УДК 004.056.5

КОНЦЕПТУАЛЬНИЙ АНАЛІЗ УРАЗЛИВОСТІ 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 Національного авіаційного університету

Проведено концептуальний аналіз уразливості державних інформаційних ресурсів, який дозволяє зробити висновок про надто широкий спектр, багатошаровість та масштабність тих обставин, унаслідок яких порушуватиметься цілісність, доступність та конфіденційність інформації. У зв'язку з цим, ефективна комплексна система захисту державних інформаційних ресурсів повинна неодмінно враховувати увесь перелік обставин, через які потенційні небезпеки та загрози інформації можуть бути дієвими щодо можливості вільного доступу до інформації органів державного управління.

Ключові слова: державні інформаційні ресурси, комплексна система захисту інформації, загроза, класифікація загроз, інформаційно-телекомунікаційна система.

The conceptual analysis of vulnerability of state informative resources, which allows to make a conclusion about a wide spectrum, multi-layredness and scale of those circumstances, which can broke integrity, availability and confidentiality of information. In connection with what, the effective complex system of defence of state informative resources must necessarily take into account all list of circumstances at which potential dangers and threats of information can be effective in relation to possibility of access to information of organs of state administration.

Keywords: state informative resources, the complex system for protection of information, threat, classification of threats, information-telecommunication system.

Актуальність дослідження

У законі України «Про засади внутрішньої і зовнішньої політики» ст. 6 визначено, що «Основними засадами внутрішньої політики у сфері національної безпеки і оборони є: ... своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз національним інтересам у ….. інформаційній сфері».

В Указі Президента України «Про нову редакцію Стратегії національної безпеки України» зазначено, що «на тлі посилення загроз і зростання нестабільності у світі постають нові виклики міжнародній безпеці», у інформаційній сфері зокрема. В цьому ж Указі визначені ключові завдання політики національної безпеки у внутрішній сфері щодо забезпечення інформаційної безпеки, а саме: стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного національного інформаційного продукту, *зокрема, сучасних засобів і систем захисту інформаційних ресурсів*; забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури; *розробка та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними стандартами держав — членів ЄС, у тому числі згідно з вимогами Конвенції про кіберзлочинність*; створення національної системи кібербезпеки.

У Законі України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 р. № 3475-IV, який прийнято для подальшого вдосконалення системи забезпечення інформаційних ресурсів держави, проведення єдиної державної політики в Україні у сфері забезпечення інформаційної безпеки держави, визначено термін *державні інформаційні ресурси*, які являють інформацію, що є власністю держави та необхідність захисту якої визначено законодавством.

Таким чином, виникає необхідність постійного уточнення як внутрішніх, так і зовнішніх загроз державним інформаційним ресурсам, що у свою чергу, впливатиме на організацію комплексної системи захисту державних інфор-

маційних ресурсів, забезпечуватиме актуальність проведення досліджень у вказаному напрямку.

Аналіз останніх досліджень та публікацій

Питання щодо проблеми забезпечення захисту державних інформаційних ресурсів, розгляду загроз, їх класифікації в комплексі заходів національної безпеки держави розглядались у роботах Г. Г. Почепцова, В. Г. Хахановського, М. Я. Швеця, О. В. Бойченка, В. М. Богуша, І. В. Арістової, А. І. Марущака, В. П. Бабака, О. К. Юдіна та ін. Але необхідність подальших досліджень обґрунтовується наявністю прогалин у законодавстві, організаційних та програмно-технічних вад у комплексі заходів, спрямованих на побудову дієвої системи захисту державних інформаційних ресурсів, що у свою чергу повинно ґрунтуватися на аналізі та знанні загроз їм.

Мета статті — концептуальний аналіз уразливості державних інформаційних ресурсів для подальшої побудови їх ефективної комплексної системи захисту та визначення основних загроз.

Виклад основного матеріалу

За тлумачним словником, слово «ресурси» походить від французького *ressourse* — допоміжні засоби (грошові кошти, цінності, запаси, можливості, джерела прибутків тощо) [1]. Наявність корисних ресурсів у будь-якій сфері діяльності — це гарантія і застава її стабільності та процвітання. В сучасному понятті в складі ресурсів можна виділити матеріальні, енергетичні, трудові, фінансові, технологічні та інформаційні ресурси. Якщо розглядати поняття інформаційних ресурсів, то їх можна визначити як «сукупність документів в інформаційних системах (бібліотеках, архівах, банках даних тощо)».

У Концепції формування системи національних електронних інформаційних ресурсів (затверджено розпорядженням Кабінету Міністрів України від 5 травня 2003 р. № 259-р.) визначено, що національні електронні інформаційні ресурси — це «ресурси незалежно від їх змісту, форми, години та місця створення, форми власності, призначені для задоволення потреб громадянина, суспільства, держави. Національні ресурси включають державні, комунальні та приватні ресурси». При цьому визначено, що «державні ресурси — ресурси, які є об'єктом права державної власності».

У праці [2] наводиться поняття національних інформаційних ресурсів та системи національних інформаційних ресурсів, що, у свою чергу, пов'язано з формуванням системи національних ресурсів як одним із основних напрямків Національної програми інформатизації.

Інформаційна безпека національних ресурсів, складовим елементом якої є державні інформаційні ресурси, забезпечується їх власниками (для державних інформаційних ресурсів власником є державні органи управління) шляхом створення комплексної системи захисту інформації щодо несанкціонованого доступу та дотримання належного рівня їх захисту.

В Україні приділяється достатньо уваги захисту ДІР. З метою забезпечення єдиного підходу щодо захисту державних інформаційних ресурсів на виконання постанови Кабінету Міністрів України від 24.02.2003 № 208 «Про заходи щодо створення електронної інформаційної системи "Електронний Уряд"» у рамках Національної системи конфіденційного зв'язку в м. Києві, створюється окрема підсистема для телекомунікаційного забезпечення функціонування Єдиного веб-порталу органів виконавчої влади. На сьогодні підключення органів державної влади до мережі Інтернет здійснюється через захищений вузол Інтернет-доступу Держспецзв'язку. Подальше підключення органів державної влади до мережі Інтернет має здійснюватись виключно через захищений вузол Інтернет-доступу НСКЗ.

На виконання завдань Національної програми інформатизації у межах виконання проекту «Забезпечити антивірусний захист державних інформаційних ресурсів» створено Центр антивірусного захисту інформації (ЦАЗІ). Одним із основних завдань ЦАЗІ є впровадження єдиної технологічної політики щодо антивірусного захисту інформації в ІТС органів державної влади, а також централізованого забезпечення їх антивірусними програмними продуктами, сертифікованими у встановленому законодавством України порядку [3].

Реалізація державної політики щодо захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах полягає у [3; 4]:

- розробленні пропозицій до визначення загальної стратегії та пріоритетних напрямів діяльності у сфері захисту державних інформаційних ресурсів в ІТС;
- виконанні обов'язків уповноваженого органу у сфері захисту інформації в інформаційно-телекомунікаційних системах;
- розробленні порядку та вимог до захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах, а також погодження проектів нормативно-правових актів з цих питань;

- розробленні критеріїв та порядку оцінювання стану захищеності державних інформаційних ресурсів в інформаційно-телекомунікаційних системах тощо.

На основі цього запропоновано зміст реалізації державної політики з питань захисту державних інформаційних ресурсів в ІТС [3]:

- захист державних інформаційних ресурсів (ДІР);
- створення єдиної системи антивірусного захисту інформації;
- взаємодія з органами державної влади;
- взаємодія з адміністрацією домену .ua;
- міжнародне співробітництво в галузі інформаційних ресурсів;
- визначення рівня захищеності ІТС органів державної влади.

Таким чином, розкриваючи зміст визначення рівня захищеності ІТС органів державної влади, що становить розробку критеріїв та порядку оцінювання стану захищеності ДІР в ІТС та організацію та здійснення оцінювання стану захищеності ДІР в ІТС, виникає актуальне питання в рамках реалізації державної політики з питань захисту ДІР щодо подальшої розробки методологічних основ інформаційно-аналітичної підтримки процесів прийняття рішень щодо оцінювання захищеності державних інформаційних ресурсів. У цілому зміст захисту ДІР, наведено в праці [3], показано на рис. 1.

Звідси виникає необхідність визначення основних загроз безпеці інформації ДІР.

Узагальнений механізм атаки [5] можливо застосувати стосовно ДІР із певними доповненнями та особливостями (рис. 2).

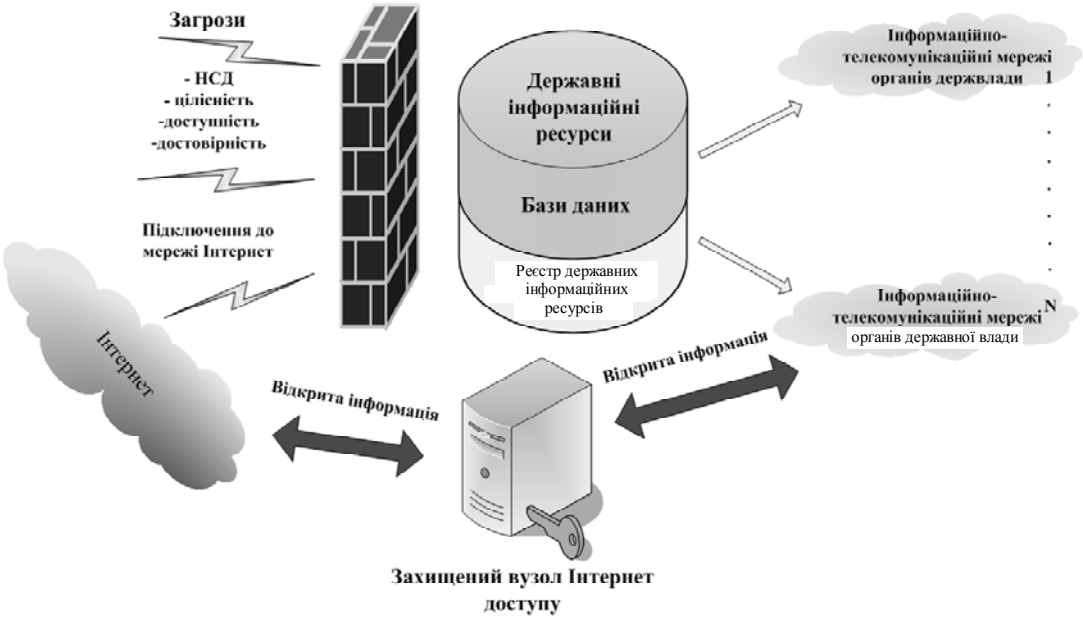

Рис. 1. Захист державних інформаційних ресурсів

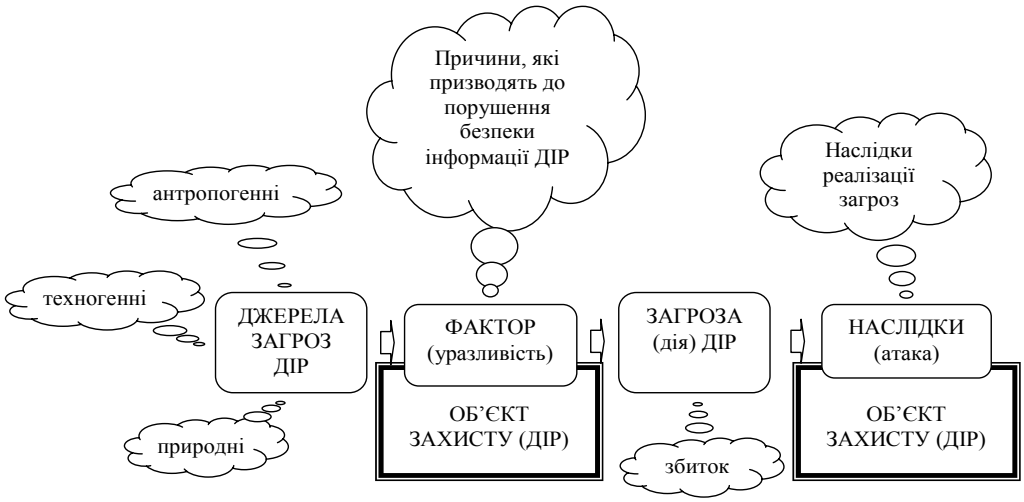

Рис. 2. Механізм атаки державних інформаційних ресурсів

Таким чином, загрози ДІР можливо порівняти із загрозами інформаційним ресурсам, які розглядаються як потенційно можливі випадки антропогенного, техногенного або природного (стихійного) характеру, що можуть спричинити небажаний вплив на ІТС, а також на інформацію, яка зберігається в ній. Виникнення загрози, тобто віднаходження джерела актуалізації певних подій у загрози характеризується таким елементом, як уразливість. Саме за наявності вразливості, як певної характеристики системи, відбувається активізація загроз. Безперечно, що загрози за своєю сутністю відповідно до теорії множин є не вичерпними, а отже, не можуть бути піддані повному описові [6]. У праці [4] вказано, що спеціально уповноважений центральний орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації «здійснює заходи щодо виявлення загрози державним інформаційним ресурсам від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дає рекомендації з питань запобігання такій загрозі».

Розглядаючи та поєднуючи різні підходи, можна виділити такі основні види загроз ДІР [2; 5; 6; 7; 8]:

загрози доступності (розкриття інформаційних ресурсів, несанкціонований доступ до ДІР);

загрози цілісності (умисний антропогенний вплив);

загрози конфіденційності (викрадення, утрата інформації та засобів її обробки);

загроза збою в роботі самого обладнання;

загрози ненавмисних помилок користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи.

При чому загрози доступності, цілісності, конфіденційності є базовими, решта більш поширеними.

За джерелами походження:

антропогенного походження — вчинення людиною різноманітних дій з руйнування інформаційних систем, ресурсів, програмного забезпечення тощо. Джерелами загроз виступають суб'єкти, дії яких можуть бути кваліфіковані як навмисні або випадкові злочини. Ця група джерел загроз найбільш чисельна та становить найбільший інтерес з точки зору організації захисту;

техногенного походження — визначається технократичною діяльністю людини, прикладами яких можуть бути транспортні аварії (катастрофи), пожежі, неспровоковані вибухи чи їх загроза, раптове руйнування каналів зв'язку, аварії на інженерних мережах і спорудах життєзабезпечення, аварії головних серверів системи управління тощо;

природного походження — об'єднує обставини, що складають непереборну силу, тобто такі обставини, які носять об'єктивний і абсолютний характер, що поширюється на всіх, прикладами яких є небезпечні геологічні, метеорологічні, гідрологічні явища, деградацію ґрунтів чи надр, природні пожежі, масове руйнування (через природні катаклізми) каналів зв'язку, зміна стану водних ресурсів та біосфери тощо.

За ступенем гіпотетичної шкоди:

загроза — явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію національних інтересів у інформаційній сфері і створюють небезпеку для системи управління ДІР, життєзабезпечення їх системостворюючих елементів;

небезпека — безпосередня дестабілізація функціонування системи управління ДІР.

За повторюваністю вчинення:

повторювані — такі загрози, які мали місце раніше;

продовжувані — неодноразове здійснення загроз, що складається з ряду тотожних загроз, які мають спільну мету.

За сферами походження:

екзогенні — джерело дестабілізації системи лежить поза її межами;

ендогенні — алгоритм дестабілізації системи перебуває у самій системі.

За ймовірністю реалізації:

вірогідні — такі загрози, які за виконання певного комплексу умов обов'язково настануть;

неможливі — такі загрози, які за виконання певного комплексу умов ніколи не настануть;

випадкові — такі загрози, які за виконання певного комплексу умов кожного разу протікають по-різному.

За рівнем детермінізму:

закономірні — такі загрози, які носять стійкий, повторюваний характер, що зумовлені об'єктивними умовами існування та розвитку системи інформаційної безпеки;

випадкові — такі загрози, які можуть або трапитися або не трапитися.

За значенням:

допустимі — такі загрози, які не можуть призвести до колапсу системи;

неприпустимі — такі загрози, які: 1) можуть у разі їх реалізації призвести до колапсу і системної дестабілізації системи; 2) можуть призвести до змін, не сумісних із подальшим існуванням системи ДІР.

За структурою впливу:

системні — загрози, що впливають одразу на усі складові елементи системи управління ДІР;

структурні — загрози, що впливають на окремі структури системи;

елементні — загрози, що впливають на окремі елементи структури системи.

За характером реалізації:

реальні — активізація алгоритмів дестабілізації є неминучою і не обмежена часовим інтервалом і просторовою дією;

потенційні — активізація алгоритмів де стабілізації можлива за певних умов середовища функціонування органу державного управління;

здійснені — такі загрози, які втілені у життя;

уявні — псевдоактивізація алгоритмів дестабіліза-ії, або ж активізація таких алгоритмів, що за деякими ознаками схожі з алгоритмами дестабілізації, але такими не є.

За ставленням до них:

об'єктивні — такі загрози, які підтверджуються сукупністю обставин і фактів, що об'єктивно характеризують навколишнє середовище. При цьому ставлення до них суб'єкта управління не відіграє вирішальної ролі через те, що об'єктивні загрози існують незалежно від волі та свідомості суб'єкта. Відтак об'єктивні загрози, не відображені в офіційних документах, у зв'язку з чим їх можна назвати ненормативними загрозами;

суб'єктивні — така сукупність чинників об'єктивної дійсності, яка вважається суб'єктом управління системою безпеки загрозою. За даного випадку визначальну роль у ідентифікації тих чи інших обставин і чинників відіграє воля суб'єкта управління, який і приймає безпосереднє рішення про надання статусу або ідентифікації тих чи інших подій як загрози безпеці.

За об'єктом впливу:

особа; суспільство; держава.

На основі проведеного аналізу загроз можна побудувати таку загальну систему класифікації загроз безпеці інформації ДІР (рис. 3).

Основні результати

Проведений концептуальний аналіз уразливості державних інформаційних ресурсів дозволяє зробити висновок про надто широкий спектр, багатошаровість та масштабність тих обставин, в результаті яких може порушуватись цілісність, доступність та конфіденційність інформації державних інформаційних ресурсів. У зв'язку з цим, ефективна комплексна система захисту ДІР повинна неодмінно враховувати увесь перелік обставин, за яких потенційні небезпеки та загрози інформації можуть бути дієвими щодо можливості доступу до інформації органів державного управління.

Висновок

Аналіз розглянутого матеріалу дозволяє зробити висновок про подальше вдосконалення комплексної системи захисту державних інформаційних ресурсів, що самостійно враховуватиме якомога більше загроз. Розглянута загальна система класифікації загроз ДІР повинна допомогти розробляти певні управлінські моделі впливу на них. Це, у свою чергу, вказує на необхідність подальшого розгляду проблем формування та функціонування системи забезпечення державних інформаційних ресурсів органів державної влади.

ЛІТЕРАТУРА

1. *Мастяниця Й. І.* Інформаційні ресурси України: проблеми державного регулювання: монографія / Й. І. Мастяниця. — К. : НІСД, 2006. — 141 с.

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

3. *Біла* книга Держспецзв'язку. — Режим доступу: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=49942&cat_id=49941

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

5. *Богуш В. М.* Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. — К. : МК-Прес, 2005. — 432 с.

6. http://pidruchniki.ws/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi.

7. *Бойченко О. В.* Загрози інформаційної безпеці в діяльності ОВС України / О. В. Бойченко. [Електронний ресурс]. — Режим доступу: http://archive.nbuv.gov.ua/portal/soc_gum/Kyuv/2009_1/1-5/06.pdf

8. *Поняття* та види загроз національним інтересам та національній безпеці в інформаційній сфері. [Електронний ресурс]. — Режим доступу: http://libfree.com/190308080_politologiyaponyattya_vidi_zagroz_natsionalnim_interesam_natsionalniy_bezpetsi_informatsiyniy_sferi.html.

REFERENCES

1. *Mastyanytsya Y. I.* Information Resources of Ukraine : problems of government control : monograph / Y. I. Mastyanytsya. — K. : NISS , 2006. — 141 s.

2. *Information* Security. Regulatory support : textbooks / O. K. Yudin. — K. : NAU, 2011. — 640 p.

3. *White* Paper of State Service. — Mode of access: http://www.dsszzi.gov.ua/dstszi/control/uk/publish/article?art_id=49942&cat_id=49941.

4. *Data Protection* in information and telecommuni-cation systems: Law of Ukraine of 05.07.1994 № 81/94-VR // BD. — 1994. — № 31. — S. 287 .

5. *Bogush V. M.* Information security state / V. M. Bogush, A. K. Yudin. — K.: MK-Press, 2005. — 432 p.

6. http://pidruchniki.ws/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi.

7. *Boychenko O.* Threats to information security in ATS Ukraine / O. Boychenko. Mode of access: http://archive.nbuv.gov.ua/portal/soc_gum/Kyuv/2009_1/1-5/06.pdf

8. Concept and types of threats to national interests and national security in the information sector. Mode of access: http://libfree.com/190308080_politologiyaponyattya_vidi_zagroz_natsionalnim_interesam_natsionalniy_bezpetsi_informatsiyniy_sferi.htm

Стаття надійшла до редакції 10.10.2013

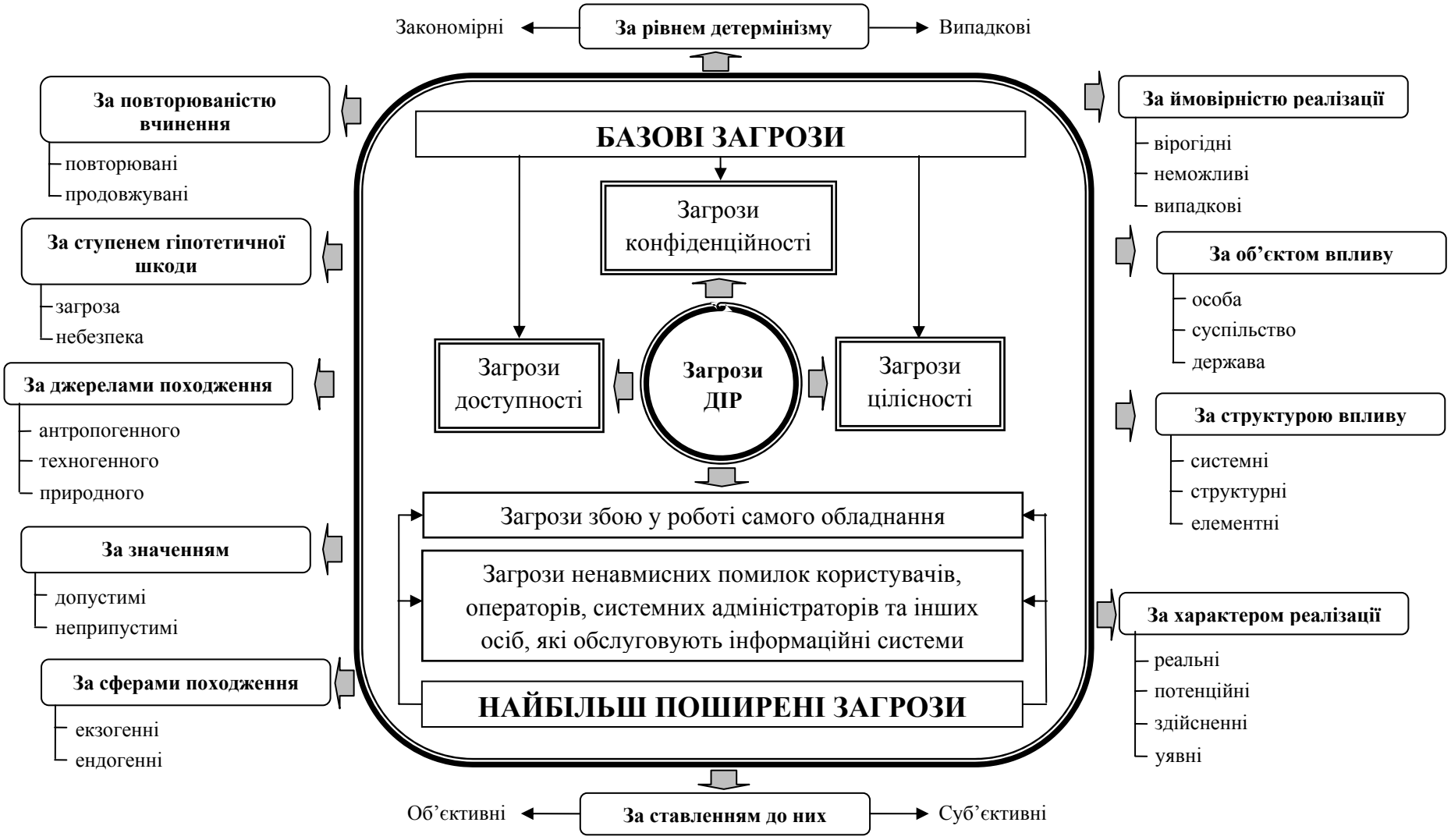

Рис. 3. Загальна система класифікації загроз безпеці інформації державних інформаційних ресурсів