УДК 004.056.5

[1]**Юдін О.К.,** д.т.н., проф.;
[2]**Бучик С.С.,** к.т.н, доц.

АНАЛІЗ ЗАГРОЗ ДЕРЖАВНИМ ІНФОРМАЦІЙНИМ РЕСУРСАМ

[1] Інститут комп'ютерних інформаційних технологій Національного авіаційного університету
[2]Житомирський військовий інститут імені С.П. Корольова Державного університету телекомунікацій

На основі аналізу основних нормативно-правових актів, інших джерел в статті визначено перелік можливих загроз державним інформаційним ресурсам та запропонована їх класифікація , що зумовлена впливом на властивості інформації відповідно до спрямування (конфіденційність, цілісність та доступність). Розроблена загальна система захисту держаних інформаційних ресурсів, запропоновано визначення загрози державним інформаційним ресурсам, зазначено про необхідність здійснення уточнення щодо визначення класів автоматизованих систем та подальшого уточнення стандартних функціональних профілів захищеності

Актуальність дослідження

До захищених інформаційних систем належать інформаційні системи, які у певних умовах експлуатації забезпечують безпеку (конфіденційність, цілісність, доступність) інформації, що функціонує в системі, та підтримує свою працездатність в умовах впливу на неї заданої множини загроз.

Загроза (дія) – це можлива небезпека (потенційна або така, що існує реально) вчинення будь-якого діяння (дії або бездіяльності), спрямованого проти об'єкта захисту (інформаційних ресурсів), яке завдає збитку власнику або користувачу, що проявляється як небезпека спотворення або втрати інформації [1].

В [2] приводиться наступне визначення загрози. Загроза *(threat)* – будь-які обставини чи події, що можуть спричинити порушення політики безпеки інформації та (або) нанесення збитку інформаційно-комунікаційній системі (ІКС).

Таким чином, загроза в загальному вигляді буде представляти собою будь-який потенційно можливий несприятливий вплив (дію або бездіяльність), який (яка) завдає збиток.

В [3] наведено визначення інформаційного ресурсу, а саме: інформаційний ресурс – це власне інформація і (або) будь-який об'єкт, що є елементом певної інформаційної технології (технічні засоби обчислювальної або телекомунікаційної техніки, програми, дані і т. ін.).

В Законі України "Про Державну службу спеціального зв'язку та захисту інформації України" від 23 лютого 2006 р. №3475-IV [4], визначено термін державні інформаційні ресурси, які представляють собою інформацію, яка є власністю держави та необхідність захисту якої визначено законодавством.

Під загрозою безпеки інформаційним ресурсам розуміють дії, які можуть призвести до спотворення, несанкціонованого використання або, навіть, до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів [5,6].

Підсумовуючи все вищевикладене можна дати визначення загрози державним інформаційним ресурсам.

Під загрозою державним інформаційним ресурсам (ЗДІР) можна розуміти 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.

Таким чином, визначення ЗДІР є актуальним питанням для побудови їх ком-

плексної системи захисту інформації (КСЗІ).

Аналіз останніх досліджень та публікацій

Питання щодо проблеми розгляду загроз, їх класифікації, розглядались у роботах Юдіна О.К., Корченка А.Г., Марущака А.І., Почепцова Г.Г., Хахановського В.Г., Швеця М.Я., Бойченка О.В., Богуша В.М., Арістової І.В., Бабака В.П., Чунарьової А.В., Чунарьова А.В. та ін. Але необхідність уточнення загроз відповідно до терміну ДІР та ЗДІР (дане поняття введено вперше) потребує досліджень для побудови в подальшому дієвої системи захисту ДІР.

Мета

Таким чином, мета статті полягає у визначенні основних ЗДІР, виходячи з аналізу основних нормативно-правових актів (НПА), інших джерел, які мають відношення або можуть бути використані для побудови ефективної КСЗІ ДІР.

Виклад основного матеріалу

В цілому, будь яка інформаційна система піддана наступним основним групам загроз [1]:

– загрози порушення конфіденційності, які спрямовані на розголошення інформації з обмеженим доступом;

– загрози порушення цілісності, які полягають у спотворенні або зміні неавторизованим користувачем інформації, що зберігається або передається;

– загрози порушення працездатності (доступності), які спрямовані на створення ситуацій, коли в результаті навмисних дій понижується працездатність автоматизованої системи, або її ресурси стають недоступними.

Розглядаючи класифікацію базових загроз інформаційним ресурсам їх можна розрізняти [6]:

– за критеріями інформаційній безпеці (загрози конфіденційності даних і програм; загрози цілісності даних, програм, апаратури; загрози доступності даних; загрози відмови від виконання операцій).

– за компонентами інформаційних систем, на які загрози націлені (інформаційні ресурси та послуги, персональні дані, програмні засоби, апаратні засоби, програмно-апаратні засоби);

– за способом здійснення (випадкові, навмисні, дії природного та техногенного характеру);

– за розташуванням джерела загроз (внутрішні та зовнішні).

Аналізуючи Доктрину інформаційної безпеки України, затверджену Указом Президента України від 8 липня 2009 року №514/2009 та ряд інших НПА [3,7,8,9] можна побудувати наступну загальну систему ЗДІР (рис.1).

Таким чином, існує достатньо розвинута нормативно-правова база (НПБ), що регламентує порядок захисту інформації в автоматизованих системах (АС), визначена велика кількість як основних, так і похідних загроз. Але словосполучення ДІР в НПА щодо захисту інформаційних ресурсів зустрічається дуже рідко. В зв'язку з чим постає питання: чи можливо класифікацію загроз в АС 1-3 класу застосувати до ДІР? Розглянемо це питання детальніше, починаючи із визначення АС.

АС – система, що здійснює автоматизоване оброблення даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення [7].

Відповідно НД ТЗІ 1.1-003-99 "Термінологія в галузі захисту інформації в комп'ютерних системах від НСД" визначає АС так: АС - організаційно-технічна система, що реалізує інформаційну технологію і об'єднує обчислювальну систему, фізичне середовище, персонал і оброблювальну інформацію. Відповідно до цього ж НД ТЗІ обчислювальна система (ОС) – сукупність програмно-апаратних засобів, призначених для обробки інформації, а комп'ютерна система (КС) – сукупність програмно-апаратних засобів, яка подана для оцінки.

Звідси АС – ширше поняття, що охоплює ОС і КС. Таким чином, системи електрозв'язку, інформаційно-телекомунікаційні, телекомунікаційні, комп'ютерні, інформаційні системи можна трактувати, як автоматизовані [1]. Інформаційні ресурси, які обробляються в цих системах, і є власністю держави, будуть вважатися державними інформаційними ресурсами.

Відповідно НД ТЗІ 2.5-005-99 "Класифікація автоматизованих систем і стандартні профілі захищеності оброблювальної інформації від несанкціонованого доступу" зі зміною №1, затвердженою наказом Адміністрації Держспецзв'язку від 15.10.2008 №172, за сукупністю характеристик АС (конфігурація апаратних засобів ОС і їх фізичне розміщення, кількість різноманітних категорій оброблюваної інформації, кількість користувачів і категорій користувачів) виділено три ієрархічні класи АС.

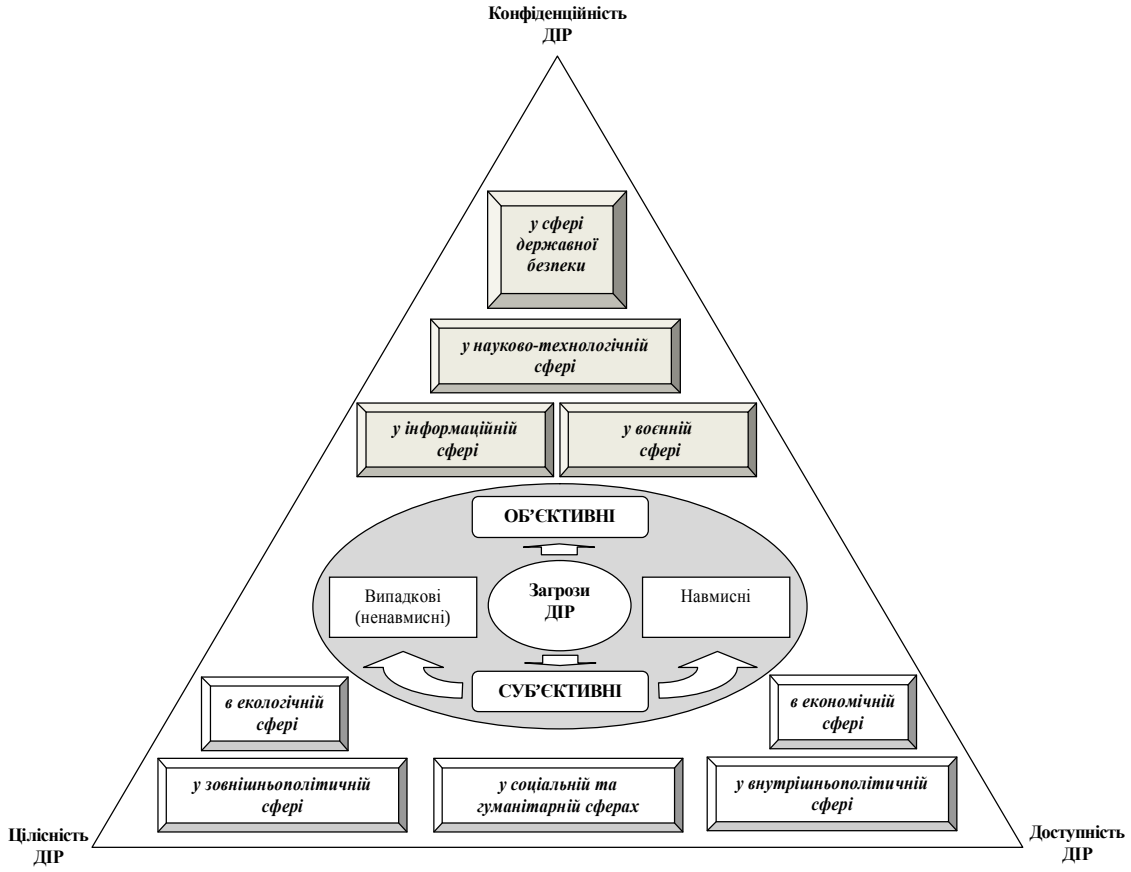

Рис.1. Загальна система ЗДІР

Клас «1» – одномашинний однокористувачевий комплекс, який обробляє інформацію однієї або кількох ступенів обмеження доступу.

Приклад – автономна персональна ЕОМ, доступ до якої контролюється з використанням організаційних заходів.

Клас «2» – локалізований багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних ступенів обмеження доступу.

Приклад – ЛОМ.

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

Приклад – глобальна мережа.

Розглядаючи міжнародний стандарт ISO/IEC 27001:2005 "*Information Security*

Management – Specification With Guidance for Use" можна говорити про необхідність введення ще одного класу АС – класу «4», який би враховував вирішення питань забезпечення захисту інформації в договорах з третіми особами.

Таким чином, ми можемо говорити про те, що ДІР міститимуться в даних класах АС і модель загроз, відповідно до [7], адекватна і може бути використана в цілому для побудови моделі загроз ДІР.

Загрози ДІР залежатимуть від характеристик операційної системи, фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу (рис.1). Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні (рис.1; табл.1).

Об'єктивні загрози об'єднують обставини, що складають непереборну силу, тобто такі обставини, які носять об'єктивний і абсолютний характер, що розповсюджується на всіх. До непереборної сили в законодавстві та договірній практиці відносять стихійні лиха або інші обставини, які неможливо передбачити або їм запобігти або можливо передбачити, але не можливо запобігти їм при сучасному рівні знань і можливостей людини. Такі джерела абсолютно не піддаються прогнозуванню, і тому заходи захисту від них повинні застосовуватися завжди (табл. 2).

В зв'язку з цим можна виділити наступні загальні загрози ДІР:

– зміна умов фізичного середовища (стихійні лиха і аварії, як землетрус, повінь, пожежа або інші випадкові події);

– збої і відмови у роботі обладнання та технічних засобів ІКСМ;

– наслідки помилок під час проектування та розробки компонентів ІКСМ (технічних засобів, технології обробки інформації, програмних засобів, засобів захисту, структур даних тощо);

– помилки персоналу (користувачів) ІКСМ під час експлуатації;

– навмисні дії (спроби) потенційних порушників.

В табл. 1 і 2 визначено перелік можливих загроз ДІР та їх класифікація відповідно до впливу на які властивості інформації вони спрямовані (к – конфіденційності, ц – цілісності та д – доступності).

Таблиця 1. Класифікація загроз ДІР суб'єктивної природи

№ з/п	Загрози суб'єктивної природи	За відношенням до суб'єкта загрози		Що порушує		
		навмисні	ненавмисні	к	ц	д
1	Поширення у інформаційному просторі викривленої, недостовірної та упередженої інформації	+			+	
2	Комп'ютерна злочинність, комп'ютерний тероризм	+		+	+	+
3	Негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет	+			+	
4	Несанкціонований доступ (користування) до ДІР	+		+	+	+
5	Розголошення інформації, яка становить державну та іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави	+		+	+	+
6	Порушення встановленого регламенту збирання, обробки, зберігання і передачі інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України	+	+	+	+	+
7	Реалізація програмно-математичних заходів з метою порушення функціонування ІКСМ	+		+	+	+
8	Перехоплення інформації в телекомунікаційних мережах	+		+	+	+
9	Зниження наукового потенціалу в галузі інформатизації	+	+	+	+	+

№ з/п	Загрози суб'єктивної природи	За відношенням до суб'єкта загрози		Що порушує		
		навмисні	ненавмисні	к	ц	д
	та зв'язку					
10	Недостатній захист від несанкціонованого доступу до інформації внаслідок використання іноземних інформаційних технологій та техніки	+		+	+	+
11	Недостатня надійність інформаційно-телекомунікаційних систем збирання, обробки та передачі інформації в умовах надзвичайних ситуацій	+	+	+	+	+
12	Низький рівень інформатизації органів державної влади	+	+	+	+	+
13	Недотримання суб'єктами правових відносин норм, вимог та правил організаційного і технічного характеру щодо захисту ДІР	+		+	+	+
14	Невикористання засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку і АС в цілому, засобів захисту інформації, які відповідають встановленим вимогам щодо захисту ДІР (мають відповідний сертифікат)	+		+	+	+
15	Нездійснення перевірки відповідності засобів обчислювальної техніки, програмного забезпечення, засобів зв'язку і АС в цілому встановленим вимогам щодо захисту ДІР (сертифікація засобів обчислювальної техніки, засобів зв'язку і АС)	+		+	+	+
16	Нездійснення контролю щодо захисту ДІР	+		+	+	+
17	Навмисна діяльність осіб, яка впливає на елементи системи управління ДІР із використанням програмних і (або) технічних засобів	+		+	+	+
18	Несправність програмних і (або) технічних засобів	+			+	+
19	Не повідомлення (несвоєчасне повідомлення) спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації або підпорядкований йому регіональний орган про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави, вимога щодо захисту якої встановлена законом	+		+	+	+
20	Оброблення в системі інформації без застосування комплексної системи захисту інформації з підтвердженою відповідністю	+		+	+	+
21	Порушення фізичної цілісності ІКСМ (окремих компонентів, пристроїв, обладнання, носіїв інформації)	+				+
22	Порушення режимів функціонування (виведення з ладу) систем життєзабезпечення ІКСМ (електроживлення, заземлення, охоронної сигналізації, вентиляції та ін.)	+			+	+
23	Порушення режимів функціонування ІКСМ (обладнання і ПЗ)	+			+	+
24	Впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховуючих пристроїв, інших засобів розвідки	+		+	+	+
25	Використання засобів перехоплення побічних електромагнітних випромінювань і наводів, акусто-електричних перетворень інформаційних сигналів	+		+		
26	Використання (шантаж, підкуп тощо) з корисливою метою персоналу, якій має доступ до ДІР	+		+	+	+
27	Крадіжки носіїв інформації, виробничих відходів (роздруків, записів, тощо)	+		+	+	+
28	Несанкціоноване копіювання носіїв інформації	+		+	+	+
29	Читання залишкової інформації з оперативної пам'яті	+		+	+	+

№ з/п	Загрози суб'єктивної природи	За відношенням до суб'єкта загрози		Що порушує		
		навмисні	ненавмисні	к	ц	д
	ЕОМ, зовнішніх накопичувачів					
30	Одержання атрибутів доступу з наступним їх використанням для маскування під зареєстрованого користувача	+		+	+	+
31	Неправомірне підключення до каналів зв'язку, перехоплення даних, що передаються, аналіз трафіку тощо	+		+	+	+
32	Впровадження і використання забороненого політикою безпеки ПЗ або несанкціоноване використання ПЗ, за допомогою якого можна одержати доступ до критичної інформації (наприклад, аналізаторів безпеки мереж)	+				+
33	Ненавмисна діяльність осіб, яка, впливає на систему управління ДІР із використанням програмних і (або) технічних засобів		+		+	+
34	Дії, що призводять до відмови системи управління ДІР (окремих компонентів), руйнування апаратних, програмних, інформаційних ресурсів (обладнання, каналів зв'язку, видалення даних, програм та ін.)		+			+
35	Ненавмисне пошкодження носіїв інформації		+			+
36	Неправомірна зміна режимів роботи АС (окремих компонентів, обладнання, ПЗ тощо), ініціювання технологічних процесів або процесів, які здійснюють тестування, результатом яких є незворотні зміни у системі (наприклад, форматування носіїв інформації)		+			+
37	Неумисне зараження ПЗ комп'ютерними вірусами		+	+	+	+
38	Невиконання вимог до організаційних заходів захисту чинних в ІКСМ розпорядчих документів		+			+
39	Помилки під час введення (виведення) даних в систему		+	+	+	+
40	Будь-які дії, що можуть призвести до розголошення конфіденційних відомостей, атрибутів розмежування доступу, втрати атрибутів тощо		+	+	+	+
41	Неправомірне впровадження і використання забороненого політикою безпеки ПЗ		+	+	+	+
42	Наслідки некомпетентного застосування засобів захисту		+	+	+	+

Таблиця 2. Класифікація загроз ДІР об'єктивної природи

№ з/п	Загрози об'єктивної природи	Що порушує			
		к	ц	д	с
1	Стихійні явища (пожежі, аварії, землетруси, повені, урагани, магнітні бурі, радіоактивне випромінювання, різноманітні непередбачені обставини, непояснені явища)		+	+	
2	Збої та відмови системи електроживлення		+	+	
3	Збої та відмови обчислювальної техніки		+	+	
4	Збої, відмови та пошкодження носіїв інформації		+	+	
5	Збої та відмови програмного забезпечення		+	+	

Основні результати

Таким чином, визначена загальна система захисту ДІР, яка може бути покладена в основу подальших досліджень щодо побудови ефективної КСЗ ДІР, показана адекватність моделі загроз в АС і її можливе використання для побудови відповідної моделі загроз ДІР, розкриті основні загальні загрози ДІР, навмисні та ненавмисні загрози, виходячи з аналізу основних НПА та інших джерел. Вводиться визначення загроз державним інформаційним ресурсам. Вказується на необхідність внесення змін до НПА щодо визначення класів АС (введення класу «4», який би враховував вирішення питань забезпечення захисту ДІР в договорах з третіми особами) у відповідності з

міжнародним стандартом *ISO/IEC* 27001:2005.

Висновки

В зв'язку із наведеним слід зробити наступні висновки:

– в результаті розробленої загальної системи захисту ДІР можливо вказати основні напрямки щодо подальшого розкриття загроз ДІР в основних сферах, які знаходяться на рис.1 у верхній частині, а саме: у сфері державної безпеки, у науково-технологічній сфері, у інформаційній та воєнній сферах;

– визначено перелік можливих загроз державним інформаційним ресурсам та запропонована їх класифікація відповідно до впливу на які властивості інформації вони спрямовані (конфіденційності, цілісності та доступності), що в цілому може бути покладено в модель загроз ДІР, але з необхідністю подальшого уточнення загроз у наведених вище сферах, що дає можливість побудови складної ієрархічної моделі загроз ДІР;

– виникає необхідність введення визначення загрози державним інформаційним ресурсам та подальше його впровадження до НПА;

– необхідність введення класу «4» АС, який би враховував вирішення питань забезпечення захисту ДІР у договорах із третіми особами, у відповідності з міжнародним стандартом *ISO/IEC* 27001:2005 та подальшого уточнення стандартних функціональних профілів захищеності.

Список літератури

1. Інформаційна безпека. Нормативно-правове забезпечення: підруч. / О.К. Юдін. – К.: НАУ, 2011. – 640 с.

2. http://wiki.tntu.edu.ua/

3. Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту: НД ТЗІ 2.5-001-99. – [Чинний від 1999.05.28]. – К.: ДСТСЗІ СБУ, 1999. - №26. – (Нормативний документ системи технічного захисту інформації).

4. 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.

5. Юдін О.К. Захист інформації в мережах передачі даних: підруч. / Г.Ф. Конахович, О.Г. Корченко, О.К. Юдін. – К.: Вид-во ТОВ НВП "ІНТЕРСЕРВІС", 2009. – 714 с.

6. Чунарьова А.В., Чунарьов А.В. Принципи організації захисту інформації в сучасних інформаційно-комунікаційних системах і мережах. – Режим доступу: http://www.rusnauka.com/16_ADEN_2010/Informatica/68642.doc.htm

7. Про захист інформації в автоматизованих системах: Закон України від 05.07.1994 №81/94-ВР//ВВР. – 1994. – №31. – С. 287.

8. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 №81/94-ВР//ВВР. – 1994. – № 31. – С. 287.

9. Типове положення про службу захисту інформації в автоматизованій системі: 1.4-001-2000. – [Чинний від 2000.12.04]. – К.: ДСТСЗІ СБУ, 2000. – №53. – (Нормативний документ системи технічного захисту інформації).

Статтю подано до редакції 14.10.2013