ing from the implementation of the threat to this resource). It is noted that the in the case of application of high-performance technology/decisions in the system of information security level of investment may be reduced to 11-13%. It is considered the prospects of application of models based on motivational and resource relations which are characteristic to of the situation "attack-defense" in the information sphere.

Index terms: risk, risk modeling, economic and cost models, the range of reasonable investment.

Архипов Александр Евгеньевич, доктор технических наук, професор кафедры информационной безопасности НТУУ «КПИ».
E-mail: sonet0515@gmail.com.
Архипов Олександр Євгенович, доктор технічних наук, професор кафедри інформаційної безпеки НТУУ «КПІ».
Oleksandr Arkhipov, Dr. Sci. Tech., Professor at the Department of Information Defence at National University of Ukraine «Kyiv Polytechnic Institute».

УДК 004.056.5

МЕТОДОЛОГІЯ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ. ПОРІВНЯЛЬНИЙ АНАЛІЗ ОСНОВНИХ ТЕРМІНІВ ТА ВИЗНАЧЕНЬ

Олександр Юдін, Сергій Бучик

У статті здійснено порівняльний аналіз основних термінів та визначень згідно керівних документів з питань захисту інформаційних ресурсів та введених авторами в попередніх дослідженнях. До таких термінів та визначень авторами віднесено та розглядаються в статті: 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. Запропоновано ці терміни та визначення покласти в основу стандарту або нормативного документу технічного захисту інформації щодо термінології в галузі захисту державних інформаційних ресурсів.

***Ключові слова**: 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.*

Актуальність дослідження. Актуальність статті обумовлюється вимогами сьогодення, а саме необхідністю забезпечення інформаційної безпеки, кібербезпеки та безпеки інформаційних ресурсів держави в цілому. Як зазначено в Указі Президента України №287/2015 Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України», одним із пріоритетів забезпечення інформаційної безпеки є «створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; розробка і реалізація скоординованої інформаційної політики органів державної влади». Що стосується основних пріоритетних напрямків забезпечення кібербезпеки і безпеки інформаційних ресурсів, то до них відповідно тематики статті можна віднести забезпечення захисту «державних інформаційних ресурсів, систем електронного врядування … з урахуванням практики держав – членів НАТО та ЄС».

Аналіз останніх досліджень та публікацій. Авторами визначалось, що з одного боку в Україні на концептуальному та нормативному рівні не визначено перелік і класифікацію загроз інформаційним ресурсам держави, з іншого боку не розроблено нормативно-правового документу та стандарту щодо поняття державних інформаційних ресурсів, його складових та відповідної їм моделі загроз [1, 2]. Також в роботах [1, 2, 3, 4, 5] авторами введено або уточнено ряд понять, які відносяться до методології захисту ДІР. Таким чином виникає необхідність узагальнення всієї термінології, яка введена або уточнена авторами в попере-

дніх роботах та порівняння цих термінів та визначень з тими, які містяться в керівних документах.

Мета статті. Мета статті полягає у здійсненні порівняльного аналізу основних термінів та визначень, які встановлені згідно керівних документів та введені авторами в попередніх дослідженнях.

Виклад основного матеріалу. Порівняльний аналіз основних термінів та визначень, згідно керівних документів та введених авторами або уточнених та доповнених наведено в табл. 1.

Таблиця 1

Порівняльний аналіз основних термінів та визначень (згідно керівних документів та введених авторами або ними уточнених та доповнених)

Визначення згідно керівних документів	**Визначення, що введено авторами**
1. Державні інформаційні ресурси – авторами здійснено уточнення та доповнення	
Державні інформаційні ресурси – представляють собою інформацію, яка є власністю держави та необхідність захисту якої визначено законодавством [6]. *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 [7].	*Державні інформаційні ресурси* (*state informative 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 informative 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 [3].
Більш розширене поняття	*Загроза державним інформаційним ресурсам* (*threat to the state informative 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 [3].
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	*Національні інформаційні ресурси* (*national informative resources*) – це результати інтелектуальної діяльності в усіх сферах життєдіяльності людини, суспільства

Визначення згідно керівних документів	**Визначення, що введено авторами**
потреб громадянина, суспільства, держави. Національні ресурси включають державні, комунальні та приватні ресурси [8].	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 informative 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 [8].	*Система національних інформаційних ресурсів (system of national informative 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	
Введено вперше	*Система державних інформаційних ресурсів (system of state informative 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 [9].	*Державні електронні інформаційні ресурси* (*state electronic informative 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].

Визначення згідно керівних документів	**Визначення, що введено авторами**
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 [10].	*Реєстр електронних державних інформаційних ресурсів (register of electronic state informative 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 informative resources)* – інформаційна система державних електронних інформаційних ресурсів, створена на базі автоматизованих систем та погоджено функціонуючих програмно-апаратних комплексів, 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 informative 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 [4].
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-аналітичну 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 [2].
12. Загрози нормативно-правового спрямування – авторами здійснено уточнення та доповнення щодо безпосередньо прив'язки до поняття загрози, введено вперше в такій постановці	
Нормативно-правове забезпеченням інформаційної безпеки – сукупність загальних і спеціальних законів, стандартів, нормативно-правових	*Загрози нормативно-правового спрямування (threat of normatively-legal aspiration)* – представляють собою загрози, які виникають в разі навмисного або

Визначення згідно керівних документів	Визначення, що введено авторами
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) [11].	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 [2].
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 (в.ч. галузі і підприємства) [11].	*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) [2].
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 [11].	*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 [2].
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 [12].	*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 [5].

Основні результати. До основних результатів статті можна віднести узагальнення термінології та визначень щодо захисту ДІР, яка введена авторами в результаті попередніх досліджень та у порівнянні з існуючими керівними документами. Визначення наведеної системи термінології та понять, введених авторами вперше, уточнених або доповнених.

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 інформа-

ційних 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.

Це в свою чергу може бути покладено в основу стандарту або нормативного документу технічного захисту інформації щодо термінології в галузі захисту державних інформаційних ресурсів.

ЛІТЕРАТУРА

[1]. Юдін О. К. Правові аспекти формування системи державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Безпека інформації. – 2014. – Том 20 (1). – С. 76-82. – Режим доступу: http://jrnl.nau.edu.ua / index. php/ Infosecurity/ article/ view/ 6578.

[2]. Юдін О. К. Методологія побудови класифікатора загроз державним інформаційним ресурсам / О. К. Юдін, С. С. Бучик, А. В. Чунарьова, О. І. Варченко // Наукоємні технології. – 2014. – № 2 (22). – С. 200–210. – Режим доступу: http://jrnl.nau.edu.ua /index.php/SBT/article/view/6820.

[3]. Юдін О.К. Аналіз загроз державним інформаційним ресурсам / О. К. Юдін, С. С. Бучик // Проблеми інформатизації та управління. – 2013. – № 4 (44). – С.93–99. – Режим доступу: http://jrnl.nau.edu.ua/index.php/PIU/article/view/6404.

[4]. Юдін О. К. Загрози державним інформаційним ресурсам: терміни та визначення / О. К. Юдін, С. С. Бучик // Захист інформації. – 2014. – Том 16 (2). – С. 121–125. – Режим доступу: http://jrnl.nau.edu.ua/index.php/ZI/article/view/6930.

[5]. Юдін О. К. Світовий простір ідентифікаторів об'єктів: аналіз, перспективи розвитку, місце українського сегменту / О. К. Юдін, С. С. Бучик, О. В. Фролов // Наукоємні технології. – 2014. – № 3 (23). – С. 295 – 302. – Режим доступу: http://jrnl.nau.edu.ua/index.php/SBT/article/view/7406.

[6]. Про Державну службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 р. №3475-IV-ВР//ВВР. – 2006. – №30 – С. 258.

[7]. 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.

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

[9]. 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

[10]. 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.

[11]. Юдін О.К. Інформаційна безпека. Нормативно-правове забезпечення : [підруч.] / Олександр Костянтинович Юдін. – К.: НАУ, 2011. – 640 с.

[12]. 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.

REFERENCES

[1]. Yudin O., Buchyk S. (2014) "Legal aspects of the state information resources system formation", Bezpeka ìnformacìì, №20(1), pp.76-82.

[2]. Yudin O., Buchyk S., A. Chunareva, O. Frolov (2014) "Methodology of construction of classifier of threats to the state informative resources", Science-based technologies, №2(22), pp.200-210.

[3]. Yudin O., Buchyk S. (2013) "AnalIz zagroz derzhavnim informatsiynim resursam", Problemi informatizatsiyi ta upravlinnya, №4(44), pp.93-99.

[4]. Yudin O., Buchyk S. (2014) "Threat state informative resources. Terms and determinations", Zahist ìnformacìï, №16(2), pp.121-125.

[5]. Yudin O., Buchyk S., Frolov O. (2014) "Svitoviy prostir identifikatoriv ob'ektiv: analiz, perspektivi rozvitku, mistse Ukrayinskogo segmentu", Science-based technologies, №3(23), pp.295-302.

[6]. Pro derzhavnu sluzhbu spetsialnogo zv'yazku ta zahistu informatsiyi Ukrayini : Zakon Ukrayini vid 23 lyutogo 2006 r. №3475-IV-VR//VVR., 2006, №30, P. 258.

[7]. Pro derzhavnu sluzhbu spetsIalnogo zv'yazku ta zahistu snformatsiyi Ukrayini [Elektronniy resurs]: Zakon Ukrayini vid 23 lyutogo 2006 r. №3475-IV-VR//VVR, 2006, №30 (iz zminami, vnesenimi zgidno iz Zakonom № 1313-VII vid 05.06.2014, VVR, 2014, № 29, p.946). – P.258. – Rezhim dostupu: http:// zakon4. rada. gov.ua/laws/show/3475-15

[8]. Kontseptsiyi formuvannya sistemi natsionalnih elektronnih informatsiynih resursiv [Elektronniy resurs]: rozporyadzhennya Kabinetu Ministriv Ukrayini vid 5 travnya 2003 r. № 259-r. – Rezhim dostupu: http://zakon2.rada.gov.ua/laws/show/259-2003-p

[9]. Polozhennya pro Reestr informatsiynih, telekomunikatsiynih ta informatsiyno-telekomunikatsiynih sistem organiv vikonavchoyi vladi, a takozh pidpriemstv, ustanov i organizatsiy, scho nalezhat do sferi yih upravlinnya [Elektronniy resurs]: zatverdzheno Postanovoyu Kabinetu Ministriv Ukrayini vid 3 serpnya 2005 r. № 688 (u redaktsiyi vid 07.09.2011 r. № 938). – Rezhim dostupu: http://search.ligazakon.ua/l_doc2.nsf /link1/ KP050688.html

[10]. Polozhennya pro Natsionalniy reestr elektronnih informatsIynih resursiv [Elektronniy resurs]: zatverdzheno Postanovoyu Kabinetu Ministriv Ukrayini vid 17 bereznya 2004 r. № 326 (u redaktsiyi vId 21.07.2010 r. № 675), Rezhim dostupu: http://zakon4.rada.gov.ua/laws/show/326-2004-п.

[11]. Yudin O.K.. (2011) "Informative security. Normatively legal providing", K.: NAU, 640 r.

[12]. Polozhennya pro poryadok formuvannya prostoru identifikatsiynih kodiv ob'ektiv Ukrayinskogo segmenta svitovogo prostoru identifikatoriv ob'ektiv [Elektronniy resurs] : zatverdzheno Rishennyam Natsionalnoyi komisiyi, scho zdiysnyue derzhavne regulyuvannya u sferi zv'yazku ta informatizatsiyi 18 kvitnya 2013. № 227. – Rezhim dostupu: http://zakon4.rada.gov.ua/laws/show/z1403-13.

МЕТОДОЛОГИЯ ЗАЩИТЫ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ. СРАВНИТЕЛЬНЫЙ АНАЛИЗ ОСНОВНЫХ ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

В статье проведен сравнительный анализ основных терминов и определений, установленных согласно руководящих документов по вопросам защиты информационных ресурсов и введенные авторами в предыдущих исследованиях. К таким терминам и определениям авторами отнесены и рассматриваются в статье: 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. Предложено данные термины и определения положить в основу стандарта или нормативного документа технической защиты информации относительно терминологии в отрасли защиты государственных информационных ресурсов.

Ключевые слова: 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.

METHODOLOGY OF DEFENCE OF STATE INFORMATIVE RESOURCES. COMPARATIVE ANALYSIS OF BASIC TERMS AND DETERMINATIONS

The comparative analysis of basic terms and determinations which are certain in obedience to leading documents in relation to security of informative resources and entered by authors in previous researches is carried out in the article. To such terms and determinations it is taken authors and examined in the article: state informative resources, threat to the state informative resources, national informative resources, national electronic informative resources, system of national informative resources, system of state informative resources, state electronic informative resources, register of electronic state informative resources, depositary of electronic state informative resources, attack on state informative resources, method of double three of security, threat of normatively-legal aspiration, threat of organizational aspiration, threat of technical aspiration, identifier of object. These terms and determinations are suggested to put in basis of standard or normative document of technical protection in relation to terminology in industry of security of state informative resources.

Key words: state informative resources, threat to the state informative resources, national informative resources, national electronic informative resources, system of national informative resources, system of state informative resources, state electronic informative resources, register of electronic state informative resources, depositary of electronic state informative resources, attack, are on state informative resources, method of double three of security, threat of normatively-legal aspiration, threat of organizational aspiration, threat of technical aspiration, identifier of object.

Юдін Олександр Костянтинович, доктор технічних наук, професор. Член експертної та науково-методичної ради Міністерства освіти та науки України в галузі «Інформаційна безпека». Член-кореспондент Академії Зв'язку України. Лауреат Державної премії України у галузі науки і техніки. Директор інституту комп'ютерних інформаційних технологій, завідувач кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету.
E-mail: kszi@ukr.net

Юдин Александр Константинович, доктор технических наук, профессор. Член экспертного и научно-методического совета Министерства образования и науки Украины в области «Информационная безопасность». Член-корреспондент Академии Связи Украины. Лауреат Государственной премии Украины в области науки и техники. Директор института компьютерных информационных технологий, заведующий кафедрой компьютеризованных систем защиты информации Национального авиационного университета.

Yudin Alexander Konstantinovich, D. of Engineering, professor. Member of expert and scientifically-methodical advice of Department of education and science of Ukraine in an area «Informative security». Corresponding member of Academy of Connection of Ukraine. Laureate of the State bonus of Ukraine in area of SciTech. Director of institute of computer information technologies, manager by the department of the computerized systems for information the National Aviation University.

Бучик Сергій Степанович, кандидат технічних наук, доцент, начальник кафедри автоматизованих систем управління Житомирського військового інституту імені С. П. Корольова.
E-mail: s_stbu@ukr.net

Бучик Сергей Степанович, кандидат технических наук, доцент, начальник кафедры автоматизированных систем управления Житомирского военного института имени С.П. Королева.

Buchyk Sergii, PhD in Eng., chief of department of automated control the system the Zhitomir Military Institute of the name of S.P. Korolyova.

УДК 004.056.5

ВИЗНАЧЕННЯ АКТУАЛЬНИХ ЗАГРОЗ БЕЗПЕЦІ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ УПРАВЛІННЯ ТЕХНОЛОГІЧНИМИ ПРОЦЕСАМИ

Сергій Гончар

З метою вирішення задач по забезпеченню безпеки інформації автоматизованих систем управління технологічними процесами приведено узагальнену модель процесу захисту інформації. Здійснено дослідження та аналіз взаємодії системи захисту інформації і дестабілізуючих факторів таких як, загрози, сприятливі умови для реалізації цих загроз, уразливості. Показано, що актуальність загрози безпеці інформації пропорційна ймовірності реалізації даної загрози та коефіцієнту її небезпеки. отримано вирази для визначення ймовірності реалізації загроз безпеці інформації та коефіцієнта їх небезпеки. Приведено метод визначення актуальних загроз безпеці інформації в автоматизованих системах управління технологічними процесами та сформульовано вихідні дані, які для цього необхідні.

Ключові слова: *загроза, безпека інформації, автоматизовані системи управління, уразливості, метод, модель.*

Вступ. На сьогоднішній день автоматизовані системи управління технологічними процесами (АСУ ТП), які включають в себе системи диспетчерського управління і збору даних, системи розподіленого управління та інші конфігурації систем управління використовуються в різних сферах промислового сектору, і кількість таких систем постійно зростає. До таких систем належать атомні і гідроелектростанції, нафто- і газопроводи, національні мережі розподілу електроенергії, транспортні системи національного і світового рівня, загальнодержавні системи зв'язку, галузеутворюючі підприємства тощо, тобто об'єкти критичної інфраструктури [1].

Очевидно, що в умовах сучасного надзвичайно інтенсивного розвитку інфраструктури провідних країн світу існує багато об'єктів критичної інфраструктури, виведення з ладу яких може призвести до надзвичайних ситуацій, пов'язаних із загибеллю людей, екологічними катастрофами, заподіянням великих матеріальних, економічних збитків тощо.

Багато держав, в першу чергу економічно розвинуті, вдосконалюють методи та способи використання інформаційних технологій і засобів для деструктивних впливів на інформаційні системи об'єктів критичної інфраструктури. При цьому, складна організація автоматизованих систем управління технологічними процесами і вимоги безперервності технологічних процесів призводять до того, що базові компоненти систем управління (індустріальні протоколи, операційні системи, системи управління базами даних тощо) старіють, не оновлюються, і їх уразливості не усуваються досить тривалий проміжок часу. Дані щодо усунення уразливостей в автоматизованих системах управління технологічними процесами