УДК 004.056.5

ПРИНЦИПИ ПОБУДОВИ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

***О. К. Юдін**, д-р техн. наук, проф.; ****С. С. Бучик**, канд. техн. наук, доц.
*Національний авіаційний університет
e-mail: kszi@ukr.net

** Житомирський військовий інститут імені С. П. Корольова
Державного університету телекомунікацій
e-mail: s_stbu@ukr.net

Введено поняття комплексної системи захисту державних інформаційних ресурсів. На основі принципів інформаційної безпеки, загальних принципів побудови систем захисту інформації та з урахуванням основних принципів побудови автоматизованих систем узагальнено та сформовано основні принципи побудови комплексної системи захисту державних інформаційних ресурсів. Запропоновано узагальнену структурну схему захисту державних інформаційних ресурсів.

Ключові слова: державні інформаційні ресурси, комплексна система захисту державних інформаційних ресурсів, принципи побудови комплексної системи захисту державних інформаційних ресурсів, структурна схема захисту державних інформаційних ресурсів.

The concept of the complex system of protection of state informative resources is entered in the articles. On the basis of principles of informative safety, general principles of construction of the systems of protection of information and taking into account basic principles the constructions of automatics system, generalized and the formed basic principles of construction of the complex system of protection of state informative resources. Offer is generalized flow diagram of protection of state informative resources.

Keywords: state informative resources, complex system of protection of state informative resources, principles of construction of the complex system of protection of state informative resources, flow diagram of protection of state informative resources.

Аналіз останніх досліджень і публікацій

Проблематиці захисту інформації в автоматизованих інформаційних системах (АІС) приділяють увагу багато вчених як в Україні, так і за кордоном.

Особливо гостро на сьогодні, з урахуванням умов постійної конкуренції не лише між недержавними структурами, а і структурами, які містять державні інформаційні ресурси, точиться боротьба за інформацію. Тому її захист завжди актуальний.

Принципи побудови комплексної системи захисту інформації (КСЗІ), загальні принципи інформаційної безпеки в автоматизованих системах (АС) розглядали такі фахівці у сфері захисту інформації, як В. М. Богуш, М. В. Грайворонський, О. А. Довидьков, В. Г. Кривуца, В. Ф. Шаньгин, О. Г. Корченко, Г. Ф. Конахович, В. Г. Грибунін та інші вчені.

Постановка завдань досліджень

Отже, метою статті є забезпечення на основі загальноприйнятих принципів інформаційної безпеки автоматизованих систем, побудови складних інформаційно-телекомунікаційних систем (ІТС) визначення основних принципів побудови комплексної системи захисту державних інформаційних ресурсів (КСЗ ДІР), надання тлумачення поняття КСЗ ДІР та подання узагальненої структури системи захисту ДІР.

Виклад основного матеріалу

Відповідно до НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», затвердженого наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22, *комплексна система захисту інформації* являє собою сукупність організаційних і інженерних заходів, програмно-апаратних засобів, які забезпечують захист інформації в автоматизованій системі.

Перед тим, як визначитися з узагальненою структурною схемою захисту ДІР необхідно розібратися, що собою становить дана система захисту.

Авторами в праці [1] надавалось визначення 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 в 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 з визначеною політикою безпеки й чинного законодавства.

Звертаючись до НД ТЗІ 3.7-003-2005 «Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі», затвердженого наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 8 листопада 2005 р. № 125 із змінами згідно з наказом Адміністрації Держспецзв'язку від 28.12.2012 № 806, можна стверджувати, що ДІР міститимуться саме в ІТС, під якою відповідно даного НД розуміється будь-яка система, яка відповідає одному з трьох наведених нижче видів АС:

– інформаційна система — організаційно-технічна система, що реалізує технологію обробки інформації за допомогою засобів обчислювальної техніки та програмного забезпечення;

– телекомунікаційна система — організаційно-технічна система, що реалізує технологію інформаційного обміну за допомогою технічних і програмних засобів шляхом передавання та приймання інформації у вигляді сигналів, знаків, звуків, зображень чи іншим чином;

– інтегрована система — сукупність двох або кількох взаємопов'язаних інформаційних та (або) телекомунікаційних систем, у якій функціонування однієї (кількох) з них залежить від результатів функціонування іншої (інших) таким чином, що цю сукупність у процесі взаємодії можна розглядати як єдину систему.

Встановлений цим НД ТЗІ порядок є обов'язковим для всіх суб'єктів системи ТЗІ в Україні незалежно від їхньої організаційно-правової форми та форми власності, в ІТС яких обробляється інформація, яка належить до *державних інформаційних ресурсів*, державної чи іншої таємниці або окремих видів інформації, необхідність захисту якої визначено законодавством. У зв'язку з цим, якщо інформація віднесена до ДІР, виникає необхідність створення КСЗІ відповідно до наведеного НД ТЗІ, але виходячи з того, що досі не створено НД ТЗІ щодо ДІР (хоча б на рівні НД, який би вводив термінологію, яка стосувалася поняття ДІР, не говорячи про певний стандарт, який закріплював дане поняття та все, що його охоплює) виникає необхідність введення поняття *комплексної системи захисту державних інформаційних ресурсів*.

Таким чином, з наведеного вище міркування випливає таке визначення КСЗ ДІР.

Комплексна система захисту державних інформаційних ресурсів — сукупність організаційних та інженерних заходів, програмно-апаратних засобів, які забезпечують захист державних інформаційних ресурсів, що підлягають захисту згідно з визначеною політикою безпеки й чинного законодавства в інформаційно-телекомунікаційних системах (інформаційних, телекомунікаційних, інтегрованих системах) держави, суспільства або громадян.

Говорячи про ІТС, у яких як інформація використовується ДІР, слід уявляти, що такі ІТС можуть складатися з декількох підсистем, які вирішують конкретні завдання. Так, наприклад, до складу Єдиної автоматизованої інформаційної системи (ЄАІС) Держмитслужби [2] входять такі елементи: автоматизована інформаційна система «Центр»; автоматизована система митного оформлення (АСМО) та локальні підсистеми митних органів, спеціалізованих митних установ та організацій, що взаємодіють із АІС «Центр»; відомча телекомунікаційна мережа (ВТМ) Держмитслужби; локальні обчислювальні мережі митних органів, спеціалізованих митних установ та організацій; інформаційно-телекомунікаційний комплекс Держмитслужби «Елект-ронна пошта»; адміністративно-правова інформаційна підсистема; підсистема інформаційного забезпечення; система електронного документообігу Держмитслужби; *комплексна система захисту інформації; підсистема криптографічного захисту інформації; система електронного цифрового підпису Держмитслужби*.

Останні три підсистеми безпосередньо відносяться до систем, які забезпечують захист інформації за відповідними спрямуваннями (нормативно-правовим, організаційним та інженерно-технічним).

Як вказано в праці [2], інформаційні ресурси ЄАІС Держмитслужби, митних органів, спеціалізованих митних установ, організацій становлять певну цінність та потребують захисту від різноманітних за своєю сутністю впливів, які можуть призвести до несанкціонованих: знищення, пошкодження або модифікації, порушення конфіденційності, а також зниження цінності.

На рис. 1 подано структурну схему елементів КСЗІ ЄАІС Держмитслужби [2].

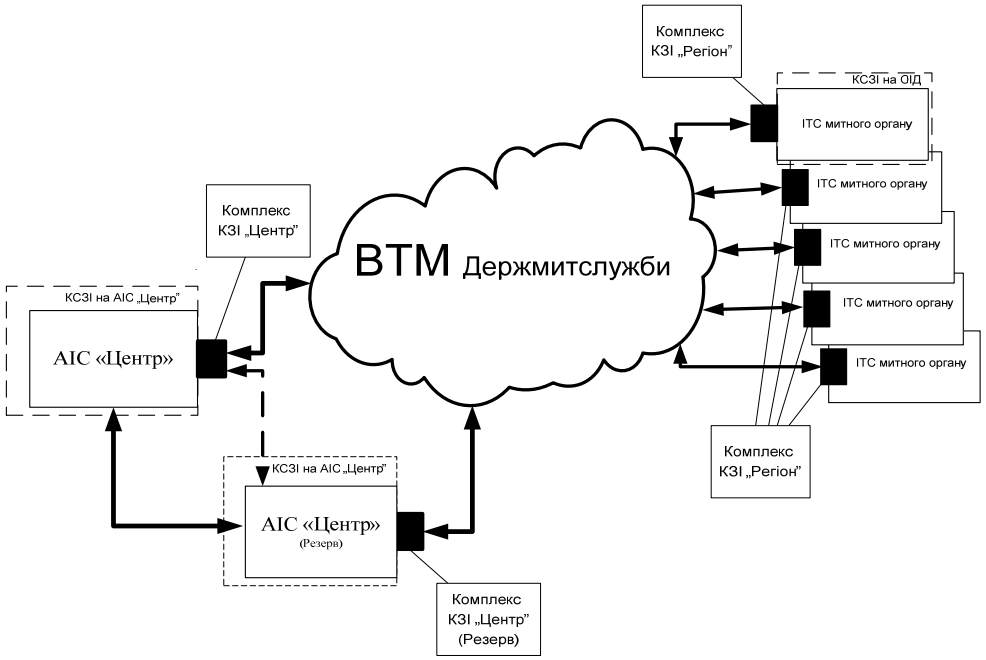

Рис. 1. Структурна схема елементів КСЗІ ЄАІС Держмитслужби

Зі схеми видно, що КСЗІ створена на кожну АІС, чи то центральна АІС, або ІТС регіональних органів. Також можна зрозуміти, що в межах АІС «Центр» передбачається додаткове створення резервної системи, яка цілком дублює головні функції основної системи.

Безпека інформації ЄАІС Держмитслужби базується на виконанні таких загальних принципів [2]: централізоване управління системою; послідовність рубежів безпеки; адекватність та ефективність захисту; безперервність захисту; забезпечення безперервного виконання функцій, які покладені на КСЗІ ЄАІС Держмитслужби, у разі відмов системи та її окремих елементів (підсистем); захист засобів забезпечення безпеки системи; прихованість захисту; фізичний розподіл ВТМ та мережі загального використання (Інтернет).

На думку авторів та відповідно до запропонованого в праці [3] методу «подвійної трійки захисту», під час проектування різних видів КСЗІ необхідно визначити три базові властивості інформації, що підлягають захисту при формуванні будь-якої політики безпеки (конфіденційність, цілісність, доступність) — перша платформа та складові, що реалізують систему захисту (методи та засоби) — друга платформа: нормативно-правові; організаційні; інженерно-технічні.

Таким чином, розглядаючи приклад побудови ЄАІС Держмитслужби, де містяться ДІР, можна стверджувати, що ДІР становлять певну цінність та вимагають захисту від різноманітних за своєю сутністю загроз, які можуть через вразливості вплинути на властивості інформації (конфіденційність, цілісність, доступність). Це вказує на шляхи зведення всіх нормативних документів, які регламентують питання щодо експлуатації АС, що містять ДІР, до єдиних вимог.

В зв’язку з чим, в подальшому виникає необхідність пов’язувати такі підсистеми в єдиний комплекс і зрозуміло, що найкращими в даному випадку принципами побудови таких складних ІТС будуть схожі з принципами побудови корпоративних інформаційних систем (КІС).

У праці [4] розкриті такі основні принципи:

– використання загальноприйнятих стандартів, які підтримуються основними виробниками програмного забезпечення;

– застосування програмного забезпечення достатньої продуктивності, з метою незмінюваності при збільшенні потужності та кількості обладнання, яке використовується — якість масштабованості програмного забезпечення;

– дотримання принципу багатоланковості, в результаті якого кожен рівень системи реалізує функції, найбільш йому притаманні;

– реалізація принципу апаратно-платформенної незалежності і системного програмного забезпечення;

– здійснення принципу комунікаційності, коли різні рівні системи можуть взаємодіяти між собою як за даними, так і за додатками.

У праці [5] наведені основні принципи забезпечення інформаційної безпеки АС: системності; комплексності; безперервності захисту; розумної достатності; гнучкості захисту;

відкритості алгоритмів та механізмів захисту; простоти та зручності використання засобів захисту.

Виходячи з декомпозиції опису системи захисту в цілому, слід виокремити основні чотири рівні [5]: рівень 1 — політика безпеки; рівень 2 — функції (профіль функції) захисту; рівень 3 — механізми захисту; рівень 4 — засоби захисту.

Аналізуючи основні принципи, які забезпечують інформаційну безпеку АС, можна узагальнити основні принципи побудови КСЗ ДІР та віднести до них:

– системність;

– централізоване управління системою;

– комплексність;

– своєчасність та безперервність захисту, послідовність їх рубежів;

– резервування основних елементів системи;

– розумну достатність та адекватність захисту;

– гнучкість захисту;

– прихованість захисту;

– відкритість алгоритмів та механізмів захисту;

– простоту та зручність використання засобів захисту;

– захист засобів забезпечення безпеки системи;

– фізичний розподіл відомчих телекомунікаційних мереж та мережі загального використання;

– забезпечення безперервного виконання функцій, які покладені на КСЗ ДІР, при відмовах системи та її окремих елементів (підсистем);

– використання загальноприйнятих стандартів;

– масштабованість програмного забезпечення;

– багатоланковість;

– апаратно-платформенну незалежність і системність програмного забезпечення;

– комунікаційність;

– достатню ефективність захисту (визначається рівнем допустимого ризику порушення основних властивостей інформації).

Виходячи з принципів побудови КСЗ ДІР, можна запропонувати узагальнену структурну схему системи захисту ДІР, показану на (рис. 2).

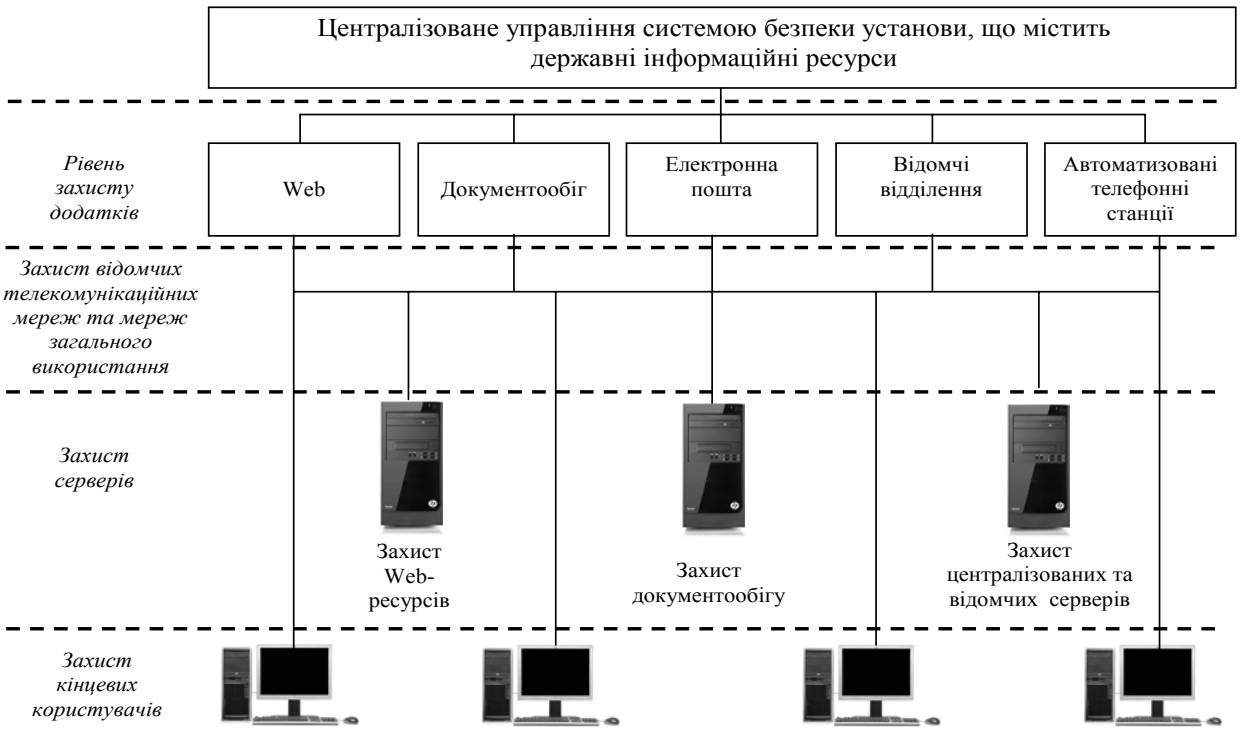

Рис. 2. Структурна схема захисту ДІР

Дана структурна схема є ієрархічною і до неї може застосовуватись доказовий підхід [5], ідея якого полягає в послідовній перевірці правильності описів системи захисту на кожному з використовуваних рівнів та адекватності переходу від одного рівня опису до наступного.

Визначимо рівень захисту додатків як R_1, рівень захисту відомчих телекомунікаційних мереж — R_2 та мереж загального використання — R_3, рівень захисту серверів — R_4, рівень захисту кінцевих користувачів — R_5.

Позначимо $F(R_i)$ як функція взаємодії даних рівнів захисту. Тоді кожному із цих рівнів буде відповідати множина підрівнів описів систем захисту L_{ij} ($i=\overline{1,5}$; $j=\overline{1,10}$), де L_{i1} відповідає опису наявних інформаційних ресурсів (ДІР); L_{i2} — опис мети та завдань захисту ДІР; L_{i3} відповідає опис політики безпеки; L_{i4} — класифікація ДІР та модель доступу до них; L_{i5} — модель порушника, L_{i6} — модель загроз; L_{i7} — опис послуг безпеки; L_{i8} — опис механізмів захисту; L_{i9} — опис засобів захисту; L_{i10} — оцінка ефективності КСЗ ДІР та корекція політики безпеки (за потребою).

Кожний із підрівнів L_{ij} (крім L_{i10}) надає вищому підрівню U певну множину послуг. У зв'язку з цим мова M_{ij} кожного ij-го підрівня використовує послуги U_{ij+1}, що надаються нижнім підрівнем.

Отже, схема формалізованого опису системи захисту ДІР може бути подана таким чином (рис. 3).

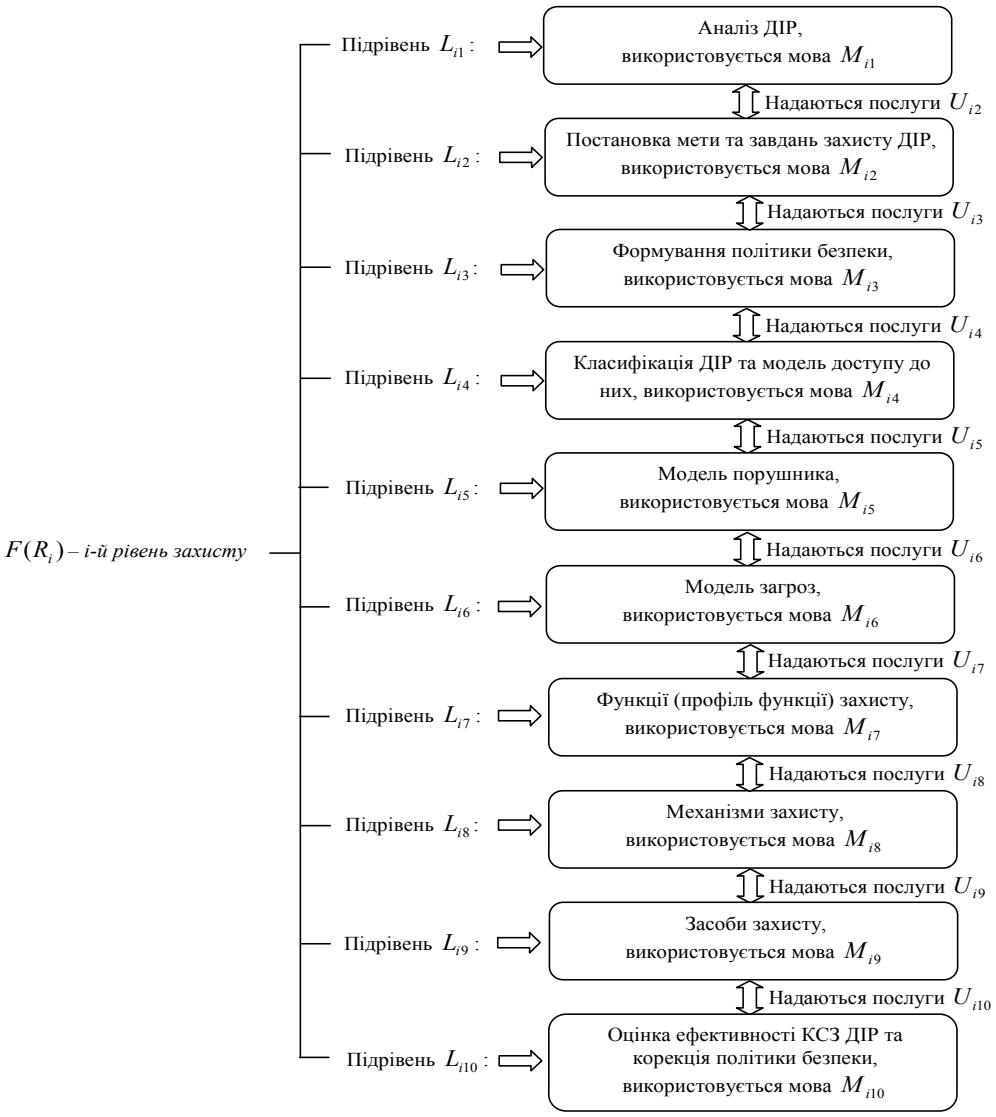

Рис. 3. Схема формалізованого опису системи захисту ДІР

Дана схема може бути адаптована відповідно до структури управління процесами моделі взаємодії відкритих систем ISO/OSI [6].

Згідно з методологічним підходом та існуючою практикою французьких та німецьких шкіл інформаційної безпеки, політику безпеки можна розглядати як єдину політику або окремі часткові політики рівнів безпеки.

Основні результати

До основних результатів, отриманих в статті, можна віднести введення поняття комплексної системи захисту державних

інформаційних ресурсів на основі принципів інформаційної безпеки, загальних принципів побудови систем захисту інформації та з урахуванням основних принципів побудови автоматизованих систем, узагальнених та сформованих основних принципів побудови КСЗ ДІР.

Як наслідок, запропонована узагальнена структурна схема захисту ДІР та на її основі наведена схема формалізованого опису системи захисту ДІР.

Висновки

Отже, у статті надано визначення поняття КСЗІ ДІР, що має лягти в основу НД ТЗІ в ІТС, які містять ДІР. Узагальнені та визначені основні принципи побудови КСЗ ДІР та приведена узагальнена структурна схема захисту ДІР, схема формалізованого опису системи захисту ДІР. Це повинно допомогти розробникам ІТС обґрунтованіше підходити як до побудови самих ІТС, так і до побудови КСЗІ в цих системах. Також, як зазначено в статті, досі не створено НД ТЗІ ДІР, не згадуючи про певний стандарт, який закріплював дане поняття та все, що його охоплює. В зв'язку з цим, виникає необхідність закріплення на законодавчому рівні окремо виділеного напрямку з питань захисту ДІР, що має втілюватись у певні стандарти, НД ТЗІ, інші нормативно-правові документи щодо захисту інформації.

Подальшим напрямком досліджень автори вбачають відпрацювання узагальненого підходу щодо побудови загальної структури багаторівневої КСЗ ДІР.

ЛІТЕРАТУРА

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

2. *Положення* про Єдину автоматизовану інформаційну систему Державної митної служби України (затверджено наказом Державної митної служби України від 04.11.2010 № 1341). — [Електронний ресурс]. — Режим доступу: http://sfs.gov.ua/data/normativ/000/000/62603/2.doc.

3. *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) / Технічні науки. — С. 200–210.

4. *Шаньгин В. Ф.* Информационная безопасность / Владимир Федорович Шаньгин. — М. : ДМК Пресс, 2014. — 702 с.

5. *Богуш В. М.* Теоретичні основи захищених інформаційних технологій: навч. посіб. / Б. М. Богуш, О. А. Довидьков, В. Г. Кривуца. — К. : ДУІКТ, 2010. — 454 с.

6. *Юдін О. К.* Захист інформації в мережах передачі даних / О. К. Юдін, О. Г. Корченко, Г. Ф. Конахович. — К.: Вид-во ТОВ «НВП» ІНТЕРСЕРВІС», 2009. — 716 с.

Стаття надійшла до редакції 20.02.2015