформаційних війн.

До них можна віднести: загрози інформаційному забезпеченню державної політики України; загрози розвитку вітчизняної індустрії інформатизації, телекомунікації і зв'язку, ефективного використання вітчизняних інформаційних ресурсів; порушення технологій зберігання, обробки, передачі і висвітлення інформації; загрози безпеці інформаційних і телекомунікаційних засобів і систем; протиправне збирання і використання інформації; несанкціонований доступ до інформації, що знаходиться в базах даних і знань.

Наявні ДІР та їх обсяги, класи з однієї сторони постійно динамічно зростають, з іншої сторони — не сформована конкретизована правова та інженерно-технічна концепція (методології, технології, методи, моделі тощо) протидії порушникам ДІР різних класів, відповідно не до кінця визначена нормативно-правова база та її складова — термінологія (відсутній єдиний стандарт термінів ІБ ДІР).

Гостро стоїть необхідність внесення змін у законодавчу базу щодо визначення класифікації ДІР, порядку їх зберігання, обробки, передачі, висвітлення, а також відсутня модель порушника та відповідно дієва методологія оцінки ризику ДІР, не класифіковані та не деталізовані їх загрози, відсутня система кодифікації ДІР та її адаптація до світових стандартів (у т. ч. до світового дерева ідентифікаторів).

Це призводить до ***протиріччя*** між наявними ДІР і нормативно-правовими, організаційними та інженерно-технічними напрямками їх захисту, та як наслідок, наявна недосконала система оперативного управління та захисту інформаційних ресурсів держави на основі організації системи мінімізації ризиків ДІР та формування динамічного комплексу ФПЗ.

Тому, визначення теоретичних та практичних аспектів побудови та захисту українського сегмента дерева ідентифікаторів ДІР ***є актуальним.***

Таким чином, матеріали статті присвячені вирішенню важливої ***науково-прикладної проблеми*****:** підвищення ефективності системи оперативного управління та захисту інформаційних ресурсів держави на основі організації системи мінімізації ризиків ДІР та формування динамічного комплексу ФПЗ.

Вирішення даної науково-прикладної проблеми повинно сформувати методологічне і технологічне підґрунтя для створення власного стандарту захисту ДІР в Україні.

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

Аналіз останніх досліджень та публікацій

Значний внесок у розвиток нормативно-правового, організаційного та інженерно-технічного захисту інформаційних ресурсів зробили вітчизняні та закордонні наукові дослідники. Серед них: Арістова І. В., Астахов А. М., Бабак В. П., Баранник В. В., Богуш В. М., Бойченко О. В., Бурячок В. Л., Василіу Є. В., Віхорев С. В., Горбенко І. Д., Грайворонський М. В., Додонов О. Г., Дудикевич В. Б., Задірака В. К., Катеринчук І. С., Касперський Е. В., Когаловський М. Р., Конахович Г. Ф., Корнейко О. В., Корченко А. Г., Крихен Д., Майер Н., Марущак А. І., Медведовський І. Д., Мельніков В. П., Мохор В. В., Нестеренко О. В., Новіков О. М., Олійник О. В., Поповський В. В., Почепцов Г. Г., Хамди М., Хахановський В. Г., Шаньгин В. Ф., Шенон К., Шнайер Б. та ін.

Мета статті

Мета статті полягає в узагальненні розробленого групою авторів оригінального авторського погляду на теоретичні та практичні аспекти побудови та підвищення ефективності захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів.

Виклад основного матеріалу

Базуючись на проведеному аналізі нормативно-правового забезпечення захисту ДІР в ІТС [1], виявлено відсутність в Україні дієвого механізму побудови та захисту українського сегмента дерева ідентифікаторів ДІР, що і визначило необхідність розробки відповідних теоретичних та практичних аспектів, які б не суперечили міжнародним стандартам.

У праці [1] запропоновано інформаційно-аналітичну модель методу «подвійної трійки захисту».

Дана інформаційно-аналітична модель є підґрунтям для формування «Класифікатора загроз ДІР» з подальшим поділом класифікації за характером спрямованості та видом загроз.

Виходячи з представленої інформаційно-аналітичної моделі методу «подвійної трійки захисту», безпосередньо сам метод складається з послідовності етапів реалізації моделі «Plan-Do-Check-Act» (PDCA — цикл Шухарта–Деминга — планування — реалізація — перевірка — дія) [2], але з урахуванням першої та другої платформи ІБ (рис. 1).

Узагальнена структурна схема формування класифікатора загроз ДІР можна представити таким чином (рис. 2).

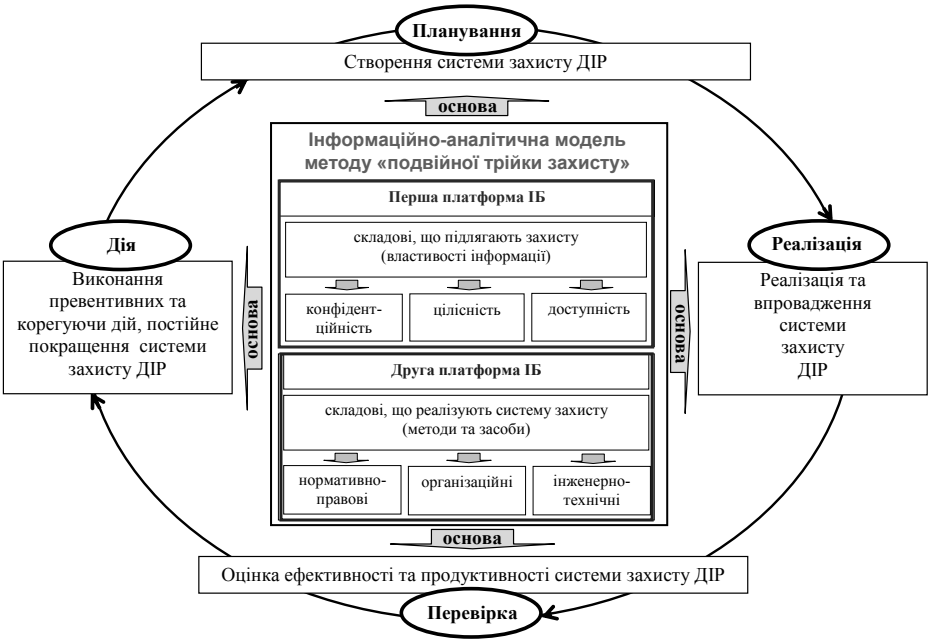


Рис. 1. Модель методу «подвійної трійки захисту» на основі моделі PDCA

Рис. 2. Структурна схема формування класифікатора загроз ДІР

Дана структурна схема повністю відображає структуру формування класифікатора загроз та інформаційно-аналітичну модель методу «подвійної трійки захисту».

Узагальнюючи попередні міркування, методологія побудови класифікатора загроз ДІР буде полягати в наступному:

1. Визначення множини загроз ДІР — ЗДІР.

2. Визначенні з цієї множини (ЗДІР) загроз нормативно-правового (НПС), організаційного (ОргС) та інженерно-технічного спрямування (ІнжТС) — ЗДІР = {НПС, ОргС, ІнжТС}.

3. Поділити загрози НПС, ОргС, ІнжТС на стратегічні і тактичні.

4. Поділити загрози НПС, ОргС, ІнжТС стратегічного та тактичного характеру за властивостями інформації (конфіденційністю, цілісністю та доступністю).

5. Визначити функціональні профілі загроз за процедурою дій порушника, яка характеризується додатковою інформацією про направленість загрози ДІР.

6. Періодично (не менше одного разу на рік) здійснювати уточнення визначених загроз або доповнення новими з відповідним повторенням п. 2–5.

Враховуючи запропоновану інформаційно-аналітичну модель методу «подвійної трійки захисту», як основу формування методології побудови класифікатора загроз ДІР з урахуванням складових процесу захисту інформаційних ресурсів, авторами була розроблена концептуальна модель інформаційної безпеки ДІР [2]. Розроблена концептуальна модель інформаційної безпеки ДІР об’єднала вимоги міжнародного стандарту ISO/IEC 15408, існуючи підходи та врахувала ті напрацювання, які були зроблені авторами. Виходячи з принципів побудови комплексної системи захисту (КСЗ) ДІР, авторами була запропонована узагальнена багаторівнева структурна схема системи захисту ДІР [4].

Дана структурна схема є ієрархічною і до неї може застосовуватись доказовий підхід, ідея якого полягає в послідовній перевірці правильності описів системи захисту на кожному з використовуваних рівнів та адекватності переходу від одного рівня опису до наступного.

Авторами розроблена типова система захисту інформації ДІР з урахуванням розробленого методу «подвійної трійки захисту» та запропонована на її основі класифікація типів систем захисту інформації і обґрунтована необхідність використання принципу комплексності захисту ДІР [5].

Розроблена структурно-логічна схема реалізації системи захисту ДІР за методом «подвійної трійки захисту», яка представлена в праці [6], з урахуванням процесного підходу (моделі PDCA) створення системи менеджменту інформаційної безпеки (СМІБ) згідно ISO/IEC 27001.

Модель складається з трьох основних блоків: системи управління інформаційною безпекою (СУІБ) ДІР; системи захисту ДІР у різних сферах захисту; системи ДІР, як складової національної безпеки.

На рис. 3 представлена структурно-логічна модель організації ієрархічної гілки кодів-вузлів українського сегмента ідентифікаторів об’єктів (ІО) державних органів (після визначеної гілки gov(1)).

Дана структурно-логічна модель стала логічним продовження проведених авторами досліджень, які були представлені в праці [1].

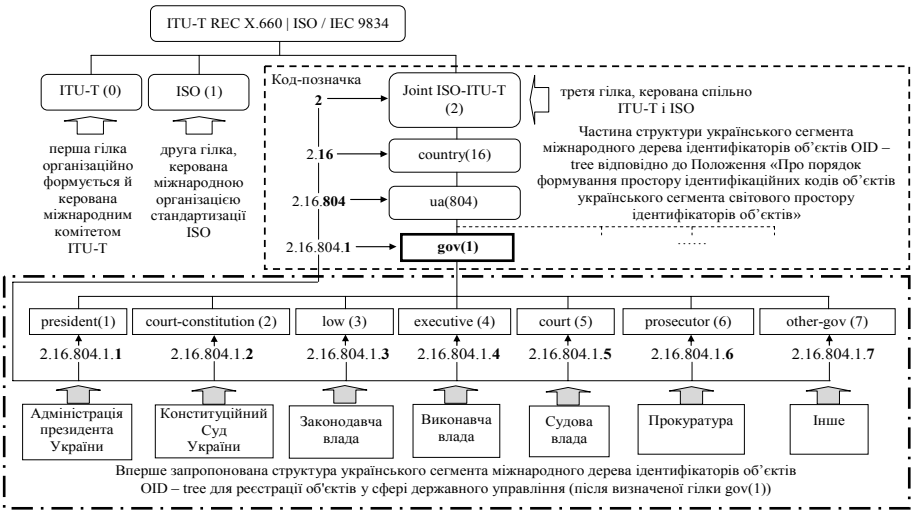


Рис. 3. Структурно-логічна модель організації ієрархічної гілки кодів-вузлів українського сегмента ідентифікаторів об’єктів державних органів (після визначеної гілки gov(1))

Дана модель дозволила створити організаційно-правове та організаційно-технічне підґрунтя формування дієздатного реєстру електронних інформаційних ресурсів країни відповідно до міжнародних вимог та стандартів.

На основі структурно-логічної моделі організації ієрархічної гілки кодів-вузлів українського сегмента ідентифікаторів об'єктів державних органів (після визначеної гілки gov(1)) — рис. 3 вперше визначено гілки щодо структури судів загальної юрисдикції.

Таким чином, встановлено відповідність системи класифікації ДІР до світових стандартів та вимог з урахування технологій кодифікації згідно світового дерева інформаційних ресурсів.

Авторами розроблена система термінів та визначень методології захисту державних інформаційних ресурсів [7]. Повний перелік введених термінів (кількість термінів уведених у розрізі розробленої методології захисту ДІР сягає 26, з них 23 введені вперше, 3 здійснено уточнення та доповнення), які є основою для формування нормативного документа «Термінологія в галузі захисту державних інформаційних ресурсів».

Постановка проблеми аналізу ризику дерева ідентифікаторів ДІР, з урахуванням методології «подвійної трійки захисту», представлено авторами в праці [8].

Уперше введено поняття «куб захисту Юдіна–Бучика». Удосконалено життєвий цикл методології оцінки ризиків безпеки ІТС, наведено механізм визначення рівня ризику ДІР.

Визначенні вихідні дані для здійснення аналізу ризиків вузлів ІТС дерева ідентифікаторів ДІР з урахуванням розкриття кубу Юдіна–Бучика.

Таким чином, визначені вихідні дані для вперше розробленого методу визначення рівня ризику застосування контрзаходів щодо визначених ресурсів та вперше розробленого методу кластеризації ризиків на основі транзитивного замикання бінарного відношення активів [9].

Удосконалено метод визначення ФПЗ вузлів ІТС дерева ідентифікаторів ДІР, який представлено в праці [10].

На основі представленого методу формалізації визначення ФПЗ вузлів ІТС дерева ідентифікаторів ДІР за функціональними критеріями розроблений програмний продукт «Інформаційна система визначення функціонального профілю захищеності автоматизованої системи від несанкціонованого доступу (ОФПАС 1.0)» [11].

Початкове вікно програми представлено на рис. 4.

Для початку створення функціонального профілю захищеності необхідно перевірити виконання вимог та необхідних умов для рівня послуги цілісність комплексу засобів захисту (КЗЗ) НЦ-1, оскільки даний рівень послуги є необхідною умовою абсолютно для всіх рівнів всіх послуг.

За умови виконання даних вимог та необхідних умов стає активною кнопка «Далі», що надає можливість продовження роботи з програмним забезпеченням.

При натисканні кнопки «Далі» відкривається головне вікно програми (рис. 5).

За допомогою даного програмного продукту можна визначати як стандартні ФПЗ (рис. 6) так і нестандартні (рис. 7).

ФПЗ являє собою перелік мінімально необхідних рівнів послуг, які повинні реалізовувати КЗЗ ІТС, щоб задовольняти певні вимоги щодо захищеності інформації, яка обробляється в даній ІТС.

Єдина вимога, якої слід дотримуватися при утворенні нових профілів захищеності, — це додержання описаних в НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу» необхідних умов для кожної із послуг, що включаються до профілю.

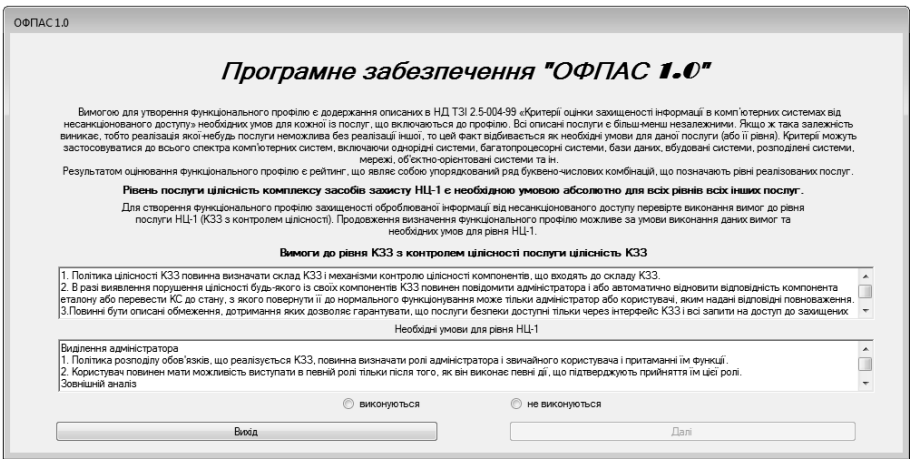


Рис. 4. Початкове вікно програми

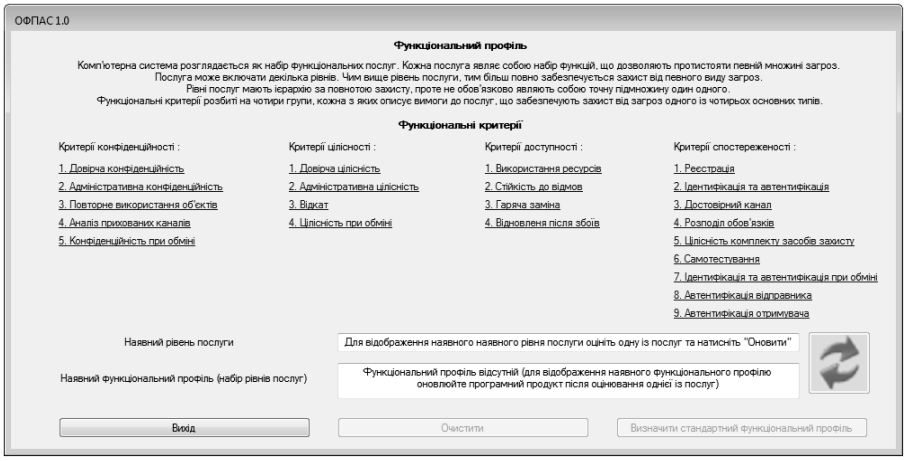


Рис. 5. Головне вікно програми

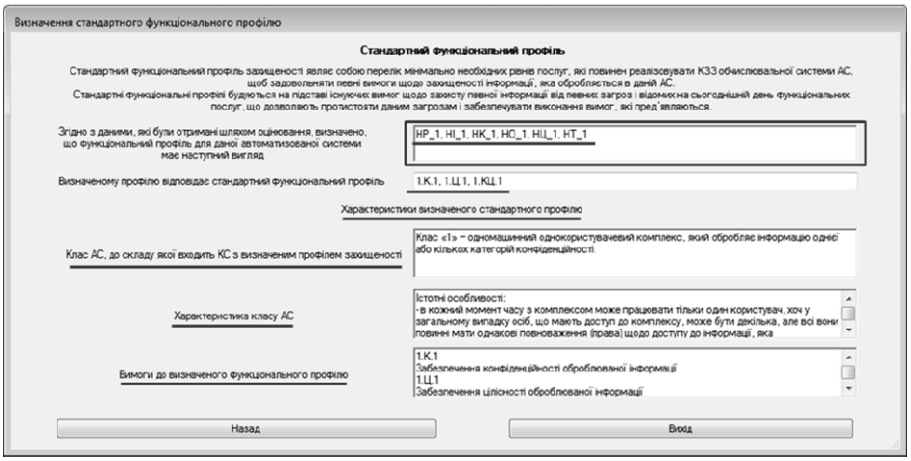


Рис. 6. Приклад визначення стандартного профілю захищеності

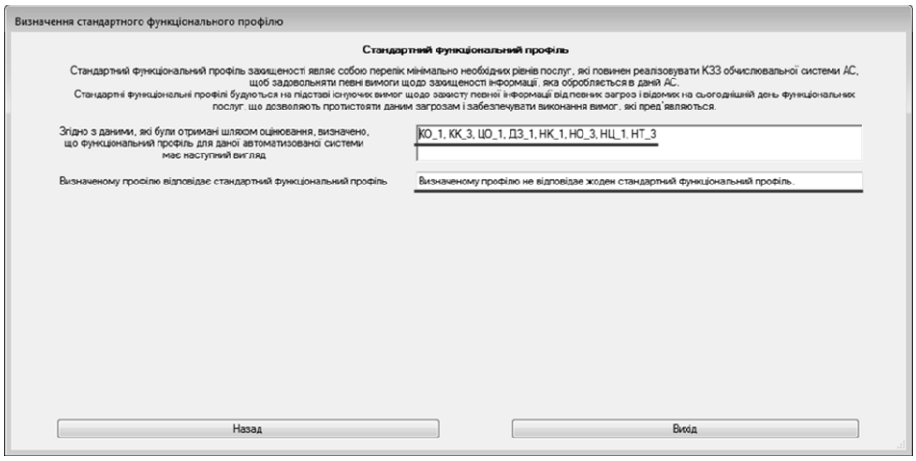


Рис. 7. Приклад визначення нестандартного профілю захищеності

Відповідно до даного нормативного документу в головному вікні програми знаходиться 22 посилання, які відповідають послугам конфіденційності, цілісності, доступності та спостережності. Удосконалення та впровадження методу визначення функціональних профілів захищеності вузлів дерева ідентифікаторів ДІР 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.

Уперше розроблено технологію побудови та захисту дерева ідентифікаторів ДІР на основі ризик-менеджменту, яка представлена авторами в праці [12].

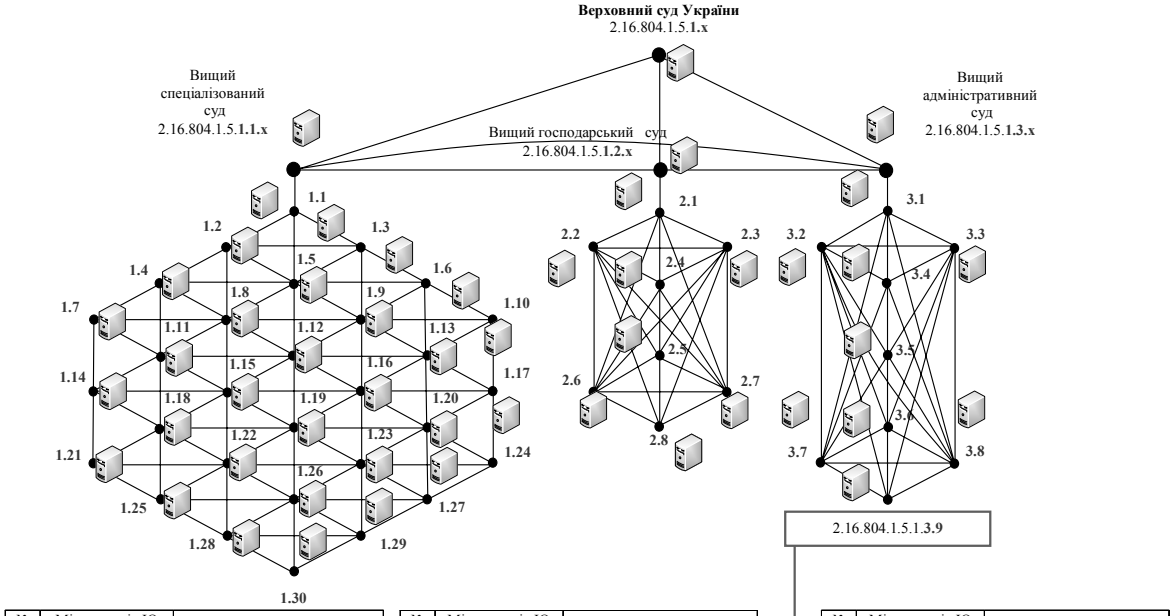
Обмеженням при реалізації даної технології є відсутність врахування пропускної здатності ліній передачі інформації між вузлами ІТС, що може бути в подальшому реалізовано шляхом

введення ваги, яка б визначала пропускну здатність відповідної лінії.

З урахуванням розробленої ієрархічної гілки кодів вузлів для наповнення Національного реєстру українського сегмента міжнародного дерева ідентифікаторів об'єктів на базі структури системи судів загальної юрисдикції, вперше представлення вузлів ІТС дерева ідентифікаторів українського сегмента на базі структури системи судів загальної юрисдикції України (до рівня апеляційних судів) може бути представлено так (рис. 8).

За п. 1–4 технології [12] необхідно здійснити розрахунок ризиків всіх вузлів ІТС українського сегмента дерева ідентифікаторів ДІР (у нашому випадку для прикладу було взято дев'ять вузлів ІТС, для розкриття технології в загальному вигляді).

На основі транзитивного замикання бінарного відношення (п. 6 технології [12]) будуємо дерево вузлів ІТС ідентифікаторів ДІР з урахуванням їх групування за α-рівнями та визначенням оптимальної топології з'єднання вузлів ІТС з урахуванням їх узагальнених інформаційних ризиків. За результатами транзитивного замикання будуємо дендограму утворення кластерів за відповідними α-рівнями (рис. 9).



№ з/п	Мітки вузлів ІО (dot notation)	Назва суду
1	2.16.804.1.5.1.**1.1**	м. Київ
5	2.16.804.1.5.1.**1.5**	Вінницький АСО*
11	2.16.804.1.5.1.**1.11**	Житомирський АСО
15	2.16.804.1.5.1.**1.15**	Київський АСО
18	2.16.804.1.5.1.**1.18**	Львівський АСО
22	2.16.804.1.5.1.**1.22**	Рівненський АСО
24	2.16.804.1.5.1.**1.24**	Тернопільський АСО
25	2.16.804.1.5.1.**1.25**	Харківський АСО
27	2.16.804.1.5.1.**1.27**	Хмельницький АСО

*АСО – апеляційний суд області

№ з/п	Мітки вузлів ІО (dot notation)	Назва суду
1	2.16.804.1.5.1.**2.1**	Дніпропетровський АГС *
2	2.16.804.1.5.1.**2.2**	Донецький АГС
3	2.16.804.1.5.1.**2.3**	Київський АГС
4	2.16.804.1.5.1.**2.4**	Львівський АГС
5	2.16.804.1.5.1.**2.5**	Одеський АГС
6	2.16.804.1.5.1.**2.6**	Рівненський АГС
7	2.16.804.1.5.1.**2.7**	Севастопольській АГС
8	2.16.804.1.5.1.**2.8**	Харківський АГС

*АГС – апеляційний господарський суд

№ з/п	Мітки вузлів ІО (dot notation)	Назва суду
1	2.16.804.1.5.1.**3.1**	Вінницький ААС*
2	2.16.804.1.5.1.**3.2**	Дніпропетровський ААС
3	2.16.804.1.5.1.**3.3**	Донецький ААС
4	2.16.804.1.5.1.**3.4**	Житомирський ААС
5	2.16.804.1.5.1.**3.5**	Київський ААС
6	2.16.804.1.5.1.**3.6**	Львівський ААС
7	2.16.804.1.5.1.**3.7**	Одеський ААС
8	2.16.804.1.5.1.**3.8**	Севастопольській ААС
9	2.16.804.1.5.1.**3.9**	Харківській ААС

*ААС – апеляційний адміністративний суд

Рис. 8. Представлення вузлів ІТС дерева ідентифікаторів українського сегмента на базі структури системи судів загальної юрисдикції України (до рівня апеляційних судів)

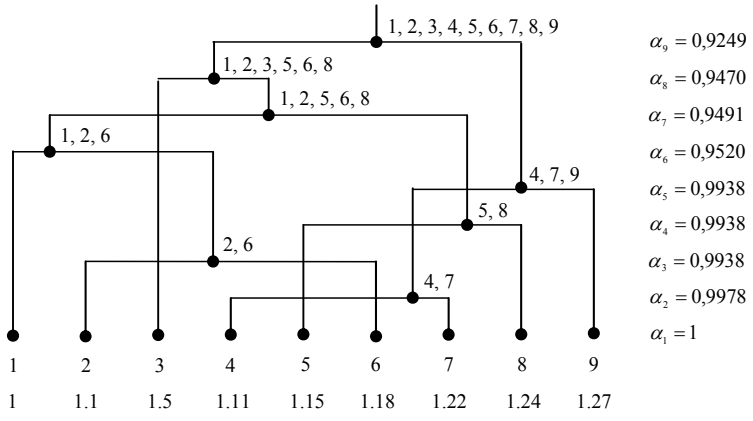


Рис. 9. Дендограма утворення кластерів за відповідними α-рівнями

Визначимо, який з α-рівнів є оптимальним. Для цього визначимо оптимальну кількість кластерів — $K_{\text{опт}}$. Відповідно з алгоритмом об'єктивної комп'ютерної кластеризації здійснимо ієрархічний перебір гіпотез про кількість кластерів для підвибірок А та В (рис. 10), які отримуються відповідно до адрес диполів (табл. 1).

Здійснимо перебір кластеризацій за критерієм несуперечливості, який розраховується за формулою:

$$CY_{AB} = \frac{k - \Delta k}{k} \to \min,$$

де k — кількість кластерів, які виділені на вибірках А і В (відмінних та тих, які співпадають); Δk — кількість кластерів, які співпадають.

Як видно з рис. 10 $CY_{AB} = 0$ при $K_A = K_B = 2$, що і є в даному випадку оптимальною кластеризацією.

Крайні значення, коли $K_A = K_B = 1$ та $K_A = K_B = 8$ є тривіальними і не розглядаються.

Запишемо об'єднані адреси об'єктів за яких $CY_{AB} = 0$ (табл. 2).

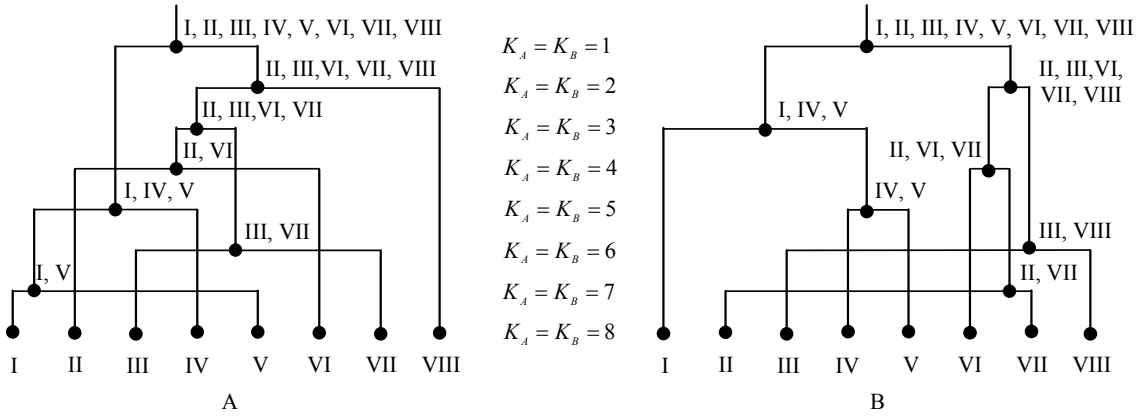


Рис. 10. Ієрархічний перебір гіпотез про кількість кластерів для підвибірок А та В

Таблиця 1

Таблиця адрес диполів для підмножин А і В

Адреси диполів	I	II	III	IV	V	VI	VII	VIII
A	4	2	5	4	7	1	5	3
B	7	6	8	9	9	2	6	8

Таблиця 2

Таблиця визначення кластерів за адресами об'єктів

Адреса	Диполь	Об'єкти об'єднані в кластер	Номер кластеру	Мітка вузла ІТС ІО
I	4 – 7	4	I	2.16.804.1.5.1.**1.11**
IV	4 – 9	7		2.16.804.1.5.1.**1.22**
V	7 – 9	9		2.16.804.1.5.1.**1.27**
II	2 – 6	1	II	2.16.804.1.5.1.**1**
III	5 – 8	2		2.16.804.1.5.1.**1.1**
VI	1 – 2	3		2.16.804.1.5.1.**1.5**
VII	5 – 6	5		2.16.804.1.5.1.**1.15**
VIII	3 – 8	6		2.16.804.1.5.1.**1.18**
		8		2.16.804.1.5.1.**1.24**

У випадку наявності декількох нульових значень критерію несуперечливості необхідно деякі диполі «перевернути» та здійснити розрахунок сумарного критерію несуперечливості CY_{Σ}.

Здійснюючи порівняння табл. 2, з погляду отриманих об'єктивних кластерів і рис. 9, оптимальним α-рівнем є $\alpha_8 = 0{,}9470$.

Матриця замикання по транзитивності дозволяє нам визначити, існує чи ні можливість передати повідомлення з одного місця в інше.

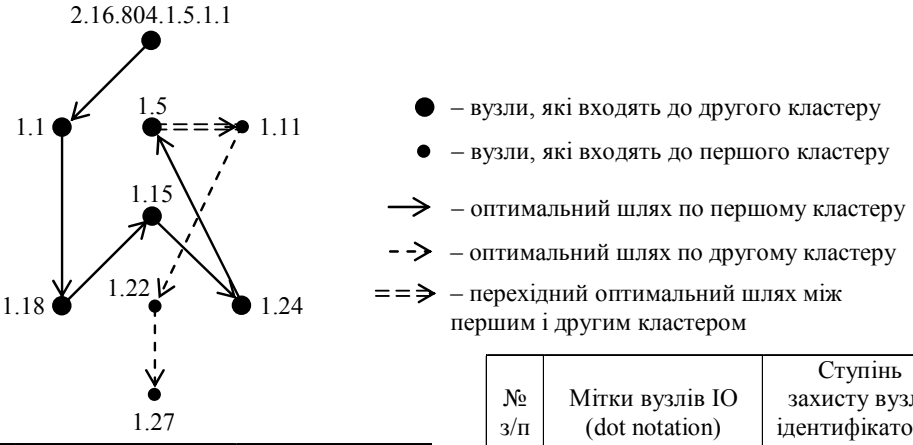
В нашому випадку, за дендограмою утворення кластерів за відповідними α-рівнями (рис. 9) та визначеними алгоритмом об'єктивної комп'ютерної кластеризації кластерами (рис. 10, табл. 2) прослідкуємо оптимальний шлях пере-

дачі повідомлень між вузлами ієрархічного дерева ІО з урахуванням значення усередненого ризику на вузлах ІТС (рис. 11).

На рис. 12 показане наочне представлення оптимального шляху передачі повідомлень між вузлами ІТС, які були розкриті на рис. 8.

Відповідно до 7 пункту технології [12], необхідно періодично (не менше ніж 1 раз на рік) здійснювати уточнення класифікатора загроз державним інформаційним ресурсам та перегляд відповідно п. 1–6 представленої технології оцінювання ризиків, визначення оптимальної топології з'єднання вузлів і функціональних профілів їх захищеності. Результат використання транзитивного замикання бінарного відношення середніх рівнів ризику вузлів ІТС та визначення оптимального α-рівня дозволяє отримати оптимальний шлях передачі повідомлень між вузлами ієрархічного дерева ІО та розбити цей шлях на кластери за рівнями ризику, що дозволяє до 50 % зменшити ризик несанкціонованого доступу до повідомлень, які передаються між вузлами ІТС.

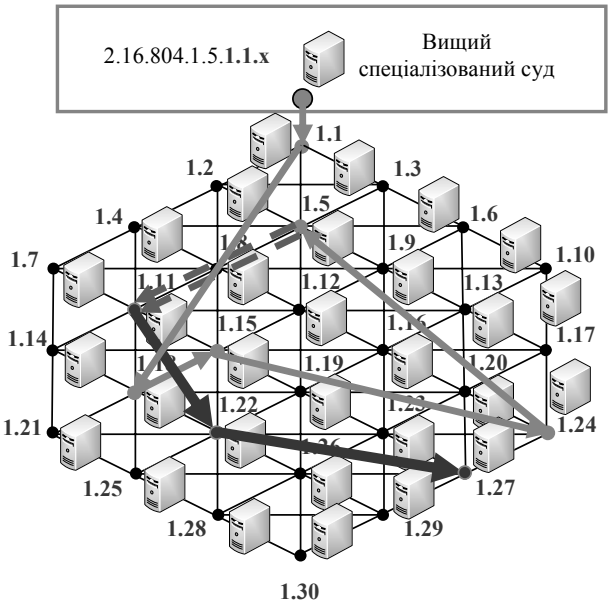
Таким чином загальна концепція проведених досліджень може бути представлена так (рис. 13).



№ з/п	Мітки вузлів ІО (dot notation)	Ступінь захисту вузла ідентифікаторів об'єктів
І кластер		
4	2.16.804.1.5.1.**1.11**	0,59
7	2.16.804.1.5.1.**1.22**	0,59
9	2.16.804.1.5.1.**1.27**	0,58

№ з/п	Мітки вузлів ІО (dot notation)	Ступінь захисту вузла ідентифікаторів об'єктів
ІІ кластер		
1	2.16.804.1.5.1.**1**	0,7
2	2.16.804.1.5.1.**1.1**	0,68
3	2.16.804.1.5.1.**1.5**	0,63
5	2.16.804.1.5.1.**1.15**	0,66
6	2.16.804.1.5.1.**1.18**	0,68
8	2.16.804.1.5.1.**1.24**	0,65

Рис. 11. Оптимальний шлях передачі повідомлень між вузлами ІТС ієрархічного дерева ІО



№ з/п	Мітки вузлів ІО (dot notation)	Ступінь захисту вузла ідентифікаторів об'єктів
І кластер		
4	2.16.804.1.5.1.**1.11**	0,59
7	2.16.804.1.5.1.**1.22**	0,59
9	2.16.804.1.5.1.**1.27**	0,58
ІІ кластер		
1	2.16.804.1.5.1.**1**	0,7
2	2.16.804.1.5.1.**1.1**	0,68
3	2.16.804.1.5.1.**1.5**	0,63
5	2.16.804.1.5.1.**1.15**	0,66
6	2.16.804.1.5.1.**1.18**	0,68
8	2.16.804.1.5.1.**1.24**	0,65

Рис. 12. Наочне представлення оптимального шляху передачі повідомлень між вузлами ІТС

Рис. 13. Загальна концепція проведених досліджень

Основні результати

У статті представлені такі наукові результати.

1. Уперше 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.

2. Уперше 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».

3. Уперше 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.

4. 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 відповідно до міжнародних стандартів.

5. Уперше 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.

6. 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.

7. Уперше 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 коригування 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 коригування в умовах процесів захисту.

Отримані наукові результати є практичною базою для побудови та захисту українського сегмента вузлів ІТС дерева ідентифікаторів ДІР.

Висновок

Проведені дослідження дозволяють зробити таки висновки:

1. 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 системи класифікації ДІР 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 (кількість термінів введених у розрізі розробленої методології захисту ДІР сягає 26, з них 23 введені вперше, 3 здійснено уточнення та доповнення), яка є основою для формування нормативного документа «Термінологія в галузі захисту державних інформаційних ресурсів».

2. Уперше 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.

3. Уперше розроблено методологію побудови класифікатора загроз ДІР в ІТС на основі організаційно-правового методу «подвійної трійки захисту» з урахуванням сформованої класифікації загроз інформаційним ресурсам, що дозволило вперше розробити та впровадити «Класифікатор загроз ДІР». 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.

4. Уперше 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 класи кодифікації загроз ДІР. Дана модель стає організаційно-правовим та організаційно-технічним підґрунтям формування дієздатного реєстру електронних інформаційних ресурсів країни у відповідності до міжнародних вимог та стандартів.

5. Удосконалено метод визначення стандартних ФПЗ ІТС від несанкціонованого доступу до ДІР на основі вперше розробленої 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 дерева ідентифікаторів ДІР та нові підходи для удосконалення методології оцінки ризиків безпеки ІТС відповідно до міжнародних стандартів і вимог.

6. Уперше розроблено комплекс заходів 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, які згруповані за рівнями ризику, та підлягають першочерговим організаційно-технічним діям з формування профілів захищеності.

7. Удосконалено методологічні та технологічні основи побудови комплексної системи захисту ДІР, а також концептуальну модель ІБ ДІР на основі різних класів загроз та кластерного розбиття систем захисту ДІР, що надало можливість розробити метод і модель визначення ефективності впроваджених методів та моделей на основі теорії ризиків та встановленої політики безпеки.

8. Уперше розроблено технологію на базі представлених методів та моделей аналізу ефективності і мінімізації системи ризиків вузлів ІТС, сформовано профілі захищеності вузлів ІТС дерева ідентифікаторів ДІР, 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. Впровадження розробленої технології надало змогу в 1,5–2 рази знизити інформаційний ризик вузла ІТС інформаційних об'єктів ДІР згідно визначеного ідентифікатора та до 50% зменшити ризик несанкціонованого доступу до повідомлень, які передаються між вузлами ІТС.

9. Удосконалення та впровадження методу визначення функціональних профілів захищеності вузлів дерева ідентифікаторів ДІР, який 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.

10. 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 ІТС об'єктів інформатизації державного призначення за умов проведення оцінки ефективності захисту ДІР та адекватності впровадженим методам.

ЛІТЕРАТУРА

1. **Юдін О. К.** Державні інформаційні ресурси. Методологія побудови класифікатора загроз: монографія / О. К. Юдін, С. С. Бучик. — К. : НАУ, 2015. — 214 с.

2. **Information** Security Management — Specification With Guidance for Use: ISO/IEC 27001 : 2013 [Електронний ресурс]. — Режим доступу: http://www.iso.org/iso/catalogue_detail?csnumber= 54534.

3. **Юдін О. К.** Концептуальна модель інформаційної безпеки державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Наукоємні технології. — 2014. — № 4 (24). — С. 462–466, DOI: 10.18372/2310-5461.24.7518.

4. **Юдін О. К.** Принципи побудови комплексної системи захисту державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Наукоємні технології. — 2015. — № 1 (25). — С. 15–20, DOI: 10.18372/2310-5461.25.8216.

5. **Юдін О. К.** Аналіз класифікацій типів систем захисту інформації / О. К. Юдін, С. С. Бучик // Проблеми інформатизації та управління. — 2015. — № 3 (51). — С. 116–125.

6. **Юдін О. К.** Загальна модель формування системи захисту державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик, О. В. Фролов // Наукоємні технології. — 2015. — № 4 (28). — С. 332–337, DOI: 10.18372/2310-5461.28.9678.

7. **Юдін О. К.**, Бучик С. С. Система термінів та визначень методології захисту державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Безпека інформації. — 2016 — №3 (18). — С. 107–114, DOI: 10.18372/2225-5036.22.11100.

8. **Бучик С. С**. Теоретичні основи аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів / С. С. Бучик // Наукоємні технології. — 2016. — № 1 (29). — С. 70–77, DOI: 10.18372/2310-5461.29.10091.

9. Бучик С.С. Методологія аналізу ризиків дерева ідентифікаторів державних інформаційних ресурсів / С. С. Бучик // Захист інформації. — 2016 — №1 (18). — С. 81 — 89, DOI: 10.18372/2410-7840.18.10116.

10. **Бучик С. С.** Теоретичні основи визначення стандартних функціональних профілів захищеності автоматизованої системи від несанкціонованого доступу / С. С. Бучик, С. В. Мельник // Наукоємні технології. — 2016. — № 2 (30). — С. 195–205, DOI: 10.18372/2310-5461.30.10564.

11. **А. с. 66492** Україна. Комп'ютерна програма. Інформаційна система визначення функціонального профілю захищеності автоматизованої системи від несанкціонованого доступу / С. С. Бучик, С. В. Мельник (Україна). — № 67055; заявл. 10.05.16.

12. **Юдін О. К.** Технологія побудови та захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів на основі ризик-менеджменту / О. К. Юдін, С. С. Бучик // Захист інформації. — 2016 — №2 (18). — С. 107–114, DOI: 10.18372/2410-7840.18.10589.

Бучик С. С., Юдін О. К.

ТЕОРЕТИЧНІ ТА ПРАКТИЧНІ АСПЕКТИ ПОБУДОВИ ТА ЗАХИСТУ УКРАЇНСЬКОГО СЕГМЕНТА ДЕРЕВА ІДЕНТИФІКАТОРІВ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

У статті викладено теоретичні та практичні аспекти побудови та захисту українського сегмента дерева ідентифікаторів державних інформаційних ресурсів з посиланням на власні авторські оригінальні розробки у розрізі визначеної загальної концепції проведених досліджень. Визначено протиріччя між наявними державними інформаційними ресурсами і нормативно-правовими, організаційними та інженерно-технічними напрямками їх захисту, та як наслідок, наявність недосконалої системи оперативного управління та захисту інформаційних ресурсів держави на основі організації системи мінімізації ризиків державних інформаційних ресурсів та формування динамічного комплексу функціональних профілів захищеності. З наявного протиріччя показана науково-прикладна проблема: підвищення ефективності системи оперативного управління та захисту інформаційних ресурсів держави на основі організації системи мінімізації ризиків державним інформаційним ресурсам та формування динамічного комплексу функціональних профілів захищеності. Узагальнені отримані наукові результати є практичною базою для побудови та захисту українського сегмента вузлів інформаційно-телекомунікаційних систем дерева ідентифікаторів державних інформаційних ресурсів.

Ключові слова: державні інформаційні ресурси, метод «подвійної трійки захисту», класифікація загроз, нормативно-правове спрямування, організаційне спрямування, інженерно-технічне спрямування, ідентифікатор об'єкта, ризик, інформаційно-телекомунікаційна система.

Buchyk S. S., Yudin O. K.

THEORETICAL AND PRACTICAL ASPECTS OF CONSTRUCTION AND SECURITY OF THE UKRAINIAN SEGMENT OF THE TREE OF IDENTIFIERS OF THE STATE INFORMATION RESOURCES

In the articles expounded theoretical and practical aspects of construction and security of the Ukrainian segment of tree of identifiers of state informative resources are with reference to own authorial original developments in the cut of certain general conception of the conducted researches. Contradiction is certain between present state informative resources and normatively-legal, organizational and technical directions of their security, and as a result, presence of the imperfect system of operative management and security of informative resources of the state on the basis of organization of the system of minimization of risks of state informative resources and forming of dynamic complex of functional types of security. From present contradiction the scientifically-applied problem is shown: increase of efficiency of the system of operative management and security of informative resources of the state on the basis of organization of the system of minimization of risks to the state informative resources and forming of dynamic complex of functional types of security. The generalized is got scientific results are a practical base for a construction and security of the Ukrainian segment of knots of the information-telecommunication system of tree of identifiers of state informative resources.

Key words: state information resources, method of «double three of security», classification of threats, normatively-legal aspiration, organizational aspiration, technical aspiration, object identifier, risk, information-telecommunication system.

Бучик С. С., Юдин О. К.

ТЕОРЕТИЧЕСКИЕ И ПРАКТИЧЕСКИЕ АСПЕКТЫ ПОСТРОЕНИЯ И ЗАЩИТЫ УКРАИНСКОГО СЕГМЕНТА ДЕРЕВА ИДЕНТИФИКАТОРОВ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ

В статье изложены теоретические и практические аспекты построения и защиты украинского сегмента дерева идентификаторов государственных информационных ресурсов со ссылкой на собственные авторские оригинальные разработки в разрезе определенной общей концепции проведенных исследований. Определены противоречия между имеющимися государственными информационными ресурсами и нормативно-правовыми, организационными и инженерно-техническими направлениями их защиты, и как следствие, наличие несовершенной системы оперативного управления и защиты информационных ресурсов государства на основе организации системы минимизации рисков государственных информационных ресурсов и формирования динамического комплекса функциональных профилей защищенности. Из имеющегося противоречия показана научно-прикладная проблема: повышение эффективности системы оперативного управления и защиты информационных ресурсов государства на основе организации системы минимизации рисков государственным информационным ресурсам и формирования динамического комплекса функциональных профилей защищенности. Обобщенные полученные научные результаты являются практической базой для построения и защиты украинского сегмента узлов информационно-телекоммуникационных систем дерева идентификаторов государственных информационных ресурсов.

Ключевые слова: государственные информационные ресурсы, метод «двойной тройки защиты», классификация угроз, нормативно-правовое направление, организационное направление, инженерно-техническое направление, идентификатор объекта, риск, информационно-телекоммуникационная система.

Стаття надійшла до редакції 13.02.2017 р.
Прийнято до друку 14.02.2017 р.
Рецензент – д-р техн. наук, проф. О. М. Новіков