УДК 004.056.5

ЗАГАЛЬНА МОДЕЛЬ ФОРМУВАННЯ СИСТЕМИ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

О. К. Юдін**, д-р техн. наук, проф.; ****С. С. Бучик,** канд. техн. наук, доц.; ***О. В. Фролов

*Національний авіаційний університет
e-mail: kszi@ukr.net
** Житомирський військовий інститут імені С. П. Корольова
e-mail: s_stbu@ukr.net

Розглянуто актуальне питання забезпечення захисту державних інформаційних ресурсів на усіх напрямках державної політики з питань національної безпеки. З урахуванням попередніх досліджень авторами представлено загальну модель формування системи захисту державних інформаційних ресурсів у вигляді структурно-логічної схеми на основі методології «подвійної трійки захисту». Модель подана у складі трьох основних блоків: системи управління інформаційною безпекою державних інформаційних ресурсів; напрямків захисту державних інформаційних ресурсів у сферах захисту; представлення державних інформаційних ресурсів як складової національної безпеки. Більш детально розкрито перший блок (система управління інформаційною безпекою державних інформаційних ресурсів) з урахуванням основних етапів впровадження даної системи згідно з міжнародними стандартами серії ISO/IEC 2700x. Визначено основні напрямки подальших досліджень: визначення політики безпеки державних інформаційних ресурсів та впровадження системи управління ризиками.

Ключові слова: державні інформаційні ресурси, система управління інформаційною безпекою державних інформаційних ресурсів, система захисту державних інформаційних ресурсів, метод «подвійної трійки захисту».

The article deals with topical issues of protection of state informative resources in all areas of state policy of national security. The authors presented a general model of the system of protection of state informative resources in the form of structural and logical scheme on the basis of methodologies of "double triple protection". A model is presented in composition three basic blocks: control system by informative security of state informative resources; directions of protection of state informative resources in the spheres of security; presentation of state informative resources as component of national safety. More in detail the first block (control system by informative security of state informative resources) is exposed taking into account to the basic stages of introduction of this system according to the international standards of series of ISO/IEC 2700x. Certain basic directions of further researches: determination of policy of security of state informative resources and introduction of control system by risks.

Keywords: state informative resources, information security management system of state informative resources, system of state informative resources protection, methodologies of "double triple protection".

Актуальність дослідження

У зв'язку зі змінами та подіями, які відбуваються в Україні, актуальним постає питання розгляду місця державних інформаційних ресурсів (ДІР) з позиції законодавчих актів, які змінюються в загальній моделі політики інформаційної безпеки держави. Так, останнім часом, активізовано законодавчі процеси у вказаному напрямку: внесено суттєві зміни до Закону Україні «Про основи національної безпеки України», прийнято рішення Ради національної безпеки та оборони України «Про Стратегію національної безпеки України», введеного в дію Указом Президента України від 26 травня 2015 р. № 287/2015. Нажаль, досі гальмується процес введення в дію такого стратегічно важливого документа, як «Доктрина інформаційної безпеки України», оскільки створено лише проект останнього.

У новій «Стратегії національної безпеки України» визначені актуальні загрози національній безпеці України, серед яких є «інформаційно-психологічна війна». В «Основах національної безпеки України» в інформаційній сфері важливе місце займає «вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України».

Розглядаючи комплексне питання національної безпеки України, можна відмітити особливо актуальний момент — необхідність забезпечення захисту ДІР в усіх напрямках державної політики з питань національної безпеки.

Таким чином, на сучасному етапі розвитку інформаційних ресурсів, розгляд загальної моделі формування системи захисту ДІР є назрілим та актуальним.

Аналіз останніх досліджень та публікацій

Прикро, що загальна модель формування системи захисту ДІР чітко не визначена. Питаннями побудови воєнно-політичної моделі держави та її місця в загальній моделі формування державної політики національної безпеки займався Богда-

нович В. Ю. [1]. Марущак А. І., Олійник О. В., Арістова І. В., Сосніна О. В. розглядали окреслену тематику в іншому аспекті.

Мета статті — побудова загальної моделі формування системи захисту ДІР у вигляді структурно-логічної схеми на основі методології «подвійної трійки захисту».

Виклад основного матеріалу

Відповідно до Закону Україні «Про основи національної безпеки України» на сучасному етапі реальні та потенційні загрози національній безпеці розглядаються у таких сферах: зовнішньополітичній; державної безпеки; воєнній та сфері безпеки державного кордону України; внутрішньополітичній; економічній; науково-технологічній; цивільного захисту; екологічній; соціальній та гуманітарній; інформаційній. Таким чином, можна говорити про завдання захисту ДІР у сфері національної безпеки та розглядати самі ДІР як її складову.

Методологія «подвійної трійки захисту» авторами представлена в праці [2], де запропоновано інформаційно-аналітичну модель даного методу, як основу формування методології з урахуванням складових процесу захисту інформаційних ресурсів. Результатом роботи є формування двох платформ інформаційної безпеки (ІБ).

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.

У праці [3] наведено розширене поняття ДІР. *Державні інформаційні ресурси* — 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.

Загальна методологія побудови та оцінки ефективності систем захисту припускає наступну послідовність: загрози; модель порушника та його цілі; уразливості; політика безпеки, або методи зниження загроз; системи захисту; оцінка захищеності [4].

Але звертаючись до міжнародного стандарту серії ISO/IEC 27001 можна простежити більш детальні вимоги до етапів побудови системи менеджменту інформаційної безпеки (СМІБ) [5].

Даний стандарт потребує процедурного підходу для створення, впровадження, експлуатації, постійного контролю, аналізу, підтримання в робочому стані та покращення СМІБ організації, який полягає у використанні моделі «Plan-Do-Check-Act» (PDCA — цикл Шухарта–Деминга — планування — реалізація — перевірка — дія).

Розглядаючи як приклад створення СМІБ, модель набуває наступного вигляду.

Plan (планування) — фаза створення СМІБ, створення переліку активів, оцінка ризиків та вироблення заходів. Встановлення політики, цілей, процесів та процедур, які відносяться до менеджменту ризиків та покращенню захисту інформації (ЗІ) для отримання результатів у відповідності з загальною політикою та цілями організації.

Do (реалізація) — етап реалізації та впровадження відповідних заходів. Реалізація та експлуатація політики, засобів управління, процесів та процедур в сфері СМІБ.

Check (перевірка) — фаза оцінки ефективності та продуктивності СМІБ.

Act (дія, підтримка та покращення) — виконання превентивних та корегуючих дій з метою досягнення постійного покращення СМІБ.

Підсумовуючи все вище викладене структурно-логічну схему реалізації системи захисту ДІР за методологією «подвійної трійки захисту» можна представити так (рис. 1), з урахуванням процесного підходу (моделі PDCA) створення 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.

СУІБ ДІР побудована за процесним підходом та з урахуванням основних етапів впровадження даної системи згідно зі стандартом ISO/IEC 27001. До основних ресурсів, на які розповсюджуватиметься дія СУІБ ДІР в органах державного управління відносяться: інформаційні ресурси, засоби зберігання та обробки інформації, програмне забезпечення, допоміжні сервіси та системи життєзабезпечення, персонал.

Модель політики інформаційної безпеки ДІР (ПІБ ДІР) представляє собою систему правил, які регламентують порядок обробки інформації та скоординованих заходів, що забезпечують зниження ризику нанесення шкоди ДІР, який може реалізовуватись шляхом атакування.

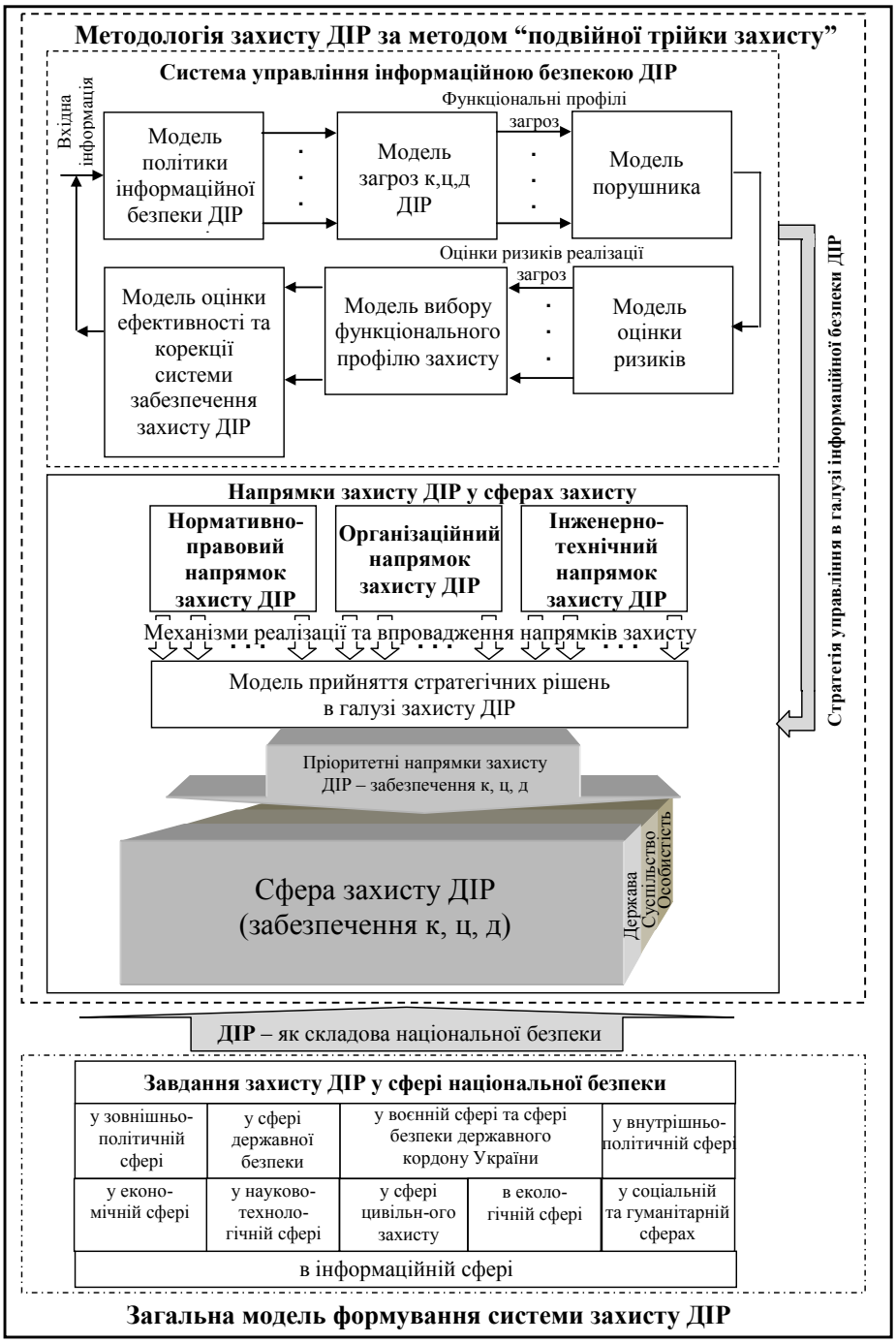

Рис. 1. Структурно-логічна схема реалізації системи захисту ДІР методом «подвійної трійки»

Основна мета ПІБ ДІР — забезпечити безпеку ресурсів інформаційно-телекомунікаційної системи (ІТС) шляхом впровадження максимально ефективних і оптимальних за витратами засобів забезпечення безпеки, мінімізувати рівень інформаційних ризиків з метою недопущення завдання збитків організаціям, у яких здійснюється обробка інформації, що віднесена до ДІР.

ПІБ ДІР є основою для управління інформаційними ризиками за допомогою аналізу загроз безпеки інформації, оцінки потенційного збитку від реалізації цих загроз і їхньої прийнятності для експлуатації ІТС організації, в якій здійснюється обробка інформації що віднесена до ДІР.

ПІБ ДІР визначає перелік необхідних для її забезпечення внутрішньо-нормативних документів, які повинні розроблятися після її прийняття.

Моделі загроз і порушників є основним інструментом забезпечення аналізу інформації при прийнятті рішень щодо розгортання, підтримки та удосконалення системи забезпечення інформаційної безпеки ДІР. Для проведення аналізу інформаційних ризиків і визначення вимог до системи інформаційної безпеки ДІР розробляються моделі загроз і порушників.

Модель загроз ДІР повинна будуватися з урахуванням впливу на основні властивості інформації, як складові методології «подвійної трійки захисту» (конфіденційність — К, цілісність — Ц, доступність — Д) та враховувати особливості функціонування, склад ІТС, технології обробки інформації та ін. Для цього необхідно визначити перелік суттєвих загроз ДІР та їх класифікувати за результатами впливу на властивості інформації, описати способи та методи їхнього здійснення. Таким чином, для кожної загрози ДІР необхідно визначити: на порушення яких властивостей інформації вона спрямована; джерела виникнення; можливі способи здійснення загроз.

Авторами в праці [6] представлено класифікатор загроз ДІР, який має лягти в основу для побудови моделі загроз ДІР. Також авторами представлено введене ними визначення загрози ДІР. *Загроза ДІР* — 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 [7]. Підсумовуючи вище викладене слід зазначити, що модель загроз ДІР має представляти абстрактно формалізований або неформалізований опис методів і засобів реалізації загроз ДІР та є необхідною складовою політики інформаційної безпеки ДІР.

Модель порушника. Відповідно до праці [8] *порушник* — користувач, який здійснює несанкціонований доступ до інформації. Таким чином, як порушник виступає особа, яка може отримати доступ до роботи з включеними до складу ІТС (в якій здійснюється обробка інформації, що віднесена до ДІР) засобів. Вона може унаслідок необізнаності, помилково, цілеспрямовано, свідомо чи несвідомо, використовуючи різні можливості, методи та засоби, здійснити спробу виконати операції, які призвели або можуть призвести до порушення властивостей інформації, що визначені політикою безпеки ДІР. Отже, модель порушника також є складовою ПІБ ДІР та представляє собою абстрактно формалізований або неформалізований опис порушника.

Модель порушника повинна визначати: можливу мету порушника та рівень його небезпеки для ІТС, в якій обробляється інформація що віднесена до ДІР; категорії осіб, із числа яких може визначатись порушник; припущення щодо кваліфікації порушника; припущення щодо характеру його дій.

Модель оцінки ризиків. Відповідно до праці [8] ризик — функція ймовірності реалізації певної загрози, виду і величини завданих збитків. За змістом міжнародного стандарту ISO/IEC 27005: 2008 ризик інформаційної безпеки являє собою потенційну можливість використання уразливостей активів або групи активів конкретною загрозою для нанесення збитку організації. В наступній інтерпретації міжнародного стандарту ISO/IEC 27005: 2011 ризик визначається як вплив невизначеності на мету, хоча інформаційна безпека також асоціюється з потенційними загрозами, які використовують уразливості інформаційного активу або групи інформаційних активів і, таким чином, наносять збиток організації. Як відмічалося вище, ПІБ ДІР є основою керування інформаційними ризиками. Існує багато методик оцінювання ризиків в автоматизованих системах (АС).

Автори пропонують здійснювати оцінку ризиків за вимогами міжнародних стандартів ISO/IEC 27005 та BS 7799, які визначають: основні елементи процесу управління ризиками; процесну модель (сутність даної моделі розглядалась вище); загальний підхід до управління ризиками; процеси аналізу та оцінювання ризиків; способи обробки ризиків; процес комунікації ризиків; приклади ризиків, загроз, уразливостей, активів, збитків, вимог законодавства та нормативної бази.

Необхідну відмітити, що при використанні даних стандартів і в цілому при використанні стандартів серії ISO/IEC 2700x можна говорити про певну їх гнучкість з точки зору їх адаптації до існуючої нормативної бази в державі.

Таким чином, *модель оцінки ризиків* представлятиме собою відповідний процес менеджменту ризиків інформаційної безпеки згідно з ISO/IEC 27005:2011, а саме: встановлення контексту; оцінки ризику; обробки ризику; прийняття ризику; обміну інформацією відносно ризику; моніторинг та перегляд ризику.

Модель процесу управління ризиками представлена на рис. 2. Як ми бачимо, вона також відповідає процесному підходу (моделі «Plan-Do-Check-Act») розглянутому вище.

Модель вибору функціонального профілю захисту призначена для визначення переліку мінімально необхідних рівнів послуг, які повинен реалізовувати комплекс засобів захисту (КЗЗ) обчислювальної системи ІТС для задоволення певних вимог щодо захищеності інформації, яка обробляється в даній ІТС.

Функціональні профілі можуть бути стандартними, які будуються на підставі існуючих вимог щодо захисту певної інформації від певних загроз і відомих на сьогодні функціональних послуг та залежно від завдань, які стоять перед КЗЗ, вводитися власні.

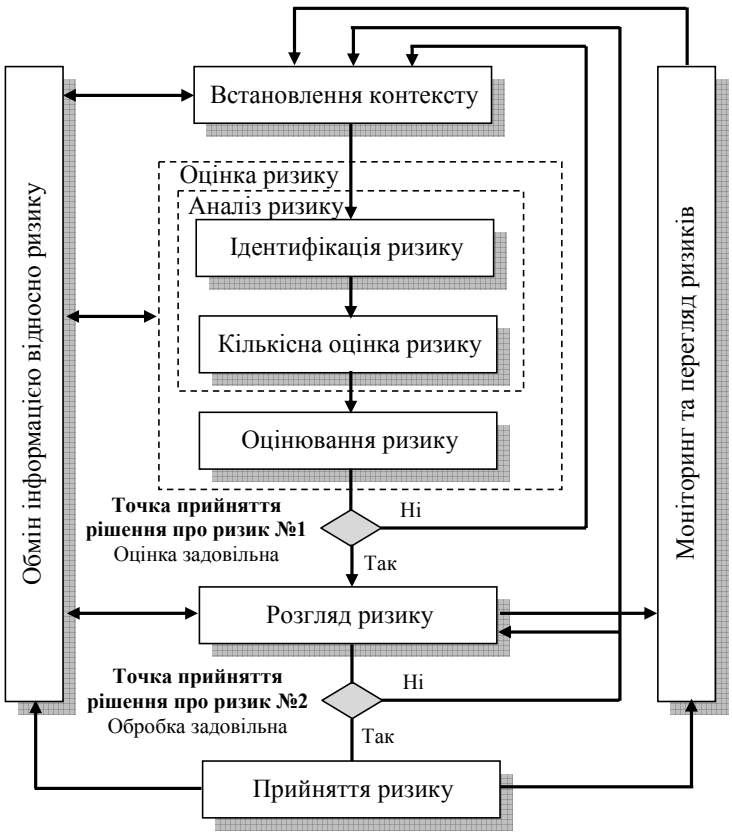

Рис. 2. Модель процесу управління ризиками згідно з ISO/IEC 27005

Функціональні профілі визначають відповідно до вимог нормативного документу технічного захисту інформації (НД ТЗІ) 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». Також, як визначено в даному документі ТЗІ «єдина вимога, якої слід дотримуватися при утворенні нових профілів, — 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».

Модель оцінки ефективності та корекції — реалізується через математичні моделі, які дають можливість проведення аналізу атак на ДІР та визначення ефективності захисту. Необхідно обов'язково вчиняти дії по усуненню причин невідповідності вимог СМІБ з метою попередження повтору. При цьому необхідно: виявляти невідповідності; визначати причини невідповідностей; оцінювати потреби в діях певного характеру з метою гарантувати убезпечення від виникнення подальших невідповідностей; визначати з метою реалізації потребуючі корегування дії; фіксувати результати вчинених дій; аналізувати потребу в коригуючих діях, що належні до застосування.

Первісним для успішного функціонування СУІБ ДІР є відпрацювання стратегії управління в галузі інформаційної безпеки ДІР, яка визначає напрямки захисту ДІР у сферах захисту, механізми реалізації та впровадження напрямків захисту. На підставі вказаного формується модель для прийняття стратегічних рішень в галузі захисту ДІР та подальшого визначення пріоритетних напрямків захисту ДІР щодо забезпечення їх конфіденційності, цілісності та доступності у сферах захисту: на державному, суспільному та особистісному рівні. У свою чергу, ДІР є складовими національної безпеки, що призводить до визначення завдань у цій сфері щодо їх захисту.

Основні результати

До основних результатів можна віднести представлення загальної моделі формування системи захисту ДІР у вигляді структурно-логічної схеми на основі методології «подвійної трійки захисту» та визначення ДІР, як складової національної безпеки.

Висновок

Таким чином, розглянуто актуальне питання забезпечення захисту ДІР в усіх напрямках державної політики з питань національної безпеки. Представлено загальну модель формування системи захисту ДІР у вигляді структурно-логічної

схеми на основі методу «подвійної трійки захисту» Визначено ДІР як складову національної безпеки. Це вказує напрямок та шляхи відпрацювання та визначення в подальшому відповідних вимог до показників захищеності ДІР в автоматизованих системах різних класів, основним з яких є визначення принципу контролю доступу до ДІР (політика безпеки ДІР) та впровадження системи управління ризиками.

ЛІТЕРАТУРА

1. *Богданович В. Ю.* Роль та місце воєнно-політичної моделі держави у розробленні та здійсненні політики забезпечення її воєнної безпеки / В. Ю. Богданович // Наука і оборона, № 1. — К. : МОУ, 1999. — С. 34–37.

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.

3. *Юдін О. К.* Правові аспекти формування системи державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Безпека інформації. — 2014. — Т. 20 (1). — С. 76–82.

4. *Грушо А. А.* Теоретические основы компьютерной безопасности : учеб. пособие для студентов высш. учеб. заведений / А. А. Грушо, Э. А. Применко, Е. Е. Тимонина. — М. : Издательский центр «Академия», 2009. — 272 с.

5. *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.

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

7. *Юдін О. К.* Аналіз загроз державним інформаційним ресурсам / О. К. Юдін, С. С. Бучик // Проблеми інформатизації та управління. — 2013. — № 4 (44). — С. 93–99.

8. *Термінологія* в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. — [Чинний від 28.04.1999]. — К. : ДСТСЗІ СБУ, 1999. — №22. — Режим доступу: http://www.dstszi.gov.ua/dstszi/control/uk/doccatalog/list?currDir=41640.

Стаття надійшла до редакції 03.11.2015