УДК 004.056.5

КОНЦЕПТУАЛЬНА МОДЕЛЬ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ 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

Проведено аналіз побудови моделей безпеки інформаційних ресурсів. Акцентовано увагу на необхідності включення в будь-яку модель інформаційної безпеки підходів загальних критеріїв. Побудовано концептуальну модель інформаційної безпеки державних інформаційних ресурсів, розкриті її основні компоненти. Визначено напрямки подальших досліджень щодо аналізу існуючих і побудови власних структурних схем систем захисту інформації для інформаційних систем, які містять державні інформаційні ресурси.

Ключові слова: державні інформаційні ресурси, модель інформаційної безпеки, інформаційна безпека.

The analysis of construction of models of safety of informative resources is conducted in the article. The accented attention is on the necessity of including for any model of informative safety of approaches of the General criteria. Built conceptual model of informative safety of state informative resources, exposed her basic components. Shown directions of further researches in relation to the analysis of existing and to the construction for the informative systems which contain the state informative resources of flow diagrams of the systems of information protection.

Keywords: state informative resources, model of informative safety, informative safety.

Аналіз останніх досліджень і публікацій

Питанням побудови моделей інформаційної безпеки ресурсів приділяють увагу багато вчених як в Україні, так і за кордоном. Але зрозуміло, що у зв'язку з прагненням України щодо вступу до Європейського союзу, виникає необхідність введення критеріїв інформаційної безпеки, які б відповідали міжнародним стандартам. Так, відповідно до стандарту ISO/IEC 15408 «Критерії оцінки безпеки інформаційних технологій» (Загальні критерії) загальна схема забезпечення інформаційної безпеки, яку представив професор В. Ф. Шаньгин [1], має такий вигляд (рис. 1). Як визначено в [1] на схемі показано взаємодію основних суб'єктів та об'єктів забезпечення інформаційної безпеки, як це запропоновано в стандарті ГОСТ Р ИСО/МЭК 15408-1-2002, що діє з 2004 р. в Росії і є повним аналогом Загальних критеріїв (нажаль в Україні цей стандарт досі не введено). Дана схема можна використовувати як основу для побудови концептуальної моделі ІБ ДІР. Подібна ж схема моделі побудови інформаційної безпеки виробництва представлена в [2]. Ця модель відрізняється від попередньої тим, що введено позначення впливів (природний та управляючий).

У цілому модель (рис. 2) виконана також за стандартом ISO/IEC 15408.

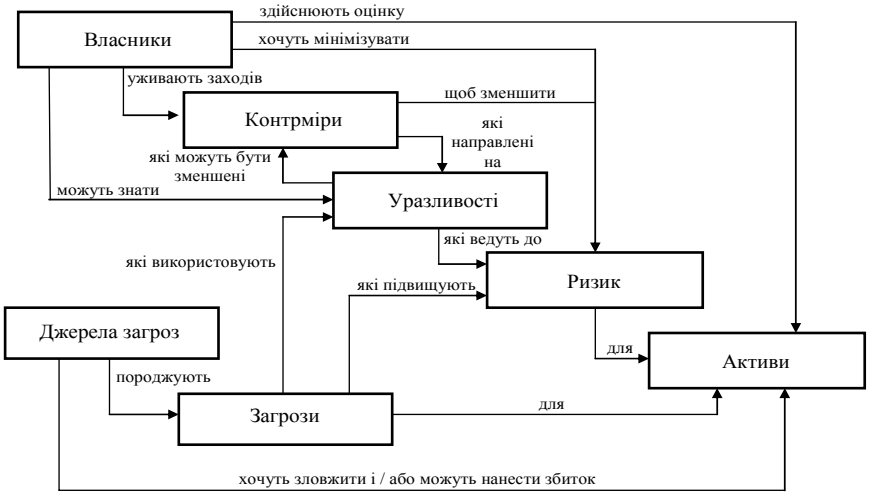

Рис. 1. Загальна схема забезпечення інформаційної безпеки відповідно до стандарту ISO/IEC 15408 «Критерії оцінки безпеки інформаційних технологій»

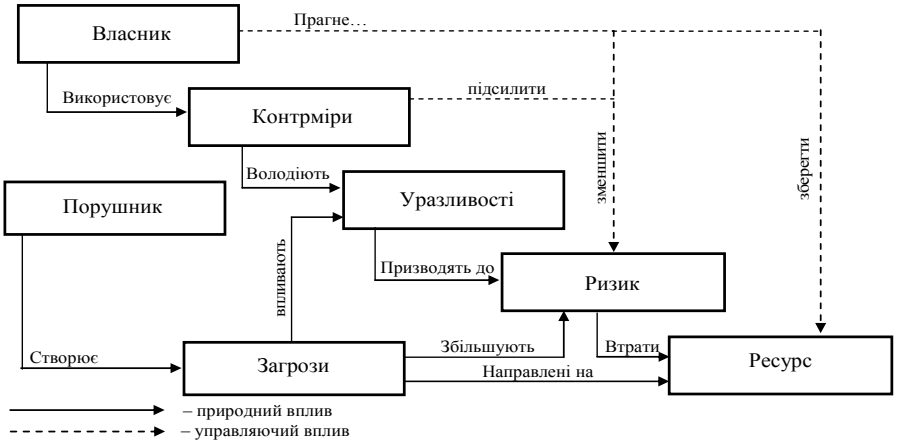

Рис. 2. Модель побудови системи інформаційної безпеки виробництва

У праці [3] представлена узагальнена концепція побудови системи безпеки інформації (УКЗІ), під якою автори розуміють інструментально-методологічну базу, що забезпечує оптимальну практичну реалізацію стратегій захисту на регулярній основі з урахуванням мінімальних витрат. Там же представлена і структура УКЗІ, але дана система не прив'язана до стандарту ISO/IEC 15408.

У праці [4] авторами представлена принципова модель забезпечення безпеки конфіденційної інформації (рис. 3), але дана модель також не до кінця враховує підхід стандарту ISO/IEC 15408.

І нарешті в праці [5] наводиться концептуальна модель безпеки інформації (рис. 4), але вона також не до кінця враховує підхід стандарту ISO/IEC 15408.

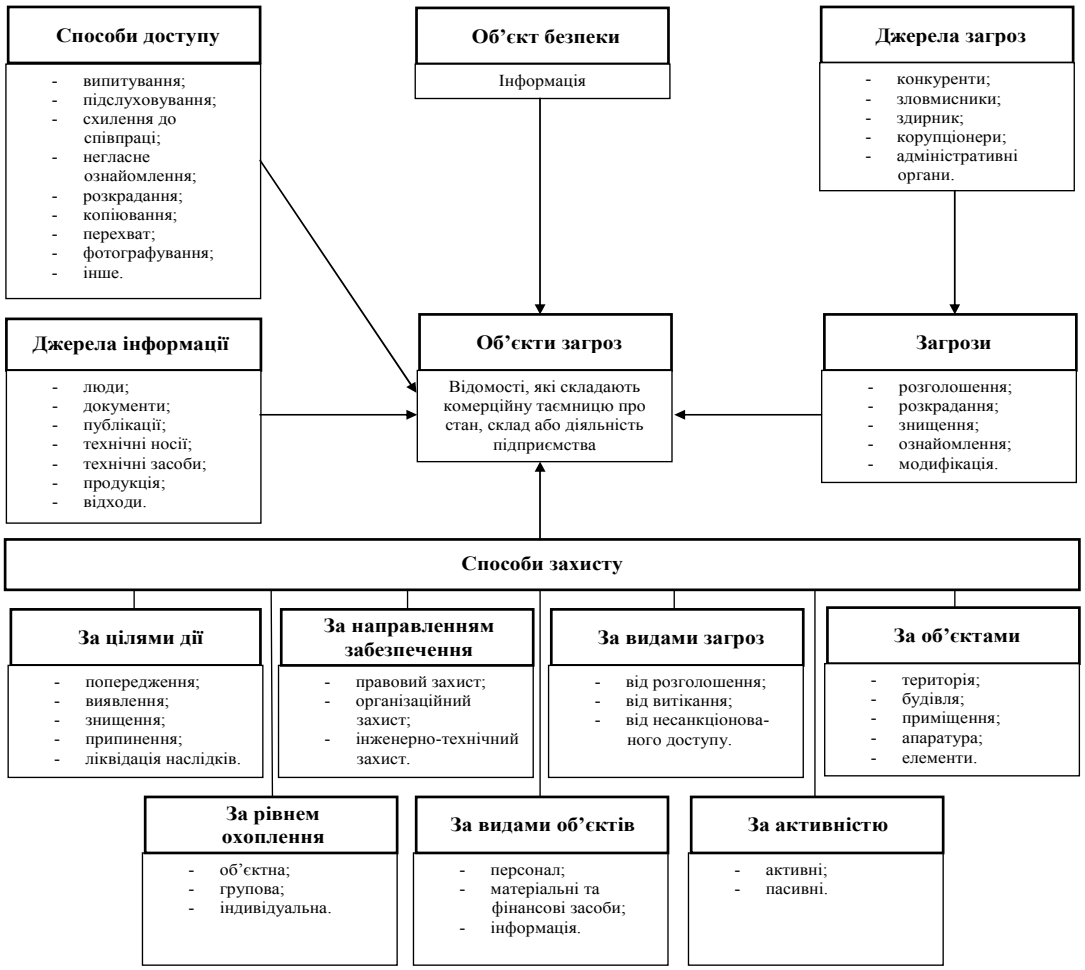

Рис. 3. Принципова модель забезпечення безпеки конфіденційної інформації

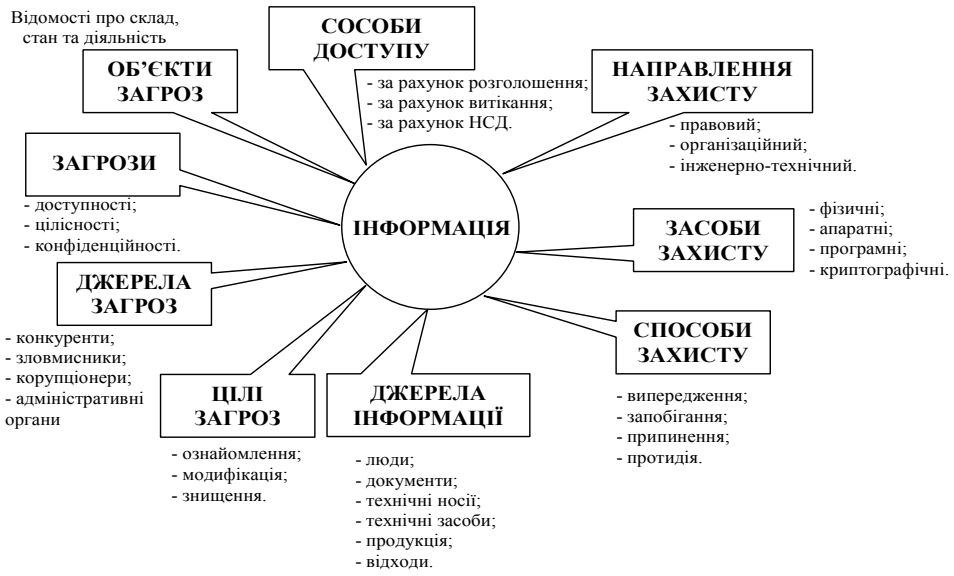

Рис. 4. Концептуальна модель безпеки інформації

Постановка задач досліджень

Мета статті полягає у побудові концептуальної моделі інформаційної безпеки державних інформаційних ресурсів виходячи з існуючих моделей, з обов'язковим урахуванням підходів міжнародного стандарту ISO/IEC 15408, попередніх досліджень, які були здійсненні авторами.

Виклад основного матеріалу

Закон України «Про Державну службу спеціального зв'язку та захисту інформації України» (від 23 лютого 2006 року № 3475-IV зі змінами від 09 квітні 2014 року) державні інформаційні ресурси (ДІР) визначає наступним чином: ***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.

Також останніми змінами до Закону (від 09 квітня 2014 року) у тексті «інформація, яка є власністю держави» в усіх відмінках замінено «державні інформаційні ресурси». Тим самим, інформація, яка є власністю держави остаточно визначена як державні інформаційні ресурси.

У праці [6] було надано розширене визначення поняття ДІР.

Державні інформаційні ресурси — це результат 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.

Інформаційна безпека (ІБ) згідно з працею [7] визначається як стан захищеності інформаційного середовища держави, суспільства та особистості, якій забезпечує його формування, збереження, використання і розвиток в інтересах громадян, організації чи держави. Там же наведено більш розширене визначення ІБ.

Інформаційна безпека — це стан захищеності властивостей інформації (інформаційних ресурсів), що належить державі, суспільству і особистості, за якого забезпечується її оброблення, зберігання, поширення і прогресивний розвиток незалежно від (або в умовах) наявності чи реалізації внутрішніх і зовнішніх інформаційних загроз.

До основних компонентів концептуальної моделі ІБ ДІР можуть бути віднесені:

– об'єкти загроз ДІР;

– загрози ДІР (нормативно-правового, організаційного, інженерно-технічного спрямування)

за відповідними властивостями інформації (конфіденційність, цілісність, доступність);

– джерела загроз ДІР;

– уразливості ДІР;

– ризик реалізації загрози ДІР через уразливість;

– цілі джерел загроз ДІР;

– джерела відомостей про ДІР;

– способи неправомірного оволодіння ДІР (способи доступу до ДІР);

– напрями захисту ДІР (нормативно-правовий, організаційний, інженерно-технічний);

– способи захисту ДІР;

– засоби захисту ДІР

Об'єкти загроз ДІР (відповідно до визначеного авторами поняття ДІР) — всі інформаційні ресурси держави, суспільства або громадян, які підлягають захисту згідно визначеної політики безпеки й чинного законодавства.

Загрози 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 (дане визначення було запропоновано авторами в праці [8]). У праці [9] «через призму загальних напрямів забезпечення безпеки інформації (правовий захист, організаційний захист, інженерно-технічний захист)» загрози ДІР можуть бути визначені як загрози відповідного спрямування:

– загрози нормативно-правового спрямування — 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;

– загрози організаційного спрямування — 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);

– загрози інженерно-технічного спрямування — 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.

Джерела загроз ДІР — носії загроз безпеці інформації ДІР (кібертерористи та кіберзловмисники, персонал підданий корупційним діям, адміністративно-управлінські органи державної влади і т. д.). У цілому всі джерела загроз безпеці інформації можна розділити на три групи обумовлені діями суб'єкта (антропогенні джерела загроз); обумовлені технічними засобами (техногенні джерела загроз); зумовлені стихійними джерелами.

Уразливості ДІР — чинники, що призводять до порушення безпеки інформації на конкретному об'єкті інформаційної діяльності.

Ризик реалізації загрози ДІР. Існує декілька визначень поняття ризику:

Ризик — функція ймовірності реалізації певної загрози, виду і величини завданих збитків [10].

Ризик — потенційна можливість використання уразливостей активу або групи активів реальною загрозою для заподіяння збитку організації (ISO/IEC 27005:2008).

Ризик — комбінація ймовірності події і її наслідків (BS 7799-3:2006).

Таким чином *ризик реалізації загрози ДІР* — потенційна можливість використання уразливостей державних інформаційних ресурсів реальною загрозою для заподіяння збитку державі, суспільству, окремому громадянину.

Цілі джерел загроз ДІР — ознайомлення з конфіденційними відомостями, їх модифікація з корисною метою, знищення для нанесення прямого матеріального збитку.

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.

Способи неправомірного оволодіння ДІР (способи доступу до ДІР) — розголошення джерелами конфіденційних відомостей, витік інформації через технічні засоби, несанкціонований доступ до відомостей, що підлягають охороні.

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 [9]. До основних напрямків захисту ДІР відносяться відповідно до комплексного підходу до захисту ДІР нормативно-правовий, організаційний та інженерно-технічний.

Способи захисту ДІР — будь-які міри, шляхи, способи та дії, які забезпечують попередження протиправних дій, їх запобігання, припинення та протидію несанкціонованому доступу до ДІР.

Засоби захисту ДІР — фізичні, апаратні, програмні засоби та криптографічні методи. Криптографічні методи можуть бути реалізовані як апаратно так і змішано програмно-апаратними засобами. Таким чином, враховуючи також запропоновану авторами інформаційно-аналітичну модель методу «подвійної трійки захисту», як основу формування методології побудови класифікатора загроз ДІР [9] з урахуванням складових процесу захисту інформаційних ресурсів, концептуальна модель ІБ ДІР може бути представлено таким чином (рис. 5).

Рис. 5. Концептуальна модель інформаційної безпеки державних інформаційних ресурсів

Основні результати

До основного результату роботи можна віднести розроблення концептуальної моделі інформаційної безпеки державних інформаційних ресурсів, яка в собі об'єднала вимоги міжнародного стандарту ISO/IEC 15408, існуючи підходи та врахувала ті напрацювання, які були зроблені авторами в попередніх працях.

Висновки

Таким чином, у статті отримало подальший розвиток питання побудови моделей інформаційної безпеки в цілому і державних інформаційних ресурсів в конкретному випадку. Це шлях для подальших досліджень з погляду побудови структурних схем системи захисту інформації інформаційних систем, які містять державні інформаційні ресурси.

ЛІТЕРАТУРА

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

2. *Возможная* методика построения системы информационной безопасности предприятия. — Режим доступу: http://sec4all.net/konf2.html

3. Юдін О. К. Захист інформації в мережах передачі даних / О. К. Юдін, О. Г. Корченко, Г. Ф. Конахович. — К. : НВП «ІРТЕРСЕРВІС», 2009. — 716 с.

4. *Поповский В. В*. Защита информации в телекоммуникационных системах. Т. 1: учеб. / В. В. Поповский, А. В. Персиков. — Х. : ООО «Компания СМИТ», 2006. — 238 с.

5. *Концептуальная* модель информационной безопасности. — Режим доступу: http://www.pki-exam.narod.ru/ib/t2/p2.html.

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

7. *Юдін О. К.* Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О. К. Юдін. — К. : НАУ, 2011. — 640 с.

8. *Юдін О. К.* Загрози державним інформаційним ресурсам: терміни та визначення / О. К. Юдін, С. С. Бучик // Захист інформації. — 2014. — Т. 16 (2) / Технічні науки. — С. 121–125.

9. *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.

10. *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. — (Нормативний документ системи технічного захисту інформації).

Стаття надійшла до редакції 28.11.2014.