© Yudin O., Buchyk S. The system of terms and determinations in security methodology of state information resources // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 3, p. 289-296.

DOI: 10.18372/2225-5036.22.11100

СИСТЕМА ТЕРМІНІВ ТА ВИЗНАЧЕНЬ МЕТОДОЛОГІЇ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Олександр Юдін[1], Сергій Бучик[2]

[1]Національний авіаційний університет, Україна
[2]Житомирський військовий інститут імені С.П. Корольова, Україна

ЮДІН Олександр Костянтинович, д.т.н.

Рік та місце народження: 1966 рік, м. Київ, Україна.
Освіта: Київський інститут інженерів цивільної авіації (з 2000 року – Національний авіаційний університет), 1989 рік.
Посада: директор Інституту комп'ютерних інформаційних технологій з 2012 року.
Наукові інтереси: інформаційна безпека.
Публікації: більше 300 наукових та навчально-методичних праць, серед яких монографії, словники, підручники, навчальні посібники, наукові статті та патенти на винаходи.
E-mail: kszi@ukr.net

БУЧИК Сергій Степанович, к.т.н.

Рік та місце народження: 1971 рік, м. Твер, Росія.
Освіта: Житомирське вище військове училище радіоелектроніки ППО, 1993 рік.
Посада: начальник кафедри автоматизованих систем управління з 2012 року.
Наукові інтереси: інформаційна безпека, теорія прийняття рішень.
Публікації: більше 120 наукових та навчально-методичних праць.
E-mail: s_stbu@ukr.net

Анотація. *У статті запропоновано систему термінів та визначень методології захисту державних інформаційних ресурсів у порівнянні їх з тими, що використовуються в керівних документах з питань захисту інформаційних ресурсів та введеними авторами в попередніх дослідженнях. До таких термінів та визначень авторами віднесено та розглянуто наступні: державні інформаційні ресурси, загроза державним інформаційним ресурсам, національні інформаційні ресурси, національні електронні інформаційні ресурси, система національних інформаційних ресурсів, система державних інформаційних ресурсів, державні електронні інформаційні ресурси, реєстр електронних державних інформаційних ресурсів, депозитарій електронних державних інформаційних ресурсів, атака на державні інформаційні ресурси, метод «подвійної трійки захисту», загрози нормативно-правового спрямування, загрози організаційного спрямування, загрози інженерно-технічного спрямування, ідентифікатор об'єкта, об'єкти загроз державним інформаційним ресурсам, джерела загроз державним інформаційним ресурсам, уразливості державних інформаційних ресурсів, ризик реалізації загрози державним інформаційним ресурсам, цілі джерел загроз державним інформаційним ресурсам, джерела відомостей про державні інформаційні ресурси, способи неправомірного оволодіння державними інформаційними ресурсами (способи доступу до державних інформаційних ресурсів), напрями захисту державних інформаційних ресурсів, способи захисту державних інформаційних ресурсів, засоби захисту державних інформаційних ресурсів, комплексна система захисту державних інформаційних ресурсів. Запропоновано ці терміни та визначення покласти в основу для формування нормативного документа в галузі захисту державних інформаційних ресурсів.*

Ключові слова: *державні інформаційні ресурси, загроза державним інформаційним ресурсам, захист державних інформаційних ресурсів, система державних інформаційних ресурсів, метод «подвійної трійки захисту».*

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.

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 кла-

сів, відповідно не до кінця визначена нормативно-правова база та її складова – термінологія (відсутній єдиний стандарт термінів інформаційної безпеки ДІР). Таким чином, введення нормативно-правової термінології в галузі захисту ДІР може бути розглянуто як підґрунтя для формування нормативного документа, який встановлює термінологію стосовно їх захисту та/або внесення змін до чинної нормативної бази відповідного спрямування, що і обумовлює *актуальність* статті.

Аналіз останніх досліджень та публікацій

На основі проведених авторами попередніх досліджень, а саме визначених правових аспектів формування системи ДІР, введеного класифікатора ДІР, аналізу світового дерева ідентифікаторі об'єктів та місця українського сегмента в ньому [1], розроблених моделей та принципів інформаційної безпеки ДІР [2-4] 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 в свою чергу може бути розглянута як підґрунтя для формування нормативного документа, який встановлює термінологію стосовно захисту ДІР та/або дозволить внести зміни до чинної нормативної бази відповідного спрямування.

Мета статті полягає у введенні системи термінів та визначень для формування нормативного документа, який встановлює термінологію стосовно захисту державних інформаційних ресурсів та/або дозволить запропонувати зміни до чинної нормативної бази відповідного спрямування.

Виклад основного матеріалу

Загальна система термінів та визначень, яка запропонована в результаті раніше проведених досліджень, представлено на рис. 1.

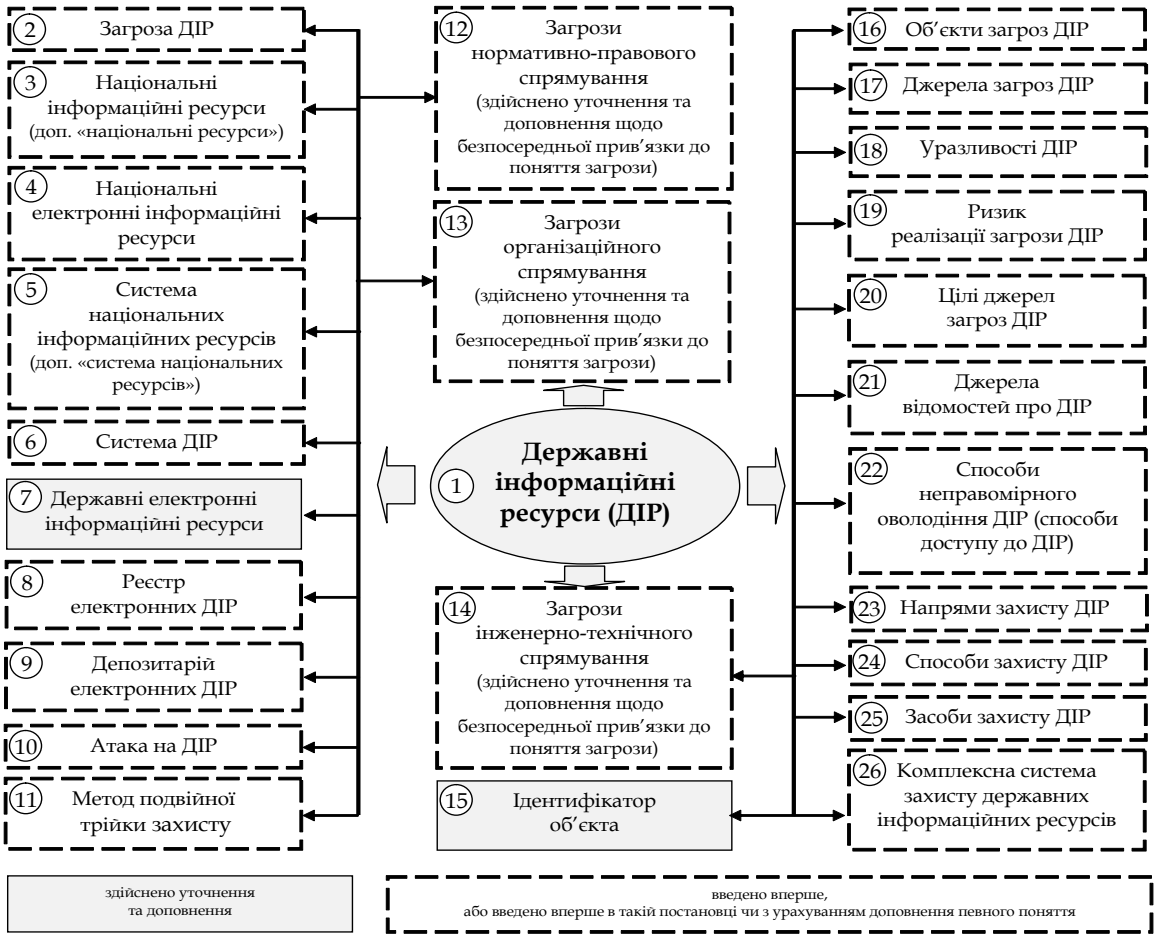

Рис. 1. Терміни, які введені авторами для формування (уточнення) нормативних документів, які встановлюють термінологію стосовно захисту ДІР

Порівняльний аналіз основних термінів та визначень, які представлені на рис. 1, згідно керівних документів та введених авторами або уточнених та доповнених наведено в табл. 1.

Порівняльний аналіз основних термінів та визначень Таблиця 1

Визначення згідно керівних документів	**Визначення, що введено авторами**
1. Державні інформаційні ресурси – авторами здійснено уточнення та доповнення	

Продовження табл. 1

Державні інформаційні ресурси – систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень [5].	*Державні інформаційні ресурси* (*state information resources*) – це результати інтелектуальної та практичної діяльності, що сформовані в усіх сферах життєдіяльності людини, суспільства і держави, зафіксовані і систематизовані на відповідних матеріальних носіях інформації, як окремі документи і масиви документів, банки і бази даних та знань, усі види архівів і бібліотек, музейні фонди, інформаційні ресурси які обробляються й передаються у інформаційних системах державного і/або загального призначення, інші ресурси, що містять дані, відомості і знання, які є об'єктом права власності держави незалежно від форми власності на час їх створення і мають споживчу цінність, а також такі, що призначені для розвитку і задоволення потреб громадян, суспільства, держави та підлягають захисту згідно визначеної політики безпеки й чинного законодавства [1].
2. Загроза державним інформаційним ресурсам – введено вперше	
Введено вперше	*Загроза державним інформаційним ресурсам* (*threat to the state information resources*) – протиправні дії, які можуть призвести до спотворення, несанкціонованого використання або руйнування державних інформаційних ресурсів (їх безпосередніх властивостей: конфіденційності, цілісності, доступності), які є власністю держави та необхідність захисту яких визначено законодавством [1].
Більш розширене поняття	*Загроза державним інформаційним ресурсам* (*threat to the state information resources*) – це потенційний або реальний стан небезпеки державним інформаційним ресурсам та безпосередньо їх властивостям (конфіденційності, цілісності, доступності), який може бути сформовано на основі реалізації будь-якого процесу та/або вчиненні діяння (та/або бездіяльності), спрямовано на порушення політики безпеки об'єкта інформаційної діяльності (державних інформаційних ресурсів) та такий, що завдає збитку державі [1].
3. Національні інформаційні ресурси – введено вперше з урахуванням доповнення поняття національні ресурси	
Національні ресурси – ресурси незалежно від їх змісту, форми, часу та місця створення, форми власності, призначені для задоволення потреб громадянина, суспільства, держави. Національні ресурси включають державні, комунальні та приватні ресурси [6].	*Національні інформаційні ресурси* (*national information resources*) – це результати інтелектуальної діяльності в усіх сферах життєдіяльності людини, суспільства і держави, зафіксовані на відповідних матеріальних носіях інформації як окремі документи і масиви документів, бази і банки даних та знань, усі види архівів, бібліотеки, музейні фонди та інші, що містять дані, відомості і знання, які є об'єктом права власності будь якого суб'єкта України і мають споживчу цінність (політичну, економічну, наукову, освітню, соціокультурну, оборонну, ринкову, історичну, інформаційну тощо) [1].
4. Національні електронні інформаційні ресурси – введено вперше	
Введено вперше	*Національні електронні інформаційні ресурси* (*national electronic information resources*) – інформаційні ресурси незалежно від їх змісту, форми, часу та місця створення, форми власності, які існують та використовуються в електронному вигляді та призначені для задоволення потреб громадянина, суспільства, держави. Національні електронні ресурси включають державні, комунальні та приватні ресурси [1].
5. Система національних інформаційних ресурсів – введено вперше з урахуванням доповнення поняття система національних ресурсів	
Система національних ресурсів – організована за єдиною технологією сукупність національних ресурсів, необхідних для розв'язання завдань соціально-економічного розвитку держави та внесених до Національного реєстру електронних інформаційних ресурсів [6].	*Система національних інформаційних ресурсів (system of national information resources)* – організована за єдиною технологією сукупність національних ресурсів, необхідних для розв'язання завдань соціально-економічного розвитку держави та внесених до Національного реєстру електронних інформаційних ресурсів; реєстр ресурсів – сукупність даних, упорядкованих для обліку і реєстрації ресурсів [1].
6. Система державних інформаційних ресурсів – введено вперше	

Продовження табл. 1

Введено вперше	*Система державних інформаційних ресурсів (system of state information resources)* – це організований державою упорядковано-інтегрований комплекс організаційно-технічних, нормативно-правових технологій, методів і заходів, а також взаємозв'язана і погоджено-функціонуюча сукупність суб'єктів інформаційної діяльності (державних, суспільства та окремих громадян) об'єднаних цілями й завданнями щодо формування, накопичення, збереження, достовірного оброблення, передавання, висвітлення та захисту державних інформаційних ресурсів у межах чинного законодавства України [1].
7. Державні електронні інформаційні ресурси – авторами здійснено уточнення та доповнення	
Державні електронні інформаційні ресурси – відображена та задокументована в електронному вигляді інформація, необхідність захисту якої визначено законодавством [7].	*Державні електронні інформаційні ресурси* (*state electronic information resources*) – державні інформаційні ресурси незалежно від їх змісту, форми, часу і місця створення, які існують та використовуються в електронному вигляді та призначені для задоволення потреб громадян, суспільства, держави. Державні електронні інформаційних ресурсів є складовою Національного реєстру електронних інформаційних ресурсів [1].
8. Реєстр електронних державних інформаційних ресурсів – введено вперше	
Національний реєстр – це інформаційно-телекомунікаційна система, призначена для реєстрації, обліку, накопичення, оброблення і зберігання відомостей про склад, зміст, розміщення, умови доступу до електронних інформаційних ресурсів та задоволення потреб юридичних і фізичних осіб в інформаційних послугах [8].	*Реєстр електронних державних інформаційних ресурсів (register of electronic state information resources)* – інформаційна система, призначена для реєстрації , обліку, накопичення, оброблення та зберігання відомостей про склад, зміст, умови доступу до електронних державних інформаційних ресурсів, розміщених у Національному депозитарії та такі, що мають споживчу цінність, а саме: політичну, економічну, наукову, освітню, соціокультурну, оборонну, ринкову, історичну, інформаційну тощо [1].
9. Депозитарій електронних державних інформаційних ресурсів – введено вперше	
Введено вперше	*Депозитарій електронних державних інформаційних ресурсів (depositary of electronic state information resources)* – інформаційна система державних електронних інформаційних ресурсів, створена на базі автоматизованих систем та погоджено функціонуючі програмно-апаратні комплекси, що забезпечують збір, облік, аудит, зберігання, оновлення, захист і доступ до електронних державних інформаційних ресурсів на основі інформаційних технологій та інформаційно-комунікаційних систем згідно визначеної політики безпеки та чинного законодавства [1].
10. Атака на державні інформаційні ресурси – введено вперше	
Введено вперше	*Атака на державні інформаційні ресурси (attack, are on state information resources)* – це можливі наслідки реалізації загрози державним інформаційним ресурсам, що сформовані на основі взаємодії джерела загрози через наявні фактори уразливості об'єкту інформаційної діяльності та такі, що приводять до різних видів збитків державі [1].
11. Метод подвійної трійки захисту – введено вперше	
Введено вперше	*Метод подвійної трійки захисту (method of double three of security)* – визначає базові характеристики класифікації загроз для різних видів та розподіляє їх за базовими принципами: характером спрямованості, рівню загрози, виду загрози та її функціонального профілю. Інформаційно-аналітична модель складається з двох платформ: *перша платформа ІБ* – складові, що підлягають захисту (властивості інформації): конфіденційність; цілісність; доступність; *друга платформа ІБ* - складові, що реалізують систему захисту (методи та засоби): нормативно-правові; організаційні; інженерно-технічні [1].
12. Загрози нормативно-правового спрямування – авторами здійснено уточнення та доповнення щодо безпосередньо прив'язки до поняття загрози, введено вперше в такій постановці	

Продовження табл. 1

Нормативно-правове забезпеченням інформаційної безпеки – сукупність загальних і спеціальних законів, стандартів, нормативно-правових актів, обов'язкових правил і норм, процедур та заходів тощо, які встановлені або санкціоновані державою, стосовно сфери інформаційних технологій та їх безпеки, а також такі, що забезпечують захист інформації на правовій основі і діють відносно суб'єктів інформаційної діяльності (державних органів, підприємств, організацій та населення (окремої особистості) [9].	*Загрози нормативно-правового спрямування (threat of normatively-legal aspiration)* – представляють собою загрози, які виникають в разі навмисного або ненавмисного порушення (впливу або/та дії на процес створення та застосування) спеціальних законів, інших нормативно-правових актів, правил, процедур та заходів, що забезпечують захист інформації на правовій основі [1].
13. Загрози організаційного спрямування – авторами здійснено уточнення та доповнення щодо безпосередньо прив'язки до поняття загрози, введено вперше в такій постановці	
Організаційне забезпеченням інформаційної безпеки – сукупність технологій, норм, методів і засобів, які регламентують взаємодію власників інформаційних ресурсів, персоналу систем, користувачів з інфраструктурою та між собою в процесі розроблення, впровадження та експлуатації інформаційних систем та їх безпеки згідно з установленим нормативно-правовим і чинним законодавством (т.ч. галузі і підприємства) [9].	*Загрози організаційного спрямування (threat of organizational aspiration)* – виникають у результаті навмисного або ненавмисного порушення регламентації виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, що виключає або суттєво утруднює реалізацію процесів протидії несанкціонованому порушенню властивостей інформації (інформаційних ресурсів) [1].
14. Загрози інженерно-технічного спрямування – авторами здійснено уточнення та доповнення щодо безпосередньо прив'язки до поняття загрози, введено вперше в такій постановці	
Інженерно-технічне забезпеченням інформаційної безпеки – сукупність спеціальних органів, а також інженерно-технічних технологій, засобів і заходів які взаємопов'язано функціонують з метою захисту інформаційних ресурсів (інформації) та їх властивостей, а також такі, що перешкоджають або унеможливлюють реалізації загроз та завданню збитків суб'єктам інформаційної діяльності [9].	*Загрози інженерно-технічного спрямування (threat of technical aspiration)* – загрози, що пов'язані з використанням різноманітних фізичних, апаратних, програмних, програмно-апаратних методів та засобів, які реалізують процеси розголошення, витоку, несанкціонованого доступу, інших форм незаконного спотворення і втручання до інформаційних ресурсів, а також призводять до різних видів збитків власнику ресурсів [1].
15. Ідентифікатор об'єкта – авторами здійснено уточнення та доповнення	
Ідентифікатор об'єкта – значення, що відрізняється від інших подібних значень, яке пов'язується з інформаційним об'єктом і є упорядкованим списком первинних цілочисельних значень від кореня (Root) міжнародного дерева ідентифікаторів об'єктів до вершини, який однозначно ідентифікує цю вершину [10].	*Ідентифікатор об'єкта (identifier of object)* – значення вузла, що відрізняється від інших подібних значень та логічно пов'язується з інформаційним об'єктом, унікально його визначає та однозначно ідентифікує, як вузол дерева міжнародних ідентифікаторів об'єктів. Список значень вузлів дерева (Root) є впорядкована послідовність первинних цілих значень, що починаються від кореня міжнародного дерева до вершини або/чи вузла ідентифікації [1].
16. Об'єкти загроз державним інформаційним ресурсам – введено вперше	
Введено вперше	*Об'єкти загроз ДІР* (відповідно до визначеного автором поняття ДІР) – всі інформаційні ресурси держави, суспільства або громадян, які підлягають захисту згідно визначеної політики безпеки й чинного законодавства [2].
17. Джерела загроз ДІР – введено вперше	

Продовження табл. 1

Введено вперше	*Джерела загроз ДІР* – носії загроз безпеці інформації ДІР (кібертерористи та кіберзловмисники, персонал підданий корупційним діям, адміністративно-управлінські органи державної влади і т.д.) [2].
18. Уразливості ДІР – введено вперше	
Введено вперше	*Уразливості ДІР* – фактори, що призводять до порушення безпеки інформації на конкретному об'єкті інформаційної діяльності [2].
19. Ризик реалізації загрози ДІР – введено вперше	
Введено вперше	*Ризик реалізації загрози ДІР* – потенційна можливість використання уразливостей державних інформаційних ресурсів реальною загрозою для заподіяння збитку державі, суспільству, окремому громадянину [2].
20. Цілі джерел загроз ДІР – введено вперше	
Введено вперше	*Цілі джерел загроз ДІР* – ознайомлення з конфіденційними відомостями, їх модифікація з корисною метою, знищення для нанесення прямого матеріального збитку [2].
21. Джерела відомостей про ДІР – введено вперше	
Введено вперше	*Джерела відомостей про ДІР* – люди, документи та документообіг в цілому (паперовий, електронний), відкриті публікації, технічні носії інформації, технічні засоби виробничої та трудової діяльності, продукція та відходи виробництва [2].
22. Способи неправомірного оволодіння ДІР (способи доступу до ДІР) – введено вперше	
Введено вперше	*Способи неправомірного оволодіння ДІР (способи доступу до ДІР)* – розголошення джерелами конфіденційних відомостей, витік інформації через технічні засоби, несанкціонований доступ до відомостей, що підлягають охороні [2].
23. Напрями захисту ДІР – введено вперше	
Введено вперше	*Напрями захисту ДІР* – це нормативно-правові категорії, орієнтовані на забезпечення комплексного захисту інформації від внутрішніх та зовнішніх загроз на державному рівні, на рівні підприємства або організації, а також на рівні окремої особистості [1].
24. Способи захисту ДІР – введено вперше	
Введено вперше	*Способи захисту ДІР* – будь-які міри, шляхи, способи та дії, які забезпечують попередження протиправних дій, їх запобігання, припинення та протидію несанкціонованому доступу до ДІР [2].
25. Засоби захисту ДІР – введено вперше	
Введено вперше	*Засоби захисту ДІР* – фізичні, апаратні, програмні засоби та криптографічні методи. Криптографічні методи можуть бути реалізовані як апаратно, так і змішано програмно-апаратними засобами [2].
26. Комплексна система захисту державних інформаційних ресурсів – введено вперше	
Введено вперше	*Комплексна система захисту державних інформаційних ресурсів* – сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист державних інформаційних ресурсів, що підлягають захисту згідно визначеної політики безпеки й чинного законодавства в інформаційно-телекомунікаційних системах (інформаційних, телекомунікаційних, інтегрованих системах) держави, суспільства або громадян [3].

Основні результати

До основних результатів статті можна віднести введення системи термінології в галузі захисту ДІР (кількість термінів введених у розрізі розробленої методології захисту державних інформаційних ресурсів сягає 26, з них 23 введені вперше, 3 здійснено уточнення та доповнення), що може бути розглянуто як підґрунтя для формування нормативного документа, який встановлює термінологію стосовно їх захисту та/або дозволить запропонувати внесення змін до чинної нормативної бази відповідного спрямування.

Висновок

Таким чином, в статті здійснено порівняльний аналіз основних термінів та визначень згідно керівних документів та введених авторами в попередніх дослідженнях, а саме понять: державні інформаційні ресурси, загроза державним інформаційним ресурсам, національні інформаційні ресурси, національні електронні інформаційні ресурси, система національних інформаційних ресурсів, система державних інформаційних ресурсів, державні електронні інформаційні ресурси, реєстр електронних державних інфор-

маційних ресурсів, депозитарій електронних державних інформаційних ресурсів, атака на державні інформаційні ресурси, метод подвійної трійки захисту, загрози нормативно-правового спрямування, загрози організаційного спрямування, загрози інженерно-технічного спрямування, ідентифікатор об'єкта, об'єкти загроз державним інформаційним ресурсам, джерела загроз державним інформаційним ресурсам, уразливості державних інформаційних ресурсів, ризик реалізації загрози державним інформаційним ресурсам, цілі джерел загроз державним інформаційним ресурсам, джерела відомостей про державні інформаційні ресурси, способи неправомірного оволодіння державними інформаційними ресурсами (способи доступу до державних інформаційних ресурсів), напрями захисту державних інформаційних ресурсів, способи захисту державних інформаційних ресурсів, засоби захисту державних інформаційних ресурсів, комплексна система захисту державних інформаційних ресурсів.

Введена система термінології в галузі захисту державних інформаційних ресурсів може бути розглянуто як підгрунтя для формування нормативного документа, який встановлює термінологію стосовно їх захисту та/або дозволить внести зміни до чинної нормативної бази відповідного спрямування.

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] Юдін О.К. Концептуальна модель інформаційної безпеки державних інформаційних ресурсів / О.К. Юдін, С.С. Бучик // Наукоємні технології. – 2014. – № 4 (24). – С. 462 – 466.

[3] 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.

[4] 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.

[5] Про Державну службу спеціального зв'язку та захисту інформації України [Електронний ресурс] : Закон України від 23 лютого 2006 р. №3475-IV-ВР//ВВР. – 2006. – №30 (із змінами, внесеними згідно із Законом № 1313-VII від 05.06.2014, ВВР, 2014, № 29, ст.946). – С.258. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/3475-15

[6] Концепції формування системи національних електронних інформаційних ресурсів [Електронний ресурс] : розпорядження Кабінету Міністрів України від 5 травня 2003р. № 259-р. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/259-2003-р

[7] Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління [Електронний ресурс] : затверджено Постановою Кабінету Міністрів України від 3 серпня 2005 р. № 688 (у редакції від 07.09.2011 р. № 938). – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/KP050688.html

[8] Положення про Національний реєстр електронних інформаційних ресурсів [Електронний ресурс]: затверджено Постановою Кабінету Міністрів України від 17 березня 2004 р. № 326 (у редакції від 21.07.2010 р. № 675). – Режим доступу: http://zakon4.rada.gov.ua/laws/show/326-2004-п

[9] Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення: [підручник] / О.К. Юдін. – К.: НАУ, 2011. – 640 с.

[10] Положення про порядок формування простору ідентифікаційних кодів об'єктів Українського сегмента світового простору ідентифікаторів об'єктів [Електронний ресурс] : затверджено Рішенням Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації 18 квітня 2013 р. № 227. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/z1403-13

УДК 004.056.5 (045)

Юдин А.К., Бучик С.С. Система терминов и определений методологии защиты государственных информационных ресурсов

Аннотация. *В статье предложена система терминов и определений методологии защиты государственных информационных ресурсов в сравнении их с теми, которые используются в руководящих документах по вопросам защиты информационных ресурсов и введенными авторами в предыдущих исследованиях. К таким терминам и определениям авторами отнесено и рассмотрено следующее: государственные информационные ресурсы, угроза государственным информационным ресурсам, национальные информационные ресурсы, национальные электронные информационные ресурсы, система национальных информационных ресурсов, система государственных информационных ресурсов, государственные электронные информационные ресурсы, реестр электронных государственных информационных ресурсов, депозитарий электронных государственных информационных ресурсов, атака на государственные информационные ресурсы, метод двойной тройки защиты, угрозы нормативно-правового направления, угрозы организационного направления, угрозы инженерно-технического направления, идентификатор объекта, объекты угроз государственным информационным ресурсам, источники угроз государственным информационным ресурсам, уязвимости государственных информационных ресурсов, риск реализации угрозы государственным ин-*

формационным ресурсам, цели источников угроз государственным информационным ресурсам, источники сведений о государственных информационных ресурсах, способы неправомерного овладения государственными информационными ресурсами (способы доступа к государственным информационным ресурсам), направления защиты государственных информационных ресурсов, способы защиты государственных информационных ресурсов, средства защиты государственных информационных ресурсов, комплексная система защиты государственных информационных ресурсов. Предложено эти термины и определения положить в основу для формирования нормативного документа в отрасли защиты государственных информационных ресурсов.
Ключевые слова: *государственные информационные ресурсы, угроза государственным информационным ресурсам, защита государственных информационных ресурсов, система государственных информационных ресурсов, метод «двойной тройки защиты».*

Yudin O., Buchyk S. The system of terms and determinations in security methodology of state information resources

Abstract. *A system of terms and determinations of methodology of defence of state information resources in comparison that in leading documents on the questions of defence of information resources and that introduced by the authors in previous researches is presented in the article. To such terms and determinations the authors apply the following ones: state information resources, threat to the state information resources, national information resources, national electronic information resources, system of national information resources, system of state information resources, state electronic information resources, register of electronic state information resources, depositary of electronic state information resources, attack on state information resources, method of double three of defence, threat of normatively-legal aspiration, threat of organizational aspiration, threat of technical aspiration, object identifier, objects of threats to the state information resources, source of threats to the state information resources, vulnerability of state information resource, risk realization threat state information resource, aim source threat state information resource, source information about state information resource, method illegal capture state information resource (methods of access are to the state information resources), direction defence state information resource, method defence state information resource, facility defence state information resource, complex system defence state information resource. These terms and determinations are offered to be put in the basis of forming of a normative document in the matter of defence of state information resources.*
Key words: *state information resources, threat to the state information resources, security of state information resources, system of state information resources, method of double three of security.*

Отримано *3 жовтня 2016 року*, затверджено редколегією 20 *жовтня 2016 року*