УДК 004.056.5

МЕТОДОЛОГІЯ ПОБУДОВИ КЛАСИФІКАТОРА ЗАГРОЗ ДЕРЖАВНИМ ІНФОРМАЦІЙНИМ РЕСУРСАМ

***О. К. Юдін**, д-р техн. наук, проф.; ****С. С. Бучик**, канд. техн. наук, доц.;
***А. В. Чунарьова**, канд. техн. наук; ***О. І. Варченко**

*Національний авіаційний університет
e-mail: kszi@ukr.net
** Житомирський військовий інститут імені С. П. Корольова
Державного університету телекомунікацій

Уперше розглянуто питання системного підходу та подано основи методології побудови загального класифікатора загроз державним інформаційним ресурсам. Запропоновано основні концептуальні підходи класифікації загроз державним інформаційним ресурсам (за характером, типом, спрямуванням, методикою кодування загроз тощо), докладно розкрито типи загроз державним інформаційним ресурсам нормативно-правового спрямування. Наведено приклади класифікації та методики кодування загроз державним інформаційним ресурсам нормативно-правового спрямування.

Ключові слова: державні інформаційні ресурси, нормативно-правове спрямування, класифікація загроз, загроза, конфіденційність, цілісність, доступність, стандарт.

On the base of the conducted researches the question of approach of the systems is considered and the bases of methodology of construction of general classifier of threats to the State informative resources are presented. Basic conceptual approaches of classification of threats of state informative resources (on the character, type, aspiration, methods of code of threats, and others like that) are presented, the types of threats to the state informative resources of normatively-legal aspiration are exposed more in detail. Examples of classification and methods of code of threats to the state informative resources of normatively-legal aspiration are made.

Keywords: state informative resources, normatively-legal aspiration, classification of threats, threat, confidentiality, integrity, availability, standard.

Аналіз останніх досліджень і публікацій

Проведений аналіз нормативно-правового забезпечення захисту державних інформаційних ресурсів (ДІР) в інформаційній сфері нашого суспільства свідчить про малосистемний характер відповідної діяльності, спостерігається нечітка спрямованість визначення класів загроз різним видам ДІР (мало деталізовані, або відсутні). Крім того, на концептуальному та нормативному рівнях не визначено перелік і класифікацію загроз інформаційним ресурсам держави, не розроблено нормативно-правового документу, стандарту щодо поняття *державних інформаційних ресурсів*, його складових та відповідної їм моделі загроз [1; 2; 3].

Звертаючись до теми створення класифікатора загроз інформаційним ресурсам, слід зазначити, що даному питанню приділяли увагу як вітчизняні, так і зарубіжні вчені, а саме: Новіков О. М., Богуш В. М., Мохор В. В., Горбенко І. Д., Хорошко В. О., Корнейко О. В., Грайворонський М. В., Корченка О. Г., Марущак А. І., Мельніков В. П., Віхорев С. В., Касперский Е. В., Медведовський І. Д., Олійник О. В., Соснін О. В. та ін. Але питанню створення класифікатора загроз ДІР приділялась незначна увага, про що свідчить існуюча нормативно-правова база щодо їх захисту.

Постановка завдань досліджень

Проводячи аналітично-правовий аналіз побудови класифікатора та моделі загроз державним інформаційним ресурсам, а також розглядаючи загально-сформовану систему та найбільш поширені класифікації загроз інформаційним ресурсам підприємств, організацій і установ з різними формами власності, можна зробити висновок про відсутність загально-спрямованої системи класифікації загроз ДІР.

Мета статті

Отже, *мета статті* — проведення аналізу існуючого нормативно-правового та законодавчого забезпечення (НПЗ) вітчизняних і міжнародних стандартів у галузі інформаційної безпеки (ІБ).

Необхідно побудувати основи методології створення класифікатора загроз, принципів та методик представлення, семантики і системи кодування різних класів загроз ДІР (ЗДІР).

У межах досліджень необхідно визначити концептуальні питання побудови класифікатора ЗДІР та більш докладно представити зазначену модель для першого широкого класу загроз нормативно-правового спрямування.

Відповідна діяльність органів державної влади носить розрізнений відомчий характер

щодо формування реєстру ДІР та безпосередньо системи класифікації загроз ресурсам держави. Не розроблено положення про модель загроз і порушника державних інформаційних ресурсів, за якою можливим було визначення ймовірних намірів порушника, ступеня небезпечності дій і несанкціонованих процесів; категорії осіб, серед яких може знаходитись порушник, припущення про кваліфікацію та характер його дій тощо. Не повною мірою стандартизована політика безпеки державних інформаційних ресурсів, яка має являти собою певний набір вимог, правил, обмежень, рекомендацій згідно з класифікацією ресурсів і загроз. З наведеного аналізу можна зрозуміти, що існує певна проблематика, а деякі питання потребують негайного подальшого вдосконалення.

Виклад основного матеріалу

Основи методології створення «Класифікатора загроз державним інформаційним ресурсам»

Розглядаючи існуючі підходи до класифікації загроз інформаційним ресурсам, можна встановити багато напрямів та підходів, а саме [4; 5; 6]:

- за критеріями інформаційної безпеки (загрози конфіденційності, цілісності, доступності інформаційній системі, а також безпосередньо властивостям інформації);
- за компонентами інформаційних систем, на які спрямовані загрози (інформаційні ресурси та послуги, персональні дані, програмно-апаратні засоби тощо);
- за способом здійснення (випадкові чи навмисні дії, природного та техногенного характеру тощо);
- за розміщенням джерела загроз (внутрішні та зовнішні);
- інші.

Зазначені підходи до класифікації загроз виправдані і мають сенс. Так, джерела загроз можуть знаходитися як у середині організації — внутрішні джерела, так і ззовні — зовнішні джерела. Поділ джерел на суб'єктивні та об'єктивні виправданий виходячи з попередніх міркувань стосовно ризику збитку інформації. Поділ на внутрішні та зовнішні джерела виправданий тому, що для однієї й тієї ж загрози методи як реалізації, так і відбивання загроз можуть бути різними.

Усі джерела загроз безпеці інформації можна розділити на три групи:

• зумовлені діями суб'єкта (антропогенні джерела загроз);

• зумовлені технічними засобами (техногенні джерела загроз);

• зумовлені стихійними джерелами.

Аналізуючи Закони України «Про захист інформації в автоматизованих системах» від 05.07.1994 № 81/94-ВР//ВВР, Доктрину інформаційної безпеки України, затверджену Указом Президента України від 8 липня 2009 року № 514/2009 та «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 81/94-ВР//ВВР, існуючі стандарти, технічні специфікації, та сучасне нормативно-правове забезпечення, можна побудувати таку загальну систему законодавчої бази (базовий перелік), що впливає на формування класифікації ЗДІР (рис. 1), а також визначити напрями аналізу нормативно-правових актів (НПА):

- аналіз існуючих доктрин та законів України, які регламентують питання інформаційного суспільства, ресурсів та інформаційної безпеки України;
- аналіз державних стандартів і нормативних документів, які спрямовані на класифікацію інформаційних систем та засобів захисту за вимогами безпеки;
- аналіз технічних специфікацій, які регламентують різні аспекти реалізації засобів захисту та побудови комплексних систем і комплексів засобів захисту інформації;
- інші підходи [1; 2; 4; 7; 8; 9; 10; 11; 12].

Одними із найважливіших нормативно-технічних документів, які стимулюють розвиток захисту інформаційних систем і мереж, є документи, що стандартизують вимоги та критерії оцінки безпеки, встановлюють правила побудови моделей порушників і загроз, регламентують профілі захисту, загальні та відомчі характеристики комплексів обробки та захисту тощо [13–20]. Дані НПА — це стандартизована система забезпечення захисту інформаційних ресурсів, призначена для взаємодії між державними органами, виробниками і споживачами, що визначає правові та організаційні засади захисту важливої для держави, суспільства й особи інформації, охорона якої забезпечується державою відповідно до чинного законодавства.

Захист інформаційних ресурсів стосовно цих НПА здійснюється для органів державної влади, органів місцевого самоврядування, органів управління та інших державних і/або не державних формувань, підприємств, установ, організацій, утворених згідно із законодавством України.

Автори цих досліджень ставлять перед собою завдання вперше розробити методологію створення «Класифікатора загроз державним інформаційним ресурсам», а також запропонувати принципи та методику опису профілів, функціональної послідовності й кодування, семантику різних класів загроз ДІР.

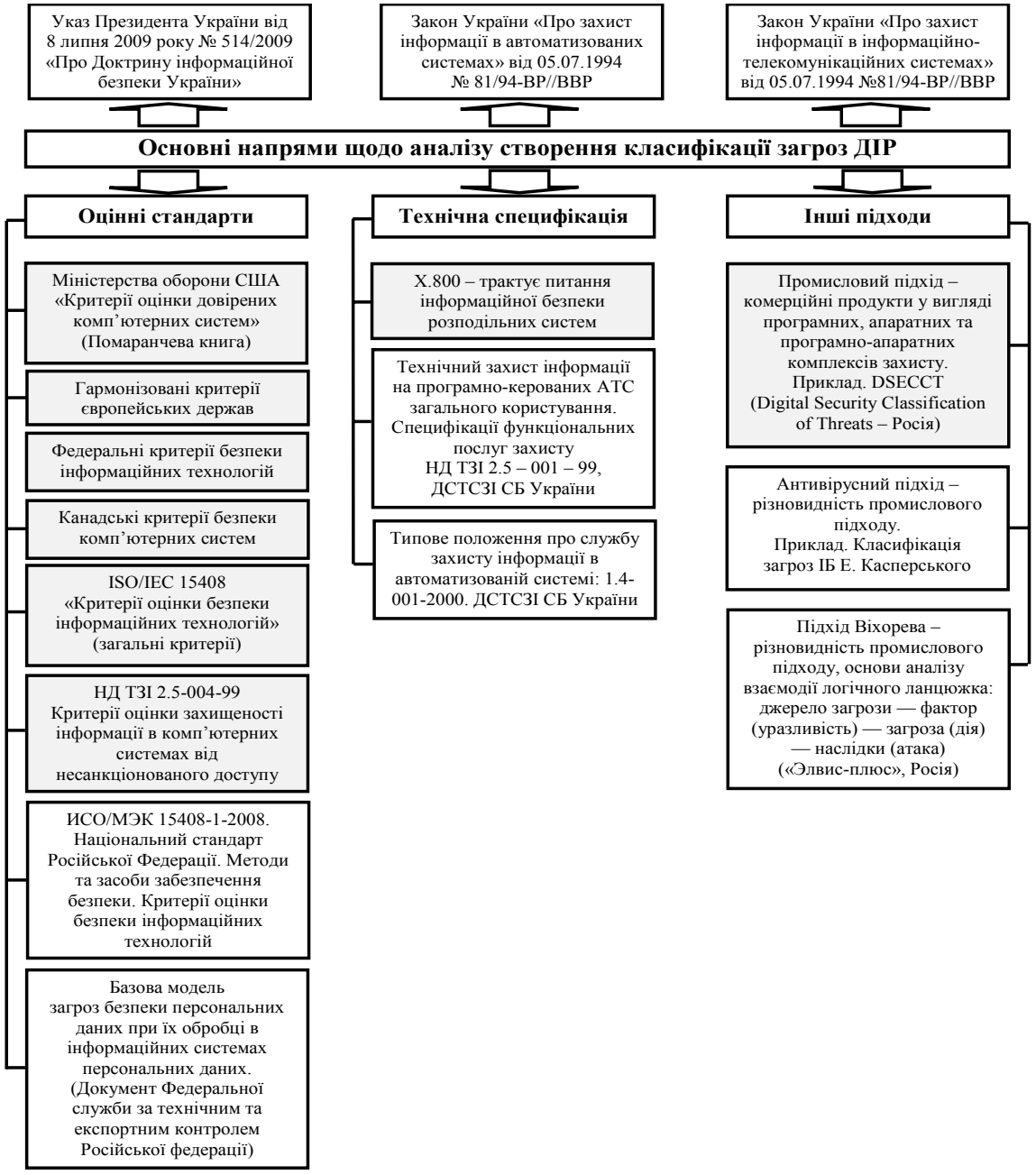

Рис. 1. Основні нормативно-правові документи, що формують напрями аналізу створення класифікації загроз ДІР

Відокремлене місце у державних НПА посідають ключові питання побудови комплексних систем захисту інформації (КСЗІ) як базова крапка в реалізації політики безпеки організацій чи установ з різними формами власності. З метою розробки «Класифікатора загроз державним інформаційним ресурсам» було проведено дослідження напрямів класифікації загроз у нормативних документах та стандартах України, які відповідають за побудову КСЗІ та визначають норми і положення щодо захисту інформаційних об'єктів та їх ресурсів (табл. 1). Сучасний підхід до класифікації загроз інформаційним ресурсам як державний, так і приватний, не дає системного підходу та методик поетапного визначення класів. Існує фрагментарний підхід до визначення характеру, типу, виду та джерел загроз ДІР.

Однак дана фрагментарність, як не дивно, належить не тільки до загроз ДІР, а також і до загального класу загроз ресурсам інформаційних систем державного або загального (не державного) призначення. Проведені дослідження дають можливість стверджувати, що на сьогодні відсутня узагальнена система класифікації та представлення загроз ДІР, джерел їх виникнення та методів реалізації. Дана ситуація ускладнює або унеможливлює процес побудови деталізованих моделей загроз, а також моделі порушника ДІР.

Таблиця 1

Базові підходи до класифікації загроз

Нормативний документ	Підхід до класифікації загроз
НД ТЗІ 1.1.002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу»	– загрози оброблюваній в автоматизованій системі інформації залежать від характеристик обчислювального середовища, фізичного середовища, персоналу й оброблюваної інформації; – загрози можуть мати або об'єктивну, або суб'єктивну природу; – загрози, що мають суб'єктивну природу, можуть бути випадковими або навмисними; – формування загроз за результатом їх впливу на властивості інформації: конфіденційності, цілісності і доступності
НД ТЗІ 1.4-001-00 «Типове положення про службу захисту інформації в автоматизованій системі»	Для кожної із загроз необхідно визначити: – на порушення яких властивостей інформації або автоматизованої системи (АС) вона спрямована (рекомендується користуватись чотирма основними градаціями – порушення конфіденційності, цілісності, доступності інформації, а також порушення спостереженості та керованості АС); – джерела виникнення (які суб'єкти АС або суб'єкти, зовнішні відносно до неї, можуть ініціювати загрозу); – можливі способи здійснення загроз
НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу»	Визначено загрози інформації чотирьох класів: конфіденційність, цілісність, доступність, спостереженість
ДСТУ 3396.0-96 «Захист інформації. Технічний захист інформації. Основні положення»	Джерелами загроз може бути діяльність іноземних розвідок, а також навмисні або ненавмисні дії юридичних і фізичних осіб. Загрози можуть здійснюватися: технічними каналами, каналами спеціального впливу, методами та засобами несанкціонованого доступу до інформаційних ресурсів

Методологічний підхід до формування класифікатора загроз ДІР

У статті подано основи методології створення класифікатора, основні підходи, методика кодування різних класів загроз ДІР, а також приклади побудови класифікатора для першого широкого класу загроз, сформованих на основі нормативно-правового спрямування. Більш докладно побудова класифікатора буде наведена в циклі статей «Класифікатор загроз ДІР» та в повному обсязі в монографії.

Авторами пропонується методологічний підхід, щодо формування класифікатора загроз ДІР на базі запропонованого методу так званої *подвійної трійки захисту*.

Спираючись на сучасну вітчизняну і міжнародну нормативно-правову базу та власний науково-професійний досвід, виділимо основні концептуальні позиції або складові реалізації процесу інформаційної безпеки. Зазначений підхід щодо створення класифікатора пропонується формувати з погляду двох взаємопов'язаних платформ захисту інформації (*подвійної трійки захисту*). По-перше, необхідно визначити платформу мети захисту таким чином, щоб вона відповідала загальним цілям будь-якої КСЗІ. Простіше, необхідно узагальнено відповісти на запитання: що підлягає захисту згідно зі встановленими задачами і вимогами. По-друге, потрібно розглянути зворотний бік цього питання: яким чином виконуються процедури захисту інформаційних ресурсів, а саме які методи і засоби реалізують мету захисту. Даний метод дозволить визначити базові характеристики класифікації загроз для різних видів та розподілити їх за базовими принципами: характер спрямованості, вид загрози та її функціональний профіль.

Для обґрунтування двох платформ методу *подвійної трійки захисту* звернемося до визначення поняття інформаційна безпека згідно з вітчизняними і міжнародними стандартами.

Інформаційна безпека — це стан захищеності властивостей інформації (інформаційних ресурсів), що належить державі, суспільству і особистості, за якого забезпечуються її оброблення, збе-

рігання, поширення і прогресивний розвиток незалежно від (або в умовах) наявності чи реалізації внутрішніх і зовнішніх інформаційних загроз [1].

Під властивостями інформації або інформаційних ресурсів згідно з приписами чинного законодавства слід розуміти три основні складові: *конфіденційність, цілісність, доступність*.

Інформаційна безпека, як складова нормального процесу функціонування підприємств, потребує комплексного підходу до розроблення та впровадження методів і засобів захисту інформаційних ресурсів як на технічному, так і на організаційному рівні, тобто реалізації інтегрованого процесу — управління інформаційною безпекою. Цей процес забезпечує механізми, які дозволяють реалізувати політику інформаційної безпеки організації чи об'єкта інформаційної діяльності в цілому. Це регламентується найбільш актуальними у сфері захисту інформації стандартами серії ISO 27000 та безпосередньо основоположними:

- ISO/IEC 27001:2005 «Інформаційні технології. Методи забезпечення безпеки. Системи управління інформаційною безпекою. Вимоги» [21];
- ISO/IEC 27002:2005 «Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою (раніше ISO/IEC 17799:2005)» [22];
- ISO/IEC 27005:2008 «Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки» [23].

Згідно з міжнародними стандартами інформаційна безпека досягається реалізацією відповідних заходів щодо управління процесами бізнесу, які можуть бути визначені політиками, методами, процедурами, організаційними структурами, устаткуванням і функціями програмного забезпечення тощо. Ці заходи управління безпекою необхідно впроваджувати таким чином, щоб забезпечити впевненість у тому, що встановлена цілі і завдання безпеки організації досягнуті та контролюються адміністрацією та службою безпеки підприємства. Інформація і процеси, що підтримують її, а також АС оброблення, зберігання й передавання інформації — важливі ділові активи. Конфіденційність, цілісність і доступність інформації є істотними активами для підтримання конкурентоспроможності підприємств, грошового обігу, прибутковості, юридичної гнучкості й комерційного іміджу організації [21; 22].

Таким чином можна визначити три базових властивості інформації, що підлягають захисту при формуванні будь-якої політики безпеки та безпосередньо при проектуванні різних видів КСЗІ. Тобто, існує законодавчо затверджена трійка властивостей інформації, яка є підґрунтям опису першої платформи *подвійної трійки захисту*.

Розглядаючи другий етап створення основ методології формування класифікатора, необхідно встановити базові напрями забезпечення безпеки інформації та її властивостей.

Напрями забезпечення безпеки інформації — 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.

Під *забезпеченням ІБ* розуміється сукупність нормативно-правових, організаційних і технічних заходів, призначених для досягнення стану захищеності потреб особистостей, суспільства і держави в обробленні, зберіганні та поширенні інформації [1].

Нині процес захисту інформаційних ресурсів реалізується трьома взаємопов'язаними напрямами, які також є обов'язковими для формування і реалізації політики безпеки будь-якого підприємства, організації чи установи з різними формами власності [21; 22].

З урахуванням вітчизняних і міжнародних НПА, а також практики, що склалася натепер, можна відокремити такі базові напрями захисту інформації [1].

Нормативно-правове забезпечення ІБ — сукупність загальних і спеціальних законів, стандартів, нормативно-правових актів, обов'язкових правил і норм, процедур та заходів тощо, які встановлені або санкціоновані державою, стосовно сфери інформаційних технологій та їх безпеки, а також такі, що забезпечують захист інформації на правовій основі і діють відносно суб'єктів інформаційної діяльності (державних органів, підприємств, організацій та населення (окремої особистості). Правовий захист інформації як нормативно-правовий ресурс впроваджується на міждержавному і державному рівнях та визначається міждержавними договорами, конвенціями, деклараціями та реалізується патентами, стандартами, нормативними документами, рекомендаціями, авторським правом та ліцензіями тощо. На державному рівні правовий захист регулюється державними та відомчими актами.

Організаційне забезпеченням ІБ — сукупність технологій, норм, методів і засобів, які регламентують взаємодію власників інформаційних ресурсів, персоналу систем, користувачів з інфраструктурою та між собою в процесі розроблення, впровадження та експлуатації інформаційних систем та їх безпеки згідно з установленим нормативно-правовим і чинним законодавством (зокрема галузі і підприємства). Тобто, це регла-

ментація виробничої діяльності та взаємовідносин виконавців на нормативно-правовій основі, що виключає або суттєво утруднює неправомірне (несанкціоноване) порушення властивостей інформації та реалізації внутрішніх та зовнішніх загроз.

Інженерно-технічне забезпечення ІБ — сукупність спеціальних органів, а також інженерно-технічних технологій, засобів і заходів, які взаємопов'язано функціонують з метою захисту інформаційних ресурсів (інформації) та їх властивостей, а також такі що перешкоджають або унеможливлюють реалізації загроз та завданню збитків суб'єктам інформаційної діяльності. Основними завданнями інженерно-технічного захисту є попередження та протидія процесам розголошення, витоку, несанкціонованого доступу та інших форм незаконного втручання і спотворення інформаційних ресурсів.

Нормативно-правове забезпечення являє собою основу галузі ІБ та є двигуном для подальшого впровадження законодавчої бази до організаційних й інженерно-технічних засад. Організаційний захист забезпечує: організацію режиму й охорони об'єктів інформаційної діяльності, роботу з кадрами та організацію документообігу; розробку, впровадження й експлуатацію технічних засобів безпеки, інформаційно-аналітичну діяльність із виявлення внутрішніх і зовнішніх загроз підприємства (організації) тощо. Організаційні заходи відіграють суттєву роль у створенні надійного механізму захисту інформації, оскільки можливості несанкціонованого втручання в діяльність організацій значною мірою обумовлюються не тільки технічними аспектами, а ще і зловмисними діями порушника та недбалістю користувачів або персоналу. Впливу цих аспектів майже неможливо запобігти за допомогою традиційних інженерно-технічних заходів. У свою чергу, різноманітність цілей і завдань об'єктів захисту та заходів що провадяться, передбачає розгляд деякої системної класифікації засобів інженерно-технічного захисту за видом, орієнтацією та іншими характеристиками, що в подальшому приводить і до різноманіття класів загроз.

Комплексний підхід до питань ІБ потребує послідовної інтеграції сукупності організаційно-правових і організаційно-технічних методів і заходів, які забезпечують (або зводили до мінімуму вплив загроз) надійний захист інформаційних ресурсів у сучасних умовах розвитку інформаційного простору держави.

Наведені результати досліджень дозволяють встановити таку трійку другої платформи методу *подвійної трійки захисту*, платформи — технологій та процедур захисту інформаційних ресурсів, що є обов'язковою для реалізації політики і побудови різних видів систем безпеки. Зазначена трійка послідовно пов'язана від складової нормативно-правового до інженерно-технічного забезпечення ІБ, де кожний попередній елемент є основою для наступного.

Авторами запропоновано інформаційно-аналітичну модель методу *подвійної трійки захисту*, як основу формування методології з урахуванням складових процесу захисту інформаційних ресурсів.

Перша платформа 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.

Дана інформаційно-аналітична модель є підґрунтям для формування «Класифікатора загроз ДІР» з подальшим поділом класифікації за характером спрямованості та видом загроз. Функціональний профіль загрози визначено за процедурою дій порушника.

Таким чином, на основі проведених досліджень ЗДІР можна представити та безпосередньо визначити їх клас за характером спрямованості, через призму загальних напрямів забезпечення безпеки інформації (правовий захист, організаційний захист, інженерно-технічний захист), отримавши таку початкову класифікацію та методику кодування в цілому для ДІР (01; 02; 03 — базові коди класифікації загроз за спрямованістю, рис. 2), де:

– *загрози нормативно-правового спрямування (01)* — являють собою загрози, які виникають у 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 (02)* — 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 (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.

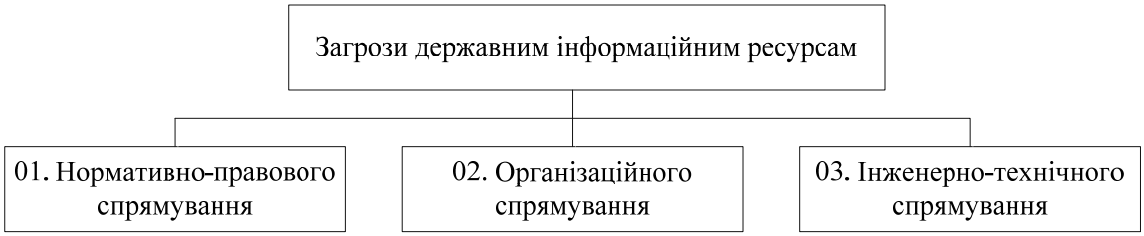

Рис. 2. Класифікація загроз ДІР за характером спрямування

Розглянемо докладніше *загрози ДІР нормативно-правового спрямування*.

Спираючись на підходи, які представлені згідно з чинним законодавством, що регламентує питання захисту інформаційних ресурсів (наприклад ті, що описані в Критеріях оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу, НД ТЗІ 2.5-004-99, затверджені наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28 квітня 1999 р. № 22 із змінами згідно з наказом Адміністрації Держспецзв'язку від 28.12.2012 № 806), а також загальноприйняті стандарти, технічні специфікації інші нормативно-правові документи, наведемо таку ітерацію для формування класу загроз відповідно до сегментів властивостей інформації.

Як приклад розглянемо процедуру класифікації загроз нормативно-правового спрямування, які сформовано за видами, відповідно до основних властивостей інформації (рис. 3).

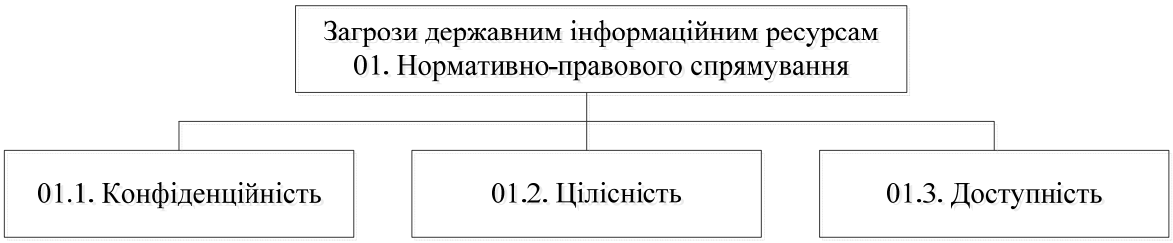

Рис. 3. Поділ загроз відповідно до основних властивостей інформації

Загрози конфіденційності виникають у результаті несанкціонованого копіювання, витоку та втрати ДІР і засобів їх обробки, а також — несанкціонованого використання ДІР користувачем або програмним забезпеченням, *загрози цілісності — в результаті* несанкціонованої модифікації, спотворення ДІР та нав'язування фальшивої інформації з метою порушення встановлених правил їх використання, *загрози доступності* — через блокування, знищення або несанкціонованого отримання ДІР та засобів їх обробки.

Проведений аналіз загроз представлений держаними нормативними документами, міжнародними та вітчизняними стандартами, приватними дослідженнями, а також особисті дослідження та попит авторів дають можливість сформувати перший перелік базових загроз ДІР нормативно-правового спрямування [1; 4; 7; 10; 11; 13–18; 24; 25].

До *основних загроз конфіденційності ДІР* можна віднести такі загрози:

– розголошення переліку відомостей, що становлять державну таємницю (або є власністю держави);

– витік ДІР іноземним фірмам та їхнім представництвам;

– несанкціоноване копіювання носіїв ДІР;

– недотримання вимог чинного законодавства щодо захисту та збереження ДІР;

– порушення положення про спеціальне діловодство та документообіг ДІР;

– порушення положення про збереження відомостей, що становлять державну таємницю (або є власністю держави);

– порушення режиму збереження ДІР;

– порушення норм конституційного законодавства;

– відсутність розробленого плану захисту ДІР в АС;

– відсутність наказу про створення комплексної системи захисту інформації (КСЗІ);

– відсутність акту проведення категорування АС, приміщення де проводиться обробка ДІР;

– відсутність наказу про створення комісії з проведення обстеження АС;

– відсутність розробленої моделі загроз та моделі порушника;

– невідповідність розробленої політики безпеки технічному завданню;

– відсутність технічного завдання на створення КСЗІ в АС та/або невідповідність нормам чинного законодавства;

– відсутність узгодження з Держспецзв'язком технічного завдання на створення КСЗІ в АС;

– відсутність контролю за навчанням користувачів АС з питань захисту ДІР;

– відсутність наказу про створення служби захисту інформації та положення про службу захисту інформації;

– відсутність системи управління інформаційною безпекою;

– відсутність системи оцінки ризику;

– комп'ютерна злочинність, комп'ютерний тероризм ^{к,ц,д};

– порушення встановленого регламенту збирання, обробки, зберігання і передачі інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України ^{к,ц,д};

– низький рівень інформатизації органів державної влади ^{к,ц,д,01,02,03};

– зниження наукового потенціалу в галузі інформатизації та зв'язку ^{к,ц,д,01,02,03};

– використання (шантаж, підкуп тощо) з корисливою метою персоналу, якій має доступ до ДІР ^{к,ц,д,01,02};

– крадіжки носіїв інформації, виробничих відходів (роздруків, записів тощо) ^{к,ц,д,01,02};

– відсутність створеної комплексної системи захисту інформації з підтвердженою відповідністю.

До *основних загроз цілісності ДІР* належать такі загрози:

– модифікація переліку відомостей, що дозволені до опублікування у відкритому вигляді відповідно до норм чинного законодавства;

– поширення в інформаційному просторі викривленої, недостовірної та упередженої інформації;

– комп'ютерна злочинність, комп'ютерний тероризм ^{к,ц,д};

– негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережу Інтернет;

– порушення встановленого регламенту збирання, обробки, зберігання і передачі інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України ^{к,ц,д};

– низький рівень інформатизації органів державної влади ^{к,ц,д,01,02,03};

– використання (шантаж, підкуп тощо) з корисливою метою персоналу, який має доступ до ДІР ^{к,ц,д,01,02};

– крадіжки носіїв інформації, виробничих відходів (роздруків, записів тощо) ^{к,ц,д,01,02}.

До *основних загроз доступності ДІР* можна віднести такі загрози:

– порушення положення про порядок доступу/допуску суб'єктів до відомостей, що становлять державну таємницю (або є власністю держави);

– знищення або блокування ДІР;

– комп'ютерна злочинність, комп'ютерний тероризм ^{к,ц,д};

– порушення встановленого регламенту збирання, обробки, зберігання і передачі інформації з обмеженим доступом в органах військового управління та на підприємствах оборонно-промислового комплексу України ^{к,ц,д};

– низький рівень інформатизації органів державної влади ^{к,ц,д,01,02,03};

– зниження наукового потенціалу в галузі інформатизації та зв'язку ^{к,ц,д,01,02,03};

– використання (шантаж, підкуп тощо) з корисливою метою персоналу, який має доступ до ДІР ^{к,ц,д,01,02};

– крадіжки носіїв інформації, виробничих відходів (роздруків, записів тощо) ^{к,ц,д,01,02}.

Позначками у верхньому індексі проставлені властивості інформації (к — конфіденційність, ц — цілісність, д — доступність) та те, що дані загрози відносяться і до інших спрямувань (02 — організаційного та 03 — інженерно-технічного спрямування).

Надалі кожну загрозу необхідно віднести:

– за джерелом загрози (антропогенні, техногенні, стихійні);

– за відношенням до інформаційного об'єкта (внутрішні, зовнішні);

– за характером загрози (навмисні, ненавмисні);

– за структурою впливу (системні, структурні, елементні);

– за рівнем впливу (фізичні засоби, мережеве обладнання, мережеві додатки та сервіси, операційна система, системи управління базами даних).

Далі введено класифікатор загроз ДІР.

Узагальнений класифікатор загроз ДІР являє собою перелік найсуттєвіших загроз по відношенню до захищених інформаційних систем та мереж, де оброблюються, передаються та зберігаються ДІР. Даний класифікатор будується на підставі аналізу існуючих уразливостей та джерел загроз ДІР .

Семантика класифікатора загроз ДІР

Опис класифікатора складається з чотирьох числових частин. Класифікатор включає: позначення спрямування загрози (01,02,03), позначення, що характеризує тип загроз (0х.1. конфіденційність, 0х.2. цілісність , 0х.3. доступність), позначення виду загрози залежно від типу (0х.1.х., 0х.2.х., 0х.3.х.), додаткова інформація про направленість загрози.

Всі частини класифікатора відділяються один від одного крапкою (рис. 4).

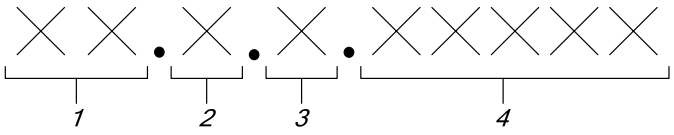

Рис. 4. Класифікатор загроз державним інформаційним ресурсам
(*1* — спрямування; *2* — тип; *3* — вид; *4* — додаткова інформація)

Приклад представлення класифікатора та системи кодування загроз ДІР нормативно-правового спрямування

На основі вищенаведеного можна скласти наступну (як приклад) класифікацію ДІР нормативно-правового спрямування (табл. 2).

Висновки

Отже, в статті визначені основні напрями аналізу створення класифікації загроз ДІР, які характеризують існуючі доктрини та закони України, що регламентують питання інформаційної безпеки України чи захист інформації, де є інформаційні ресурси; аналізу оцінних стандартів, які направлені на класифікацію інформаційних систем та засобів захисту за вимогами безпеки; аналізу технічних специфікацій, які регламентують різні аспекти реалізації засобів захисту, інших підходів. Наведено початкову класифікацію ДІР на основі трьох основних спрямувань захисту інформаційних ресурсів в АС (нормативно-правове спрямування, організаційне спрямування, інженерно-технічне спрямування), а також розкрито типи загроз нормативно-правового спрямування.

У статті вперше розроблено методологію побудови класифікатора загроз, принципи та методику представлення, семантику і систему кодування різних класів загроз ДІР, а також розроблено класифікатор для першого широкого класу загроз, сформованих на основі нормативно-правового спрямування.

ЛІТЕРАТУРА

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

2. *Yudin O.* The analysis of normatively-legal providing of defence of state informative resources in information-telecommunication systems / O. Yudin, S. Buchyk / Science-based technologies. — 2013. — № 2 (18) / Engineering Sciences. — P. 202–206.

3. *Юдін О. К.* Правові аспекти формування системи державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик / Безпека інформації. — 2014. — № 20 (1) / Технічні науки. — С. 76–82.

4. *Галатенко В. А.* Основы информационной безопасности / В. А. Галатенко. — [Електронный ресурс]. — Режим доступа: http://www.intuit.ru

5. *Юдін О. К.* Концептуальний аналіз уразливості державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Наукоємні технології. — 2013. — № 3 (19) / Технічні науки. — С. 299–304.

6. *Юдін О. К.* Аналіз загроз державним інформаційним ресурсам / О. К. Юдін, С. С. Бучик // Проблеми інформатизації та управління. — 2013. — № 4 (44) / Технічні науки. — С. 93–99.

7. *Марущак А. І.* Інформаційні ресурси держави: зміст та проблема захисту / А. І. Марущак // Правова інформатика. — 2009. — № 1. — С .64–70.

8. *Марущак А. І.* Щодо поняття «інформаційні ресурси держави» / А. І. Марущак // Інформаційна безпека людини, суспільства, держави. — 2009. — №1 (1). — С. 11–15.

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

10. *Вихорев С.* Классификация угроз информационной безопасности / С. Вихорев. — [Електронный ресурс]. — Режим доступа: http:// http://www.elvis.ru

11. *Касперский Е.* Основные классы угроз в компьютерном сообществе 2003 года, их причины и способы устранения, JetInfo, 2003 г. №12. — [Електронный ресурс]. — Режим доступа: http://jetinfo.isib.ru/2003/12/2/article2.12.2003.html

12. *Классификация* угроз Digital Security (Digital Security Classification of Threats). — [Електронный ресурс]. — Режим доступа: http://www.dsec.ru/products/grif/fulldesc/classification

13. *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).

14. *Термінологія* в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 1.1-003-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

15. *Загальні* положення з захисту інформації в комп'ютерних системах від НСД: НД ТЗІ 1.1-002-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

16. *Критерії* оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу: НД ТЗІ 2.5-004-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

Таблиця 2

Приклад класифікації загроз ДІР нормативно-правового спрямування

Спрямування загроз	Вид загроз	Функціональний профіль загроз	Додаткова інформація про направленість загрози														
			Джерело загроз			За відношенням до інформаційного об'єкта		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)	Мережеве обладнання	Мережеві додатки та сервіси	Операційна система	Система управління базами даних
01. Нормативно-правове спрямування	01.1. Конфіденційність	01.1.1. Розголошення переліку відомостей, що становлять державну таємницю (або є власністю держави)	1	0	0	1	0	1	0	1	0	0	0	0	0	0	1
		01.1.2. Витік ДІР іноземним фірмам та їхнім представництвам	1	0	0	0	1	1	0	1	0	0	0	0	0	0	1
		……	…	…	.	…	…	…	…	…	…	…	…	…	…	…	…
	01.2. Цілісність	01.2.1. Модифікація переліку відомостей, що дозволені до опублікування в відкритому вигляді відповідно до норм чинного законодавства	1	0	0	1	0	1	1	1	1	1	0	0	0	0	1
		01.2.2. Поширення у інформаційному просторі викривленої, недостовірної та упередженої інформації	1	0	0	1	1	1	0	1	1	1	0	0	0	0	1
		……	…	…	.	…	…	…	…	…	…	…	…	…	…	…	…
	01.3. Доступність	01.3.1. Порушення положення про порядок доступу/допуску суб'єктів до відомостей, що становлять державну таємницю (або є власністю держави)	1	0	0	1	0	1	0	1	0	0	0	0	0	0	1
		01.3.2. Знищення або блокування ДІР	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
		……	…	…	.	…	…	…	…	…	…	…	…	…	…	…	…

Примітка. 1 та 0 – віднесення (1) або не віднесення (0) даного виду загрози до подальших елементів класифікації.

17. *Класифікація* автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу: НД ТЗІ 2.5-005-99. — [Чинний від 1999.04.28]. — К. : ДСТСЗІ СБУ, 1999. — № 22. — (Нормативний документ системи технічного захисту інформації).

18. *Захист* інформації. Технічний захист інформації. Основні положення: ДСТУ 3396.0-96. — [Чинний від 1996.10.10]. — К. : Держстандарт України, 1996. — 20 с.

19. *Захист* інформації. Технічний захист інформації. Порядок проведення робіт: ДСТУ 3396.1-96. — [Чинний від 1997.07.01]. — К. : Держстандарт України, 1997. — 32 с.

20. *Захист* інформації. Технічний захист інформації. Терміни і визначення: ДСТУ 3396.2-97. — [Чинний від 1998.01.01]. — К. : Держстандарт України, 1998. — 20 с.

21. *Information* Security Management — Specification With Guidance for Use: ISO/IEC 27001:2005. — [Електронный ресурс]. — Режим доступа: http://www.standarts.-org/standarts/listing/iso_27001.

22. *Information* technology – Security techniques – Code of practice for information security management: ISO/IEC 27002: 2005. — [Електронный ресурс]. — Режим доступа: http://www.iso.org/iso/catalogue_detail?csnumber=39612.

23. *Information* technology – Security techniques – Information security risk management: ISO/IEC 27005:2008. — [Електронный ресурс]. — Режим доступа: http://www.iso.org/iso/catalogue_detail?csnumber=42107.

24. *Базовая* модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). Утверждена Заместителем директора ФСТЭК России от 15 февраля 2008 г. — [Електронный ресурс]. — Режим доступа: http://fstec.ru

25. *Классы* информационной безопасности в международных стандартах. — [Електронный ресурс]. — Режим доступа: http://www.arinteg.ru/articles/klassy-informatsionnoy-bezopasnosti-v-mezhdunarodnykh-standartakh-30970.html

Стаття надійшла до редакції 24.05.2014.