ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

УДК 004.056.5

ІЄРАРХІЧНИЙ КЛАСИФІКАТОР АВТОМАТИЗОВАНИХ СИСТЕМ ПРИКОРДОННОГО ВІДОМСТВА

ЮДІН О.К., СТРЕЛЬБІЦЬКИЙ М.А.

Формулюється та доводиться теорема безпеки для взаємодіючих систем, що дозволить раціоналізувати обсяг робіт із забезпечення нормативного рівня захисту. Крім того, наводиться класифікація автоматизованих систем з урахуванням масштабу, ступеня взаємодії та виду інформації, яка обробляється.

Ключові слова: теорема безпеки для взаємодіючих систем, ієрархічний класифікатор автоматизованих систем.

Keywords: theorem of safety for interacting systems, hierarchical classifier automated systems.

1. Вступ

Стратегія національної безпеки України чітко визначає загрози інформаційній безпеці, кібербезпеці і безпеці інформаційних ресурсів України: ведення інформаційної війни проти України, уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак, а також фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом [1]. Державна прикордонна служба України (ДПСУ), як суб'єкт забезпечення національної безпеки, зобов'язана протидіяти визначеним загрозам та забезпечити ефективну реалізацію політики у сфері захисту та охорони державного кордону України, а також охорони суверенних прав України в її виключній (морській) економічній зоні, у тому числі шляхом створення системи інтегрованого управління безпекою державного кордону, розвитку її інформаційної складової, зокрема забезпечення інформаційної безпеки. Стратегією передбачені пріоритети забезпечення інформаційної безпеки, окремими з яких є захищеність об'єктів критичної інфраструктури та державних інформаційних ресурсів.

Будь-яка система захисту передбачає обґрунтування необхідності її створення. На даному етапі проводиться аналіз нормативно-правових документів, визначається необхідність забезпечення захисту інформації та здійснюється її класифікація за правовим режимом, за рівнем обмеження доступу до неї, за вимогами до забезпечення конфіденційності, цілісності та доступності. На теперішній час розроблена достатньо представницька система класифікації автоматизованих інформаційних систем, але загальноприйнятих положень у даний час не існує. Найважливіше призначення класифікації – опис ключових властивостей об'єктів, який надає можливість використовувати її для ідентифікації конкретних систем. Уточнення класифікації автоматизованих системи дозволить в подальшому сформувати відповідні профілі захищеності складових інформації, яка циркулює в автоматизованій системі, а саме: конфіденційність, цілісність та доступність.

Метою дослідження є формування ієрархічного класифікатора автоматизованих систем, що містять державні інформаційні ресурси за масштабом, ступенем взаємодії та видом інформації, яка обробляється ними.

2. Основна частина дослідження

Інтегрована інформаційно-телекомунікаційна система (ІІТС) прикордонного відомства складається з множини взаємодіючих інформаційно-телекомунікаційних систем (ІТС), інформаційних систем (ІС) та підсистем (ПС) [2]. Окремі з них передбачають однокористувацький режим роботи, деякі – автономне функціонування в межах інформаційної системи, частина – спільне використання інформаційних ресурсів. Особливістю ІІТС ДПСУ є наявність міжвідомчих ІТС, розпорядником яких є Адміністрація Державної прикордонної служби України. В процесі модернізації складової ІІТС, особливо в частині захисту інформації, необхідно також враховувати взаємодію ІТС одна з одною. У випадку спільного використання інформаційних ресурсів декількома ІТС модернізація однієї із них вимагатиме перегляду систем захисту всіх інших.

Відповідно до НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні профілі захищеності оброблюваної інформації від несанкціонованого доступу" виділено три ієрархічні класи автоматизованих систем (АС):

клас «1» – одномашинний однокористувацький комплекс, який обробляє інформацію однієї або кількох ступенів обмеження доступу;

клас «2» – локалізований багатомашинний багатокористувацький комплекс, який обробляє інформацію різних ступенів обмеження доступу;

клас «3» – розподілений багатомашинний багатокористувацький комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Розглядаючи міжнародний стандарт ISO/IEC 27001:2005 "Information Management – Specification With Guidance for Use", можна стверджувати про необхідність запровадження четвертого класу автоматизованих систем – клас «4», який би враховував вирішення питань забезпечення захисту інформації в договорах з третіми особами [3].

Варто зазначити, що наведена класифікація автоматизованих систем дозволяє виокремити їх за масштабом, але не показує ступінь взаємодії з

іншими АС. З точки зору захисту інформації в одній АС такої класифікації цілком достатньо. Навіть у випадку взаємодії декількох автоматизованих систем, використовуючи наведену класифікацію, їх можна розглядати як одну, але більшого масштабу.

Разом із тим, такий підхід не є раціональним, оскільки вимагає проведення всього комплексу робіт (нормативно-правові, організаційні, інженерно-технічні) для системи вищого рівня (метасистеми). При цьому, у випадку модернізації однієї системи захист необхідно проводити для загальної АС (метасистеми). Таким чином, виникає питання, чи зміниться безпека системи в цілому при модернізації однієї підсистеми за умови, що рівень безпеки підсистеми та взаємодія з системою безпечні після модернізації.

Наведене вище дозволяє сформувати теорему безпеки для взаємодіючих систем (транзитивність безпеки).

Теорема. *Якщо підсистеми A, B, C безпечні та безпечна взаємодія A з B та B з C, то взаємодія A з C через B безпечна, і навпаки* (рис. 1).

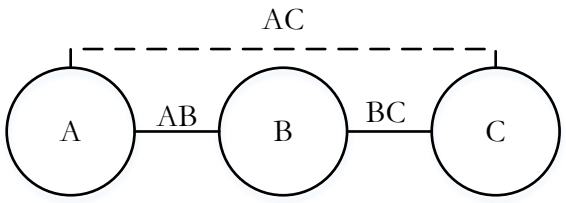

Рис. 1. Пояснення до теореми безпеки для взаємодіючих систем

Доведення. Припустимо, що взаємодія A з C через B не є безпечною. Для реалізації такого випадку повинна бути порушена безпека хоча б однієї підсистеми або порушена безпека взаємодії, що суперечить умові теореми. Зворотній напрям доводиться аналогічними міркуваннями. Теорема доведена.

Наслідком теореми є теоретичне обґрунтування безпеки системи в цілому з причини безпечності всіх складових. Припущення щодо порушення безпеки призводить до порушення безпеки хоча б однієї підсистеми або порушення безпеки взаємодії, що є недопустимим з умови та наслідку теореми.

В умовах інтеграції з європейським та світовим демократичним співтовариством виникло завдання взаємодії з автоматизованими системами інших держав або міжнародних організацій. Прикладом такого є підключення ІТС автоматизації прикордонного контролю (АПК) прикордонного відомства "Гарт-1" до єдиної міжнародної системи розшуку злочинців – баз даних Інтерполу [4, 5]. Таким чином, модернізація ІТС АПК є фактично модернізацією ІІТС в цілому як АС класу "3" відповідно до класифікації автоматизованих систем НД ТЗІ 2.5-005-99, а це в свою чергу вимагає проведення комплексу робіт із забезпечення захисту інформації.

Використання теореми безпеки для взаємодіючих систем у процесі модернізації дозволить обґрунтовано обмежити обсяг робіт із забезпечення захисту ІІТС при зміні її складових.

Враховуючи викладене, у класифікації складових ІІТС прикордонного відомства пропонується врахувати як масштаб системи, так і ступінь її взаємодії з іншими системами та розширити класи АС. Для того щоб класифікація АС відповідала своєму призначенню, необхідно забезпечити повноту класифікатора. Використання ієрархічного методу класифікації, як послідовного розподілу об'єктів на підлеглі класифікаційні угрупування, дозволить забезпечити зазначену вимогу та встановити взаємозв'язок між ними.

Загальну множину АС розіб’ємо на дві підмножини: автоматизовані системи, що взаємодіють з АС інших держав або міжнародних організацій, та автоматизовані системи, що взаємодіють тільки з внутрішньодержавними АС. Це дозволить розділити системи на підконтрольні національним правоохоронним органам та непідконтрольні. Внутрішньодержавні АС поділяються на міжвідомчі та внутрішньовідомчі. Автоматизовані системи відомств (установ, організацій тощо) поділяються на автономні та такі, які взаємодіють з декількома АС всередині відомства (не автономні). Зазначені автоматизовані системи відповідно розподіляються на локалізовані та розподілені АС. Семантика такого розподілу полягає в тому, чи контролюються всі складові системи (в тому числі мережева складова) відомством (локалізованість), чи ні (розподіленість). Прикладом взаємодії локалізованих ІТС прикордонного відомства може бути ІС "Гарт-6" – фінансового забезпечення та ІТС "Гарт-7" – кадрового забезпечення, що розгортаються, як правило, в одній будівлі органу охорони державного кордону та контролюються відповідними підрозділами військової частини повністю. Локалізовані АС в свою чергу розподіляються на багатомашинні та одномашинні системи, останні – на багатокористувацькі та однокористувацькі. Наведену вище класифікацію представимо у вигляді класифікаційної структури (рис. 2).

У відповідності з класифікаційною структурою сформуємо визначення для кожного класу АС, які обробляють інформацію однієї або декількох ступенів обмеження доступу:

1-й клас – одномашинний однокористувацький комплекс в межах однієї АС;

2-й клас – одномашинний багатокористувацький комплекс в межах однієї АС;

3-й клас – локалізований багатомашинний багатокористувацький комплекс в межах однієї АС;
4-й клас – розподілений багатомашинний багатокористувацький комплекс в межах однієї АС;
5-й клас – локалізований багатомашинний багатокористувацький комплекс в межах декількох АС одного відомства;
6-й клас – розподілений багатомашинний багатокористувацький комплекс в межах декількох АС одного відомства;
7-й клас – розподілений багатомашинний багатокористувацький комплекс в межах декількох АС як відомчої належності, так і з міжвідомчими автоматизованими системами;
8-й клас – розподілений багатомашинний багатокористувацький комплекс в межах декількох АС, які взаємодіють з автоматизованими системами інших держав або міжнародних організацій.

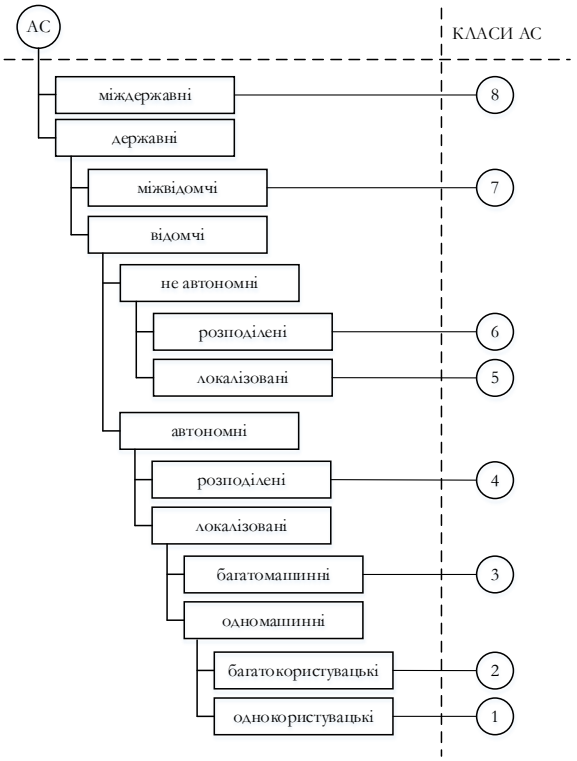

Рис. 2. Класифікаційна структура автоматизованих систем

Співвідношення класифікації автоматизованих систем відповідно до НД ТЗІ 2.5-005-99 і ISO/IEC 27001:2005 та запропонованої наведено в табл. 1.
Вимоги до системи захисту залежать від ступеня обмеження доступу до інформації, яка обробляється в автоматизованих системах.
Відповідно до положень Закону України від 13 січня 2011 року № 2939-VI «Про доступ до публічної інформації» інформація поділяється на відкриту публічну та публічну з обмеженим доступом, зокрема: конфіденційну, службову, таємну («таємно», «цілком таємно», «особливої важливості») інформації.
Таким чином, будь-яку складову ІІТС можна класифікувати відповідно до класів та типу інформації, яка обробляється (табл. 2).

У випадку обробки інформації різних ступенів обмеження доступу їх перелік пропонується відокремлювати нижнім підкреслюванням або вказувати найвищий гриф обмеження доступу.

Таблиця 1
Співвідношення запропонованої класифікації та класифікації АС відповідно до НД ТЗІ 2.5-005-99 та ISO/IEC 27001:2005

Запропонована класифікація	Класифікація АС відповідно до НД ТЗІ 2.5-005-99			ISO/IEC 27001:2005
	клас «1»	клас «2»	клас «3»	клас «4»
1-й клас	+	-	-	-
2-й клас	-	-	-	-
3-й клас	-	+	-	-
4-й клас	-	-	+	-
5-й клас	-	+	-	-
6-й клас	-	-	+	-
7-й клас	-	-	+	+
8-й клас	-	-	+	+

Таблиця 2
Класифікатор складових ІІТС за класом ІТС (ІС, ПС) та видом інформації, яка обробляється

Клас	Відкрита публічна інформація	Публічна інформація з обмеженим доступом				
		Конфіденційна	Службова	Таємна інформація		
				Таємно	Цілком таємно	Особливої важливості
1-й клас	1.В	1.К	1.С	1.Т	1.ЦТ	1.ОВ
2-й клас	2.В	2.К	2.С	2.Т	2.ЦТ	2.ОВ
3-й клас	3.В	3.К	3.С	3.Т	3.ЦТ	3.ОВ
4-й клас	4.В	4.К	4.С	4.Т	4.ЦТ	4.ОВ
5-й клас	5.В	5.К	5.С	5.Т	5.ЦТ	5.ОВ
6-й клас	6.В	6.К	6.С	6.Т	6.ЦТ	6.ОВ
7-й клас	7.В	7.К	7.С	7.Т	7.ЦТ	7.ОВ
8-й клас	8.В	8.К	8.С	8.Т	8.ЦТ	8.ОВ

Проведемо класифікацію інтегрованої міжвідомчої інформаційно-телекомунікаційної системи щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон – "Аркан". Відповідно до функцій [6] суб'єкти системи "Аркан" здійснюють поповнення інформаційних ресурсів та надають інформацію з інформаційних ресурсів інформаційних систем органів виконавчої влади, тобто здійснюють міжвідомчу взаємодію. Це визначає клас даної ІТС як 7-й, а саме розподілений багатомашинний багатокористувацький комплекс, який обробляє

інформацію різних ступенів обмеження доступу в межах декількох ІТС (ІС, ПС) як відомчої належності, так і з міжвідомчими автоматизованими системами.

Аналіз переліку інформаційних ресурсів (баз даних) та функціональних завдань системи "Аркан" показав вид інформації, що обробляється, а саме: відкрита, конфіденційна та службова інформації. Таким чином, ІТС "Аркан" має класифікацію 7.В_К_С.

3. Висновок

Наведена класифікація автоматизованих систем дозволить в подальшому сформувати відповідні профілі захищеності складових інформації, яка циркулює в автоматизованій системі, а саме: конфіденційності, цілісності та доступності.

Сформульована та доказана теорема безпеки для взаємодіючих систем (транзитивність безпеки) дозволить науково обґрунтовано раціоналізувати обсяг робіт із забезпечення нормативного рівня захисту систем вищого рівня при модернізації їх складових.

Література: 1. *Про Стратегію національної безпеки України* / Указ Президента України від 26 травня 2015 року № 287/2015. **2.** *Про прийняття на озброєння військ програмних компонентів глобальної автоматизованої інформаційної системи прикордонних військ України (шифр „Гарт")* / Наказ Державного комітету у справах охорони державного кордону України від 20 серпня 2002 р. № 474. **3.** *Державні інформаційні ресурси. Методологія побудови класифікатора загроз* : Монографія / Юдін О.К., Бучик С.С. К.: НАУ, 2015. 214 с. **4.** *Прикордонники презентували Прем'єр-міністру України Стратегію розвитку відомства* [Електрон. ресурс] Режим доступу: http://dpsu.gov.ua/ua/ about/news/news_8319.htm. **5.** *Представники іноземної делегації ознайомилися з інноваціями прикордонного контролю* [Електрон. ресурс] Режим доступу: http://www.kmu.gov.ua/control/publish/article?art_id=248441509. **6.** *Про затвердження Положення про інтегровану міжвідомчу інформаційно-телекомунікаційну систему щодо контролю осіб, транспортних засобів та вантажів, які перетинають державний кордон* / Наказ від 03.04.2008 N 284/287/214/150/64/175/266/75. Адміністрація Державної прикордонної служби України, Державна митна служба України, Державна податкова адміністрація України, Міністерство внутрішніх справ України, Міністерство закордонних справ України, Міністерство праці та соціальної політики України, Служба безпеки України, Служба зовнішньої розвідки України. Зареєстровано в Міністерстві юстиції України 12 травня 2008 р. за N 396/15087.

Transliterated bibliography:

1. *Pro Stratehiiu natsionalnoi bezpeky Ukrainy* / Ukaz Prezydenta Ukrainy vid 26 travnia 2015 roku № 287/2015.

2. *Pro pryiniattia na ozbroiennia viisk prohramnykh komponentiv hlobalnoi avtomatyzovanoi informatsiinoi systemy prykordonnykh viisk Ukrainy (shyfr „Hart")* / Nakaz Derzhavnoho komitetu u spravakh okhorony derzhavnoho kordonu Ukrainy vid 20 serpnia 2002 r. № 474.

3. *Derzhavni informatsiini resursy. Metodolohiia pobudovy klasyfikatora zahroz* : monohrafiia / Yudin O.K., Buchyk S.S. K.: NAU, 2015. 214 s.

4. *Prykordonnyky prezentuvaly Premier-ministru Ukrainy Stratehiiu rozvytku vidomstva* [Elektron. resurs] Rezhym dostupu: http://dpsu.gov.ua/ua/about/news/news_8319.htm.

5. *Predstavnyky inozemnoi delehatsii oznaiomylysia z innovatsiiamy prykordonnoho kontroliu* [Elektron. resurs] Rezhym dostupu: http://www.kmu.gov.ua/control/publish/article?art_id=248441509.

6. *Pro zatverdzhennia Polozhennia pro intehrovanu mizhvidomchu informatsiino-telekomunikatsiinu systemu shchodo kontroliu osib, transportnykh zasobiv ta vantazhiv, yaki peretynaiut derzhavnyi kordon* / Nakaz vid 03.04.2008 N 284/287/214/150/64/175/266/75 Administratsiia Derzhavnoi prykordonnoi sluzhby Ukrainy, Derzhavna mytna sluzhba Ukrainy, Derzhavna podatkova administratsiia Ukrainy, Ministerstvo vnutrishnikh sprav Ukrainy, Ministerstvo zakordonnykh sprav Ukrainy, Ministerstvo pratsi ta sotsialnoi polityky Ukrainy, Sluzhba bezpeky Ukrainy, Sluzhba zovnishnoi rozvidky Ukrainy. Zareiestrovano v Ministerstvi yustytsii Ukrainy 12 travnia 2008 r. za N 396/15087

Надійшла до редколегії 12.03.2017

Рецензент: д-р техн. наук, проф. Бараннік В.В.

Юдін Олександр Костянтинович, д-р техн. наук, професор, Директор інституту комп'ютерних інформаційних технологій, завідувач кафедри комп'ютеризованих систем захисту інформації Національного авіаційного університету, 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. Адреса: Україна, 03680, Київ, пр. Космонавта Комарова 1, корп. 6. E-mail: kszi@ukr.net

Стрельбіцький Михайло Аналолійович, канд. техн. наук, доцент, докторант Національної академії Державної прикордонної служби України ім. Б. Хмельницького. Адреса: Україна, 29003 м. Хмельницький, вул. Шевченка, 46. E-mail: m.strelb@ukr.net

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. Address: Ukraine, 03680, Kiev, pr. Kosmonavta Komarova 1, korp. 6. E-mail: kszi@ukr.net

Strelbtskiy Mykhailo Anatoliyovych, PhD in Eng., doctoral of National Academy of State Border Service of Ukraine named after B. Khmelnytskyi. Address: Ukraine, 29003, Hmel'nic'kij, Shevchenka Str, 46. E-mail: kszi@ukr.net