УДК 004.056.5

КЛАСИФІКАЦІЯ ЗАГРОЗ ДЕРЖАВНИМ ІНФОРМАЦІЙНИМ РЕСУРСАМ ІНЖЕНЕРНО-ТЕХНІЧНОГО СПРЯМУВАННЯ. МЕТОДОЛОГІЯ ПОБУДОВИ КЛАСИФІКАТОРА

***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

У статті продовжена тематика побудови класифікатора загроз державним інформаційним ресурсам, методологія побудови якого авторами запропонована раніше. Визначено загрози інженерно-технічного спрямування та наведено приклад їх класифікації. Здійснено завершення створення класифікатора загроз державним інформаційним ресурсам, який в цілому містить загрози нормативно-правового, організаційного та інженерно-технічного спрямування.

Ключові слова: державні інформаційні ресурси, класифікатор загроз, загроза, інженерно-технічне спрямування, конфіденційність, цілісність, доступність.

In the article the continued subjects of construction of classifier of threats to the state informative resources, methodology of construction of which by authors was offered before. Certain threats of technical aspiration and an example of their classification is made. Completion of creation of classifier of threats is carried out to the state informative resources, which on the whole contains the threats of normatively-legal, organizational and technical aspiration.

Keywords: state informative resources, classifier of threats, threat, technical aspiration, confidentiality, integrity, availability.

Актуальність дослідження

Актуальність дослідження зумовлена необхідністю розкриття загроз державним інформаційним ресурсам (ДІР) інженерно-технічного спрямування, що є подальшим розвитком раніше опублікованих авторами праць, основними з яких можна вважати [1, 2].

Аналіз останніх досліджень та публікацій

Ретельний аналіз проблеми створення методології побудови класифікатора загроз ДІР авторами закладено в працях [1, 2, 3, 4], де викладено ряд сучасних теоретичних та практичних підходів до вирішення нормативно-правових, організаційних та інженерно-технічних завдань для реалізації процесу захисту інформаційних ресурсів держави.

Інженерно-технічній складовій при захисті інформаційних ресурсів приділяли уваги багато вчених та організацій, яки займаються питаннями інформаційної безпеки. Дане питання є обов'язковим елементом нормативно-правової бази (міжнародних, державних, галузевих стандартів, нормативних документів технічного захисту інформації (НДТЗІ).

У класифікаторі загроз інформаційної безпеки DSECCT (Digital Security Classification of Threats), розробленому фахівцями компанії Digital Security [5], загрози інформаційної безпеки поділяються на технологічні та організаційні.

В свою чергу, технологічні — на фізичні (застосування різного роду технічних засобів охорони і споруд, призначених для створення фізичних перешкод на шляхах проникнення в систему) та технічні (засновані на використанні технічних пристроїв і програм, які входять до складу автоматизованої системи (АС) і виконують функції захисту: засоби аутентифікації; апаратне шифрування; інше).

У роботі С. В. Віхорева [6] загрозами безпеці інформації є: розкрадання (копіювання) інформації; знищення інформації; модифікація (викривлення) інформації; порушення доступності (блокування) інформації; заперечення автентичності інформації; нав'язування хибної інформації. У подальшому визначається, що носіями загроз безпеці інформації є джерела загроз, які поділяються на: обумовлені діями суб'єкта (антропогенні джерела загроз); обумовлені технічними засобами (техногенні джерела загроз); обумовлені стихійними джерелами.

Розглядаючи перелік типових загроз інформаційної безпеки, пов'язаних з міжнародним стандартом ISO/IEC 27002:2005, можна констатувати відсутність у прямій постановці класифікації загроз інженерно-технічного спрямування (у перелік типових загроз інформаційній безпеці згідно з приведеним стандартом входять: фізичні

загрози; нецільове використання комп'ютерного обладнання в мережі Інтернет співробітниками організації; загрози витоку конфіденційної інформації; загрози витоку інформації по технічним каналам; загрози несанкціонованого доступу; загрози недоступності ІТ сервісів та руйнування (втрати) інформаційних активів; загрози порушення цілісності та несанкціонованої модифікації даних; загрози антропогенних та природних катастроф; юридичні загрози).

Управління інформаційними ризиками тісно пов'язане із успішним вирішенням питання класифікації загроз інформаційним ресурсам.

В своєму підході при класифікації загроз О. М. Астахов [7] окремо не виділяє загрози інженерно-технічного спрямування. Його підхід заснований на міжнародних стандартах з інформаційної безпеки. Класифікація загроз інформаційній безпеці А. Г. Корченка [8] виконана за такими основними базовими ознаками: за дією на характеристики безпеки інформації (К-тип, Ц-тип, Д-тип, КЦ-тип, КД-тип, ЦД-тип, КЦД-тип, де К-конфеденційність, Ц-цілісність, Д-доступність та відповідно наприклад КЦ-тип представляє собою загрозу конфіденційності та цілісності) та за природою джерела (об'єктивна і суб'єктивна).

В указаній класифікації в прямій постановці не визначені загрози інженерно-технічного спрямування.

У системній класифікації загроз безпеки інформації, яка запропонована А. А. Малюком в працях [9, 10], вона здійснюється за параметрами класифікації, значенням параметрів та змістом значення параметра (табл. 1).

Отже, в даній класифікації також відсутня пряма постановка визначення загроз інженерно-технічного спрямування.

Таблиця 1

Системна класифікація загроз безпеки інформації

Параметри класифікації	Значення параметрів	Зміст значення параметрів
1. Види	1.1. Фізична цілісність	Знищення (викривлення)
	1.2. Логічна структура	Викривлення структури
	1.3. Зміст	Несанкціонована модифікація
	1.4. Конфіденційність	Несанкціоноване отримання
	1.5. Право власності	Привласнення чужого права
2. Природа походження	2.1. Випадкова	Відмови, збої, помилки, стихійні лиха, побічні впливи
	2.2. Навмисна	Злочинні дії людей
3. Передумова появи	3.1. Об'єктивні	Кількісна недостатність елементів системи, якісна недостатність елементів системи
	3.2. Суб'єктивні	Розвідувальні органи іноземних держав, промисловий шпіонаж, кримінальні елементи, недоброякісні співробітники
4. Джерело загроз	4.1. Люди	Сторонні особи, користувачі, персонал
	4.2. Технічні пристрої	Реєстрації, передачі, зберігання, видачі
	4.3. Моделі, алгоритми, програми	Загального призначення, прикладні, допоміжні
	4.4. Технологічні схеми обробки	Ручні, інтерактивні, внутрішньомашинний, мережеві
	4.5. Зовнішнє середовище	Стан атмосфери, побічні шуми, побічні сигнали

В НДТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі» затвердженого наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04 грудня 2000 року № 53 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806 приведені основні загрози для інформації в АС та вказано, що основою для проведення аналізу ризиків і формування вимог до комплексної системи захисту інформації (КСЗІ) є розробка моделі загроз для інформації та моделі порушника. Щодо класифікації загроз, то вона побудована за загальноприйнятою ознакою. Зокрема, загрози для інформації, що обробляється в АС, залежать від характеристик обчислювальної системи (ОС), фізичного середовища, персоналу, технологій обробки та інших чинників і можуть мати об'єктивну або суб'єктивну природу. Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні. Жодного прямого посилання на класифікацію загроз, що наведена авторами в [2] немає.

Отже, із проведеного аналізу слідує, що технічному напрямку захисту інформаційних ресурсів завжди приділялась значна увага, але в запропонованому авторами класифікаторі загроз [2] інженерно-технічне спрямування не вирізнялось в прямій постановці.

Мета статті — полягає у розробці класифікатора загроз державним інформаційним ресурсам інженерно-технічного спрямування з урахуванням розробленої методології побудови їх класифікатора [2].

Виклад основного матеріалу

Перш ніж навести опис загроз ДІР інженерно-технічного спрямування, нагадаємо про складові, що відносяться до методології побудови класифікатора.

Визначено, що підґрунтям для формування «Класифікатора загроз ДІР» є запропонована авторами методологія «подвійної трійки захисту» інформаційних ресурсів, основою якої є дві платформи [2].

Перша платформа інформаційної безпеки (ІБ) — складові, що підлягають захисту (властивості інформації): конфіденційність; цілісність; доступність. Друга платформа ІБ — складові, що реалізують систему захисту (методи та засоби): нормативно-правові; організаційні; інженерно-технічні.

Відповідно до цього отримана наступна початкова класифікація та методика кодування в цілому для ДІР (рис. 2), де загрози *інженерно-технічного спрямування (03)* — загрози, 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.

Далі введемо поділ загроз відповідно до першої платформи основних властивостей інформації (рис. 3).

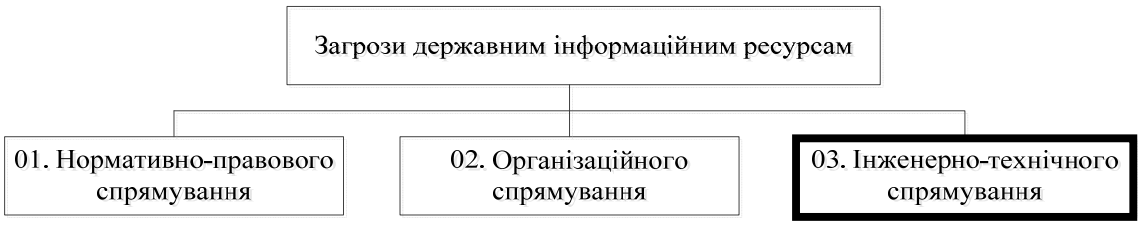

Рис. 2. Класифікація загроз ДІР за характером спрямування

Рис. 3. Поділ загроз інженерно-технічного спрямування відповідно до основаних властивостей інформації

Здійснимо опис загроз ДІР *інженерно-технічного спрямування*. Авторами ретельно було вивчено попит формування класифікації загроз, розглянуто і доповнено переліки сучасними видами з урахуванням вимог різних галузей діяльності суспільства та країни.

Пропонується ввести додаткові принципи класифікації (представлені в середній частині рис. 3), по-перше: загрози ДІР *стратегічного* характеру (03_1). До них требо віднести загрози, що стосуються питань національної безпеки, відсутності або не виконання цільових програм чи доктрин, послабленням галузевих взаємозв'язків органів державної й законодавчої влади, тощо. Практично всі ці загрози загального типу та мають вплив на всі три властивості

ресурсу одночасно: конфіденційність, цілісність, доступність (03_1.1_2_3.1, К,Ц,Д[01,02,03]). Більшість зазначеного типу загроз представлено в законодавчих та нормативних актах, таких як : Концепції, Доктрини, Державні Програми тощо.

По-друге, необхідно професійно деталізувати питання захисту інформаційних ресурсів безпосередньо для самої інформаційної системи обробки, а також процесів зберігання і передачі ДІР (ІС ДІР, РеєстрЕлДІР, ДепозитарійЕлДІР) — загрози ДІР тактичного характеру (03_2). Однак, формалізуємо цей розподіл тільки підкреслюючи додаткові принципи класифікації за стратегічним або тактичним характером, а кодифікацію зробимо наскрізну за наявністю повного переліку загроз.

Представлений нижче перелік, зрозуміло, не є повним і догматичним. Більш широкий опис буде відображено у монографії «Класифікатор загроз Державним інформаційним ресурсам». Класифікація також динамічно буде поновлюватись й коректуватись на основі постійного розвитку інформатизації суспільства.

Таким чином, до ***основних стратегічних загроз ДІР за інженерно-технічним спрямуванням*** *(03_1.1_2_3)* можна віднести такі:

Стратегічні 03_1.1_2_3.

03_1.1_2_3.1 загрози розвитку вітчизняної індустрії інформатизації, включаючи індустрію засобів інформаційно-телекомунікаційних систем та захисту інформації, забезпеченню потреб внутрішнього ринку в її продукції і виходу цієї продукції на світовий ринок, а також забезпеченню накопичення, зберігання й ефективного використання вітчизняних інформаційних ресурсів [к,ц,д,02,03];

03_1.1_2_3.2 діяльність іноземних політичних, економічних і військових розвідувальних та інформаційних структур, спрямована проти інтересів України в інформаційній сфері [к,ц,д,01,02,03];

03_1.1_2_3.3 реалізація процесів прагнення деяких країн домінувати й обмежити інтереси України у світовому інформаційному просторі, витиснення її із зовнішнього і внутрішнього інформаційних ринків, а також блокування інформаційних ресурсів (в т.ч. ДІР) [к,ц,д,02,03];

03_1.1_2_3.4 організація діяльності космічних, повітряних, морських і наземних технічних та інших засобів (видів) розвідки іноземних держав [к,ц,д,02,03];

03_1.1_2_3.5 розробка деякими державами концепцій *інформаційних воєн*, що передбачають створення засобів небезпечного впливу на інформаційні сфери інших країн, порушення нормального функціонування інформаційних і телекомунікаційних систем зберігання інформаційних ресурсів, одержання несанкціонованого доступу до них (в т.ч. ДІР) [к,ц,д,01,02,03];

03_1.1_2_3.6 створення несприятливої криміногенної обстановка, що супроводжується зрощуванням державних і кримінальних структур в інформаційній сфері, одержання кримінальними структурами права доступу до інформації (у т.ч. ДІР), що не підлягає поширенню, посилення впливу організованої злочинності на життя суспільства, зниження ступеня захищеності законних інтересів громадян, суспільства і держави в інформаційній сфері [к,ц,д,02,03];

03_1.1_2_3.7 недостатня активність органів державної влади щодо інформування суспільства про свою діяльність, роз'яснення прийнятих рішень, формування системи відкритих державних ресурсів і розвитку системи доступу до них громадян [к,ц,д,01,02,03];

03_1.1_2_3.8 відставання України від провідних країн світу за рівнем інформатизації органів державної влади і місцевого самоврядування, промисловості, сфери послуг і побуту громадян, тощо [к,ц,д,01,02,03];

03_1.1_2_3.9 відсутність системи моніторингу показників і характеристик інформаційної безпеки України та її застосування у найважливіших сферах діяльності суспільства і держави [к,ц,д,02,03].

Тактичні 03_2.1.

До *основних тактичних* ***загроз конфіденційності ДІР за інженерно-технічним спрямуванням*** *(03_2.1)* можна віднести такі:

03_2.1.1 відсутність (не виконання) сформованої політики безпеки при зберіганні, обробці, передачі та відображенні ДІР в автоматизованих (інформаційній) системах різних класів [к,ц,д,01,02,03];

03_2.1.2 оброблення, зберігання, передача і відображення інформації в АС ДІР без застосування комплексної системи захисту інформації (КСЗІ) з підтвердженою відповідністю ресурсу до ІзОД [к,ц,д,01,02,03];

03_2.1.3 відсутність або порушення загальної встановленої системи розподілу доступу (моделі доступу, матриці доступу, атрибутів доступу, системи ідентифікації і автентифікації, тощо), не виконання правил і вимог зміни паролів або ідентифікаторів до інформаційних ресурсів або\чи інформаційної системи ДІР [к,ц,д,01,02,03];

03_2.1.4 несанкціоноване перехоплення, одержання та використання атрибутів доступу з наступним їхнім використанням для процедур маскування під авторизованого Адміністратора (власника інформаційної системи, адміністратора

безпеки, користувача, тощо) інформаційної системи ДІР, Реєстру ЕлДІР або Депозитарію ЕлДІР [к,ц,д,01,02,03];

03_2.1.5 відсутність вимог та технічних характеристик моніторингу і контролю (корекції процесів) за робочими процесами ІС, а також не визначення оцінки ефективності щодо захисту ДІР [к,ц,д,01,02,03];

03_2.1.6 неналежне виконання Адміністратором (власником інформаційної системи, адміністратором безпеки, користувачами, тощо) інформаційної системи ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР своїх обов'язків (забезпечення функціонування ІС відповідно до вимог політики безпеки, здійснення контролю доступу, створення і супровід КСЗІ, визначення оцінки ефективності КСЗІ і корекція процесів, своєчасне оновлення інформаційного ресурсу та належного ПЗ, інші роботи пов'язані з Реєстром ЕлДІР або Депозитарієм ЕлДІР) [к,ц,д,01,02,03];

03_2.1.7 відсутність (повна або часткова) процедур реалізації методів і засобів технічного та криптографічного захисту ДІР, а також контролю за цими процесами згідно чинного законодавства [к,ц,д,01,02,03];

03_2.1.8 відсутність або порушення загальної встановленої системи розподілу доступу, зміни, збереження й управління криптографічними ключами при їх використанні згідно чинного законодавства [к,ц,д,01,02,03];

03_2.1.9 відсутність організаційних заходів та їх впровадження, щодо виявлення технічних пристроїв і програм, які загрожують штатному функціонуванню інформаційних систем, запобігання перехопленню й витоку інформації технічними каналами (в т.ч. неправомірне підключення — «врізання» до комутативних або без комутативних каналів зв'язку, тощо), а також відсутність контролю за виконанням спеціальних вимог із захисту ДІР [к,ц,д,01,02,03];

Зрозуміло, що вище наведений перелік загроз конфіденційності ресурсу, може і повинно бути віднесено до загроз цілісності і доступності у тих частинах, які відображають порушення цих властивостей. Тому, з метою створення повного переліку загроз класифікатора представимо ще раз деякі загрози означені вище, однак з кодифікацією, яка відноситься до цілісності або доступності.

До *основних загроз* ***цілісності ДІР організаційного спрямування*** *(03_2.2)* можна віднести такі:

03_2.2.1 — 03_2.2.9 (*див. загрози 03_2.1.1 — 03_2.1.9*);

03_2.2.10 несанкціонована модифікація процедур штатного функціонування або не авторизоване внесення змін в стандартне ПЗ сервісів і додатків АС ДІР різних класів (несанкціонована фальсифікація та модифікація текстів та функцій ПЗ, нехтування правилами і проектами змін, відсутність документального оформлення порушень або змін тощо) [ц,д,01,02,03];

03_2.2.11 несанкціонована модифікація процедур штатного функціонування або не авторизоване внесення змін в ПЗ операційної системи (ОС) АС ДІР різних класів (несанкціонована фальсифікація та модифікація текстів та функцій ОС, нехтування проектами і проектами змін, відсутність документального оформлення порушень або змін ОС тощо) [ц,д,01,02,03];

03_2.2.12 несанкціонована модифікація процедур штатного функціонування або не авторизоване внесення змін в ПЗ, що забезпечує стандартні режими встановлених послуг АС ДІР різних класів (несанкціонована фальсифікація та модифікація текстів та функцій ПЗ, нехтування правилами і проектами змін, відсутність документального оформлення порушень або змін ПЗ тощо) [ц,д,01,02,03];

03_2.2.13 несанкціонована модифікація процедур штатного функціонування або не авторизоване внесення змін в ПЗ системи електронного документообігу (в т.ч. електронної комерції) ІС ДІР, Реєстр ЕлДІР або Депозитарій ЕлДІР (несанкціонована фальсифікація та модифікація текстів та функцій ПЗ, нехтування проектами змін, відсутність документального оформлення порушень або змін, тощо) [ц,д,01,02,03];

03_2.2.14 розробка, впровадження та супроводження комп'ютерних вірусів, шпигунських програмних продуктів, програмних закладок, інших типів шкідливого ПЗ, яке порушує штатне функціонування та встановлену політику безпеки ІС ДІР, РеєструЕл ДІР або Депозитарію ЕлДІР з зловмисною метою [ц,д,02,03];

03_2.2.15 навмисно або\чи не навмисно залишені Адміністратором ІС ДІР, Реєстру ЕлДІР або Депозитарію ЕлДІР (власником інформаційної системи, адміністратором безпеки, авторизованими користувачами, розробником, тощо) не документовані функції, залишкові дані роботи ІС та ПЗ (Люки різних типів), використання яких дозволяє змінити або порушити стандартні режими роботи АС ДІР різних класів [ц,д,02,03];

03_2.2.16 навмисно або\чи не навмисно залишені Адміністратором ІС ДІР, Реєстру ЕлДІР або Депозитарію ЕлДІР (власником інформаційної системи, адміністратором безпеки, авторизованими користувачами, розробником, тощо) не документовані функції, залишкові дані роботи ІС та ПЗ (Люки різних

типів), використання яких дозволяє обминути механізми захисту інформації та порушити встановлену політику безпеки [ц,д,02,03];

03_2.2.17 відсутність (повна\часткова) процедур, щодо впровадження, використання та регулярного оновлення антивірусних баз і ліцензованого ПЗ, а також загального репозитарію ДІР[ц,д,02,03];

03_2.2.18 відсутність ПЗ або програмно-апаратних засобів і методів резервування та архівації важливих критичних даних [ц,д,02,03];

03_2.2.19 порушення режимів функціонування (виведення з ладу, тощо) систем життєзабезпечення ІС ДІР (електроживлення, заземлення, охоронної сигналізації, вентиляції та ін.)[ц,д,02,03];

03_2.2.20 подання власником або\чи Адміністратором інформаційного ресурсу (власником інформаційної системи, адміністратором безпеки, авторизованими користувачами, тощо) недостовірних відомостей (даних) до інформаційної системи ДІР, Реєстру ЕлДІР або Депозитарію ЕлДІР та їх навмисна (не навмисна) фальсифікація й модифікація[01,02,03].

До *основних загроз* ***доступності ДІР інженерно-технічним спрямування*** *(03.3)* можна віднести такі:

03_2.3.1—03_2.3.9 (*див. загрози 03_2.1.1 — 03_2.1.9; 03_2.2.1 — 03_2.2.9*);

03_2.3.10—03_2.3.19 (*див. загрози 03_2.2.10 — 03_2.2.19*);

03_2.3.20 відсутність (повна\часткова) процедур перевірки технічного стану й контролю за ним, встановлення оцінки ефективності роботи, а також не виконання системи вимог та обмежень на технічні характеристики, які відображують штатні режими роботи ІС ДІР, Реєстру ЕлДІР або Депозитарію ЕлДІР[02,03];

03_2.3.21 відсутність (повна\часткова) процедур перевірки технічного стану й контролю за ним, встановлення оцінки ефективності роботи, а також не виконання системи вимог та обмежень на технічні характеристики, які відображують штатні режими роботи комплексів засобів захисту ІС ДІР, Реєстру ЕлДІР або ДепозитаріюЕлДІР[02,03];

03_2.3.22 відсутність (повна\часткова) процедури перевірки засобів обслуговування, ремонту й ефективності надання послуг (в т.ч. третіми особами) користувачам ІС ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР[02,03];

03_2.3.23 відсутність (повна\часткова) керування потоками та\чи зміна їх напряму (в т.ч. шляхом генерації несправжніх повідомлень для перевантаження системи, переривання тощо), як сукупності функцій і процедур, які забезпечують неможливість передачі інформації прихованими каналами (тобто в обхід КЗЗ) або в більш вузькому значенні сукупність процедур, які забезпечують неможливість передачі інформації від об'єкта ІС з більш високим рівнем доступу до об'єкта ІС з більш низьким рівнем доступу[02,03];

03_2.3.24 протидія процесу, що забезпечує повернення об'єкта ІС або саму ІС ДІР до відомого попереднього стану (процесу) після виконання над об'єктом певної операції або серії операцій[02,03];

03_2.3.25 не санкціоновані дії (процеси), які обмежують (повна\часткова) можливості використання певного інформаційного ресурсу (програмного або\чи програмно-апаратного) АС ДІР різних класів Адміністратором (власником інформаційної системи, адміністратором безпеки, авторизованими користувачами, третьою стороною, тощо) ІС ДІР, Реєстру ЕлДІР або Депозитарію ЕлДІР[02,03];

03_2.3.26 не санкціоноване обмеження або порушення здатності продовжувати функціонування процесів в умовах виникнення збоїв і відмов окремих компонентів ІС ДІР, Реєстру ЕлДІР або Депозитарію ЕлДІР[02,03];

03_2.3.27 не санкціоновані дії (процеси), які обмежують (повна\часткова) можливість встановлення (інсталяції) ІС ДІР, Реєстр ЕлДІР або Депозитарію ЕлДІР або інформаційного об'єкта у відомий чи визначений штатний стан (режим)[02,03];

03_2.3.28 не санкціоноване обмеження або порушення здатності продовжувати функціонування процесів надання встановлених послуг (різних типів) ІС ДІР, Реєстру ЕлДІР або Депозитарію ЕлДІР[02,03].

Позначками у верхньому індексі проставлено вплив на властивості інформації (к — конфіденційність, ц — цілісність, д — доступність) та на відповідні спрямування (01 — нормативно-правове, 02 — організаційне, 03 — інженерно-технічне).

Надалі кожну загрозу відносимо: за джерелом загрози (антропогенні, техногенні, стихійні); за відношенням до інформаційного об'єкту (внутрішні, зовнішні); за характером загрози (навмисні, ненавмисні); за структурою впливу (системні, структурні, елементні); за рівнем впливу (фізичні засоби, мережне обладнання, мережні додатки та сервіси, операційна система, системи управління базами даних).

На основі вищенаведеного та з урахуванням запропонованому авторами підходу щодо класифікатора загроз ДІР [2], можна скласти наступну (як приклад) класифікацію ДІР за

інженерно-технічним спрямуванням (табл. 2). Де 1 та 0 — віднесення (1) або не віднесення (0) даного виду загрози до подальших елементів класифікації.

Основні результати

Виходячи з вищевказаного, основним результатом дослідження автори вважають подальше удосконалення та розширення методології побудови класифікатора загроз ДІР за рахунок розробки класифікатора наступного широкого класу загроз інженерно-технічного спрямування.

Висновок

Таким чином, в статті авторами продовжена тематика побудови класифікатора загроз ДІР, а саме визначені загрози інженерно-технічного спрямування. Наведено приклад класифікації загроз ДІР інженерно-технічного спрямування.

ЛІТЕРАТУРА

1. *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.

2. *Юдін О. К.*, Методологія побудови класифікатора загроз державним інформаційним ресурсам / С. С. Бучик, А. В. Чунарьова, О. І. Варченко // Наукоємні технології. — 2014. — № 2 (22) / Технічні науки. — С. 200–210.

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

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

5. *Классификация* угроз Digital Security (Digital Security Classification of Threats). — Режим доступу: http://www.dsec.ru/products/grif/fulldesc/classification

6. *Вихорев С. В.* Классификация угроз информационной безопасности. — Режим доступу: http://www.elvis.ru/upload/iblock/f60/f602ee2337fcc7250c71c2a138fe9ecc.pdf

7. *Астахов А. М.* Искусство управления информационными рисками / А. М. Астахов. — М. : ДМК Пресс, 2010. — 312 с.

8. *Корченко А. Г.* Построение систем защиты информации на нечетких множествах / А. Г. Корченко. — К. : МК-Пресс, 2006. — 320 с.

9. *Малюк А. А.* Информационная безопасность: концептуальные и методологические основы защиты информации: учеб. пособие для вузов / А. А. Малюк. — М. : Горячая линия-Телеком, 2004. — 280 с.

10. *Малюк А. А.* Введение в защиту информации в автоматизированных системах: учеб. пособие для вузов / А. А. Малюк, С. В. Пазизин, Н. С. Погожин. — М. : Горячая линия-Телеком, 2005. — 147 с.

Стаття надійшла до редакції 19.05.2015

Таблиця 2

Приклад класифікації загроз ДІР інженерно-технічного спрямування

Спрямування загроз	Рівень загроз	Вид загроз	Функціональний профіль загроз	Джерело загроз			Відношення до інформаційного об'єкту		Характер загрози		Загрози за структурою впливу			Рівні впливу загрози				
				Антропогенні	Техногенні	Стихійні	Внутрішні	Зовнішні	Навмисні	Ненавмисні	Системні	Структурні	Елементні	Фізичні засоби (лінії зв'язку, апаратні засоби)	Мережне обладнання	Мережні додатки та сервіси	Операційна система	Системи управління базами даних
03 Інженерно-технічне спрямування	03_1	03_1.1_2_3 Конфіденційність Цілісність Доступність	……..	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
			03_1.1_2_3.2 діяльність іноземних політичних, економічних і військових розвідувальних та інформаційних структур, спрямована проти інтересів України в інформаційній сфері [к,ц,д,01,02,03];	1	0	0	1	1	1	0	1	1	1	1	1	1	1	1
			……..	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
	03_2	03_2.1 Конфіденційність	……..	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
			03_2.2.18 відсутність ПЗ або програмно-апаратних засобів і методів резервування та архівації важливих критичних даних [ц,д,02,03];	1	0	0	1	0	1	0	1	1	1	0	0	1	1	1
		……..	……..	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
		03_2.3 Доступність	03_2.3.24 протидія процесу, що забезпечує повернення об'єкта ІС або саму ІС ДІР до відомого попереднього стану (процесу) після виконання над об'єктом певної операції або серії операцій[02,03];	1	0	0	1	0	1	0	1	1	1	0	0	0	1	1
			……..	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…