МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний авіаційний університет

О. К. ЮДІН, С. С. БУЧИК

ДЕРЖАВНІ ІНФОРМАЦІЙНІ РЕСУРСИ. МЕТОДОЛОГІЯ ПОБУДОВИ КЛАСИФІКАТОРА ЗАГРОЗ

Київ 2015

УДК 004.056.5:35.078.3(02)
ББК з 973.202-018.4
Ю 163

Рецензенти:

М. Є. Шелест — генерал-лейтенант, д-р техн. наук, проф.;

О. М. Новіков — д-р техн. наук, проф.,

О. В. Корнейко — генерал-майор, канд. техн. наук, проф.,

Рекомендовано до друку вченою радою Національного авіаційного університету (протокол № 2 від 18 березня 2015 року)

Юдін О. К.

Ю 163 Державні інформаційні ресурси. Методологія побудови класифікатора загроз : монографія / Юдін О. К., Бучик С. С. — К. : НАУ, 2015. — 214 с.

ISBN 978-617-7092-61-1

Проведено аналіз сучасного забезпечення захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах. Приділено значну увагу нормативно-правовому забезпеченню захисту державних інформаційних ресурсів. Докладно розкрито в авторській інтерпретації правові аспекти формування системи державних інформаційних ресурсів, а також введено нові терміни та визначення проблематики захисту державних інформаційних ресурсів.

Проведено аналіз та систематизовано підходи до класифікації загроз інформаційним ресурсам у цілому. Представлена методологія побудови класифікатора загроз державним інформаційним ресурсам на базі запропонованого методу «*подвійної трійки захисту*». Введено поняття загроз державним інформаційним ресурсам, зміст, класифікація та розкрито їх функціональні профілі відповідно до розробленого класифікатора за певними спрямуванням системи захисту.

Розкрито місце українського сегменту ідентифікаторів об'єктів, вказано перспективи подальшого його розвитку. В монографії проведено нормативно-правовий аналіз напрямів, пов'язаних із впровадженням реєстру державних електронних інформаційних ресурсів, досліджено шляхи подальшої реалізації проблематики.

УДК 004.056.5:35.078.3(02)
ББК з 973.202-018.4

ISBN 978-617-7092-61-1

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

АС — автоматизована система
АТС — автоматична телефонна станція
ДЕІР — державні електронні інформаційні ресурси
ДІР — державні інформаційні ресурси
ЕОМ — електронна обчислювальна система
ЗДІР — загроза державним інформаційним ресурсам
ЗІ — захист інформації
ЗК — загальні критерії
ІБ — інформаційна безпека
ІКС — інформаційно-комунікаційна система
ІКСМ — інформаційно-комунікаційна система та мережа
ІО — ідентифікатор об'єкта
ІР — інформаційний ресурс
ІС — інформаційна система
ІТ — інформаційна технологія
ІТС — інформаційно-телекомунікаційна система
КЗІ — комплексний захист інформації
КЗЗ — комплекс засобів захисту
КС — комп'ютерна система
КСЗІ — комплексна система захисту інформації
ЛОМ — локальна обчислювальна мережа
МККТТ — Міжнародний консультативний комітет з телефонії і телеграфії
НД — нормативний документ
НД КЗІ — нормативний документ криптографічного захисту інформації
НД ТЗІ — нормативний документ технічного захисту інформації
НІР — національні інформаційні ресурси
НПА — нормативно-правовий акт
НПБ — нормативно-правова база
НПЗ — нормативно-правове забезпечення
НРО — Національний реєструючий орган
НСД — несанкціонований доступ
НСКЗ — національна система конфіденційного зв'язку
ОО — об'єкт оцінки
ОС — обчислювальна система

ПЗ — програмне забезпечення
РЕІР — реєстр електронних інформаційних ресурсів
РС — робоча станція
СПД — система передавання даних
ТЗІ — технічний захист інформації
ФП ЗДІР— функціональний профіль загроз державним інформаційним ресурсам
ЦАЗІ — Центр антивірусного захисту інформації

ASN.1 — Abstract Syntax Notation One
CTCPEC — Canadian Trusted Computer Product Evaluation Criteria
DSECCT — Digital Security Classification of Threats
FCITS — Federal Criteria for Information Technology Security
GIG — Global Information Grid
ITSEC — Information Technology Security Evaluation Criteria
OID — object identifier
OSI — Open Systems Interconnection.

МЕТОДОЛОГІЯ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ. ПОРІВНЯЛЬНИЙ АНАЛІЗ ОСНОВНИХ ТЕРМІНІВ ТА ВИЗНАЧЕНЬ

Визначення згідно з керівними документами	**Визначення, введені авторами**
1. Державні інформаційні ресурси	
Державні інформаційні ресурси — інформація, яка є власністю держави та необхідність захисту якої визначено законодавством [1]. *Державні інформаційні ресурси* — систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить державним органам, військовим формуванням, утвореним відповідно до законів України, державним підприємствам, установам та організаціям, а також інформація, створення якої передбачено законодавством та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень [2].	*Державні інформаційні ресурси (state informative resources)* — це результати інтелектуальної та практичної діяльності, що сформовані в усіх сферах життєдіяльності людини, суспільства і держави, зафіксовані і систематизовані на відповідних матеріальних носіях інформації, як окремі документи і масиви документів, банки і бази даних та знань, усі види архівів і бібліотек, музейні фонди, інформаційні ресурси які обробляються й передаються в інформаційних системах державного і/або загального призначення, інші ресурси, що містять дані, відомості і знання які є об'єктом права власності держави незалежно від форми власності на час їх створення і мають споживчу цінність, а також такі, що призначені для розвитку і задоволення потреб громадян, суспільства, держави та підлягають захисту згідно з визначеною політикою безпеки й чинним законодавством [3].
2. Загроза державним інформаційним ресурсам	
Введено вперше	*Загроза державним інформаційним ресурсам* (*threat to the state informative resources*) — протиправні дії, які можуть призвести

Визначення згідно з керівними документами	Визначення, введені авторами
	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 [4].
Більш розширене поняття	*Загроза державним інформаційним ресурсам (threat to the state informative resources)* — це потенційний або реальний стан небезпеки державних інформаційних ресурсів та безпосередньо їх властивостей (конфіденційності, цілісності, доступності), який може бути сформовано на основі реалізації будь-якого процесу та/або вчиненні діяння (та/або бездіяльності), спрямовано на порушення політики безпеки об'єкта інформаційної діяльності (державних інформаційних ресурсів) та такий, що завдає збитку державі [4].
3. Національні інформаційні ресурси — введено вперше з урахуванням доповнення поняття «національні ресурси»	
Національні ресурси — ресурси незалежно від їх змісту, форми, часу та місця створення, форми власності, призначені для задоволення потреб громадянина, суспільства, держави. Національні ресурси включають державні, комунальні та приватні ресурси [5].	*Національні інформаційні ресурси* (*national informative resources*) — це результати інтелектуальної діяльності в усіх сферах життєдіяльності людини, суспільства і держави, зафіксовані на відповідних матеріальних носіях інформації як окремі документи і масиви документів, бази і банки даних та знань, усі види архівів, бібліотеки, музейні фонди тощо, які містять

Визначення згідно з керівними документами	Визначення, введені авторами
	дані, відомості і знання, що є об'єктом права власності будь-якого суб'єкта України і мають споживчу цінність (політичну, економічну, наукову, освітню, соціокультурну, оборонну, ринкову, історичну, інформаційну тощо) [3].
4. Національні електронні інформаційні ресурси — введено вперше	
Введено вперше	*Національні електронні інформаційні ресурси (national electronic informative resources)* — інформаційні ресурси незалежно від їх змісту, форми, часу та місця створення, форми власності, які існують та використовуються в електронному вигляді та призначені для задоволення потреб громадянина, суспільства, держави. Національні електронні ресурси включають державні, комунальні та приватні ресурси [3].
5. Система національних інформаційних ресурсів — введено вперше з урахуванням доповнення поняття «система національних ресурсів»	
Система національних ресурсів — організована за єдиною технологією сукупність національних ресурсів, необхідних для розв'язання завдань соціально-економічного розвитку держави та внесених до Національного реєстру електронних інформаційних ресурсів [5].	*Система національних інформаційних ресурсів (system of national informative resources)* — організована за єдиною технологією сукупність національних ресурсів, необхідних для розв'язання завдань соціально-економічного розвитку держави та внесених до Національного реєстру електронних інформаційних ресурсів; реєстр ресурсів — сукупність даних, упорядкованих для обліку і реєстрації ресурсів [3].

Визначення згідно з керівними документами	Визначення, введені авторами
6. Система державних інформаційних ресурсів — введено вперше	
Введено вперше	*Система державних інформаційних ресурсів (system of state informative resources)* — це організований державою упорядковано-інтегрований комплекс організаційно-технічних, нормативно-правових технологій, методів і заходів, а також взаємозв'язана і погоджено-функціонуюча сукупність суб'єктів інформаційної діяльності (державних, суспільства та окремих громадян), об'єднаних цілями й завданнями щодо формування, накопичення, збереження, достовірного оброблення, передавання, висвітлення та захисту державних інформаційних ресурсів у межах чинного законодавства України [3].
7. Державні електронні інформаційні ресурси — авторами здійснено уточнення та доповнення	
Державні електронні інформаційні ресурси — відображена та задокументована в електронному вигляді інформація, необхідність захисту якої визначено законодавством [6].	*Державні електронні інформаційні ресурси (state electronic informative resources)* — державні інформаційні ресурси незалежно від їх змісту, форми, часу і місця створення, які існують та використовуються в електронному вигляді та призначені для задоволення потреб громадян, суспільства, держави. Державні електронні інформаційні ресурси є складовою Національного реєстру електронних інформаційних ресурсів [3].

Визначення згідно з керівними документами	**Визначення, введені авторами**
8. Реєстр електронних державних інформаційних ресурсів — введено вперше	
Національний реєстр — це інформаційно-телекомунікаційна система, призначена для реєстрації, обліку, накопичення, оброблення і зберігання відомостей про склад, зміст, розміщення, умови доступу до електронних інформаційних ресурсів та задоволення потреб юридичних і фізичних осіб в інформаційних послугах [7].	*Реєстр електронних державних інформаційних ресурсів (register of electronic state informative resources)* — інформаційна система, призначена для реєстрації, обліку, накопичення, оброблення та зберігання відомостей про склад, зміст, умови доступу до електронних державних інформаційних ресурсів, розміщених у Національному депозитарії та такі, що мають споживчу цінність, а саме: політичну, економічну, наукову, освітню, соціокультурну, оборонну, ринкову, історичну, інформаційну тощо [3].
9. Депозитарій електронних державних інформаційних ресурсів — введено вперше	
Введено вперше	*Депозитарій електронних державних інформаційних ресурсів (depositary of electronic state informative resources)* — інформаційна система державних електронних інформаційних ресурсів, створена на базі автоматизованих систем та погоджено функціонуючих прог-рамно-апаратних комплексів, що забезпечують збір, облік, аудит, зберігання, оновлення, захист і доступ до електронних державних інформаційних ресурсів на основі інформаційних технологій та інформаційно-комунікаційних систем згідно з визначеною політикою безпеки та чинним законодавством [3].

Визначення згідно з керівними документами	Визначення, введені авторами
10. Атака на державні інформаційні ресурси — введено вперше	
Введено вперше	*Атака на державні інформаційні ресурси (attack, are on state informative resources)* — це можливі наслідки реалізації загрози державним інформаційним ресурсам, що сформовані на основі взаємодії джерела загрози через наявні фактори уразливості об'єкта інформаційної діяльності та такі, що призводять до різних видів збитків державі [8].
11. Метод подвійної трійки захисту — введено вперше	
Введено вперше	*Метод подвійної трійки захисту (method of double three of security)* — визначає базові характеристики класифікації загроз для різних видів та розподіляє їх за базовими принципами: характером спрямованості, рівнем загрози, видом загрози та її функціональним профілем. Інформаційно-аналітична мо-дель складається з двох платформ: *перша платформа ІБ* — складові, що підлягають захисту (власти-вості інформації): конфіденційність; цілісність; доступність; *друга платформа ІБ* — складові, що реалізують систему захисту (методи та засоби): нормативно-правові; організаційні; інженерно-технічні [9].
12. Загрози нормативно-правового спрямування — авторами здійснено уточнення та доповнення щодо безпосередньо прив'язки до поняття загрози, введено вперше в такій постановці	
Нормативно-правове забезпечення інформаційної без-	*Загрози нормативно-правового спрямування (threat of normatively-*

Визначення згідно з керівними документами	Визначення, введені авторами
пеки — 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 ді-яльності (державних органів, підприємств, організацій та населення (окремої особис-тості) [10].	*legal aspiration)* — це 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 [9].
13. Загрози організаційного спрямування — авторами здійснено уточнення та доповнення щодо безпосередньо прив'язки до поняття загрози, введено вперше в такій постановці	
Організаційне забезпечення інформаційної безпеки — 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 (у тому числі галузі і підприємства) [10].	*Загрози організаційного спрямування (threat of organizational aspiration)* — 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) [9].

Визначення згідно з керівними документами	Визначення, введені авторами
14. Загрози інженерно-технічного спрямування — авторами здійснено уточнення та доповнення щодо безпосередньо прив'язки до поняття загрози, введено вперше в такій постановці	
Інженерно-технічне забезпечення інформаційної безпеки — 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 [10].	*Загрози інженерно-технічного спрямування (threat of technical aspiration)* — загрози, що 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 [9].
15. Ідентифікатор об'єкта — авторами здійснено уточнення та доповнення	
Ідентифікатор об'єкта — значення, що відрізняється від інших подібних значень, яке пов'язується з інформаційним об'єктом і є упорядкованим списком первинних цілочислових значень від кореня (Root) міжнародного дерева ідентифікаторів об'єктів до вершини, який однозначно ідентифікує цю вершину [11].	*Ідентифікатор об'єкта (identifier of object)* — значення вузла, що відрізняється від інших подібних значень та логічно пов'язується з інформаційним об'єктом, унікально його визначає та однозначно ідентифікує як вузол дерева міжнародних ідентифікаторів об'єктів. Список значень вузлів дерева (Root) є впорядкованою послідовністю первинних цілих значень, що починаються від кореня міжнародного дерева до вершини або/чи вузла ідентифікації [12].

ВСТУП

Актуальність теми монографії. Рівень інформаційного суспільства провідної держави світу характеризується показниками сучасних наукоємних технологій, а також роллю, що відіграють інформаційно-телекомунікаційні системи (ІТС) щодо інтеграції державних інформаційних ресурсів у всі сфери життєдіяльності країни та суспільства. Розвиток сучасних комунікаційних відносин в інформаційному просторі держави, сукупність політичних, економічних, військових і соціальних рішень у країні залежить від взаємодії та спільного використання інформаційних потоків загального й спеціального призначення.

Отже, подальший розвиток національної безпеки і оборони держави, досягнення стратегічних цілей можливо реалізувати тільки на основі сучасних інфраструктур між різними відомчими і міжрегіональними рівнями, об'єднаних у єдиний інформаційно-телекомунікаційний простір з динамічним розподілом функцій управління. Зазначений простір повинен забезпечити інформаційну й функціональну взаємодію окремих державних структур, міністерств, відомств між собою в інтегрованому процесі впровадження, використання та висвітлення інформаційних ресурсів держави.

Гостра необхідність інформатизації системи управління, створення баз даних та знань державних інформаційних ресурсів (ДІР) зумовлена сьогодні, насамперед, проведенням в державі нової економічної політики, зростанням кількості техногенних катастроф, загостренням військової агресії з боку інших держав. Зазначимо, що безпосередньо інформаційна війна як соціально-технічний інструмент стала важливою частиною військово-політичного втручання інших держав у життєві процеси України.

Сучасний етап розвитку нашої країни визначається політичною, економічною, соціальною нестабільністю та дестабілізацією суспільних факторів та відносин на платформі реалізації великого спектра напрямів ведення інформаційних війн.

Значну роль у протидії інформаційній війні слід приділяти захисту державних інформаційних ресурсів на основі сформованої інформаційної політики країни та впровадженню комплексного підходу до побудови систем захисту. Нормативно-правові акти та питання створення політики безпеки, моделі загроз, моделі поруш-

ника, профілів захисту ДІР в Україні не сформовані або розглядались дуже загально. Загрози інформаційній безпеці держави відіграють базову роль щодо формування політики та самої системи захисту. За своєю загальною спрямованістю до загроз інформаційній безпеці України згідно з чинним законодавством можна віднести:

- загрози інформаційному забезпеченню державної політики України;
- загрози розвитку вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікації і зв'язку, а також забезпеченню накопичення, зберігання й ефективного використання вітчизняних інформаційних ресурсів;
- загрози безпеці інформації обмеженого доступу, зокрема державній таємниці;
- загрози безпеці інформаційних і телекомунікаційних засобів і систем;
- монополізація інформаційного ринку України;
- блокування діяльності державних засобів масової інформації з інформування громадськості в Україні та за її межами;
- протиправне збирання і використання інформації;
- порушення технології обробки інформації;
- впровадження в апаратні і програмні вироби компонентів, що реалізують функції, не передбачені політикою безпеки;
- розробка і поширення програм, що порушують нормальне функціонування інформаційних та інформаційно-телекомунікаційних систем, у тому числі систем захисту інформації;
- радіоелектронний вплив з метою виведення з ладу, пошкодження чи руйнування засобів і систем обробки інформації, телекомунікації і зв'язку;
- вплив на парольно-ключові системи захисту автоматизованих систем обробки і передачі інформації;
- перехоплення інформації в мережах передачі даних та лініях зв'язку, дешифрування цієї інформації і нав'язування хибної інформації;
- використання не сертифікованих вітчизняних і закордонних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікації і зв'язку під час створення і розвитку інформаційної інфраструктури України;

- несанкціонований доступ до інформації, що знаходиться в банках і базах даних;
- порушення законних обмежень на поширення інформації тощо.

Однак на сьогодні, на жаль, відсутня чітка класифікація загроз ДІР, їх визначення, пріоритетність, функціональність профілів тощо.

Нині важливо мати науково обґрунтований перехід до нових методологій і технологій побудови сучасних інформаційних систем ДІР, їх класифікації, опису, кодифікації з метою організації ефективного управління в умовах сталих процесів або в кризових ситуаціях.

Зазначимо, що в даному випадку повинна досягатися основна мета створення інформаційної системи ДІР та концепції її захисту — забезпечення стійкого функціонування різних галузей на зовнішньому й внутрішньому ринку послуг, а також підвищення обороноздатності та національної безпеки країни. Оперативне управління, обробка, використання, висвітлення ДІР у цих умовах здобуває важливе тактичне та стратегічне значення. Від якісного, оперативного представлення, надійної організації системи вільного або авторизованого доступу до електронних ДІР залежить стабілізація роботи різноманітних структур країни, а також широке коло завдань національної безпеки.

Ідея створення «Класифікатора загроз ДІР» виникла в авторів на основі вивчення та адаптації стандартів серії ISO 27001 до вітчизняних умов і стандартів. Так, система менеджменту захисту інформації (ISO 27001) являє собою частину загальної системи менеджменту, що заснована на підході ділових ризиків. Це, у свою чергу, обумовлює створення каталогів загроз інформаційній безпеці, які в організації є закритими для загального користування (відносяться до інформації з обмеженим доступом). У зв'язку із цим, виникає логічна необхідність створення такого каталогу загроз державним інформаційним ресурсам. Дослідження показали декілька глобальних недоліків вітчизняної нормативно-правової системи в галузі інформаційної безпеки держави.

1. Відсутність змісту і визначень на нормативно-правовому рівні: електронні ДІР, депозитарій та репозитарій ДІР, система ДІР країни, загрози ДІР та їх зміст і класифікація, модель порушника ДІР тощо.

2. Відсутність класифікатора ресурсів та класифікатора загроз ДІР, а також їх кодифікатора згідно з вітчизняною та світовою системою кодифікації електронних ресурсів тощо.

Аналізуючи основні напрямки забезпечення інформаційної безпеки (ІБ), одним із елементів якої є державні інформаційні ресурси, можна дійти висновку, що для забезпечення комплексного захисту основних властивостей інформації (конфіденційності, цілісності, доступності) від загроз у сучасних ІТС обов'язково відокремлюють такі основні напрями захисту інформації: правовий захист, організаційний захист, інженерно-технічний захист. Це, у свою чергу, вказує шлях щодо аналізу та подальшої розробки методологічних основ захисту ДІР.

У Законі України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 р. № 3475-IV визначено термін *державні інформаційні ресурси* [1]. В редакції Закону № 1194-VII від 09.04.2014 р. [2] було відкориговано дане визначення, але не зовсім повне і вимагає подальшого удосконалення.

Загалом, аналіз нормативно-правових актів щодо захисту ДІР в ІТС свідчить про малосистемний характер відповідної діяльності. Не повною мірою визначені загрози ДІР (зокрема відсутнє саме визначення), що робить актуальним питання розробки їх класифікатора загроз, де будуть визначені основні загрози та запропоновані певні функціональні профілі загроз.

У зв'язку із цим виникає *протиріччя* між наявними ДІР, які постійно тільки зростають, та не до кінця визначеною термінологією (відсутність єдиного стандарту), необхідністю внесення змін у законодавчу базу, відсутністю моделі порушника та відповідно до дієвої методології оцінки ступеня захищеності ДІР, не деталізовані їх загрози, що у свою чергу, обумовлює актуальність проведення досліджень у цьому напрямку.

Таким чином, подолання вищезазначених труднощів, що виникають під час організації захисту ДІР, є актуальною проблемою, яка не може бути до кінця ефективно вирішена відомими методами і засобами і потребує постійного пошуку нових рішень.

Отже, існує важлива науково-технічна проблема підвищення ефективності організації захисту ДІР, для вирішення якої необхідна розробка методологічних основ побудови та захисту ДІР, одним із напрямків якого є розробка їх класифікатора загроз.

Зв'язок роботи з науковими програмами, планами, темами. Монографія розроблена відповідно до планів науково-дослідних робіт кафедри комп'ютеризованих систем захисту інформації Інституту комп'ютерних інформаційних технологій Національного авіаційного університету.

Мета і завдання дослідження. Мета дослідження монографії — підвищення ефективності захисту ДІР на базі розробки методології побудови класифікатора загроз та його представлення згідно з українським сегментом ідентифікаторів світової системи кодифікації інформаційних об'єктів.

Для досягнення мети в монографії вирішуються такі завдання:

– аналіз нормативно-правового забезпечення захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах;

– аналіз уразливості державних інформаційних ресурсів;

– створення правових аспектів формування системи державних інформаційних ресурсів;

– створення теоретичних засад щодо термінології та визначення загроз державним інформаційним ресурсам;

– розробка методології побудови класифікатора загроз державним інформаційним ресурсам;

– розробка класифікації загроз державним інформаційним ресурсам нормативно-правового, організаційного та інженерно-технічного спрямування;

– Аналіз світового простору ідентифікаторів об'єктів, місце українського сегменту в ньому;

– створення теоретичних засад щодо нормативно-правового забезпечення, змісту та визначення реєстру електронних інформаційних ресурсів;

– розробка пропозицій щодо організації ієрархічної гілки кодів вузлів українського сегменту міжнародного дерева ідентифікаторів об'єктів.

Об'єкт дослідження — процеси захисту державних інформаційних ресурсів, а також їх класифікації, збору, висвітлення, кодифікації.

Предмет дослідження — методології, методи і моделі побудови та захисту українського сегменту ідентифікаторів об'єктів державних інформаційних ресурсів.

Методи дослідження. Для дослідження та розробки класифікатора загроз державним інформаційним ресурсам використовуються методи, моделі та положення системного аналізу, складності систем, експертного оцінювання, методи та засоби захисту інформаційних ресурсів тощо.

Наукова новизна отриманих результатів полягає в подальшому розвитку теорії та розробці методології побудови та захисту державних інформаційних ресурсів шляхом побудови їх класифікатора загроз та внесення пропозицій щодо подальшого створення українського сегменту дерева ідентифікаторів об'єктів.

Основні наукові результати, отримані авторами:

– уперше запропоновано метод «подвійної трійки» захисту державних інформаційних ресурсів, що надає можливість для подальшого розвитку нормативної бази з даного питання, а також лягло в основу побудови класифікатора їх загроз;

– дістала подальший розвиток термінологія в галузі захисту інформації. Було введено такі більш розширені поняття: «державні інформаційні ресурси», державні електронні інформаційні ресурси, ідентифікатор об'єкта;

– вперше введена така термінологія в галузі захисту інформації: загроза державним інформаційним ресурсам, національні інформаційні ресурси, національні електронні інформаційні ресурси, система національних інформаційних ресурсів, система державних інформаційних ресурсів, реєстр електронних державних інформаційних ресурсів, депозитарій електронних державних інформаційних ресурсів, атака на державні інформаційні ресурси;

– здійснено уточнення та доповнення щодо безпосередньо прив'язки до поняття загрози, введено вперше в такій постановці поняття: «загрози нормативно-правового спрямування», загрози організаційного спрямування, загрози інженерно-технічного спрямування, що дає напрямок та основу для створення НД ТЗІ «Термінологія в галузі захисту державних інформаційних ресурсів» та виділення в окремий напрямок даного питання;

– вперше розроблено методологію побудови класифікатора загроз ДІР згідно зі світовим деревом ідентифікаторів.

Практичне значення отриманих результатів. Розроблений класифікатор загроз державних інформаційних ресурсів дозволяє підвищити ефективність захисту ДІР на базі впровадження різних

класів загроз їх функціональних профілів шляхом побудови моделі порушника та застосування відповідно методів та засобів захисту.

Апробація результатів монографії. Матеріали, які викладені в монографії, доповідались та обговорювались на таких симпозіумах, конференціях та семінарах.

1. IX Mezinarodni vedecko-prakticka conference «Predni vedecke novinky — 2013», 27.08.2013–05.09.2013, Pracha, Česká republika [13].

2. IX Международна научна практична конференция «Новини на научния прогрес — 2013», 17.08.2013–25.08.2013, София, Република България [14].

3. IV Міжнародна науково-технічна конференція ITSEC (20–23 травня 2014, Київ, Україна) [15].

4. X Mezinarodni vedecko-prakticka conference «Aktualni vymozenosti vedy — 2014», 27.06.2014 — 30.06.2014, Pracha, Česká republika [16].

5. X Miedzynarodowej naukowi-praktycznej konferencji «Dynamika naukowych badan — 2014», 07–15 lipca 2014 roku, Przemysl, Polska [17].

6. The XI Internathional research and practice conference «Modern european science — 2014», June 30–July 7, 2014, Sheffield, UK [18].

7. XX Всеукраїнська науково-практична конференція «Проблеми створення, розвитку та застосування високотехнологічних систем спеціального призначення», 28 листопада 2014 року, Житомир, Україна [19].

8. The XI Internathional research and practice conference «Fundamental and science — 2014», October 30–November 7, 2014, Sheffield, UK [20].

9. X Miedzynarodowej naukowi-praktycznej konferencji «Perspektywiczne opracowania sa nauka i technikami — 2014», 07–15 listopada 2014 roku, Przemysl, Polska [21].

10. X Международна научна практична конференция, «Бъдещего въпроси от света на науката — 2014», 17–25 декември, 2014, София, Республика България [22].

11. Науково-технічна конференція «Інформаційна безпека України» 12–13 березня 2015 року, Київ, Україна [23].

12. XII Міжнародна науково-технічна конференція «АВІА–2015», 28–29.04.2015 року, Київ, Україна [24].

13. XVII Міжнародна науково-практична конференція «Безпека інформації у інформаційно-телекомунікаційних системах» 26–28.05.2015 року, Київ, Україна [25].

14. IV Міжнародна науково-технічна конференція «Захист інформації і безпека інформаційних систем», 04–05.06.2015 року, Львів, Україна [26].

Публікації. За темою монографії опубліковано 27 наукових робіт, у тому числі 12 статтей у науково-технічних фахових виданнях, з них 8 — у виданнях України, що входять до наукометричних баз даних, та 15 тез доповідей у збірниках матеріалів конференцій. Опубліковані результати охоплюють усі положення, які виносяться в монографії.

Структура й обсяг монографії. Монографія складається з переліку умовних скорочень, основних термінів та визначень, які введені авторами, вступу, трьох глав і чотирьох додатків. Загальний обсяг роботи становить 214 сторінок друкованого тексту, 37 рисунків, 9 таблиць і список використаної літератури з 125 найменувань.

Розділ 1

АНАЛІЗ ІСНУЮЧОГО ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ В ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМАХ

1.1. Аналіз нормативно-правового забезпечення захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах

Аналізуючи основні напрями забезпечення інформаційної безпеки в цілому [10], елементом якої є державні інформаційні ресурси (ДІР), можна зробити висновок, що для забезпечення комплексного захисту інформації (КЗІ) від загроз відокремлюють такі основні напрями захисту інформації: правовий, організаційний, інженерно-технічний.

Вивчаючи поняття нормативно-правового забезпечення (НПЗ) в цілому, можна надати визначення щодо поняття *нормативно-правового забезпечення захисту ДІР*, під яким слід розуміти сукупність правових норм, які визначають порядок створення, правовий статус і функціонування захищених інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем (далі ІТС), регламентують порядок одержання, перетворення та використання інформації та інформаційних ресурсів, які є власністю держави.

Отже, нормативно-правове забезпечення регламентує та визначає порядок захисту встановлених політикою безпеки властивостей інформації (конфіденційності, цілісності та доступності) під час створення та експлуатації інформаційної мережі; регламентує порядок ефективного знешкодження і попередження загроз для ресурсів шляхом побудови комплексної системи захисту інформації (КСЗІ); статус інформаційної системи (ІС) з погляду інформаційної безпеки (ІБ); права, обов'язки й відповідальність персоналу роботи яких пов'язані з ІБ; правові положення окремих видів процесу керування та управління доступом у захищених ІТС; порядок створення й використання захищених ІТС; етапи побудови ІТС [10; 27; 28; 29].

Це у свою чергу вказує шлях щодо аналізу та подальшої розробки методологічних основ оцінки захищеності ДІР, побудови КСЗІ, яка повинна включати заходи та засоби, що реалізують способи, методи, механізми захисту інформації (ЗІ) від:

– витоку інформації технічними каналами;

– несанкціонованих дій та несанкціонованого доступу (НСД) до інформації;

– спеціального впливу на інформацію.

Зрозуміло, що вимоги до функціонального складу комплексу засобів захисту (КЗЗ) ДІР будуть залежати також як і для автоматизованих систем (АС) від характеристики оброблюваної інформації, обчислювальних систем (ОС), фізичного середовища, персоналу і організаційної підсистеми. Таким чином, основною метою всіх заходів щодо забезпечення захисту ДІР є убезпечення безпеки інформації під час її оброблення в ІТС.

Отже, вивчення та подальше удосконалення одного з основних напрямів ЗІ — правового захисту відносно до ДІР — актуальне.

Дослідження НПЗ ІБ в цілому розглядались у роботах А. І. Марущака, М. Я. Швеця, В. М. Богуша, А. Г. Корченка, О. В. Бойченка та ін. Але саме аналізу НПЗ захисту ДІР приділялось уваги не багато, особливо це стосується побудови певної загальної (на основі існуючої нормативно-правової бази та пропозицій щодо її покращення) системи.

Проаналізуємо наявність поняття ДІР в основних нормативно-правових актах (НПА). Вперше офіційно поняття ДІР в Україні з'явилося у Законі України «Про захист інформації в інформаційно-телекомунікаційних системах», де в ст.10 щодо повноваження державних органів у сфері захисту інформації вказано, що вони здійснюють заходи щодо виявлення загроз *державним інформаційним ресурсам* від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дають рекомендації з питань запобігання таким загрозам.

Можна зробити висновок, що для побудови ефективної КСЗІ необхідно: виявити можливі загрози та надати рекомендації щодо їх запобігання.

З часом був виданий Указ Президента України «Про заходи щодо захисту інформаційних ресурсів держави» від 10.04.2000 р., яким у складі Служби безпеки України як орган державного управління створено Департамент спеціальних телекомунікаційних систем та захисту інформації, якому доручено реалізацію державної політики у сфері захисту *державних інформаційних ресурсів* у мережах передавання даних, криптографічного та технічного захисту інформації. Таким чином був створений орган виконавчої влади,

якому доручено питання реалізації державної політики щодо захисту ДІР.

У подальшому необхідно було вирішувати питання, яке б регулювало певний порядок здійснення захисту ДІР. Таким НПА став Наказ новоствореного Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України «Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах» № 76 від 24.12.2001 р., який був чинний більше п'яти років (*втратив чинність Наказом того ж Департаменту від 16.06.2006 р. №74*), у якому вперше з'являється визначення поняття «державні інформаційні ресурси», яке буде наведено нижче.

Надалі поняття ДІР можна прослідкувати в Постанові КМУ від 16 листопада 2002 р. №1772 «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту ДІР в інформаційних та телекомунікаційних системах», яка визначає механізм взаємодії органів виконавчої влади з питань захисту ДІР в ІТС. У цьому ж НПА визначено, що органи виконавчої влади з метою захисту ДІР в ІТС:

– визначають перелік інформаційних та телекомунікаційних систем, які містять ДІР, та погоджують його з Адміністрацією Держспецзв'язку;

– здійснюють згідно з вимогами НПА з питань ЗІ під методичним керівництвом Адміністрації Держспецзв'язку заходи щодо захисту ДІР в ІТС, у тому числі підключених до глобальних мереж передавання даних;

– збирають, узагальнюють та аналізують інформацію про вчинення несанкціонованих дій і здійснюють заходи щодо усунення їх наслідків; невідкладно (протягом доби) інформують Адміністрацію Держспецзв'язку про спробу вчинення чи вчинення несанкціонованих дій;

– надають на запит Адміністрації Держспецзв'язку інформацію про технічні та програмні засоби, що використовуються для надання мережевих послуг, а також про зміни у способах або видах підключення до глобальних мереж передавання даних;

– оновлюють за рекомендаціями Адміністрації Держспецзв'язку антивірусні програмні засоби, використовуючи при цьому лише ті з них, які пройшли державну експертизу.

Нарешті, в Законі України «Про Державну службу спеціального зв'язку та захисту інформації України» від 23 лютого 2006 р.

№ 3475-IV, остаточно визначено термін «державні інформаційні ресурси», які являють собою інформацію, яка є власністю держави та необхідність захисту якої визначено законодавством (***надалі буде запропоновано нове визначення ДІР, яке було впроваджено в 2014 р. та внесені відповідні зміни до наведеного закону України***). В цьому законі, в ст. 16, прописані обов'язки Державної служби спеціального зв'язку та захисту інформації України щодо ДІР, які полягають у:

- розробленні порядку та вимог щодо захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах криптографічного та технічного захисту інформації, яка є власністю держави, або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом;
- методичному керівництві та координації діяльності органів державної влади, органів місцевого самоврядування, військових формувань, підприємств, установ і організацій незалежно від форм власності у сфері криптографічного та технічного захисту інформації, а також з питань, пов'язаних із запобіганням вчиненню порушень безпеки інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, виявленням та усуненням наслідків інших несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах;
- накопиченні та аналізу даних про вчинення та/або спроби вчинення несанкціонованих дій щодо державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, а також про їх наслідки, інформування правоохоронних органів для вжиття заходів із запобігання та припинення злочинів у зазначеній сфері;
- оцінюванні стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, надання відповідних рекомендацій;
- погодженні проектів нормативно-правових актів з питань захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах;
- здійсненні технічного регулювання у сферах захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

Нарешті, в результаті подальшого удосконалення НПЗ захисту ДІР розробляються «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», затверджені Постановою КМУ від 29.03.2006 р. № 373, які визначають загальні вимоги та організаційні засади забезпечення захисту державних інформаційних ресурсів або інформації (вимога щодо захисту якої встановлена законом) в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Дані Правила прийшли на зміну Наказу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України «Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах» № 76 від 24.12.2001 р.

Досліджуючи проблему захисту ДІР в ІТС, наступним важливим правовим документом, який регламентує порядок захисту, стає безпосередньо «Порядок оцінки стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах», введений у дію в 2008 р. Даний НПА регламентує правові та організаційні засади проведення оцінювання стану захищеності державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах органів державної влади, органів місцевого самоврядування, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій незалежно від форм власності.

Також у цьому НПА визначено об’єкт оцінки стану захищеності як стан захищеності ДІР, які обробляються в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах незалежно від наявності КСЗІ та мети оцінки захищеності ДІР, а саме виявлення існуючих загроз.

Підсумовуючи вищенаведене, в Білій книзі Держспецзв’язку [30] вводиться цілий розділ, присвячений захисту ДІР в ІТС. У цьому розділі йдеться про реалізацію державної політики щодо захисту ДІР в ІТС, намічені основні шляхи щодо заходів відповідно до визначених завдань, показано основні практичні заходи реалізації захисту ДІР в Україні, а саме в державних органах влади.

На основі наведеного аналізу можна подати загальну систему основного НПЗ захисту ДІР (рис. 1.1).

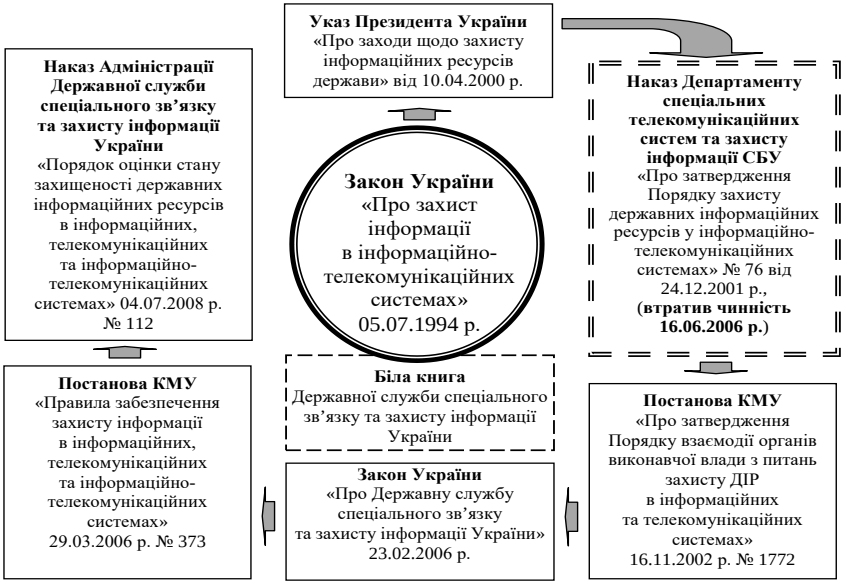

Рис. 1.1. Загальна система основного НПЗ захисту ДІР

Отже, було проаналізовано основні НПА, у яких розглянуто поняття «державні інформаційні ресурси». Хоча дане поняття з'явилося ще в Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» у 1994 р., саме остаточне визначення цього поняття було наведено лише в Законі України «Про Державну службу спеціального зв'язку та захисту інформації України» 2006 р.

Аналіз НПА щодо захисту державних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах свідчить про малосистемний характер відповідної діяльності.

Виходячи із праці [31], для побудови ефективної КСЗІ необхідно: виявити можливі загрози та надати рекомендації щодо їх запобігання. У цьому напрямку і формується основне НПЗ захисту ДІР, але з наведеного аналізу можна побачити, що не всі питання ще розглянуті, а деякі потребують подальшого вдосконалення.

Не чітко визначено загрози різним видам інформації (або мало деталізовані), на концептуальному рівні не закріплено перелік органів державної влади, повноваження яких дозволяли б повністю

захистити інформаційні ресурси держави, не розроблено стандарт щодо визначення поняття «державні інформаційні ресурси» та його складових. Не розроблено положення про модель порушника ДІР, за якою можна б було визначити можливі наміри порушника, ступінь небезпечності, категорію осіб, з-поміж яких може бути порушник, припущення про кваліфікацію порушника та характер його дій. Не повною мірою розроблена політика безпеки ДІР, яка б надавала певний набір вимог, правил, обмежень, рекомендацій, які регламентують порядок оброблення інформації і спрямовані на захист ДІР від певних загроз. Як вказано в праці [32], наслідком таких лише теоретичних недоліків стає, приміром, неконтрольоване несанкціоноване поширення баз даних, сформованих в органах державної влади, які містять докладну інформацію про майновий стан фізичних та юридичних осіб, місце їх проживання (реєстрації), номери телефонів та інші персональні дані, хоча згідно із Законом України «Про інформацію» від 2 жовтня 1992 р. № 2657-XII, ст. 11 «не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини. До конфіденційної інформації про фізичну особу належать, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження. Кожному забезпечується вільний доступ до інформації, яка стосується його особисто, крім випадків, передбачених законом». У цьому ж законі в ст. 3, де описані основні напрями державної інформаційної політики, відсутній напрямок, який стосується поняття ДІР.

1.2. Концептуальний аналіз уразливості державних інформаційних ресурсів

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 міжна-

родній 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», звідки виникає необхідність постійного уточнення як внутрішніх, так і зовнішніх загроз державним інформаційним ресурсам, що у свою чергу, впливатиме на організацію комплексної системи захисту державних інформаційних ресурсів, забезпечуватиме актуальність проведення досліджень у вказаному напрямку.

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 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 базуватися на аналізі та знанні загроз їм.

За тлумачним словником, слово «ресурси» походить від французького *ressourse* — допоміжні засоби (грошові кошти, цінності, запаси, можливості, джерела прибутків тощо) [32]. 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 [10] 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 КСЗІ щодо НСД та дотримання належного рівня їх захисту.

В Україні приділяється достатньо уваги захисту ДІР. З метою забезпечення єдиного підходу щодо захисту ДІР на виконання Постанови Кабінету Міністрів України від 24.02.2003 р. № 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 Ін-

тернет-доступу Держспецзв'язку. Подальше підключення органів державної влади до мережі Інтернет має здійснюватись винятково через захищений вузол Інтернет-доступу національної системи конфіденційного зв'язку (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 [30].

Реалізація державної політики щодо захисту ДІР в ІТС полягає у [30; 31]:

- розробленні пропозицій до визначення загальної стратегії та пріоритетних напрямів діяльності у сфері захисту ДІР в ІТС;
- виконанні обов'язків уповноваженого органу у сфері ЗІ в ІТС;
- розробленні порядку та вимог до захисту ДІР в ІТС, а також погодження проектів НПА з цих питань;
- розробленні критеріїв та порядку оцінювання стану захищеності ДІР в ІТС тощо.

На основі цього наведемо зміст реалізації державної політики з питань захисту ДІР в ІТС [30]:

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

Отже, 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 як побудови систем захисту, так і оцінки захищеності ДІР.

Загалом зміст захисту ДІР наведено на рис. 1.2.

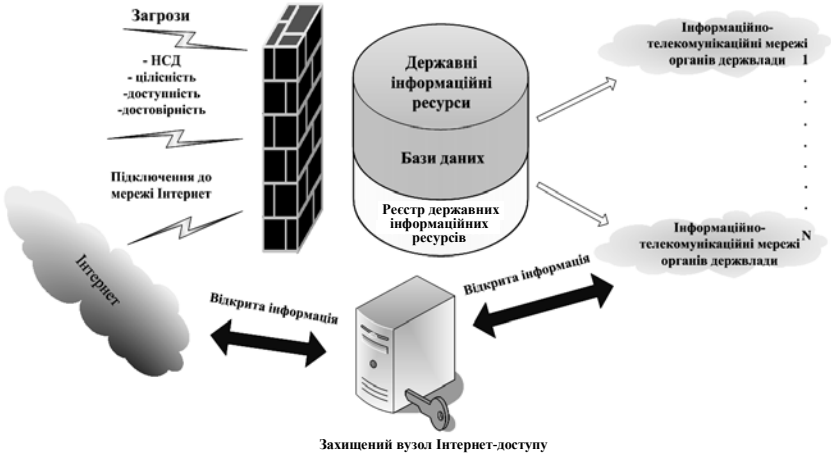

Рис. 1.2. Захист ДІР

Звідси виникає необхідність визначення основних загроз безпеці інформації ДІР.

Узагальнений механізм атаки [29] можливо застосувати стосовно ДІР з певними доповненнями та особливостями (рис. 1.3).

Рис. 1.3. Механізм атаки ДІР

Таким чином, загрози ДІР можна 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 вразливість. 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 [34].

У праці [31] 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, можливо виділити такі основні види загроз ДІР [10; 29; 34; 34; 36]:

1. Загрози доступності (розкриття інформаційних ресурсів, несанкціонований доступ до ДІР).
2. Загрози цілісності (умисний антропогенний вплив).
3. Загрози конфіденційності (викрадення, утрата інформації та засобів її обробки).
4. Загроза збою в роботі самого обладнання.
5. Загрози ненавмисних помилок користувачів, операторів, системних адміністраторів та інших осіб, які обслуговують інформаційні системи.

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 інтерес з погляду 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, деградація 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 низки 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 дестабілізації можлива за певних умов середовища функціонування органу державного управління;

– здійснені — такі загрози, які втілені у життя;

– уявні — псевдоактивізація алгоритмів дестабілізації, 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 цим їх можна назвати ненормативними загрозами;

– суб'єктивні — така сукупність чинників об'єктивної дійсності, яка вважається суб'єктом управління системою безпеці загроз.

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 в якості загроз безпеці.

За об'єктом впливу:

– особа;

– суспільство;

– держава.

На основі проведеного аналізу загроз можливо побудувати загальну систему класифікації загроз безпеці інформації ДІР, показану на рис. 1.4.

Проведений концептуальний аналіз уразливості державних інформаційних ресурсів дозволяє зробити висновок про надто широкий спектр, багатошаровість та масштабність тих обставин, у результаті яких може порушуватись цілісність, доступність та конфіденційність інформації державних інформаційних ресурсів.

У зв'язку із 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.

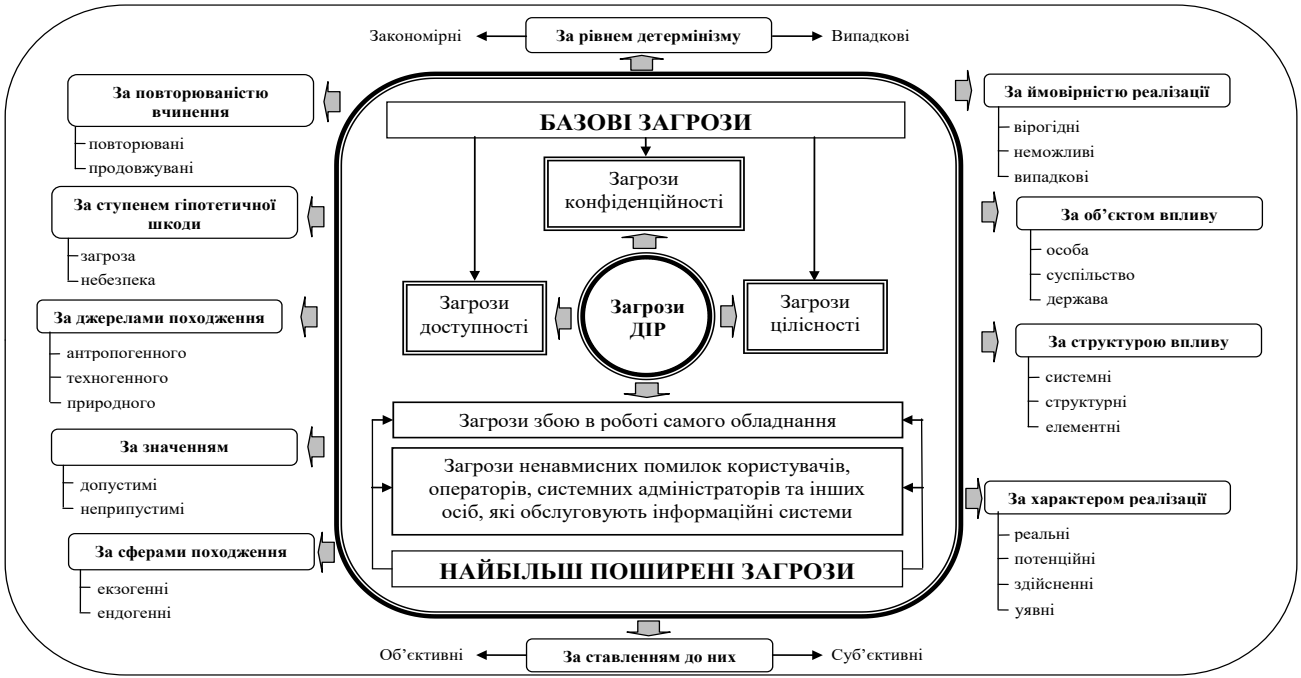

Рис. 1.4. Загальна система класифікації загроз безпеці інформації ДІР

1.3. Правові аспекти формування системи державних інформаційних ресурсів

Стрімке зростання новітніх технологій, а також розвиток інфраструктури інформаційно-комунікаційних мереж державного та загального призначення призвело до створення інтегрованого інформаційного простору держави та всього суспільства. Інформаційні технології знаходять усе ширше застосування в таких сферах, як: державні системи управління, фінансовий обіг і ринок цінних паперів, розвинута система електронних платежів, система послуг зв'язку та телебачення, системи управління транспортом, високотехнологічні виробництва (особливо атомні, хімічні тощо) і т. ін. Будь-яке несанкціоноване та протиправне втручання в інформаційний простір наведених сфер життєдіяльності держави й суспільства може призвести до тяжких та не передбачуваних наслідків.

Особливого значення в сучасних умовах розвитку інформаційного суспільства держави відіграють її ресурси, система організації і вільного доступу до них всіх категорій суб'єктів інформаційної діяльності. ДІР набувають базової значущості під час реалізації процесів глобалізації інфраструктур, а також в умовах інтеграції України до світового інформаційного простору.

Проведений аналіз нормативно-правового спрямування щодо процесів інформатизації та забезпечення захисту ДІР свідчить про малосистемний характер відповідної діяльності в країні, спостерігається нечітка спрямованість визначення класів різних видів ДІР (мало деталізовані або відсутні) тощо. Крім того, на концептуальному та нормативному рівні не обґрунтовано змістовне наповнення та не надано деталізоване визначення інформаційним ресурсам держави, не повною мірою розроблені НПА, стандарти щодо поняття державних інформаційних ресурсів, їх складових та класифікації [10; 29; 36; 37].

Звертаючись до теми класифікації ДІР в цілому, слід зазначити, що даному питанню приділяли увагу як вітчизняні, так і зарубіжні вчені. До них можна віднести: О. М. Новікова, В. М. Богуша, В. В. Мохора, О. Г. Додонова, О. В. Нестеренко, А. В. Бойченка, І. Д. Горбенко, В. О. Хорошко, О. В. Корнейко, М. В. Грайворонського, О. Г. Корченка, А. І. Марущака, В. П. Мельнікова, С. В. Віхорева, Е. В. Касперського, І. Д. Медведовського, О. В. Олійника та ін.

Але питанню створення класифікації та розширенню поняття і визначення ДІР приділялось недостатньо уваги, про що свідчить існуюче НПЗ.

Аналітично-правовий аналіз та визначення ДІР. Аналітично-правовий аналіз, а також проведені дослідження на базі існуючого НПЗ, галузі інформаційних технологій та їх безпеки дають можливість зробити висновок про недосконаліть класифікації та змістовного наповнення поняття ДІР в країні. Відповідна діяльність органів державної влади носить розрізнений відомчий характер щодо формування реєстру ДІР (зокрема електронного) та безпосередньо системи класифікації ресурсів держави.

Наведений авторами матеріал має достатнє підґрунтя, сформоване на попередніх дослідженнях та сталих підходах до аналізу різних класів інформаційних ресурсів [10; 29; 37; 38]. Тому, що б не втратити логіку викладення матеріалу, наведемо основні отримані висновки і положення із зазначеного напрямку.

У нормативному документі НД «Технічний захист інформації на програмно-керованих АТС загального користування. Специфікації функціональних послуг захисту» (НД ТЗІ 2.5-001–99, затверджений наказом ДСТСЗІ СБУ від 29.05.1999 р. № 26) наведено визначення поняття інформаційного ресурсу, а саме: *інформаційний ресурс* (ІР) — 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.).

Офіційно словосполучення «державні інформаційні ресурси», вперше з’явилося в Законі України «Про захист інформації в інформаційно-телекомунікаційних системах» (Закон України від 05.07.1994 р. № 81/94-ВР зі змінами від 19.03.2009 р.), де в ст. 10 установлено повноваження державних органів у сфері захисту інформації та визначено, що вони здійснюють заходи щодо виявлення *загроз державним інформаційним ресурсам* від несанкціонованих дій в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах та дають рекомендації з питань запобігання таким загрозам.

Надалі поняття ДІР можна прослідкувати в таких законодавчих актах: Указ Президента України «Про заходи щодо захисту інформаційних ресурсів держави» (від 10.04.2000 р. № 582/2002); Законах України «Про інформацію» (від 2 жовтня 1992 р. № 2657-XII-ВР)

та «Про Національну програму інформатизації» (від 04 лютого 1992 року № 74/98); Постанова КМУ «Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту ДІР в інформаційних та телекомунікаційних системах» (від 16 листопада 2002 року № 1772), яка визначає механізм взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах; розроблено та введено в дію «Концепцію формування системи національних електронних інформаційних ресурсів» (затверджена розпорядженням КМ України від 05 травня 2003 року № 259-р.), де ДІР визначено як складову національних інформаційних ресурсів; низку інших НПА.

Визначено, що національні ресурси є важливою складовою стратегічних ресурсів держави, значущість якої зростає з розвитком інформаційних технологій та їх використанням в усіх сферах суспільного життя.

У «Концепції формування системи національних електронних інформаційних ресурсів» в основних термінах наведені визначення *національні ресурси* та *система національних ресурсів*, але виникає необхідність уточнення та доповнення цих понять, у тому числі і введення поняття «національні електронні інформаційні ресурси». Виходячи з проведеного аналізу остаточно поняття можна навести у такому вигляді.

Національні інформаційні ресурси — це результати інтелектуальної діяльності в усіх сферах життєдіяльності людини, суспільства і держави, зафіксовані на відповідних матеріальних носіях інформації як окремі документи і масиви документів, бази і банки даних та знань, усі види архівів, бібліотеки, музейні фонди та інші, що містять дані, відомості і знання, які є об'єктом права власності будь-якого суб'єкта України і мають споживчу цінність (політичну, економічну, наукову, освітню, соціокультурну, оборонну, ринкову, історичну, інформаційну тощо).

Національні електронні інформаційні ресурси — інформаційні ресурси незалежно від їх змісту, форми, часу та місця створення, форми власності, які існують та використовуються в електронному вигляді та призначені для задоволення потреб громадянина, суспільства, держави. Національні електронні ресурси включають державні, комунальні та приватні ресурси.

Система національних інформаційних ресурсів — організована за єдиною технологією сукупність національних ресурсів, необхідних для розв'язання завдань соціально-економічного розвитку держави та внесених до Національного реєстру електронних інформаційних ресурсів (реєстр ресурсів — сукупність даних, упорядкованих для обліку і реєстрації ресурсів).

Питання термінології ДІР у зазначених НПА не розглядалось і тільки в Законі України «Про Державну службу спеціального зв'язку та захисту інформації України» (від 23 лютого 2006 року № 3475-IV), вперше, остаточно визначено термін «державні інформаційні ресурси».

Державні інформаційні ресурси — інформація, яка є власністю держави та необхідність захисту якої визначено законодавством. Дане визначення є загальним (відсутня ідеологія класифікації ресурсів) та не задовольняє сучасні вимоги стандартизації і відповідності темпам розвитку інформаційно-правового простору суспільства.

Це визначення є повним еквівалентом визначенню, наведеному в [39]: «Государственные информационные ресурсы — это ресурсы, которые как элемент имущества находятся в собственности государства».

Також наступним рядком пропонуються обов'язкові кроки класифікації з подальшою деталізацією за розділами ... Государственные ресурсы делятся на следующие группы:

- федеральные ресурсы;
- информационные ресурсы, находящиеся в совместном ведении Российской Федерации и субъектов РФ;
- информационные ресурсы субъектов РФ.

У Федеральному Законі Російської федерації (РФ) «Об информации, информационных технологиях и о защите информации» (зі змінами від 02 липня 2013 року №187-ФЗ) визначено, що «Информация, содержащаяся в государственных информационных системах, а также иные имеющиеся в распоряжении государственных органов сведения и документы являются *государственными информационными ресурсами*».

Отже, даним законом РФ наголошується, що інформація, яка знаходиться та обробляється в державних інформаційних системах, належить до ДІР.

Прикладом докладної класифікації ДІР РФ може слугувати підхід до представлення бібліотечної, музейної або архівної складової. Так, до бібліотечних інформаційних ресурсів РФ згідно із законодавством відносяться:

- публічні бібліотеки всіх рівнів (федеральні, регіональні та муніципальні);
- системи науково-технічних бібліотек та інформаційно-довідкових фондів;
- інформаційно-бібліотечна система Російської академії наук;
- бібліотечна система вищих навчальних закладів;
- мережа сільськогосподарських бібліотек;
- інші системи мережі.

Під час побудови інформаційних систем і мереж було враховано галузеві та регіональні принципи, встановлено основи побудови мереж та кількісні показники існуючих фондів.

На жаль, вітчизняна НПБ такої класифікації та нормативно-правової підтримки для ДІР не має.

Проблема визначення поняття ДІР та шляхів реалізації державної політики з зазначеного напряму є предметом професійної уваги провідних вітчизняних науковців, зокрема: І. В. Арістової [40], О. В. Олійника [41]. Однак більш чітке і комплексне визначення, на думку авторів, останнім часом наведено в роботах А. І. Марущака [32; 42].

Так, загальним висновком із проведеного дослідження доктора А. І. Марущака є визначений зміст поняття. *Інформаційні ресурси держави* — це взаємозв'язана, упорядкована, систематизована, закріплена на матеріальних носіях інформація, яка створена, зібрана на законних підставах органами державної влади або іншими суб'єктами за рахунок державного бюджету.

Така трактовка має право на існування й підтвердженням цьому є також джерела РФ: «Государственные информационные ресурсы — информационные ресурсы, полученные и оплаченные из федерального бюджета» [42].

Автори О. Соснін, А. Марущак приділяють значну увагу аналізу джерела фінансування процесів створення ДІР та наполягають на внесенні фрази «за рахунок державного бюджету» до визначення. Дане питання є неоднозначним та звужує юридично-фінансовий напрям формування ДІР.

Державні інформаційні ресурси та їх система. Введення термінів та визначень. Насамперед, розглядаючи концептуальні питання класифікації національних інформаційних ресурсів, необхідно надати більш докладне визначення ДІР, їх системи і реєстру та на цій платформі, а в подальшому сформувати визначення і напрями класифікації загроз ДІР. На думку авторів, основою для визначення ДІР може слугувати тлумачення, запропоноване «Концепцією формування системи національних електронних інформаційних ресурсів» для національних ресурсів, яке буде скоректоване відносно державного об'єкта власності та більш деталізоване за класами ресурсів.

Таким чином, ґрунтуючись на попередніх дослідженнях, поняттях і загальних визначеннях інформаційних ресурсів, національних інформаційних ресурсів (НІР), наведемо нове, більш широке та сучасне визначення ДІР.

Державні інформаційні ресурси — це результати інтелектуальної та практичної діяльності, що сформовані в усіх сферах життєдіяльності людини, суспільства і держави, зафіксовані і систематизовані на відповідних матеріальних носіях інформації як окремі документи і масиви документів, банки і бази даних та знань, усі види архівів і бібліотек, музейні фонди, інформаційні ресурси, які обробляються й передаються в інформаційних системах державного і/або загального призначення, інші ресурси, що містять дані, відомості і знання, які є об'єктом права власності держави незалежно від форми власності на час їх створення і мають споживчу цінність, а також такі, що призначені для розвитку і задоволення потреб громадян, суспільства, держави та підлягають захисту згідно із визначеною політикою безпеки й чинним законодавством.

Державні інформаційні ресурси є складовою національних інформаційних ресурсів та мають споживчу цінність, а саме: політичну, економічну, наукову, освітню, соціокультурну, оборонну, ринкову, історичну, інформаційну тощо. Будь-який суб'єкт інформаційних відносин України має право доступу до Державних інформаційних ресурсів згідно з визначеною політикою безпеки та чинним законодавством.

Зважаючи на міжнародний досвід, основою зростання сьогодні будь-якої країни у світовій економіці, згідно з концептуальними завданнями Всесвітнього економічного форуму, є так звані п'ять

«і»: інформація, інфраструктури, інтелектуальний капітал, інвестиції, інновації. Реалізація зазначених «і», а також організація накопичення, зберігання, оброблення, підтримка інформаційних ресурсів суспільства неможлива без системного державного підходу на основі інтегрованої інформаційної системи.

Одне з найвідоміших визначень інформаційної системи запропонував М. Р. Когаловський [44]: «інформаційною системою називається комплекс, що включає обчислювальне і комунікаційне обладнання, програмне забезпечення, лінгвістичні засоби та *інформаційні ресурси*, а також персонал, який забезпечує підтримку динамічної інформаційної моделі деякої частини реального світу для задоволення інформаційних потреб користувачів». Зрозуміло, що *інформаційні ресурси* є складовими інформаційної системи та відповідно до форми власності можуть належати як державі, так і окремим недержавним організаціям, установам, фізичним та юридичним особам.

Державна система забезпечення інформаційних ресурсів та їх безпеки повинна представляти організаційне об'єднання державних органів, а також сил та засобів інформатизації суспільства, що виконують свої функції на основі правового доступу під контролем і захистом виконавчих органів та згідно з чинним законодавством. Державна система інформаційних ресурсів та їх безпеки складає найважливішу ланку загальної системи національних інформаційних ресурсів, зокрема особистості, суспільства і держави.

Основними завданнями такої системи є:

• реалізація процесів інформатизації країни, а також виявлення і прогнозування дестабілізуючих факторів і загроз інформаційним ресурсам, що є життєво важливим для особистості, суспільства та держави;

• здійснення комплексу оперативно-організаційних і довготривалих програм, заходів із створення, накопичення, обробки й висвітлення інформаційних ресурсів та забезпечення системи вільного доступу користувачів згідно з чинним законодавством;

• створення й підтримання в режимі безперервності функціонування стандартних процесів і різних класів функціональних послуг та засобів забезпечення інформаційної безпеки тощо.

Органи (служби) інформатизації та безпеки ДІР можуть створюватися (на законодавчих засадах) як у державних, так і недержав-

них структурах для забезпечення потреб суб'єктів інформаційних відносин. Дані органи на основі укладення відповідних угод, законодавчих актів можуть бути приєднані до єдиної системи національних інформаційних ресурсів.

Натепер в Україні створені та функціонують окремі елементи системи ДІР, тобто інформаційні служби різноманітних міністерств, відомств, система технічного та криптографічного захисту інформації держави і т. ін.

Таким чином, під *системою державних інформаційних ресурсів* будемо розуміти організований державою упорядковано-інтегрований комплекс, що включає організаційно-технічні, нормативно-правові технології, методи, заходи та їх інфраструктури тощо. Спираючись на проведений аналіз, можна надати таке розширене визначення *системи державних інформаційних ресурсів.*

Система державних інформаційних ресурсів — це організований державою упорядковано-інтегрований комплекс організаційно-технічних, нормативно-правових технологій, методів і заходів, а також взаємозв'язана і погоджено-функціонуюча сукупність суб'єктів інформаційної діяльності (державних, суспільства та окремих громадян), об'єднаних цілями й завданнями щодо формування, накопичення, збереження, достовірного оброблення, передавання, висвітлення та захисту державних інформаційних ресурсів у межах чинного законодавства України.

Спираючись на поняття системи державних інформаційних ресурсів, виникає наступний крок — необхідність розгляду питання державних електронних інформаційних ресурсів (ДЕІР). Визначення ДЕІР наведено в Постанові КМ України «Про затвердження Положення про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління» (від 03.08.2005 р. № 688 зі змінами в редакції Постанови КМ України від 07.09.2011 р. № 938). Згідно з даною Постановою, *державні електронні інформаційні ресурси* — відображена та задокументована в електронному вигляді інформація, необхідність захисту якої визначено законодавством.

Із цього визначення не зрозуміло їх практичне призначення, класифікація, розташування, технології ідентифікації тощо. Більш детально про це йдеться у схваленій в Україні «Концепція створен-

ня та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів» (розпорядження КМ України від 5 вересня 2012 р. № 634-р). У рамках даної концепції складено «План заходів щодо реалізації Концепції створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів» (затверджено розпорядженням КМ України від 11 липня 2013 р. № 517-р). Отже, виникає питання уточнення поняття державних електронних інформаційних ресурсів як складової системи державних інформаційних ресурсів (системи державних електронних інформаційних ресурсів). Воно може бути наведено таким чином.

Державні електронні інформаційні ресурси — державні інформаційні ресурси незалежно від їх змісту, форми, часу і місця створення, які існують та використовуються в електронному вигляді та призначені для задоволення потреб громадян, суспільства, держави. Державні електронні інформаційні ресурси є складовою Національного реєстру електронних інформаційних ресурсів

Національний реєстр електронних інформаційних ресурсів формується згідно з розпорядженням КМ України від 05.05.2003 р. № 259-р (Концепція формування системи національних електронних інформаційних ресурсів), постанови КМ України від 17 березня 2004 р. № 326 (Положення про Національний реєстр електрон них інформаційних ресурсів), Наказу Міністерства транспорту та зв'язку від 27.04.2005 р. № 153 (Про затвердження Порядку проведення державної реєстрації електронних інформаційних ресурсів). Основна мета Національного реєстру — запровадження єдиної системи обліку електронних інформаційних ресурсів держави, яка формується з використанням новітніх досягнень у сфері інформаційно-телекомунікаційних технологій.

Національний реєстр — це інформаційно-телекомунікаційна система, призначена для реєстрації, обліку, накопичення, оброблення і зберігання відомостей про склад, зміст, розміщення, умови доступу до електронних інформаційних ресурсів та задоволення потреб юридичних і фізичних осіб в інформаційних послугах. Відповідно до «Положення про Національний реєстр електронних інформаційних ресурсів» у реєстрі мають бути зареєстровані також і *державні інформаційні ресурси* (та, за бажанням, ресурси юридичних осіб), однак у законодавчих документах відсутнє поняття

«реєстр електронних ДІР». Спираючись на попередні дослідження введемо визначення.

Реєстр електронних державних інформаційних ресурсів — інформаційна система, призначена для реєстрації, обліку, накопичення, оброблення та зберігання відомостей про склад, зміст, умови доступу до електронних державних інформаційних ресурсів, розміщених у Національному депозитарії та такі, що мають споживчу цінність, а саме: політичну, економічну, наукову, освітню, соціокультурну, оборонну, ринкову, історичну, інформаційну тощо.

Реалізація концептуальних шляхів щодо створення єдиного інформаційно-комунікаційного простору, об'єднання й класифікація ДІР та їх використання всіма суб'єктами інформаційної діяльності та управління створюють передумови для успішного розвитку всієї країни. Зрозуміло, що зусилля суспільства і влади на забезпечення інтеграції інформаційних ресурсів державних органів та місцевого самоврядування, ефективна інформаційна взаємодія підприємств, організація системи вільного доступу фізичних та юридичних осіб до ДІР тощо неможлива без реалізації конкретизованої програми створення Національного депозитарію державних електронних інформаційних ресурсів.

Зазначений підхід, повинен формувати єдині стандартні правила діяльності в інформаційному просторі країни (зокрема в глобальних мережах) для всіх учасників інформаційних відносин, незалежно від форм власності мереж передачі даних, а також технологічних рішень накопичення, зберігання, обробки, передачі і висвітлення інформації.

Державні нормативно-правові акти чітко визначають необхідність та планові дії щодо створення Національного депозитарію електронних інформаційних ресурсів. Дані процеси відображено у законодавчих актах в рамках електронного урядування, а також: у розпорядженні КМ України від 5 травня 2003 року № 259-р «Про затвердження Концепції формування системи національних електронних інформаційних ресурсів»; Законі України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» (відомості Верховної Ради України (ВВР), 2007, № 12, ст. 102); Постанові КМ України № 956 від 17 серпня 2011 року «Про затвердження Державної цільової національно-культурної програми створення єдиної інформаційної бібліотечної системи

«Бібліотека – XXI»»; розпорядженні КМ України про схвалення «Концепції створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів» від 5 вересня 2012 року № 634-р; Міністерством освіти і науки України було оприлюднено 27 листопада 2012 року проект «Положення про депозитарій електронних освітніх ресурсів».

Як нормативно-законодавчий акт «Стратегія розвитку інформаційного суспільства в Україні», схвалена розпорядженням КМ України від 15 травня 2013 року № 386-р, визначає мету, базові принципи, стратегічні цілі розвитку інформаційного суспільства в Україні в період до 2020 р. Одним із основних завдань, визначених Стратегією при формуванні сучасної інформаційної інфраструктури держави є створення Національного депозитарію електронних інформаційних ресурсів. Розробка, впровадження та супровід Національного депозитарію електронних інформаційних ресурсів, згідно з розпорядженням КМ України від 26 вересня 2011 року № 1014-р «Про затвердження плану заходів щодо реалізації Концепції розвитку електронного урядування в Україні», закріплено за Адміністрацією Державної служби спеціального зв'язку та захисту інформації, а також за державними організаціями Держінформнауки і Укрдержархів.

На жаль, усі перелічені вище акти та документи встановлюють мету, завдання й етапи інформатизації держави, але не дають відповіді на питання, що є визначенням: Депозитарій електронних державних інформаційних ресурсів? Під депозитарієм електронних ресурсів ДІР будемо розуміти таке.

Депозитарій електронних державних інформаційних ресурсів — інформаційна система державних електронних інформаційних ресурсів, створена на базі автоматизованих систем та погоджено функціонуючих програмно-апаратних комплексів, що забезпечують збір, облік, аудит, зберігання, оновлення, захист і доступ до електронних державних інформаційних ресурсів на основі інформаційних технологій та інформаційно-комунікаційних систем згідно з визначеною політикою безпеки та чинним законодавством.

Розділ 2

ВИЗНАЧЕННЯ МЕТОДОЛОГІЇ ПОБУДОВИ КЛАСИФІКАТОРА ЗАГРОЗ ДЕРЖАВНИМ ІНФОРМАЦІЙНИМ РЕСУРСАМ

2.1. Автоматизована система як об'єкт системи захисту інформації

Сьогодні за умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень та боротьби конкуруючих сторін стає інформаційний простір. Сучасні інформаційні технології надають інформаційній складовій дедалі більшої ваги і стають одним із найважливіших елементів забезпечення захисту інформації, тому завдання захисту інформації, яка зберігається в автоматизованих комп'ютерних системах, є досить актуальним. Для вирішення цього завдання використовується цілий комплекс засобів, що включає в себе нормативно-правові, організаційні та інженерно-технічні напрями захисту інформації [10].

Сучасні методи обробки, передачі й накопичення інформації сприяли появі загроз, що забезпечують можливість втрати, перекручування та розкриття даних. Тому побудова надійного захисту КС залишається актуальною, звідки виникає необхідне завдання високоякісного забезпечення безпеки АС, яке неможливо виконати без попереднього аналізу можливих загроз безпеки системи. Для вирішення цього питання необхідно чітко визначити АС як об'єкт захисту інформації.

Останнім часом проблеми, пов'язані з використанням різного роду ЗІ в повсякденній діяльності, стали особливо актуальними завдяки широкому розвитку АС. Цим проблемам присвячені праці В. В. Мельникова [45], В. І. Завгороднева [46], І. Д. Горбенка, Т. О. Гриненка [4], М. Р. Когаловського [44]. Також значний внесок у розробку питань із оцінки захисту КС внесли роботи докторів наук О. Г. Корченка [47] і В. Б. Дудикевича [49].

У процесі конструктивного поєднання діяльності держави, громадянського суспільства і людини ЗІ є одним із трьох головних напрямів діяльності органів виконавчої влади у сфері забезпечення інформаційної безпеки України [50].

У Законі України «Про інформацію» (від 02.10.1995 р. № 2658-XII-ВР//ВВР) визначено, що головними напрямами державної інформаційної політики в Україні, яку розробляють і здійснюють органи державної влади, а також відповідні органи спеціальної компетенції, є сприяння зберіганню національних інформаційних ресурсів, створення загальної системи охорони інформації та гарантування інформаційного суверенітету України. Для того щоб визначити АС як об'єкт захисту, потрібно докладно розглянути це поняття.

У НПА України наведено декілька таких понять.

Так, у ДСТУ 2226–93 «Автоматизовані системи. Терміни та визначення», який установлює терміни та визначення основних понять у галузі автоматизованих систем, автоматизована система є: «організаційно-технічною системою, що складається із засобів автоматизації певного виду (чи кількох видів) діяльності людей та персоналу, що здійснює цю діяльність».

Водночас, звертаючись до сучасних НПА з технічного захисту інформації (ТЗІ), а саме Закону України «Про захист інформації в автоматизованих системах» (від 05.07.1994 р. № 81/94-ВР//ВВР) *автоматизована система* — система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення. В НД ТЗІ 1.1-003–99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» (затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 р. № 22) *автоматизована система* є організаційно-технічною системою, що реалізує інформаційну технологію і об'єднує обчислювальну систему, фізичне середовище, персонал і інформацію, яка обробляється.

Зрозуміло, що починаючи вже з ключових термінів АС, немає однозначних визначень цих понять, діюча нормативна база з ТЗІ потребує доопрацювання та впровадження єдиної термінології.

Для розгляду АС як об'єкта захисту інформації скористаємось визначенням АС з НД ТЗІ 1.1-003–99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу», у зв'язку з тим, що воно найбільш повно на думку авторів розкриває суть поняття АС. Тепер, коли визначено поняття АС, потрібно розглянути поняття суб'єкта і об'єкта інформації.

У Законі України «Про інформацію» визначено, що *суб'єктами* інформаційних відносин є: фізичні особи; юридичні особи, об'єднання громадян, суб'єкти владних повноважень. *Об'єктом* інформаційних відносин є інформація.

Згідно із Законом України «Про захист інформації в автоматизованих системах» *об'єктом* захисту є інформація, що обробляється в АС, права власників цієї інформації та власників АС, права користувача. Захисту підлягає будь-яка інформація в АС, необхідність захисту якої визначається її власником або чинним законодавством.

Цим же законом визначено, що *суб'єктами* відносин, пов'язаних з обробкою інформації в АС, є: власники інформації чи уповноважені ними особи; власники АС чи уповноважені ними особи; користувачі інформації; користувачі АС. Як бачимо, в Законі України «Про захист інформації в автоматизованих системах» ширше розкривається зміст об'єкта захисту інформації і суб'єкта інформаційних відносин, що повинно використовуватись для розгляду АС як об'єкта захисту інформації. Зрозуміло, для узагальнення всіх понять необхідно розглянути, що являє собою *захист інформації в АС*.

Зі змісту Закону України «Про захист інформації в автоматизованих системах» випливає, що *захист інформації* — це сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією. Таким чином, захист інформації в АС — діяльність, яка спрямована на забезпечення безпеки оброблюваної в АС інформації та АС у цілому, і дозволяє запобігти або ускладнити можливість реалізації загроз, а також знизити величину потенційних збитків унаслідок реалізації загроз [НД ТЗІ 1.1-003–99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»].

Для вирішення завдання захисту інформації використовується цілий комплекс засобів, що включає технічні, програмно-апаратні засоби та адміністративні заходи захисту інформації. Побудова надійного захисту КС неможлива без попереднього аналізу класифікації АС та можливих загроз безпеці системи.

Вимоги до гарантій АС визначаються насамперед характером і важливістю оброблюваної інформації і призначенням АС. Згідно з

НД ТЗІ 2.5-005–99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» (Затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 28.04.1999 р.) за сукупністю характеристик АС виділено три ієрархічні класи АС, вимоги до функціонального складу КЗЗ яких істотно відрізняються.

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

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

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

Розглянемо істотні особливості і приклади.

У кожен момент часу з комплексом (Клас «1») може працювати тільки один користувач, хоч у загальному випадку осіб, що мають доступ до комплексу, може бути декілька, але всі вони повинні мати однакові повноваження (права) щодо доступу до інформації, яка оброблюється; технічні засоби (носії інформації) з точки зору захищеності відносяться до однієї категорії і всі можуть використовуватись для збереження всієї інформації. Прикладом такого класу може бути персональна автономна ЕОМ, доступ до якої контролюється шляхом використання організаційних заходів.

Клас «2» являє собою локалізований багатомашинний багатокористувацький комплекс, який обробляє інформацію різних категорій конфіденційності. Істотна відмінність від класу «1» — наявність користувачів з різними повноваженнями по доступу і/або технічних засобів, які можуть одночасно здійснювати обробку інформації різних категорій конфіденційності. Прикладом даного класу є звичайна локальна обчислювальна мережа (ЛОМ).

Клас «3» має істотну відмінність від попереднього класу — необхідність передавання інформації через незахищене середовище або загалом, наявність вузлів, що реалізують різну політику безпеки, наприклад — глобальна мережа.

Отже, підсумовуючи всі попередньо розглянуті питання, АС як об'єкт «триєдиної» системи захисту інформації може бути (проілюстрована) як на рис. 2.1 [51].

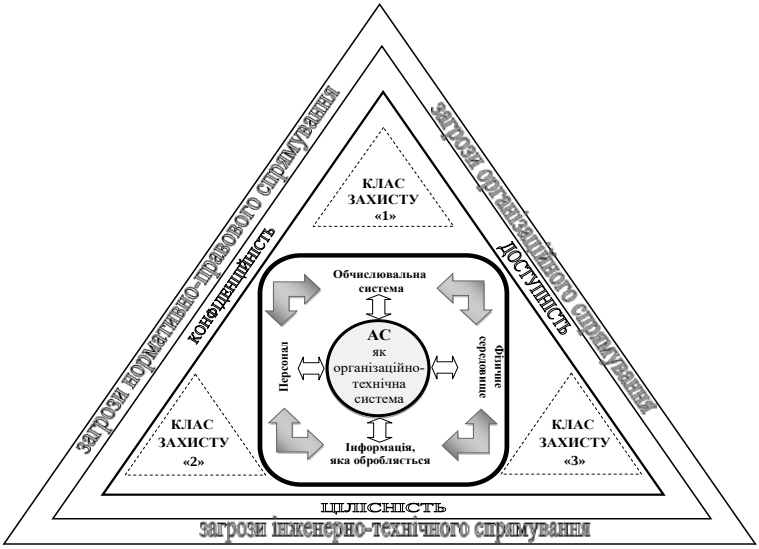

Рис. 2.1. АС як об'єкт «триєдиної» системи захисту інформації

Аналізуючи стан класифікації АС як об'єкт «триєдиної» системи ЗІ, можна зробити висновок, що узагальнена класифікація (згідно з класами захисту 1, 2, 3) використовується в межах кожного класу на підставі вимог, які забезпечують певні властивості інформації: конфіденційність, цілісність і доступність. Така класифікація корисна для полегшення вибору переліку функцій, які повинен реалізовувати КЗЗ АС. Цей підхід дозволяє мінімізувати витрати на початкових етапах створення захисту АС. Проте слід визнати, що для створення КЗЗ, який найповніше відповідає характеристикам і вимогам до конкретної АС, необхідно проведення в повному обсязі аналізу загроз і оцінки ризиків. Це у свою чергу показує шляхи для подальшої класифікації загроз нормативно-правового, організаційного та інженерно-технічного спрямування, їх розподіл за основними властивостями інформації, які впливають на стан безпеки АС. Розглянуті в даному розділі та інші впроваджені в державі НПА, що стосуються інформації та її захисту, а також внесення змін та

доповнень до діючих, потребують вжиття певних заходів з метою приведення нормативної бази системи ТЗІ відповідно до вимог цих НПА, що відображається на захисті АС у цілому.

2.2. Аналіз підходів до класифікації загроз інформаційним ресурсам

2.2.1. Аналіз основних підходів щодо створення класифікатора загроз державним інформаційним ресурсам

Одними з найбільш важливих нормативно-технічних документів, які стимулюють розвиток захищених інформаційних систем, мереж і засобів, є документи, що стандартизують вимоги та критерії оцінки безпеки [52].

Стандарти інформаційної безпеки — це стандарти забезпечення захисту, призначені для взаємодії між виробниками, споживачами і експертами з кваліфікації продуктів інформаційних технологій у процесі створення та експлуатації захищених систем оброблення інформації.

Стандарт забезпечення захисту зазвичай містить опис послідовності оцінок, які необхідно виконати, щоб вважати дану характеристику безпеки підтвердженою з погляду атестації захисту або множину характеристик безпеки, які повинна забезпечити система захисту, щоб її можна було використовувати в даному конкретному режимі забезпечення безпеки або відповідно до загальної стратегії захисту.

Аналізуючи Доктрину інформаційної безпеки України, затверджену Указом Президента України від 8 липня 2009 року № 514/2009 (Проект Указу Президента України «Про Доктрину інформаційної безпеки України» від 2014 р. у зв'язку зі втратою чинності вищенаведеного Указу на підставі Указу Президента № 504/2014 від 06.06.2014 р.), Закони України «Про захист інформації в автоматизованих системах» від 05.07.1994 р. № 81/94-ВР//ВВР та «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 р. № 81/94-ВР//ВВР, існуючі стандарти, технічні специфікації, інші підходи в області інформаційної безпеки з точки зору їх подальшого використання для побудови класифікації загроз ДІР можна виділити такі основні напрями аналізу (рис. 2.2) [4; 31; 50; 53; 54; 55; 56; 57; 58; 59; 59; 61; 62]:

– аналіз існуючих доктрин та законів України, які регламентують питання інформаційної безпеки України чи захист інформації, де є інформаційні ресурси;

– аналіз оціночних стандартів, які направлені на класифікацію інформаційних систем та засобів захисту за вимогами безпеки;

– аналіз технічних специфікацій, які регламентують різні аспекти реалізації засобів захисту;

– інші підходи.

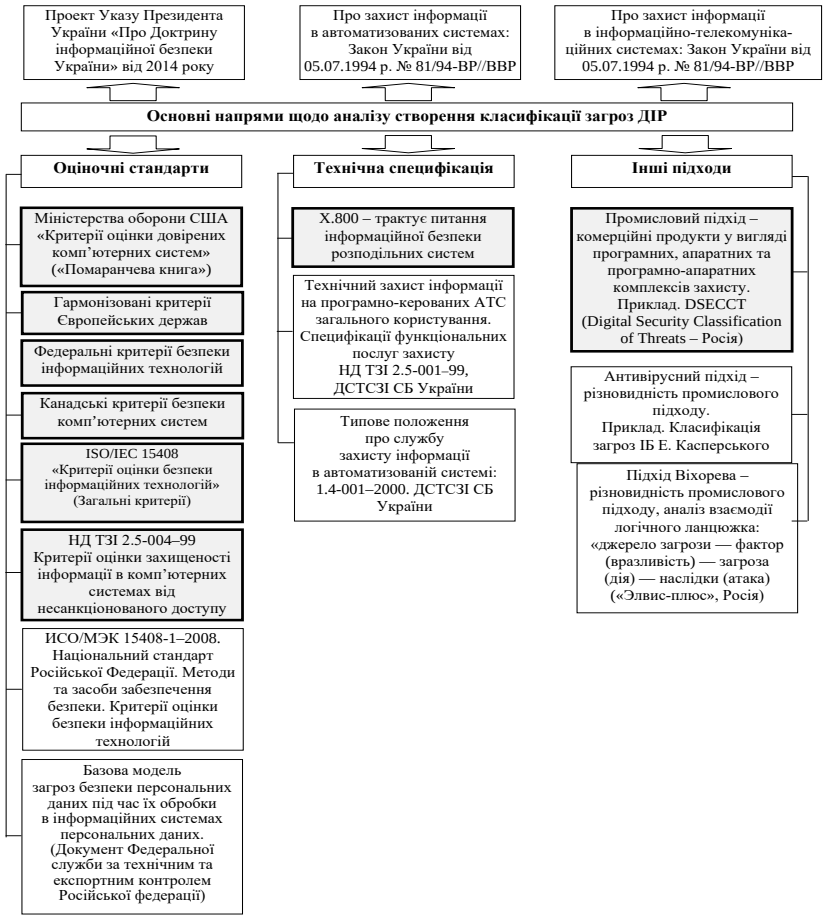

Рис. 2.2. Основні напрями аналізу створення класифікації загроз ДІР

Розглянемо основні підходи (найбільш значущі стандарти інформаційної безпеки виділені сірою заливкою на рис. 2.2), де визначена класифікація загроз в області ІБ та визначимо їх основні принципи. До них віднесемо (у хронологічному порядку):

Оціночні стандарти:

- Критерії оцінки довірених комп'ютерних систем («Помаранчева книга»).
- Європейські критерії безпеки інформаційних технологій (гармонізовані критерії Європейських держав).
- Федеральні критерії безпеки інформаційних технологій.
- Канадські критерії безпеки інформаційних технологій.
- Загальні критерії безпеки інформаційних технологій (ISO/IEC 15408).
- Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу (НД ТЗІ 2.5-004–99).

Технічні специфікації: X.800.

Інші підходи: промисловий підхід на прикладі класифікації загроз DSECCT (Digital Security Classification of Threats – Росія).

2.2.2. Підхід «Помаранчевої книги» як оціночний стандарт

Історично першим оціночним стандартом [52; 56; 63; 64], який набув широкого поширення і зробив величезний вплив на базу стандартизації ІБ в багатьох країнах, став стандарт Міністерства оборони США «Критерії оцінки довірених комп'ютерних систем» (Trusted Computer System Evaluation Criteria, TCSEC). Ця праця, яку називають найчастіше за кольором обкладинки «Помаранчевою книгою», була вперше опублікована в серпні 1983 року з метою визначення вимог безпеки, що висуваються до апаратного, програмного і спеціального забезпечення комп'ютерних систем і вироблення відповідної методології аналізу політики безпеки, що реалізується в комп'ютерних системах воєнного призначення. З її назви виходить, що йдеться не про безпечні, а про довірені системи, тобто про системи, яким можна надати певний ступінь довіри.

«Помаранчева книга» дає *поняття безпечної системи*, яка «управляє за допомогою відповідних засобів доступом до інформації, так що тільки належним чином авторизовані особи або процеси, що діють від їх імені, отримують право читати, записувати,

створювати і видаляти інформацію». Очевидно, що абсолютно безпечних систем не існує, тому є сенс оцінювати лише ступінь довіри, який можна надати тій або іншій системі.

У «Помаранчевій книзі» *довірена система* визначається як «система, що використовує достатні апаратні і програмні засоби, щоб забезпечити одночасну обробку інформації різного ступеня секретності групою користувачів без порушення прав доступу».

У даних критеріях безпека і довіра оцінюються винятково з погляду управління доступом до даних, що є одним із засобів забезпечення конфіденційності і цілісності (статичною). *Питання доступності «Помаранчева книга» не розглядає.* Відповідно питання протидії розглядаються з точки зору саме «*оцінки*», а не «*рекомендацій*» для побудови захищених ІС.

Ступінь довіри оцінюється за двома основними критеріями:

1. **Політика безпеки** — набір законів, правил і норм поведінки, які визначають, як організація обробляє, захищає і поширює інформацію. Зокрема, правила визначають, у яких випадках користувач може оперувати конкретними наборами даних. Чим вище ступінь довіри системі, тим більш суворою і багатоплановою має бути політика безпеки. Залежно від сформульованої політики можна обирати конкретні механізми забезпечення безпеки. Політика безпеки — це **активний аспект захисту**, що включає в себе аналіз можливих загроз і вибір заходів протидії.

2. **Рівень гарантованості** — ступінь довіри, який може бути надано архітектурі і реалізації ІС. Довіра безпеці може випливати як з аналізу результатів тестування, так і з перевірки (формальною або ні) загального задуму і реалізації системи в цілому і окремих її компонентів. Рівень гарантованості показує, наскільки коректні механізми, що відповідають за реалізацію політики безпеки. Це **пасивний аспект захисту**.

Із пасивних аспектів захисту в «Помаранчевій книзі» розглядаються два види гарантованості — **операційна і технологічна**.

Операційна гарантованість відноситься до архітектурних і реалізаційних аспектів системи, технологічна — до методів побудови і супроводу. Операційна гарантованість передбачає перевірку таких елементів:

– архітектура системи;
– цілісність системи;

– перевірка таємних каналів передачі інформації;
– довірене адміністрування;
– довірене відновлення після збоїв.

Операційна гарантованість — це спосіб переконатися в тому, що архітектура системи і її реалізація дійсно реалізують обрану політику безпеки.

Технологічна гарантованість охоплює увесь життєвий цикл ІС, тобто періоди проектування, реалізації, тестування, продажу і супроводу. Усі перелічені дії повинні виконуватися відповідно до жорстких стандартів, щоб виключити надходження інформації і нелегальні «закладки».

Важливим засобом забезпечення безпеки є *механізм протоколювання*. Довірена система повинна фіксувати усі події, що стосуються безпеки. Ведення протоколів має доповнюватися аудитом, тобто аналізом реєстраційної інформації.

Довірена обчислювальна база — це сукупність захисних механізмів ІС (включаючи апаратне і програмне забезпечення), що відповідають за проведення в життя політики безпеки. Якість обчислювальної бази визначається виключно її реалізацією і коректністю початкових даних, які вводить системний адміністратор. Концепція довіреної обчислювальної бази є центральною під час оцінювання ступеня довіри безпеки.

Основне призначення довіреної обчислювальної бази — виконувати функції монітора звернень, тобто контролювати допустимість виконання суб'єктами (активними сутностями ІС, діючими від імені користувачів) певних операцій над об'єктами (пасивні сутності). Монітор перевіряє кожне звернення користувача до програм або даних щодо узгодженості з набором дій, допустимих для користувача.

Монітор звернень повинен мати такі три властивості:

1. **Ізольованість**. Необхідно попередити можливість відстежування роботи монітора.

2. **Повнота**. Монітор має викликатися при кожному зверненні, не повинно бути способів обійти його.

3. **Верифікованість**. Монітор має бути компактним, щоб його можна було проаналізувати і протестувати.

Реалізація монітора звернень називається *ядром безпеки*. Ядро безпеки — це основа, на якій будуються усі захисні механізми. Окрім перелічених вище властивостей монітора звернень, ядро повинне гарантувати власну незмінність.

Межу довіреної обчислювальної бази називають *периметром безпеки*. Як вже зазначалося, компоненти, що лежать поза периметром безпеки, можуть не бути довіреними. З розвитком розподілених систем поняттю «Периметр безпеки» дедалі частіше надають інший сенс, маючи на увазі межу володінь певної організації. Те, що знаходиться усередині володінь, вважається довіреним, а те, що зовні, — ні.

Механізми безпеки. Згідно з «Помаранчевою книгою», політика безпеки повинна обов'язково включати такі елементи:

- довільне управління доступом;
- безпека повторного використання об'єктів;
- позначки безпеки;
- примусове управління доступом.

Довільне управління доступом (іноді називають *дискреційним*) — це метод розмежування доступу до об'єктів, заснований на обліку особи суб'єкта або групи, в яку суб'єкт входить. Довільність управління полягає в тому, що деяка особа (зазвичай власник об'єкта) може на власний розсуд надавати іншим суб'єктам або відбирати у них права доступу до об'єкта.

Безпека повторного використання об'єктів — важливе доповнення засобів управління доступом, що оберігає від випадкового або умисного витягання конфіденційної інформації зі «сміття». Безпека повторного використання повинна гарантуватися для областей оперативної пам'яті (зокрема, для буферів з образами екрана, розшифрованими паролями тощо), для дискових блоків і магнітних носіїв загалом.

Позначки безпеки складаються з двох частин — рівня секретності і списку категорій. Рівні секретності утворюють впорядковану множину, категорії — неупорядковану. Призначення останніх — описати предметну область, до якої відносяться дані. Для реалізації примусового управління доступом з суб'єктами і об'єктами асоціюються позначки безпеки. Позначка суб'єкта описує його благонадійність, позначка об'єкта — ступінь конфіденційності інформації, яка міститься в ньому.

Примусове (чи мандатне) управління доступом (залежить від волі суб'єктів) засноване на зіставленні позначок безпеки суб'єкта і об'єкта. Після того, як зафіксовані позначки безпеки суб'єктів і об'єктів, виявляються зафіксованими і права доступу.

Суб'єкт може читати інформацію з об'єкта, якщо рівень секретності суб'єкта не нижчий, ніж у об'єкта, а усі категорії, перераховані в позначці безпеки об'єкта, присутні в позначці суб'єкта. У такому разі говорять, що позначка суб'єкта домінує над позначкою об'єкта.

Суб'єкт може записувати інформацію в об'єкт, якщо позначка безпеки об'єкта домінує над позначкою суб'єкта. Зокрема, «конфіденційний» суб'єкт може записувати дані в секретні файли, але не може — в несекретні.

Якщо розуміти політику безпеки як правила розмежування доступу, то механізм підзвітності є доповненням подібної політики. Мета підзвітності — в кожен момент часу знати, хто працює в системі і що робить. Засоби підзвітності діляться на три категорії:

- ідентифікація і аутентифікація;
- надання довіреного шляху;
- аналіз реєстраційної інформації.

Звичайний спосіб ідентифікації — введення імені користувача при вході в систему. Стандартний засіб перевірки достовірності (аутентифікації) користувача — пароль.

Довірений шлях зв'язує користувача безпосередньо з довіреною обчислювальною базою, минувши інші, потенційно небезпечні компоненти ІС. Мета надання довіреного шляху — дати користувачеві можливість переконатися в достовірності обслуговуючої його системи.

«Помаранчева книга» передбачає наявність засобів вибіркового протоколювання як відносно користувачів, так і відносно подій.

Класи безпеки. «Помаранчева книга» Міністерства оборони США відкрила шлях до ранжування інформаційних систем за ступенем довіри безпеки.

У цій книзі визначається **чотири рівні довіри (безпеці)** — D, C, B і A :

- рівень C — довільне управління доступом;
- рівень B — примусове управління доступом;
- рівень A — верифікована безпека.

Рівень D призначений для систем, визнаних незадовільними. У міру переходу від рівня C до A до систем ставляться більш жорсткі вимоги. Рівні C і B підрозділяються на класи (C1, C2, B1, B2, B3) з поступовим зростанням ступеня довіри.

Є **шість класів безпеки** — C1, C2, B1, B2, B3, A1.

За мірою переходу від D до A зростає рівень інформаційної безпеки, а до інформаційної системи висуваються дедалі більш жорсткі вимоги (рис. 2.3).

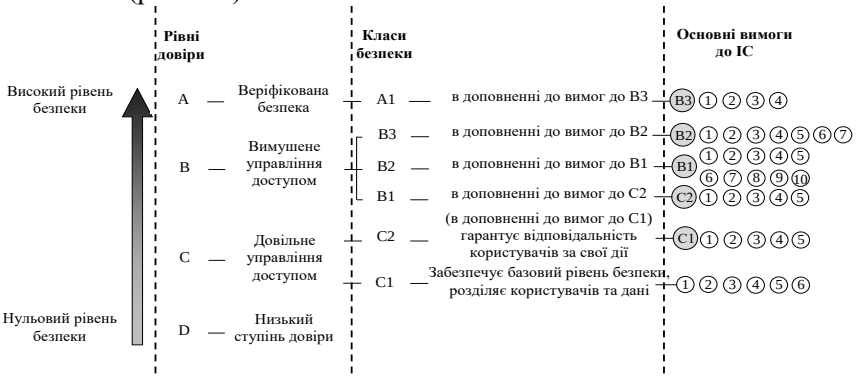

Рис. 2.3. Залежність рівня інформаційної безпеки відповідно до обраного класу безпеки та загальна структура класифікації

Щоб в результаті процедури сертифікації систему можна було віднести до деякого класу, її політика безпеки і рівень гарантованості повинні задовольняти задані вимоги.

Нижче відображені основні вимоги «Помаранчевої книги», які ставляться до рівнів і класів інформаційної безпеки.

Рівень C — Довільне управління доступом

Клас C1 забезпечує базовий рівень безпеки, розділяючи користувачів і дані. Інформаційні системи, що належать до цього класу, повинні відповідати таким основним вимогам:

1) довірена база управляє доступом іменованих користувачів до іменованих об’єктів;

2) користувачі чітко ідентифікують себе; аутентифікаційна інформація користувачів захищена від несанкціонованого доступу;

3) довірена обчислювальна база має ізольовану область для власного виконання, захищену від зовнішніх дій;

4) у наявності є апаратні або програмні засоби, що дають змогу періодично перевіряти коректність функціонування апаратних і мікропрограмних компонентів довіреної обчислювальної бази;

5) захисні механізми протестовані на відсутність способів обходу або руйнування засобів захисту довіреної обчислювальної бази;

6) описаний підхід до безпеки і його застосування під час реалізації довіреної обчислювальної бази.

Клас С2 (у доповнення до вимог до С1) гарантує відповідальність користувачів за свої дії:

1) права доступу гарантуються з точністю до користувача, а доступ до будь-якого об'єкта контролюється;

2) при виділенні об'єкта з пулу ресурсів довіреної обчислювальної бази, усуваються сліди його використання;

3) кожен користувач системи унікальним чином ідентифікується, а кожна реєстрована дія асоціюється з конкретним користувачем;

4) довірена обчислювальна база дозволяє створювати, підтримувати і захищати журнал реєстраційної інформації, що стосується доступу до об'єктів, які контролюються базою;

5) тестування підтверджує відсутність видимих недоліків у механізмах ізоляції ресурсів і захисту реєстраційної інформації.

Рівень В — Примусове управління доступом

Клас В1 (у доповнення до вимог до С2):

1) довірена обчислювальна база управляє позначками безпеки, що асоціюються з кожним суб'єктом і об'єктом, який зберігається;

2) довірена обчислювальна база забезпечує реалізацію примусового управління доступом усіх суб'єктів до усіх об'єктів, що зберігаються;

3) довірена обчислювальна база забезпечує взаємну ізоляцію процесів шляхом розподілу їх адресних просторів;

4) фахівці ретельно аналізують і тестують архітектуру і початковий код системи;

5) існує неформальна або формальна модель політики безпеки, підтримувана довіреною обчислювальною базою.

Клас В2 (у доповнення до вимог до В1):

1) усі ресурси системи, прямо або побічно доступні суб'єктам, забезпечуються позначками секретності;

2) у довіреній обчислювальній базі підтримується довірений комунікаційний шлях для користувача, що виконує операції початкової ідентифікації і аутентифікації;

3) передбачена можливість реєстрації подій, пов'язаних з організацією таємних каналів обміну з пам'яттю;

4) довірена обчислювальна база внутрішньо структурована на добре визначені, відносно незалежні модулі;

5) системний архітектор ретельно аналізує можливість організації таємних каналів обміну з пам'яттю і оцінює максимальну пропускну спроможність кожного виявленого каналу;

6) продемонстрована відносна стійкість довіреної обчислювальної бази до спроб проникнення;

7) модель політики безпеки є формальною;

8) для довіреної обчислювальної бази існують описові специфікації верхнього рівня, які точно і повно визначають її інтерфейс;

9) у процесі розробки і супроводу довіреної обчислювальної бази використовується система управління конфігураціями, що забезпечує контроль змін у специфікаціях верхнього рівня, архітектурних даних, початкових текстах, працюючій версії об'єктного коду, тестових даних і документації;

10) тести підтверджують дієвість заходів зі зменшення пропускної спроможності таємних каналів передачі інформації.

Клас В3 (у доповнення до вимог до В2):

1) для довільного управління доступом використовуються списки управління доступом із вказівкою дозволених режимів;

2) передбачена можливість реєстрації появи і накопичення подій, що несуть загрозу порушення політики безпеки системи. Адміністратор безпеки негайно отримує повідомлення про спроби порушення політики безпеки; система у разі продовження таких спроб відразу їх зупиняє;

3) довірена обчислювальна база спроектована і структурована так, щоб використовувати повний і концептуально простий захисний механізм з точно визначеною семантикою;

4) аналізується і виявляється можливість тимчасових таємних каналів;

5) існує роль адміністратора безпеки, отримати яку можна тільки після виконання явних, протокольованих дій;

6) є процедури і/або механізми, що дозволяють без послаблення захисту здійснити відновлення після збою;

7) продемонстровано стійкість довіреної обчислювальної бази до спроб проникнення.

Рівень А — Верифікована безпека

Клас А1 (у доповнення до вимог до В3):

1) тестування продемонструвало те, що реалізація довіреної обчислювальної бази відповідає формальним специфікаціям верхнього рівня;

2) представлені формальні специфікації верхнього рівня; використовуються сучасні методи формальної специфікації і верифікації систем;

3) механізм управління конфігураціями поширюється на увесь життєвий цикл і всі компоненти системи, що мають відношення до забезпечення безпеки;

4) описано відповідність між формальними специфікаціями верхнього рівня і початковими текстами.

Отже, можна зробити висновок, що дана класифікація побудована, в першу чергу, для оцінювання ступеня забезпечення ІБ в ІС. Унаслідок цього, питання протидії розглядаються з погляду саме оцінки, а не рекомендацій для побудови КСЗІ ІС.

Основним недоліком такого підходу є те, що одна і та сама реальна загроза або не підходить ні під одну із класифікаційних ознак, або навпаки, задовольняє декільком [64].

Публікація «Помаранчевої книги» стала подією в області ІБ. З'явився загальновизнаний понятійний базис, без якого навіть обговорення проблем ІБ було б складним.

«Критерії безпеки комп'ютерних систем» МО США стали першою спробою створити єдиний стандарт безпеки, розрахований на розробників, споживачів і фахівців із сертифікації комп'ютерних систем. «Помаранчева книга» стала основою для розробників усіх інших стандартів інформаційної безпеки і досі, з урахуванням доповнень і пояснень, використовується в США як керівний документ під час сертифікації комп'ютерних систем обробки інформації. Слабким місцем «Помаранчевої книги» є недостатня увага до вимог гарантії оцінки [65].

2.2.3. Підхід «Європейських критеріїв» безпеки інформаційних технологій (гармонізовані критерії Європейських держав)

Європейські критерії безпеки інформаційних технологій [Information Technology Security Evaluation Criteria (ITSEC)] — стандарт інформаційної безпеки, розроблений у країнах Європи

(Франція, Німеччина, Нідерланди та Велика Британія) у 1991 р. Європейські критерії розглядають такі завдання засобів інформаційної безпеки:

• захист інформації від несанкціонованого доступу з метою забезпечення *конфіденційності*;

• забезпечення *цілісності* інформації за допомогою захисту її від несанкціонованої модифікації або знищення;

• забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні (*доступність*).

Для вирішення проблеми визнання засобів захисту ефективними в критеріях уведене поняття гарантій засобів захисту. Гарантії включають у себе два аспекти: ефективність, що відображає відповідність засобів безпеки завданням, що вирішуються, і коректність, що характеризує процес їх розроблення й функціонування. Загальна оцінка рівня безпеки системи складається з функціональної потужності засобів захисту і рівня гарантій їхньої реалізації.

Є сім рівнів гарантій в «Європейських критеріях» — від Е0 до Е6 (у порядку зростання, рис. 2.4).

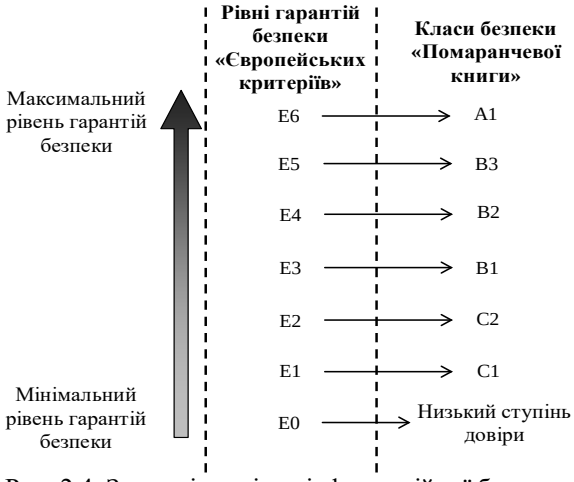

Рис. 2.4. Залежність рівня інформаційної безпеки відповідно від обраного рівня гарантії безпеки

Рівень Е0 означає мінімальні гарантії. При перевірці гарантій аналізується весь життєвий цикл системи — від початкової фази проектування до експлуатації і супроводження. Рівні гарантій від Е1 до Е6 вишикувані з наростанням вимог ретельності контролю.

Так, на рівні Е1 аналізується тільки загальна архітектура системи, а гарантії засобів захисту підтверджуються функціональним тестуванням. На рівні Е3 до аналізу залучаються вихідні тексти програм і схеми апаратного забезпечення. На рівні Е6 потрібен формальний опис функцій безпеки, загальної архітектури, а також політики безпеки.

Загалом розподіл вимог по рівнях гарантованості в європейських критеріях відповідає аналогічному розподілу для класів безпеки С1 — А1 з «Помаранчевої книги» [52; 66].

Вимоги до політики безпеки і до наявності захисних механізмів не є складовою частиною критеріїв, хоча, щоб полегшити формулювання мети оцінювання, критерії містять як додаток опис десяти наближених класів функціональності.

П'ять із них (F-C1, F-C2, F-B1, F-B2, F-B3) з урахуванням рівнів гарантованості відповідають класам безпеки «Помаранчевої книги»: F-C1, E1→C1; F-C2, E2→C2; F-B1, E3→B1; F-B2, E4→B2; F-B3, E5→B3; F-B3, E6→A1.

Є ще п'ять додаткових класів. Клас F-IN характеризується підвищеними вимогами до цілісності даних і програм, що є типовим для систем управління базами даних. Ці вимоги конкретизуються через підвищені вимоги до ідентифікації і аутентифікації користувачів, управління доступом, реєстрації і обліку, аудиту.

Клас F-AV характеризується підвищеними вимогами до доступності, що істотно, наприклад, для систем управління технологічними процесами. Ці вимоги конкретизуються через підвищені вимоги до надійності обслуговування (безперебійної реалізації критично важливих функцій) і відновлення після відмов. Незалежно від рівня завантаження повинен також гарантуватися час реакції на певні події і відсутність тупиків.

Клас F-DI характеризується підвищеними вимогами до забезпечення цілісності даних, які передаються, шляхом використання імітостійких методів виявлення і виправлення помилок.

Знання алгоритму виявлення спотворень не повинне давати можливість виробляти несанкціоновану модифікацію інформації.

Повинні виявлятися і трактуватися як помилки спроби зміни даних. Вимоги ідентифікації, аутентифікації користувачів і аудиту аналогічні класу F-IN, є додаткові вимоги щодо реєстрації й обліку помилок під час обміну даними.

Клас F-DC характеризується підвищеними вимогами до забезпечення конфіденційності при обміні даними шляхом використання криптографічних пристроїв. При цьому ключі шифрування мають бути надійно захищені від несанкціонованого доступу.

Клас F-DX характеризується підвищеними вимогами до забезпечення конфіденційності і цілісності інформації в мережевих конфігураціях шляхом наскрізного шифрування масивів даних, які передаються по каналах зв'язку, і надійної ідентифікації (як помилки) несанкціонованої зміни даних, що передаються, і даних реєстрації.

Вимоги по ідентифікації, аутентифікації користувачів і аудиту аналогічні вимогам класу F-IN. У підсистемі реєстрації і обліку мають бути компоненти реєстрації даних ідентифікації і аутентифікації користувачів, ідентифікації помилок під час обміну даними, встановлення з'єднання, повідомленою користувачеві інформації, дата і час отримання даних.

Основний зміст вимог додаткових класів безпеки ITSEC наведений в табл. 2.1

Таблиця 2.1

Вимоги додаткових класів безпеки ITSEC

Підсистеми та вимоги	Класи				
	F-IN	F-AV	F-DI	F-DC	F-DX
Підсистема управління доступом					
Ідентифікація та аутентифікація користувачів	+	–	F-IN	–	F-IN
Контроль доступу під час:					
виконання, знищення, перейменування (для об'єктів, які виконуються);	+	–	–	–	–
читання, запису, додавання, знищення, перейменування (для всіх інших об'єктів);	+	–	–	–	–
створення та знищення об'єктів деякого типу	+	–	–	–	–
Контроль доступу до переданої раніше інформації	–	–	–	–	+
Підсистема реєстрації та обліку					
Реєстрація та облік:					
ідентифікації користувача та його терміналу, успіху або відмови спроби;	+	–	+	–	F-DI
звернення до захищеного об'єкта доступу;	+	–	–	–	–
створення або знищення об'єктів доступу, які захищаються;	+	–	–	–	–
зміни складу користувачів;	+	–	–	–	–
введення або знищення носіїв даних;	+	–	–	–	–

Закінчення табл. 2.1

Підсистеми та вимоги	Класи				
	F-IN	F-AV	F-DI	F-DC	F-DX
запуску або завершення програм або процесів;	+	–	–	–	–
визначення або знищення типів;	+	–	–	–	–
привласнення типу об'єкта;	+	–	–	–	–
представлення або анулювання прав доступу для об'єкта або типу об'єкта;	+	–	–	–	–
помилок в обміні даними;	–	–	+	–	F-DI
заснування з'єднання (ім'я суб'єкта та об'єкта доступу, параметри з'єднання);	–	–	+	–	F-DI
ідентифікованих користувачів-відправників та користувачів-приймачів, переданої інформації;	–	–	–	–	+
дати та години всіх подій, що реєструються	+	–	+	–	+
Аудит	+	–	F-DI	–	F-DI
Криптографічна підсистема					
Автоматичне шифрування інформації, що передається, та дешифрування інформації, яку отримує користувач	–	–	–	+	+
Використання атестованих (сертифікованих) криптографічних засобів	–	–	–	+	=
Надійний захист ключів	–	–	–	+	=
Підсистема забезпечення цілісності					
Виключення несанкціонованої зміни даних користувача та даних реєстрації та обліку	–	–	–	–	+
Надійна ідентифікація (як помилок) несанкціонованої зміни даних	–	–	+	–	+
Підсистема забезпечення доступності					
Безвідмовність виконання критично важливих функцій	–	+	–	–	–
Реінтеграція системи після відмови та відновлення окремих компонентів	–	+	–	–	–
Гарантований час реакції на окремі події незалежно від завантаження системи	–	+	–	–	–

Примітка. У таблиці введено такі позначення:

«–» — немає вимог до цього класу; «+» — нові або додаткові вимоги; «=» — вимоги збігаються з вимогами попереднього класу; «F-IN» — вимоги збігаються з вимогами вказаного класу.

Рівні безпеки в «Європейських критеріях» — рівні для визначення ступеня безпеки системи. В цих критеріях визначені три рівні безпеки — базовий, середній і високий.

Безпека вважається *базовою*, якщо засоби захисту здатні протистояти окремим випадковим атакам.

Безпека вважається *середньою*, якщо засоби захисту здатні протистояти зловмисникам, що мають обмежені ресурси та можливості.

Безпеку можна вважати *високою*, якщо є впевненість, що засоби захисту можуть бути подолані тільки зловмисниками з високою кваліфікацією, набір можливостей і ресурсів яких не передбачувані.

«Європейські критерії» покладені в основу багатьох стандартів безпеки комп'ютерних систем. На основі цих критеріїв Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України розроблені нормативні документи системи технічного захисту інформації України стосовно технічного захисту інформації на програмно-керованих автоматичних телефонних станціях (АТС) загального користування [52].

Таким чином, в «Європейських критеріях» уперше вводиться поняття гарантованості і шкала для критеріїв гарантованості — рівні гарантії. «Європейські критерії» надають вимогам гарантованості навіть більше значення, ніж функціональним вимогам. «Європейські критерії» повністю обирають класи безпеки «Помаранчевої книги» і вводять ще п'ять додаткових класів [65]. Принципово важливою ознакою «Європейських Критеріїв» є відсутність вимог до умов, у яких повинна працювати інформаційна система [56].

Гармонізовані критерії європейських країн стали для свого часу передовим стандартом, що створило передумови для появи «Загальних критеріїв».

2.2.4. Федеральні критерії безпеки інформаційних технологій

Федеральні критерії безпеки інформаційних технологій [Federal Criteria for Information Technology Security (FCITS)] — стандарт інформаційної безпеки, розроблений Національним інститутом стандартів і технологій США (NIST) і Агентством національної безпеки США (NSA) у 90-х роках XX ст. для використання в Американському федеральному стандарті з оброблення інформації (Federal Information Processing Standard), який повинен був замінити «Помаранчеву книгу» [10; 29; 66].

«Федеральні критерії» охоплюють майже весь спектр проблем, пов'язаних із захистом та забезпеченням безпеки, оскільки включають усі аспекти конфіденційності, цілісності та доступності.

Основними об'єктами застосування вимог безпеки критеріїв є продукти інформаційних технологій (ІТ-продукти) і системи обробления інформації.

Головною метою створення «Федеральних критеріїв» було визначення універсального і відкритого для подальшого розвитку набору основних вимог безпеки, що ставляться до сучасних інформаційних технологій. Стандарт визначає обґрунтований і структурований підхід до розробки вимог безпеки, інформаційних технологій, що висуваються до продуктів, з урахуванням сфер їх застосування. Стандарт є узагальненням основних принципів убезпечення безпеки інформаційних технологій, розроблених у 80-ті роки XX ст., і забезпечує спадкоємність відносно до них з метою збереження досягнень в галузі захисту інформації.

«Федеральні критерії» містять положення, що належать тільки до окремих продуктів інформаційних технологій. Питання побудови систем обробки інформації з набору ІТ-продуктів не є предметом розгляду цього документу.

Профіль захисту. Ключовим поняттям концепції інформаційної безпеки «Федеральних критеріїв» є поняття «Профіль захисту» (*protection profile*). Профіль захисту — це нормативний документ, який регламентує всі аспекти безпеки ІТ-продукту у вигляді вимог до його проектування, технології розробки і кваліфікаційного аналізу. Як правило, один профіль захисту описує кілька близьких за структурою і призначенням ІТ-продуктів. Основна увага в профілі захисту приділяється вимогам до складу засобів захисту і якості їх реалізації, а також їх адекватності передбачуваним загрозам безпеки.

Профіль захисту складається з таких п'яти розділів:

1. Опис.
2. Обґрунтування.
3. Функціональні вимоги до ІТ-продукту.
4. Вимоги до технології розробки ІТ-продукту.
5. Вимоги до процесу кваліфікаційного аналізу ІТ-продукту.

Опис профілю містить класифікаційну інформацію, необхідну для його ідентифікації в спеціальній картотеці.

«Федеральні критерії» пропонують підтримувати таку картотеку на загальнодержавному рівні. Це дозволить будь-якій організації скористатися створеними раніше профілями захисту безпосередньо або використовувати їх як прототипи під час розробки нових.

Обґрунтування містить опис середовища експлуатації, передбачуваних загроз безпеки і методів використання ІТ-продукту. Крім того, цей розділ містить детальний перелік завдань із забезпечення безпеки, які вирішуються за допомогою даного профілю. Ця інформація дає можливість визначити, якою мірою цей профіль придатний для застосування в тій або іншій ситуації.

Передбачається, що цей розділ орієнтований на служби безпеки організацій, які вивчають можливість використання ІТ-продукту, який відповідає даному профілю захисту.

Функціональні вимоги. Розділ функціональних вимог до ІТ-продукту містить опис функціональних можливостей засобів захисту ІТ-продукту і визначає умови, в яких забезпечується безпека у вигляді переліку загроз, яким успішно протистоять запропоновані засоби захисту. Загрози, що лежать поза цим діапазоном, мають бути усунені за допомогою додаткових, тобто таких, що не входять до складу продукту, засобів убезпечення.

Розділ вимог до технології розробки ІТ-продукту охоплює всі етапи його створення, починаючи від розробки проекту і вирішуючи введенням готової системи в експлуатацію. Розділ містить вимоги як до самого процесу розробки, так і до умов, в яких вона проводиться, до використовуваних технологічних засобів, а також до документування цього процесу. Виконання вимог цього розділу є обов'язковою умовою для проведення кваліфікаційного аналізу і сертифікації ІТ-продукту.

Розділ вимог до процесу кваліфікаційного аналізу ІТ-продукту регламентує порядок проведення кваліфікаційного аналізу у вигляді методики досліджень і тестування ІТ-продукту. Обсяг необхідних досліджень залежить від найбільш імовірних типів загроз, середовища застосування і планованої технології експлуатації.

Функціональні вимоги «Федеральних критеріїв» розділені на вісім класів і визначають усі аспекти функціонування ядра безпеки (Trusted Computing Base, TCB). *Під ядром безпеки* розуміється сукупність апаратних, програмних і спеціальних компонентів обчислювальної системи, що реалізовують функції захисту і убезпечення. Таксономію класів функціональних вимог показано на рис. 2.5.

Склад і зміст включених до профілю захисту функціональних вимог визначаються середовищем експлуатації ІТ-продукту.

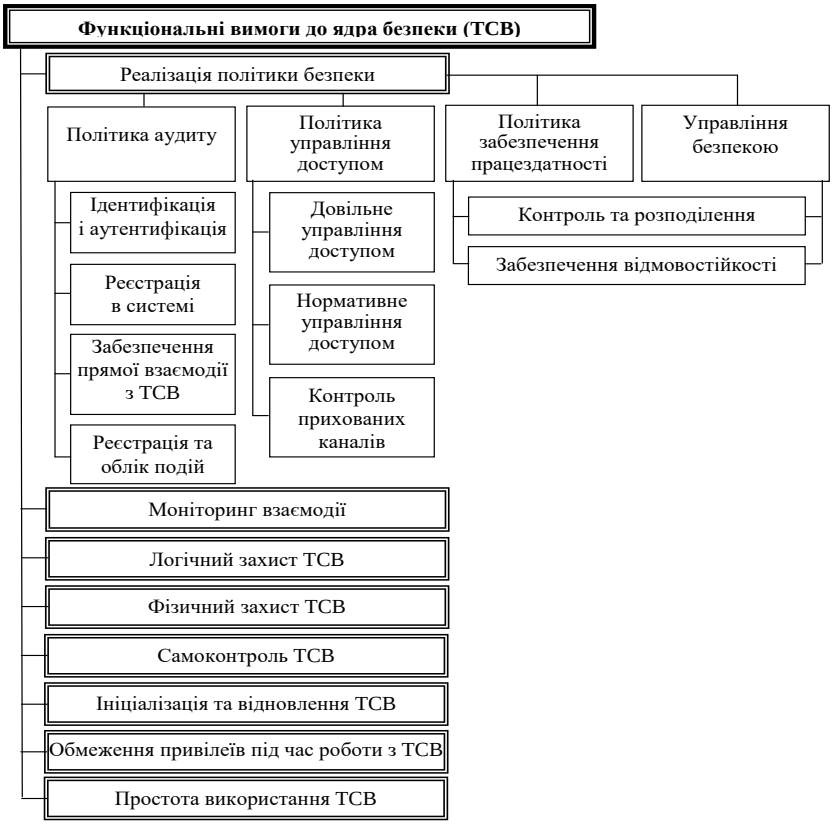

Рис. 2.5. Таксономія функціональних вимог
«Федеральних критеріїв»

Щоб обґрунтувати вибір тих або інших вимог і не вступати в протиріччя з існуючими стандартами в області безпеки ІТ-продуктів, функціональні вимоги, наведені в «Федеральних критеріях», проранжовані за рівнями за допомогою таких чотирьох критеріїв: «широта» сфери застосування, міра деталізації, функціональний склад засобів захисту, забезпечуваний рівень безпеки.

Ранжування завжди припускає встановлення деякого відношення порядку. Проте незалежне ранжування функціональних вимог за кожним з наведених критеріїв хоча і дає деяке уявлення про відмінності між функціональними можливостями засобів захисту, не дозволяє встановити чітку, лінійну шкалу рівнів безпеки.

Однозначного відношення порядку, визначеного на множині функціональних вимог, не існує, оскільки значення вимог і рівень забезпечуваного ними захисту залежать не лише від їх змісту, але і від призначення ІТ-продукту і середовища його експлуатації.

Для одних систем найбільш важливими будуть ідентифікація і аутентифікація користувачів, а для інших — реалізація політики управління доступом або забезпечення працездатності.

Тому в «Федеральних критеріях» відсутні рекомендації як щодо вибору і застосування тих або інших функціональних вимог, так і за визначенням їх ролі в системі забезпечення безпеки.

Замість жорстких вказівок цей документ містить узгоджений з попередніми йому стандартами («Помаранчева книга», «Європейські критерії») ранжований перелік функціональних вимог і надає розробникам профілю захисту можливість самостійно зробити вибір необхідних методів і засобів забезпечення безпеки, заснований на призначенні і специфіці середовища експлуатації ІТ-продукту.

Вимоги до технології розробки ІТ-продукту

Основне призначення вимог до технології розробки ІТ-продукту — забезпечити адекватність умов розробки функціональним вимогам, висуненим у відповідному розділі профілю захисту, і встановити відповідальність розробника за коректність реалізації цих вимог.

Цей розділ регламентує процес створення, тестування, документування і супроводу ІТ-продукту. Таксономія вимог до технології розробки ІТ-продукту наведено на рис. 2.6.

«Федеральні критерії» містять ранжований перелік типових вимог до технології розробки ІТ-продуктів. Виконання вимог до технології розробки є необхідною умовою для проведення процедури кваліфікаційного аналізу.

Вимоги до процесу кваліфікаційного аналізу ІТ-продукту. Вимоги до процесу кваліфікаційного аналізу ІТ-продукту покликані забезпечити надійність і коректність цього процесу.

Розділ містить три групи вимог, що регламентують аналіз, контроль і тестування ІТ-продукту.

Таксономію вимог цього розділу наведено на рис. 2.7.

Ці вимоги регламентують процес кваліфікаційного аналізу тільки загалом і, за задумом розробників стандарту, повинні слугувати основою для розробки спеціалізованих методик кваліфікації рівня безпеки, орієнтованих на різні сфери застосування і типи ІТ-продуктів.

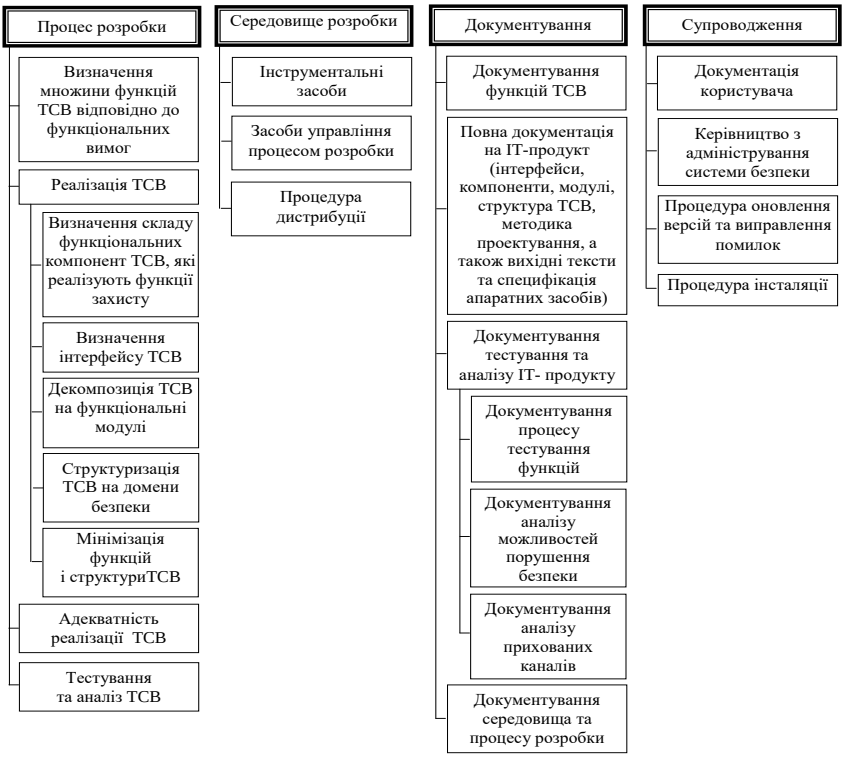

Рис. 2.6. Таксономія вимог «Федеральних критеріїв» до технології розробки ІТ-продукту

Рис. 2.7. Таксономія вимог «Федеральних критеріїв» до процесу кваліфікаційного аналізу ІТ-продукту

Отже, відповідно до «Федеральних критеріїв» процес розробки систем оброблення інформації здійснюється у вигляді послідовності таких основних етапів:

– розроблення та аналіз профілю захисту;

– розроблення і кваліфікаційний аналіз ІТ-продуктів;

– компонування й сертифікація системи оброблення інформації.

«Федеральні критерії» регламентують тільки перший етап цієї схеми — розробку та аналіз профілю захисту. Процес створення ІТ-продуктів і компонування систем оброблення інформації залишаються за межами цього стандарту.

2.2.5. «Канадські критерії» безпеки інформаційних технологій

«Канадські критерії» безпеки комп'ютерних систем [Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)] — національний стандарт інформаційної безпеки, розроблений Центром безпеки відомства безпеки зв'язку Канади (Canadian System Security Centre Communication Security Establishment) в 90-х роках XX ст. [10; 29; 67].

«Канадські критерії» розроблялися для використання як національний стандарт безпеки комп'ютерних систем. На відміну від «Помаранчевої книги», орієнтованої переважно на розробку і сертифікацію багатокористувацьких операційних систем і потребуючої певної інтерпретації для інших застосувань (наприклад, для баз даних і мереж), «Канадські критерії» були спочатку спрямовані на широкий діапазон КС. Цей стандарт може бути використаний для розробки вимог безпеки, специфікацій засобів захисту і сертифікації ПЗ робочих станцій (РС) і багатопроцесорних ОС, персональних і багатокористувацьких операційних систем, систем управління базами даних, розподілених, мережевих, убудованих, об'єктно-орієнтованих та інших систем.

У «Канадських критеріях» запропоновано оригінальний підхід до опису взаємодії користувачів із комп'ютерною системою, інваріантний відносно до політики безпеки. Усі компоненти системи, які знаходяться під керуванням ядра безпеки, називаються *об'єктами*.

Об'єкти можуть знаходитися в одному з таких трьох станів: *об'єкт-користувач, об'єкт-процес, пасивний об'єкт*, і залежно від стану позначають користувачів, процеси та об'єкти відповідно.

Під час опису критеріїв конфіденційності та цілісності (довільного та нормативного керування доступом і цілісністю) в «Канадських критеріях» використовується поняття тег.

Тега — сукупність атрибутів, асоційованих із користувачем, процесом або проектом. Тегою може бути унікальний ідентифікатор, позначка безпеки або цілісності, криптографічний ключ, таблиця прав доступу або інші атрибути відповідно до реалізованої в комп'ютерній системі політики безпеки.

Можливість застосування «Канадських критеріїв» до такої кількості різних за призначенням систем визначається використовуваним у них принципом дуального представлення вимог щодо безпеки у вигляді функціональних вимог до засобів захисту і вимог до адекватності їх реалізації (рис. 2.8).

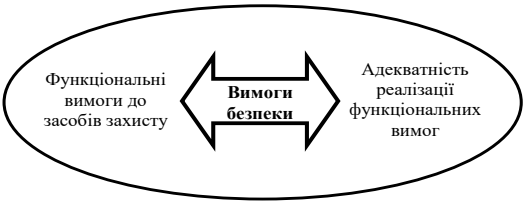

Рис. 2.8. Принцип дуальності в «Канадських критеріях»

«Канадські критерії» є добре збалансованим конгломератом «Помаранчевої книги» і «Федеральних критеріїв», посилених вимогами гарантій реалізації політики безпеки, і поряд з іншими стандартами стали основою для розроблення «Загальних критеріїв» безпеки інформаційних технологій.

«Функціональні критерії» — це часткові метрики, призначені для визначення показників ефективності засобів захисту у вигляді рівня їх можливостей з віддзеркалення загроз відповідного типу. Функціональні критерії розділяються на чотири групи: критерії конфіденційності, цілісності, працездатності і аудиту (рис. 2.9).

Ранжування по рівнях (вище наведено число рівнів, не враховуючи нульового) усередині кожної групи критеріїв проводиться на підставі потужності використовуваних методів захисту і класу відбиваних загроз відповідного типу.

Рівні з великим номером забезпечують повнішу функціональність і, відповідно, вищу міру безпеки.

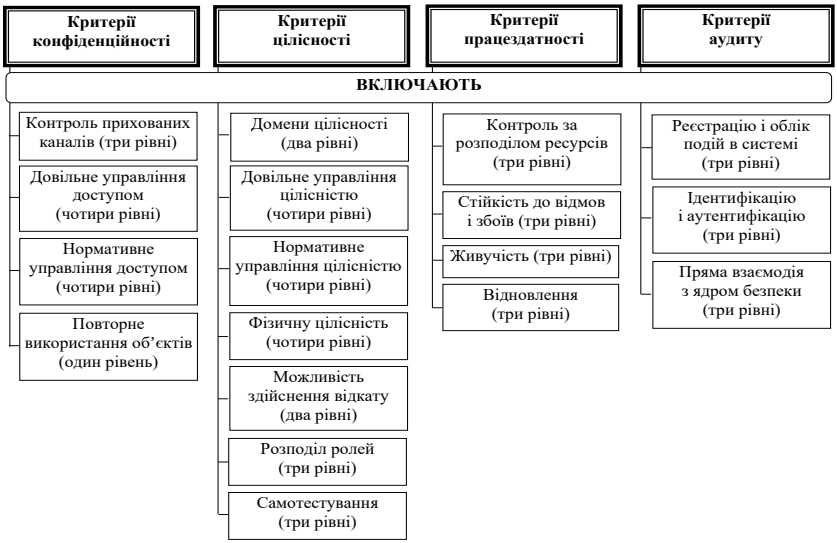

Рис. 2.9. Групи «Функціональних критеріїв»

Адекватність реалізації визначається тим, наскільки точно і послідовно засоби захисту реалізують прийняту в комп'ютерній системі політику безпеки. Згідно з «Канадськими критеріями», політика безпеки є множиною правил, що регламентують обробку, зберігання і використання інформації.

Критерії адекватності розглядаються без розподілу на підгрупи і визначають вимоги до процесу проектування і розробки комп'ютерної системи.

Рівень адекватності (від 0 до 7) привласнюється усій системі в цілому, причому вищий рівень означає повнішу і коректнішу реалізацію політики безпеки (рис. 2.10).

Рис. 2.10. Адекватність реалізації функціональних вимог до засобів захисту

Отже, «Канадські критерії» визначають ступінь безпеки КС як сукупність функціональних можливостей використовуваних засобів захисту, що характеризується частковими показниками забезпечуваного рівня безпеки, і одного узагальненого параметра — рівня адекватності реалізації політики безпеки.

До складу додатків до «Канадських критеріїв» входять керівництва із застосування функціональних критеріїв і критеріїв адекватності реалізації, а також детальний опис запропонованої в них концепції забезпечення безпеки інформації. Є додаток, який включає набір стандартних профілів захисту, що містять типові набори вимог до КС, що застосовуються в державних установах. Цей підхід має багато спільного з концепцією профілів захисту, запропонованого в «Федеральних критеріях» США.

«Канадські критерії оцінки безпеки комп'ютерних систем» стали першим стандартом ІБ, у якому на рівні структури документу функціональні вимоги до засобів захисту відокремлені від вимог гарантії оцінки (адекватності реалізації).

У «Канадських критеріях» відкидається підхід до оцінки рівня безпеки за допомогою універсальної шкали і використовується незалежне ранжування вимог за кожним розділом, що забезпечує гнучкість у підході до оцінки безпеки різних типів виробів і систем.

«Канадські критерії безпеки комп'ютерних систем» були покладені в основу «Критеріїв оцінки захищеності інформації» в КС від НСД [10], розроблених Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України для системи ТЗІ України.

2.2.6. Загальні критерії безпеки інформаційних технологій (ISO/IEC 15408)

У 1990 р. під егідою Міжнародної організації зі стандартизації (ISO) були розгорнуті роботи зі створення стандарту у галузі оцінювання безпеки інформаційних технологій (ІТ). Розробка цього стандарту мала на меті [68]:

– уніфікацію національних стандартів в галузі оцінювання безпеки ІТ;

– підвищення рівня довіри до оцінки безпеки ІТ;

– скорочення витрат на оцінювання безпеки ІТ на основі взаємного визнання сертифікатів.

Поява проекту міжнародного стандарту «Загальні критерії оцінки безпеки інформаційних технологій» стало якісно новим етапом у розвитку нормативної бази оцінки безпеки ІТ.

Загальні критерії (ЗК) узагальнили зміст і досвід використання «Помаранчевої книги», розвинули рівні гарантії оцінки «Європейських критеріїв», утілили в реальні структури концепцію типових профілів захисту «Федеральних критеріїв» США.

У «Загальних критеріях» проведено класифікування широкого набору вимог безпеки ІТ, визначено структури їх групування і принципи цільового використання. Головні переваги «Загальних критеріїв» — повнота і систематизація вимог безпеки, гнучкість у застосуванні і відкритість для наступного розвитку. У праці [69] визначено, що за оцінками фахівців у галузі інформаційної безпеки за рівнем систематизації, повнотою та можливостями деталізації вимог, універсальністю та гнучкістю у застосуванні ЗК є найбільш досконалим з існуючих на сьогодні стандартів. За своїми особливостями і будовою він має необмежені можливості для розвитку і являє собою базовий стандарт, який містить методологію завдання вимог і оцінки безпеки ІТ, а також систематизований каталог вимог безпеки.

У розробці ЗК брали участь Національний інститут стандартів і технології, а також Агентство національної безпеки (США), Установа безпеки комунікацій (Канада), Агентство інформаційної безпеки (Німеччина), Агентство національної безпеки комунікацій (Голландія), Органи виконання Програми безпеки і сертифікації ІТ (Англія), Центр забезпечення безпеки систем (Франція).

У січні 1996 р. була випущена версія 1.0 Загальних критеріїв, в травні 1998 р. — версія 2.0, а 4 червня 1999 р. міжнародна організація зі стандартизації затвердила міжнародний стандарт ISO 15408 «Критеріїв оцінки безпеки інформаційних технологій» [29].

Цей міжнародний стандарт став підсумком майже десятирічної роботи фахівців декількох країн, він увібрав у себе досвід документів національного і міжнаціонального масштабу, що існували на той час. У зв’язку із цим (з історичних причин) цей стандарт часто називають «Загальними критеріями» (або навіть ЗК) [56].

«Загальні критерії» насправді є метастандартом, що визначає інструменти оцінки безпеки ІС і порядок їх використання. На відміну від «Помаранчевої книги», ЗК не містять зумовлених «класів без-

пеки». Такі класи можна будувати, виходячи з вимог безпеки, існуючих для конкретної організації і/або конкретної інформаційної системи.

«Загальні критерії» розроблені так, щоб задовольнити потреби трьох категорій користувачів: споживачів об'єкта оцінки, розробників об'єкта оцінки і оцінювачів об'єкта оцінки. Під об'єктом оцінки (ОО) розуміється апаратно-програмний продукт або інформаційна система. До таких об'єктів відносяться, наприклад, операційні системи, обчислювальні мережі, розподілені системи, прикладні програми.

До розглянутих у ЗК аспектів безпеки належать: захист від НСД, модифікації або втрати доступу до інформації при дії загроз, що є результатом навмисних або ненавмисних дій. Захищеність від цих трьох типів загроз зазвичай називають *конфіденційністю, цілісністю* і *доступністю*.

З погляду програміста, ЗК можна вважати набором бібліотек, що допомагають писати змістовні програми, — завдання з безпеки, типові профілі захисту тощо. Як і «Помаранчева книга», ЗК містять два основні види вимог безпеки:

- **функціональні** — відповідають активному аспекту захисту, які ставляться до функцій безпеки і механізмів, що реалізовують їх;
- **вимоги довіри** — відповідають пасивному аспекту, які висуваються до технології і процесу розробки.

Для певного об'єкта оцінки — апаратно-програмного продукту або ІС ставляться вимоги безпеки, а їх виконання перевіряється.

Дуже важливо, що безпека в ЗК розглядається не статично, а водночас і до життєвого циклу об'єкта оцінки. Виділяються такі етапи:

- визначення призначення, умов застосування, цілей і вимог безпеки;
- проектування і розробка;
- випробування, оцінка і сертифікація;
- впровадження і експлуатація.

У ЗК об'єкт оцінки розглядається в контексті середовища безпеки, яка характеризується певними умовами і загрозами.

У свою чергу, загрози характеризуються такими параметрами:

- джерело загрози;
- метод дії;

- вразливі місця, які можуть бути використані;
- ресурси (активи), які можуть постраждати.

Вразливі місця можуть виникати через недолік у:

- вимогах безпеки;
- проектуванні;
- експлуатації.

Недоліки по можливості слід усунути, мінімізувати або принаймні обмежити можливий збиток від їх умисного використання або випадкової активізації.

З точки зору технології програмування в ЗК використаний застарілий бібліотечний (не об'єктний) підхід. Щоб структурувати простір вимог, у «Загальних критеріях» введена ієрархія клас–сімейство–компонент–елемент:

1. **Класи** визначають найбільш загальне, предметне угрупування вимог (наприклад, функціональні вимоги підзвітності).
2. **Сімейства** в межах класу розрізняються за складністю та іншими вимогами.
3. **Компонент** — мінімальний набір вимог, що фігурує як ціле.
4. **Елемент** — неподільна вимога.

Як і між бібліотечними функціями, між компонентами ЗК можуть існувати залежності. Вони виникають, коли компонент сам по собі недостатній для досягнення мети безпеки. Взагалі, не усі комбінації компонентів мають сенс, і поняття залежності якоюсь мірою компенсує недостатню виразність бібліотечної організації, хоча і не замінює об'єднання функцій у змістовні об'єктні інтерфейси. За допомогою бібліотек можуть формуватися два види нормативних документів: профіль захисту і завдання з безпеки.

Профіль захисту є типовим набором вимог, які повинні задовольняти продукти і/або системи певного класу (наприклад, операційні системи на комп'ютерах в урядових організаціях).

Завдання з безпеки містить сукупність вимог до конкретної розробки, виконання яких забезпечує досягнення поставлених цілей безпеки.

У ЗК немає готових класів захисту. Сформувати класифікацію в термінах «Загальних критеріїв» означає визначити декілька ієрархічно впорядкованих профілів захисту, максимально можливою мірою тих, що використовують стандартні функціональні вимоги і вимоги довіри безпеки.

Виділення деякої підмножини з усієї множини профілів захисту багато в чому має суб'єктивний характер. За деяких міркувань (одним з яких є бажання дотримуватися об'єктно-орієнтованого підходу) доцільно сформувати спочатку відправну точку класифікації, виділивши базовий (мінімальний) профіль захисту, а додаткові вимоги компонувати у функціональні пакети.

Функціональний пакет — це неодноразово використовувана сукупність компонентів, об'єднаних для досягнення певної мети безпеки. «Загальні критерії» не регламентують структуру пакетів, процедури верифікації, реєстрації тощо, відводячи їм роль технологічного засобу формування профілю захисту.

Базовий профіль захисту повинен включати вимоги до основних (обов'язковим у будь-якому випадку) можливостей. Похідні профілі виходять з базового шляхом додавання необхідних пакетів розширення.

Функціональні вимоги. Ці вимоги згруповані на основі виконуваної ними ролі або обслуговуваної мети безпеки. Всього в «Загальних критеріях» наведено 11 функціональних класів, 66 сімейств, 135 компонентів. Перелічимо класи функціональних вимог ЗК:

1) ідентифікація й аутентифікація;

2) захист даних користувача;

3) захист функцій безпеки (вимоги відносяться до цілісності і контролю цих сервісів безпеки, а також механізмів, що реалізовують їх);

4) управління безпекою (вимоги цього класу відносяться до управління атрибутами і параметрами безпеки);

5) аудит безпеки (виявлення, реєстрація, зберігання, аналіз даних, таких, що стосуються безпеки об'єкта оцінки, реагування на можливе порушення безпеки);

6) доступ до об'єкта оцінки;

7) приватність (захист користувача від розкриття і несанкціонованого використання його ідентифікаційних даних);

8) використання ресурсів (вимоги до доступності інформації);

9) криптографічна підтримка (управління ключами);

10) зв'язок (аутентифікація сторін, що беруть участь в обміні даними);

11) довірений маршрут/канал (для зв'язку з сервісами безпеки).

Наприклад, клас «Приватність» містить чотири сімейства функціональних вимог:

1. **Анонімність**. Дає змогу виконувати дії без розкриття ідентифікатора користувача іншим користувачам, суб'єктам і/або об'єктам. Анонімність може бути повною або вибірковою. В останньому випадку вона може відноситися не до усіх операцій і/або не до усіх користувачів (наприклад, у вповноваженого користувача може залишатися можливість з'ясування ідентифікаторів користувачів).

2. **Псевдоанонимність.** Нагадує анонімність, але при застосуванні псевдоніма підтримується посилання на ідентифікатор користувача для забезпечення підзвітності або для інших цілей.

3. **Неможливість асоціації**. Сімейство забезпечує можливість неодноразового використання інформаційних сервісів, але не дозволяє асоціювати випадки використання між собою і «приписати» їх одній особі. Неможливість асоціації захищає від побудови профілів поведінки користувачів (і, отже, від отримання інформації на основі подібних профілів).

4. **Скритність**. Вимоги цього сімейства спрямовані на те, щоб можна було використовувати інформаційний сервіс із приховуванням факту використання. Для реалізації скритності може застосовуватися, наприклад, широкомовне розповсюдження інформації, без вказівки конкретного адресата. Використовуються для реалізації скритності і стеганографії, коли ховається не лише зміст повідомлення (як у криптографії), але і сам факт його відправлення.

Клас «Використання ресурсів», що містить вимоги доступності, включає три сімейства:

1. **Відмовостійкість**. Вимоги цього сімейства спрямовані на збереження доступності інформаційних сервісів навіть у разі збою або відмови. У ЗК виокремлюють активну і пасивну відмовостійкість. Активний механізм містить спеціальні функції, які активізуються у разі збою. Пасивна відмовостійкість передбачає наявність надмірності з можливістю нейтралізації помилок.

2. **Обслуговування за пріоритетами**. Виконання цих вимог дозволяє управляти використанням ресурсів так, що низькопріоритетні операції не можуть перешкодити високопріоритетним.

3. **Розподіл ресурсів**. Вимоги спрямовані на захист (шляхом застосування механізму квот) від несанкціонованої монополізації ресурсів.

«Загальні критерії» — сформований документ з погляду функціональних вимог, проте в ньому є недоліки, головний з яких — відсутність об'єктного підходу. Функціональні вимоги не згруповані в осмислені набори (об'єктні інтерфейси), до яких застосовувалося б спадкоємство. У «Загальних критеріях» відсутні архітектурні вимоги, що є природним наслідком обраного підходу від «низу до верху».

Вимоги довіри безпеки. Встановлення довіри безпеки, згідно із «Загальними критеріями», ґрунтується на активному дослідженні об'єкта оцінки.

Форма представлення вимог довіри та сама, що і для функціональних вимог. Специфіка полягає в тому, що кожен елемент вимог довіри належить одному з трьох типів:

1) дії розробників;

2) представлення і зміст посвідчень;

3) дії оцінювачів.

Усього в ЗК 10 класів, 44 сімейства, 93 компоненти вимог довіри безпеки. Наведемо класи:

1) розробка (вимоги для поетапної деталізації функцій безпеки від короткої специфікації до реалізації);

2) підтримка життєвого циклу (вимоги до моделі життєвого циклу, включаючи порядок усунення недоліків і захист середовища розробки);

3) тестування;

4) оцінка вразливостей (включаючи оцінку стійкості функцій безпеки);

5) постачання і експлуатація;

6) управління конфігурацією;

7) керівництво (вимоги до експлуатаційної документації);

8) підтримка довіри (для підтримки етапів життєвого циклу після сертифікації);

9) оцінка профілю захисту;

10) оцінка завдання з безпеки.

Щодо вимог довіри в «Загальних критеріях» введені так звані оцінні рівні довіри (сім), що містять осмислені комбінації компонентів:

1. Передбачає аналіз функціональної специфікації, специфікації інтерфейсів, експлуатаційної документації, а також незалежне тес-

тування. Рівень застосовується, коли загрози не розглядаються як суттєві.

2. На додаток до першого рівня передбачає наявність проекту верхнього рівня об'єкта оцінки, вибіркове незалежне тестування, аналіз стійкості функцій безпеки, пошук розробником уразливих місць.

3. Контролюються середовища розробки і управління конфігурацією об'єкту оцінки.

4. Додається повна специфікація інтерфейсів, проекти нижнього рівня, аналіз підмножини реалізації, застосування неформальної моделі політики безпеки, незалежний аналіз уразливих місць, автоматизація управління конфігурацією. Ймовірно це найвищий рівень, якого можна досягти при існуючій технології програмування і прийнятних витратах.

5. Передбачає застосування формальної моделі політики безпеки, напівформальної функціональної специфікації і проекту верхнього рівня з демонстрацією відповідності між ними. Потрібне проведення аналізу прихованих каналів розробниками і оцінювачами.

6. Реалізація має бути представлена в структурованому вигляді. Аналіз відповідності поширюється на проект нижнього рівня.

7. Передбачає формальну верифікацію проекту об'єкта оцінки. Він застосовується до ситуацій надзвичайно високого ризику.

Отже, використання ЗК дозволяє підвищити довіру до засобів захисту та відповідно до інформації, яку необхідно захистити. Це досягається за рахунок гнучкого завдання вимог безпеки до засобів захисту інформації з урахуванням їх призначення та умов застосування, наявності найбільш повного та обґрунтованого набору вимог безпеки, наявністю методології оцінювання. ЗК відкриті і можуть бути розширені, за рахунок чого можна здійснювати уточнення або вводити додаткові вимоги.

Росія перейшла на даний стандарт ще в 2002 р. [69; 70; 71; 72]. Російський стандарт називається ГОСТ Р ИСО/МЭК 15408 «Общие критерии оценки безопасности информационных технологий» та являє собою точний переклад міжнародного стандарту. Він прийнятий постановою Госстандарту Росії від 4.04.2002 р. № 133-ст з датою введення в дію 1 січня 2004 р. Цей ГОСТ відбиває не лише процес удосконалення російських стандартів з використанням міжнародного досвіду, але і частину урядової програми зі вступу Росії в СОТ.

На жаль, в Україні робота щодо впровадження даного стандарту також велась і ведеться, але даний процес проходить дуже повільно.

Інформаційна безпека України залежить від розв'язання проблем формування і керування процесами суспільної свідомості, виробництва та репродукції інформаційних ресурсів і доступу до них, створення цивілізованого ринку інформаційних продуктів та послуг, реалізації прав громадян на інформацію [73].

2.2.7. Технічна специфікація X.800

Технічна специфікація X.800 з'явилася дещо пізніше ніж «Помаранчева книга», але найкраще трактує питання ІБ розподілених систем. Вона визначає рівні еталонної семирівневої моделі OSI, на яких можуть бути реалізовані функції безпеки, використовувані механізми безпеки, а також адміністрування засобів безпеки [56; 74]. У ній можна виділити специфічні мережеві функції (сервіси) безпеки, а також необхідні для їх реалізації захисні механізми.

Загальні функції (сервіси) безпеки подано на рис. 2.11.

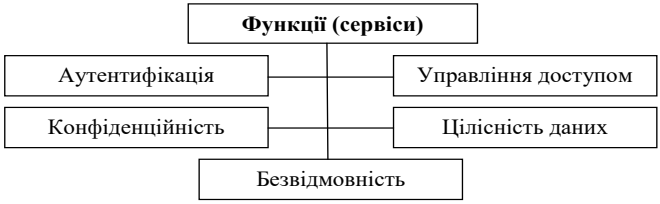

Рис. 2.11. Загальні функції (сервіси) безпеки технічної специфікації X.800

1. **Аутентифікація**. Цей сервіс забезпечує перевірку достовірності партнерів зі спілкування і перевірки достовірності джерела даних. Аутентифікація партнерів з спілкування використовується при встановленні з'єднання і, можливо, періодично під час сеансу. Вона слугує для запобігання таким загрозам, як «маскарад» і повтор попереднього сеансу зв'язку. Аутентифікація буває односторонньою (зазвичай клієнт доводить свою достовірність серверу) і двосторонньою (взаємною).

2. **Управління доступом**. Забезпечує захист від несанкціонованого використання ресурсів, доступних по мережі.

3. **Конфіденційність даних**. Забезпечує захист від несанкціонованого отримання інформації. Окремо варто згадати **конфіденційність трафіку** (це захист інформації, яку можна отримати, аналізуючи мережеві потоки даних).

4. **Цілісність даних** розділяється на підвиди залежно від того, який тип спілкування використовують партнери — зі встановленням з'єднання або без нього, чи захищаються усі дані або тільки окремі поля, чи забезпечується відновлення у разі порушення цілісності.

5. **Безвідмовність** (неможливість відмовитися від дій, які відбулися) забезпечує два види послуг: безвідмовність із підтвердженням достовірності джерела даних і безвідмовність із підтвердженням доставки. Побічним продуктом безвідмовності є аутентифікація джерела даних.

Як вказано у праці [74], функції (сервіси) безпеки відповідно до рівнів еталонної моделі OSI, на яких можуть бути реалізовані ці функції (сервіси), наведені в табл. 2.2.

Таблиця 2.2

Функції і механізми безпеки

Функції безпеки	Рівень еталонної семирівневої моделі OSI, на якому можуть бути реалізовані функції безпеки						
	1	2	3	4	5	6	7
Аутентифікація			+	+			+
Управління доступом			+	+			+
Конфіденційність з'єднання	+	+	+	+		+	+
Конфіденційність		+	+	+		+	+
Вибіркова конфіденційність						+	+
Конфіденційність трафіку	+		+				+
Цілісність із відновленням				+			+
Цілісність без відновлення			+	+			+
Вибіркова цілісність							+
Цілісність поза з'єднанням			+	+			+
Безвідмовність							+

Мережеві механізми безпеки. Для реалізації сервісів (функцій) безпеки можуть використовуватися такі механізми та їх комбінації (табл. 2.3).

Таблиця 2.3

Механізми та їх комбінації реалізації сервісів (функцій) безпеки

Механізми								
Функції безпеки	Шифрування	Електронний підпис	Управління доступом	Контроль цілісності даних	Аутентифікація	Доповнення трафіку	Управління маршрутизацією	Нотаризація
Аутентифікація партнерів	+	+			+			
Аутентифікація джерела	+	+						
Управління доступом			+					
Конфіденційність	+						+	
Вибіркова конфіденційність	+							
Конфіденційність трафіку	+					+	+	
Цілісність з'єднання	+			+				
Цілісність поза з'єднанням	+			+				
Безвідмовність	+	+		+				

1. **Шифрування**. Шифрування розділяється на симетричне (із секретним ключем, коли знання ключа шифрування дає знання ключа розшифрування) і асиметричне (з відкритим ключем, коли знання ключа шифрування не дозволяє упізнати ключ розшифрування). Розрізняють також оборотне і безповоротне шифрування. Останнє може використовуватися для обчислення криптографічних контрольних сум.

2. **Електронний цифровий підпис**. Механізм електронного підпису включає дві процедури: 1) вироблення підпису; 2) перевірку підписаної порції даних. Процедура вироблення підпису використовує інформацію, відому тільки особі, що підписує порцію даних.

Процедура перевірки підпису є загальнодоступною, вона не повинна дозволяти знайти секретний ключ того, хто підписує.

3. **Механізми управління доступом**. Можуть розміщуватися на будь-якій зі сторін, що беруть участь у спілкуванні, або в проміжній точці. Під час управління доступом можуть використовуватися такі види і джерела інформації:

- бази даних управління доступом (у такій базі, яка підтримується централізовано або на кінцевих системах, можуть зберігатися списки управління доступом або структури аналогічного призначення);
- паролі або інша аутентифікаційна інформація;
- токени, квитки або інші посвідчення, пред'явлення яких свідчить про наявність прав доступу;
- позначки безпеки, що асоціюються із суб'єктами і об'єктами доступу;
- час доступу, який запрошується;
- маршрут доступу, який запрошується;
- тривалість доступу, який запрошується.

4. **Механізми контролю цілісності даних**. У рекомендаціях X.800 розрізняються два аспекти цілісності: цілісність окремого повідомлення або поля інформації і цілісність потоку повідомлень або полів інформації. Процедура контролю цілісності окремого повідомлення (поля) базується на використанні контрольних сум. Цей механізм не захищає від дублювання повідомлень. Для перевірки цілісності потоку повідомлень (тобто для захисту від крадіжки, переупорядковування, дублювання і вставки повідомлень) використовуються порядкові номери, тимчасові штампи, криптографічне зв'язування або інші аналогічні прийоми. При спілкуванні в режимі без встановлення з'єднання використання тимчасових штампів може забезпечити обмежену форму захисту від дублювання повідомлень.

5. **Механізми аутентифікації**. Згідно з рекомендаціями X.800, аутентифікація може досягатися за рахунок використання паролів, особистих карток або інших пристроїв аналогічного призначення, криптографічних методів, пристроїв виміру і аналізу біометричних характеристик.

6. **Механізми доповнення трафіку** (вироблення і підтримка правил, які задають характеристики доповнюючих повідомлень — частоту відправки, розмір тощо). Механізми доповнення трафіку

ефективні тільки у поєднанні із засобами забезпечення конфіденційності, оскільки інакше зловмисникові буде очевидний фіктивний характер додаткових повідомлень.

7. **Механізми управління маршрутизацією**. Маршрути можуть вибиратися статично або динамічно. Кінцева система, зафіксувавши неодноразові атаки на певному маршруті, може відмовитися від його використання. На вибір маршруту здатна вплинути позначка безпеки, що асоціюється з даними, які передаються.

8. **Механізми нотаризації**. Слугують для завірення таких комунікаційних характеристик, як цілісність, час, особи відправника і одержувачів. Завірення забезпечується надійною третьою стороною, що має достатню інформацію. Зазвичай нотаризація спирається на механізм електронного підпису.

Адміністрування засобів безпеки. Воно включає розповсюдження інформації, необхідної для роботи сервісів і механізмів безпеки, а також збір і аналіз інформації про їх функціонування. Прикладами можуть слугувати поширення криптографічних ключів, установка значень параметрів захисту, ведення реєстраційного журналу тощо.

Концептуальною основою адміністрування є інформаційна база управління безпекою. Ця база може не існувати як єдине (розподілене) сховище, але кожна з кінцевих систем повинна мати в розпорядженні інформацію, необхідну для реалізації обраної політики безпеки.

Згідно з рекомендаціями X.800, зусилля адміністратора засобів безпеки повинні розподілятися за трьома напрямами:

- адміністрування інформаційної системи в цілому;
- адміністрування сервісів безпеки;
- адміністрування механізмів безпеки.

Серед дій, які відносяться до ІС в цілому, відмітимо забезпечення актуальності політики безпеки, взаємодію з іншими адміністративними службами, реагування на події, що відбуваються, аудит і безпечне відновлення.

Адміністрування сервісів безпеки включає визначення об’єктів, що захищаються, вироблення правил підбору механізмів безпеки (за наявності альтернатив), комбінування механізмів для реалізації сервісів, взаємодію з іншими адміністраторами для забезпечення узгодженої роботи. Обов’язки адміністратора механізмів безпеки визначаються переліком задіяних механізмів.

Адміністрування засобів безпеки в розподіленій ІС має багато особливостей порівняно з централізованими системами.

Так, наприклад, обов'язки адміністратора механізмів безпеки визначаються переліком задіяних механізмів і можуть включати:

– управління ключами (генерація і розподіл);

– управління шифруванням (установка і синхронізація криптографічних параметрів). Адміністрування механізмів електронного підпису;

– управління цілісністю, якщо воно забезпечується криптографічними засобами;

– адміністрування управління доступом (розподіл паролів, списків доступу тощо);

– управління аутентифікацією (розподіл інформації, необхідної для управління — паролів, ключів тощо);

– управління доповненням трафіку (вироблення і підтримка правил, які задають характеристики доповнювальних повідомлень — частоту відправки, розмір тощо). Характеристики можуть варіюватися за заданим законом залежно від дати і часу;

– управління маршрутизацією (виділення надійних шляхів);

– управління нотаризацією (поширення інформації про нотаріальні служби, адміністрування цих служб).

2.2.8. Промисловий підхід (класифікація загроз DSECCT (Digital Security Classification of Threats – Росія))

Потреба забезпечення необхідної ІБ в ІС корпоративного масштабу з розгалуженою системою передавання даних (СПД) зумовила появу нових комерційних пропозицій і, відповідно, нових комерційних продуктів у вигляді програмних, апаратних і програмно-апаратних комплексів захисту інформації. У зв'язку з цим деякими комерційними організаціями задля побудови реальних промислових комерційних продуктів було розроблено декілька типів класифікацій [63].

У класифікаторі загроз інформаційної безпеки DSECCT (*Digital Security Classification of Threats*), розробленому фахівцями компанії Digital Security, загрози розділяються за характером загрози, видом дії, причиною і об'єктом загрози. Основна мета створення фахівцями Digital Security класифікації загроз — якнайповніша, деталь-

ніша класифікація, яка описує усі існуючі загрози ІБ, за якою кожна із загроз потрапляє тільки під одну класифікаційну ознаку, і яка, таким чином, найкраще може бути застосовна для аналізу ризиків реальних ІС [59]. Класифікація загроз DSECCT входить до складу програмного продукту ГРИФ 2006 Digital Security Office [75].

Класифікація загроз ІБ DSECCT як найбільш характерна реалізація промислового підходу, показана на рис. 2.12.

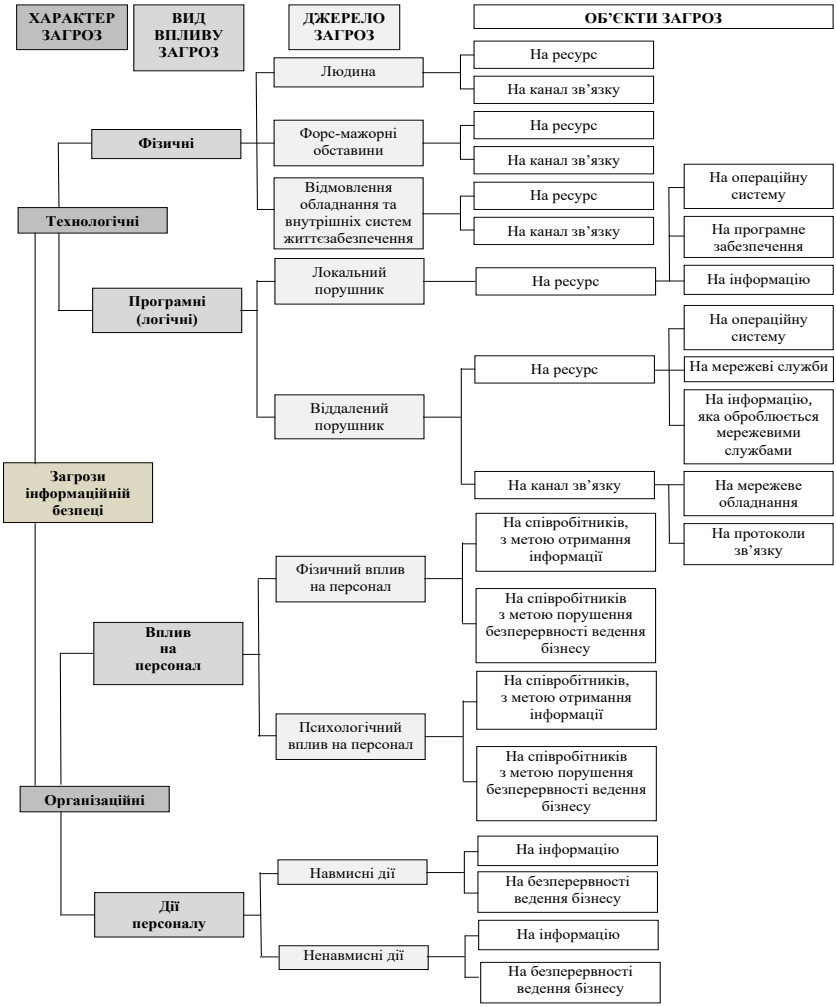

Рис. 2.12. Класифікація загроз інформаційній безпеці DSECCT

У цій класифікації усі загрози потрапляють під одну класифікаційну ознаку, таким чином загроза має бути однозначно віднесена до певного характеру, виду впливу, джерела або об'єкта загрози. У зв'язку із цим, загрози, які потрапляють під одну кваліфікаційну ознаку, можуть бути нейтралізовані з використанням одних і тих самих методів.

Аналізуючи загрози ІБ DSECCT, можна побачити, що більше уваги приділено загрозам технологічного характеру. Водночас, розглядаючи джерело загроз, яким може бути локальний порушник, не видно його вплив на канали, протоколи і лінії зв'язку, устаткування в цілому.

Відповідно до наведеної класифікації загроз ІБ DSECCT, фахівцями компанії Digital Security запропоновані заходи протидії цим загрозам [59].

Заходи протидії загрозам:

1. ***Правові і законодавчі.*** Закони, укази, нормативні акти, що регламентують правила поводження з інформацією і визначають відповідальність за порушення цих правил.

2. ***Морально-етичні.*** Норми поведінки, які традиційно склалися або складаються в суспільстві у міру поширення обчислювальної техніки. Невиконання цих норм веде до падіння авторитету, престижу організації, країни, людей.

3. ***Адміністративні або організаційні.*** Заходи організаційного характеру, які регламентують процеси функціонування АС, діяльність персоналу з метою максимального утруднення або виключення реалізації загроз безпеки:

– організація явного або прихованого контролю за роботою користувачів;

– організація обліку, зберігання, використання, знищення документів і носіїв інформації;

– організація охорони і надійного пропускного режиму;

– заходи, здійснювані при доборі і підготовці персоналу;

– заходи щодо проектування, розробки правил доступу до інформації;

– заходи під час розробки, модифікації технічних засобів.

4. ***Фізичні.*** Застосування різного роду технічних засобів охорони і споруд, призначених для створення фізичних перешкод на шляхах проникнення в систему.

5. ***Технічні.*** Засновані на використанні технічних пристроїв і програм, які входять до складу АС і виконують функції захисту:

– засоби аутентифікації;

– апаратне шифрування;

– інше.

Ці заходи протидії загрозам характерні для забезпечення інформаційної безпеки в цілому, які відповідно до [10] розділені на *правові, організаційні і інженерно-технічні*, що відповідає сучасним тенденціям. Так, для захисту інтересів суб'єктів інформаційних відношень, за представленням професора В. Ф. Шаньгина, необхідно сполучати заходи таких рівнів [76]:

– законодавчого (стандарти, закони, нормативні акти і т. д.);

– адміністративно-організаційного (дії загального характеру, які приймаються керівництвом організації, і конкретні заходи безпеки, що стосуються людей);

– програмно-технічного (конкретні технічні заходи).

2.3. Розробка методології побудови класифікатора загроз державним інформаційним ресурсам

2.3.1. Аналіз загроз державним інформаційним ресурсам. Терміни та визначення

Загальна система загроз державним інформаційним ресурсам. До захищених ІС належать ІС, 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.*

Загалом, будь-яка інформаційна система має такі основні групи загроз [10]:

- *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 знижується працездатність автоматизованої системи, або її ресурси стають недоступними.

Розглядаючи класифікацію базових загроз інформаційним ресурсам, їх можна розрізняти [77] за:

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

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

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

– розташуванням джерела загроз (внутрішні та зовнішні).

Аналізуючи *Доктрину інформаційної безпеки України,* затверджену Указом Президента України від 8 липня 2009 року № 514/2009 (Проект Указу Президента України «Про Доктрину інформаційної безпеки України» від 2014 р. у зв'язку із втратою чинності вищенаведеного Указу на підставі Указу Президента № 504/2014 від 06.06.2014 р.) та ряд інших НПА [31; 53; 54; 55], можна побудувати таку загальну систему ЗДІР, показану на рис. 2.13.

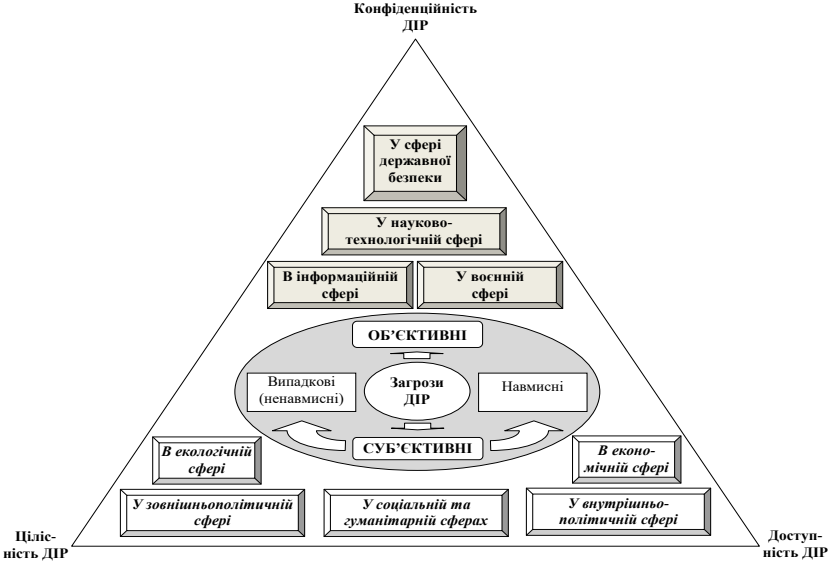

Рис. 2.13. Загальна система ЗДІР

Отже, існує достатньо розвинута нормативно-правова база (НПБ), що регламентує порядок захисту інформації в АС, визначена велика кількість як основних, так і похідних загроз. Але словос-

получення ДІР в НПА щодо захисту інформаційних ресурсів трапляється дуже рідко. У зв'язку з цим постає питання: чи можливо класифікацію загроз в АС 1–3 класу застосувати до ДІР? Розглянемо це питання докладніше, починаючи із визначення АС.

Автоматизована система — 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 [54].

Відповідно до НД ТЗІ 1.1-003–99 «Термінологія в галузі захисту інформації в комп'ютерних системах від НСД» визначає АС так:

Автоматизована система — 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 оцінювання.

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 [10]. Інформаційні ресурси які обробляються в цих системах і є власністю держави, будуть вважатися державними інформаційними ресурсами.

Відповідно до 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 р. № 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.

Клас «1» — одномашинний однокористувацький 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 багатокористувацький комплекс, який обробляє інформацію різних ступенів обмеження доступу. Приклад — ЛОМ.

Клас «3» — розподілений багатомашинний багатокористувацький 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*.

Отже, можна говорити про те, що ДІР міститимуться в даних класах АС і модель загроз, відповідно до [54], 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. 2.13, загальна система ЗДІР). Загрози, що мають суб'єктивну природу, поділяються на випадкові (ненавмисні) та навмисні (рис. 2.13, загальна система ЗДІР; табл. 2.4).

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 неможливо 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. 2.5).

У зв'язку з цим можна виділити такі загальні загрози ДІР:

- зміна умов фізичного середовища (стихійні лиха і аварії, землетрус, повінь, пожежа або інші випадкові події);
- збої і відмови у роботі обладнання та технічних засобів інформаційно-комунікаційній системи та мережі (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.

У табл. 2.4 і 2.5 визначено перелік можливих загроз ДІР та їх класифікацію відповідно до впливу на які властивості інформації вони спрямовані (к — конфіденційності; ц — цілісності та д — доступності).

Таблиця 2.4

Класифікація загроз ДІР суб'єктивної природи

№ з/п	Загрози суб'єктивної природи	За відношенням до суб'єкта загроз		Що порушує		
		навмисні	ненавмисні	к	ц	д
1	Поширення в 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 та зв'язку	+	+	+	+	+

Продовження табл. 2.4

№ з/п	Загрози суб'єктивної природи	За відношенням до суб'єкта загроз		Що порушує		
		навмисні	ненавмисні	к	ц	д
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	+		+	+	+

Продовження табл. 2.4

№ з/п	Загрози суб'єктивної природи	За відношенням до суб'єкта загроз		Що порушує		
		навмисні	ненавмисні	к	ц	д
17	Навмисна діяльність осіб, яка впливає на елементи системи управління ДІР з використанням програмних і/або технічних засобів	+		+	+	+
18	Несправність програмних і (або) технічних засобів	+			+	+
19	Неповідомлення (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 програмного забезпечення (ПЗ))	+			+	+

Продовження табл. 2.4

№ з/п	Загрози суб'єктивної природи	За відношенням до суб'єкта загроз		Що порушує		
		навмисні	ненавмисні	к	ц	д
24	Впровадження і використання комп'ютерних вірусів, закладних (апаратних і програмних) і підслуховувальних 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, який 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 електронної обчислювальної машини (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)	+				+

Закінчення табл. 2.4

№ з/п	Загрози суб'єктивної природи	За відношенням до суб'єкта загроз		Що порушує		
		навмисні	ненавмисні	к	ц	д
33	Ненавмисна діяльність осіб, яка, впливає на систему управління ДІР з 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 у 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 2.5

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		+	+	

У зв'язку з віщевикладеним слід зробити такі висновки:

– у результаті розробленої загальної системи захисту ДІР можливо вказати основні напрями щодо подальшого розкриття загроз ДІР в основних сферах, які показано на рис. 2.13 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 загалом може бути покладено в модель загроз ДІР, але з необхідністю подальшого уточнення загроз у наведених вище сферах, що дає можливість побудувати складну ієрархічну модель 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 відповідно до міжнародних стандартів ISO/IEC 27001:2005 та подальшого уточнення стандартних функціональних профілів захищеності.

Аналітично-правовий аналіз загроз державним інформаційним ресурсам. Стрімке зростання новітніх технологій, а також розвиток інфраструктури інформаційно-комунікаційних мереж державного та загального призначення, призвели до створення інтегрованого

інформаційного простору держави та всього суспільства. Інформаційні технології знаходять більше застосування у таких сферах, як: державні системи управління, фінансовий обіг і ринок цінних паперів, розвинута система електронних платежів, система послуг зв'язку та телебачення, системи управління транспортом, високотехнологічні виробництва (особливо атомних, хімічних тощо) і т. ін. Будь-яке несанкціоноване та противоправне втручання в інформаційний простір наведених сфер життєдіяльності держави й суспільства може призвести до тяжких та не передбачуваних наслідків.

Особливого значення набуває вирішення проблеми ІБ ДІР у сучасних умовах глобалізації інформаційних процесів, а також в умовах цілеспрямованих дій низки розвинених держав та ІТ-корпорацій досягти домінування у світовому інформаційному просторі й на ринку ІТ-послуг.

Міжнародний та вітчизняний досвід демонструє, що забезпечення безпеки інформаційних ресурсів повинно носити комплексний характер. Однак організація процесів безпеки має бути не просто комплексною складовою, але ще й засновуватися враховуючи всебічний аналіз можливих негативних загроз ДІР та їх можливих наслідків.

Здійснюючи аналіз напрямів забезпечення інформаційної безпеки держави, які являють нормативно-правові, організаційні, інженерно-технічні категорії, орієнтовані на забезпечення комплексного захисту інформації від внутрішніх та зовнішніх загроз на державному рівні, особливе значення набуває такий напрям, як *правовий*. *Правовий захист ДІР* повинен формуватися на тлі загальної та спеціальної законодавчої бази держави, інших нормативних актів, постанов, стандартів, правил, що забезпечують захист інформації та безпосередньо її властивостей: конфіденційності, доступності, цілісності [10; 37].

Проведений аналіз НПЗ захисту 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 рівні не визначено перелік і класифікацію загроз інформаційним ресурсам держави, не розроблено нормативно-правовий документ, стандарт із визначенням поняття *державних інформаційних ресурсів*, його складових та відповідної їм моделі загроз [3; 10; 37].

Звертаючись до теми загроз ДІР, їх класифікації загалом, слід зазначити, що даному питанню приділяли увагу як вітчизняні, так і зарубіжні вчені. До них можна віднести: О. М. Новікова, В. М. Богуша, В. В. Мохора, І. Д. Горбенка, В. О. Хорошко, О. В. Корнейко, М. В. Грайворонського, О. Г. Корченка, А. І. Марущака, В. П. Мельнікова, С. В. Віхорева, Е. В. Касперського, І. Д. Медведовського, О. В. Олійника, О. В. Сосніна та ін. Але питанню створення класифікації та в подальшому моделі загроз ДІР (не тільки нормативно-правового спрямування) приділялось недостатньо уваги, про що свідчить існуюче НПЗ ЗІ.

Проводячи аналітично-правовий аналіз побудови класифікатора та моделі загроз ДІР, 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 загальноспрямованої системи класифікації загроз ДІР.

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 ДІР, за якою можна було би визначити вірогідні наміри порушника, ступінь небезпечності дій та несанкціонованих процесів; категорію осіб, серед яких може бути порушник, припущення про кваліфікацію та характер його дій тощо. Не повною мірою стандартизована політика безпеки ДІР, яка б пропонувала певний набір вимог, правил, обмежень, рекомендацій згідно з класифікацією ресурсів і загроз. З наведеного аналізу видно, що ця проблематика існує, а деякі питання потребують негайного подальшого вдосконалення.

Наведений авторами матеріал має достатнє підґрунтя, сформоване на попередніх дослідженнях та встановлених підходах до аналізу системи загроз ДІР. Отже, щоб не втратити логіку викладення матеріалу, запропонуємо основні отримані висновки і положення із зазначеного напряму [3; 4; 10; 37; 38]. Авторами було сформовано сучасне визначення ДІР, яке наведено в розд. 1.

Однак, після формування матеріалу, 09 квітня 2014 року ВР України прийнято в цілому проект Закону про внесення змін до Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» (№ 1194-18). У згаданому законі наведений оновлений термін для ДІР:

державні інформаційні ресурси — систематизована інформація, що є доступною за допомогою інформаційних технологій, право на володіння, використання або розпорядження якою належить органам державної влади, іншим державним органам, військовим формуванням, а також інформація, створення якої передбачено законодавством, та яка обробляється фізичними або юридичними особами відповідно до наданих їм повноважень суб'єктами владних повноважень.

Загрози державним інформаційним ресурсам. Визначення. Інтереси держави в інформаційній сфері полягають у створенні умов для гармонійного розвитку інформаційної інфраструктури держави, реалізації конституційних прав і свобод людини і громадянина в інтересах зміцнення конституційного ладу, суверенітету і територіальної цілісності країни, встановлення політичної і соціальної стабільності, економічного процвітання, безумовного виконання законів і підтримки міжнародного співробітництва на основі партнерства.

Проведений аналіз висвітлює існуючу проблематику та подальші напрями досліджень — відсутність детального визначення й стандартизації класифікації ДІР, ускладнює або унеможливлює побудову *моделі загроз* ресурсам держави.

Загрози інформаційній безпеці [information security threat] — сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства і держави в інформаційній сфері [29].

На сьогодні, існує достатньо великий перелік визначень поняття загроз інформації. Це різноманіття характеризується напрямами і видами інформаційних систем, а також структурою й призначенням комплексних систем захисту інформаційних ресурсів, деталізацією структури згідно з впровадженими послугами і сервісами тощо. Наведемо основні діючі нормативні визначення.

Загроза для інформації — витік, можливість блокування чи порушення цілісності інформації; таке визначення дає ДСТУ 3396.2–97 «Захист інформації. Технічний захист інформації. Терміни та визначення».

Загроза інформації — будь-які обставини чи події, що можуть спричинити порушення політики безпеки інформації та (або) нанесення збитку інформаційно-комунікаційній системі (ІКС) [4; 78].

Загроза інформації (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 [4].

Загроза (threat) — будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків АС [НД ТЗІ 1.1-003–99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу»].

До захищених інформаційних систем належать інформаційні системи, які у певних умовах експлуатації забезпечують політику безпеки інформаційних ресурсів (конфіденційність, цілісність, доступність), що належать системі, та підтримують свою працездатність в умовах впливу на них заданої множини загроз.

Політика безпеки інформації (information security policy) визначена в державі нормативним документом НД ТЗІ 1.1-003–99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу» як: сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок оброблення інформації.

Під загрозою безпеки інформаційним ресурсам будемо розуміти дії, які можуть призвести до спотворення, несанкціонованого використання або навіть до руйнування інформаційних ресурсів керованої системи, а також програмних і апаратних засобів [4]. Отже, *загроза* в загальному вигляді буде являти собою будь-який потенційно можливий несприятливий вплив (дію або бездіяльність), який (яка) завдає збиток суб'єкту інформаційної діяльності і/або власнику ресурсів.

Загалом, будь-яка інформаційна система дістає впливу наступних основних груп загроз щодо порушення властивостей інформаційних ресурсів [10]:

- конфіденційності;
- цілісності;
- доступності.

Сучасні інтереси інформаційного суспільства та держави, що вступила у стадію постіндустріального розвитку, полягають у захисті життєво важливих інтересів у цій сфері, забезпечення реалізації конституційних прав і свобод громадянина в інтересах зміц-

нення демократії, досягнення і підтримування суспільної злагоди, підвищення творчої активності населення.

Одним із базових джерел загроз інтересам суспільства в інформаційній сфері є безперервне ускладнення інформаційних систем і мереж передачі ДІР, критично важливих інфраструктур забезпечення життя суспільства.

Ці загрози можуть проявлятися у вигляді як навмисних, так і ненавмисних помилок, збоїв і відмов інтегрованих ІКС і ПЗ, шкідливого впливу з боку злочинних структур і кримінальних елементів. Об'єктами реалізації таких структур можуть виступати системи військової, енергетичної, транспортної, комунікаційної і деяких інших інфраструктур.

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 [4].

Підсумовуючи все вищевикладене, можна дати визначення поняттю «загроза державним інформаційним ресурсам».

Загроза державним інформаційним ресурсам — це потенційний або реальний стан небезпеки державним інформаційним ресурсам та безпосередньо їх властивостям (конфіденційності, цілісності, доступності), який може бути сформовано на основі реалізації будь-якого процесу та/або вчинення діяння (та/або бездіяльності), спрямовано на порушення політики безпеки об'єкта інформаційної діяльності (державних інформаційних ресурсів) та такий, що завдає збитку державі.

Носіями загроз безпеці інформації є джерела загроз. Джерелами загроз можуть бути як суб'єктивні, так і об'єктивні прояви. Загрози, як можливі небезпечності здійснення будь-якої дії, спрямованої проти об'єкта захисту, проявляються не самі по собі, а через уразливості (фактори), що призводять до порушення безпеки інформації на конкретному об'єкті інформаційної діяльності.

Уразливості — це властиві об'єкту інформатизації, невіддільні від нього, що обумовлюються недоліками процесу функціонування, властивостями архітектури АС, протоколами обміну та інтерфейсами, ПЗ і апаратною платформою, умовами експлуатації та розташування.

Джерела загроз можуть використовувати уразливості для порушення безпеки інформації, одержання незаконної вигоди (нанесення збитків власникові, користувачеві інформації). Крім того, можливі не зловмисні дії джерел загроз з активізації інших уразливостей, що приносять шкоду.

Кожній загрозі можуть бути зіставлені різноманітні уразливості. Усунення або суттєве послаблення вразливостей впливає на можливість реалізації загроз безпеці інформації.

Існують декілька напрямів при формуванні переліку актуальних загроз на об'єкті інформаційної діяльності експертно-аналітичним методом. Як правило, спочатку визначається перелік інформаційних ресурсів, що підлягають захисту та піддаються впливу тієї чи іншої загрози, встановлюються характерні джерела цих загроз і уразливості, що сприяють реалізації загроз. На основі аналізу експертів складається таблиця взаємозв'язку джерел загроз і уразливостей, на основі яких визначаються можливі наслідки реалізації загроз (атаки) та встановлюється (обчислюється) коефіцієнт небезпеки цих атак. Коефіцієнт небезпеки атак є добутком коефіцієнтів небезпеки відповідних загроз (імовірність реалізації загрози) та джерел загроз, визначених попереднім аналізом. При цьому передбачається, що атаки, які мають імовірність небезпеки менше 0,1 або іншого встановленого рівня (припущення експертів або статистика), у подальшому можуть не розглядатися через малу ймовірність їх реалізації на об'єкті захисту. Після виявлення найбільш актуальних загроз, вживаються заходи з вибору методів і засобів для їх відбивання та мінімізації збитків на об'єкті інформаційної діяльності.

Отже, завжди існує сталий взаємозв'язок між загрозою та ймовірністю її реалізації. При формуванні визначення — загроза, вкрай необхідно мати висвітлення взаємозалежному з ним поняттю: *атака*. Атака — це наслідки загрози, що реалізована зі встановленою (або не встановленою) імовірністю. Грунтуючись на зазначеному та враховуючи попередні дослідження, надамо визначення поняттю атаки на ДІР [10; 29; 38]:

Атака на державні інформаційні ресурси — це можливі наслідки реалізації загрози державним інформаційним ресурсам, що сформовані на основі взаємодії джерела загрози через наявні фактори уразливості об'єкта інформаційної діяльності та такі, що призводять до різних видів збитків державі.

2.3.2. Методологія побудови класифікатора загроз державним інформаційним ресурсам

Виходячи з наведеного вище, необхідно провести аналіз існуючого нормативно-правового та Законодавчого забезпечення, вітчизняних і міжнародних стандартів галузі «Інформаційна безпека». Необхідно побудувати основи методології створення класифікатора загроз, принципів та методик представлення, семантики і системи кодування різних класів загроз ДІР. В межах досліджень необхідно визначити концептуальні питання побудови класифікатора ЗДІР та більш детально представити зазначену модель для першого широкого класу загроз нормативно-правового спрямування.

Основи методології створення «Класифікатора загроз державним інформаційним ресурсам»

Розглядаючи існуючі підходи до класифікації загроз інформаційним ресурсам, можна встановити велике різноманіття напрямів та підходів, а саме [4; 38; 56]:

- за критеріями інформаційній безпеці (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 розташуванням 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:

1) обумовлені діями суб'єкта (антропогенні джерела загроз);

2) обумовлені технічними засобами (техногенні джерела загроз);

3) обумовлені стихійними джерелами.

У підрозд. 2.2.1 було проведено аналіз основних підходів щодо створення класифікатора загроз державним інформаційним ресурсам, визначені напрями аналізу основних НПА, побудована загальна система законодавчої бази (базовий перелік), що впливає на формування класифікації ЗДІР (див. рис. 2.2).

Одними з 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 [55; 79–85]. 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 відповідно до органів державної влади, органів місцевого самоврядування, органів управління та інших державних і/або не державних формувань, підприємств, установ, організацій, що утворені згідно із законодавством України.

Автори наведених 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.

Відокремлене місце у державних НПА посідають ключові питання побудови 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. 2.6).

Таблиця 2.6

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 оброблюваної в автоматизованій системі інформації залежать від характеристик обчислювального середовища, фізичного середовища, персоналу і 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 спостережності та керованості АС); джерела виникнення (які суб'єкти АС або суб'єкти, зовнішні відносно до неї, можуть ініціювати загрозу); можливі способи здійснення загроз

Закінчення табл. 2.6

Нормативний документ	Підхід до класифікації 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

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, відноситься 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.

Методологічний підхід до формування класифікатора загроз ДІР

Надалі наведемо основи методології створення класифікатора, основні підходи, методику кодування різних класів загроз ДІР.

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 точки зору 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 питання: що підлягає захисту згідно зі встановленими завданнями і вимогами. По-друге, потрібно розглянути зворотну сторону 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, рівень загрози, 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, зберігання, поширення і прогресивний розвиток незалежно від (або в умовах) наявності чи реалізації внутрішніх і зовнішніх інформаційних загроз [10].

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» [86];
- ISO/IEC 27002:2005 «Інформаційні технології. Методи забезпечення безпеки. Практичні правила управління інформаційною безпекою (раніше ISO/IEC 17799:2005)» [87];
- ISO/IEC 27005:2008 «Інформаційні технології. Методи забезпечення безпеки. Управління ризиками інформаційної безпеки» [88].

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 мета 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 [86; 87].

Отже, можна визначити три базових властивості інформації, що підлягають захисту при формуванні будь-якої політики безпеки та безпосередньо під час проектування 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 інформаційної безпеки (ІБ)* розуміється — сукупність заходів нормативно-правових, організаційних і техніч-

них, призначених для досягнення стану захищеності потреб особистостей, суспільства і держави в обробленні, зберіганні та поширенні інформації [10].

На сьогодні 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 [86; 87].

З урахуванням вітчизняних і міжнародних НПА, а також практики, що склалася натепер, можна відокремити такі базові напрями захисту інформації [10].

Нормативно-правове забезпеченням 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, державному рівні 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 (у тому числі галузі і підприємства). Тобто, це регламентація 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.

Отже, на основі проведених досліджень ЗДІР можна представити та безпосередньо визначити їх клас за характером спрямованості, через призму загальних напрямів убезпечення інформації (правовий захист, організаційний захист, інженерно-технічний захист), отримавши наступну початкову класифікацію та методику кодування в цілому для ДІР (01; 02; 03 — базові коди класифікації загроз за спрямованістю, рис. 2.14), де:

- *загрози нормативно-правового спрямування (01)* — 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.

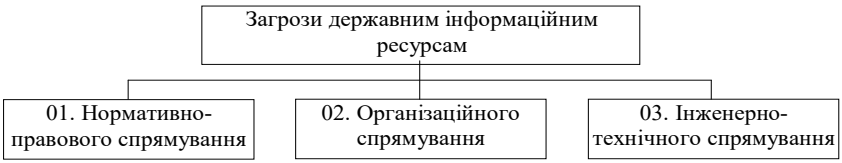

Рис. 2.14. Класифікація загроз ДІР за характером спрямування

Пропонується ввести додаткові принципи класифікації (рис. 2.15). По-перше, до загроз ДІР стратегічного характеру (01,02,03_1) треба віднести загрози, що стосуються питань національної безпеки, відсутності або невиконання цільових програм чи доктрин, послаблення 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 (01, 02, 03_1.1_2_3.1, К, Ц, Д 01, 02, 03).

Більшість зазначеного типу загроз наведено 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 (01, 02, 03_2).

Формалізуємо цей розподіл тільки підкреслюючи додаткові принципи класифікації за стратегічним або тактичним характером, а кодифікацію зробимо наскрізну за наявністю повного переліку загроз.

Загрози конфіденційності виникають у результаті несанкціонованого копіювання, витоку та втрати ДІР і засобів їх обробки, а також у результаті 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 — в результаті блокування, знищення або несанкціонованого отримання ДІР та засобів їх обробки.

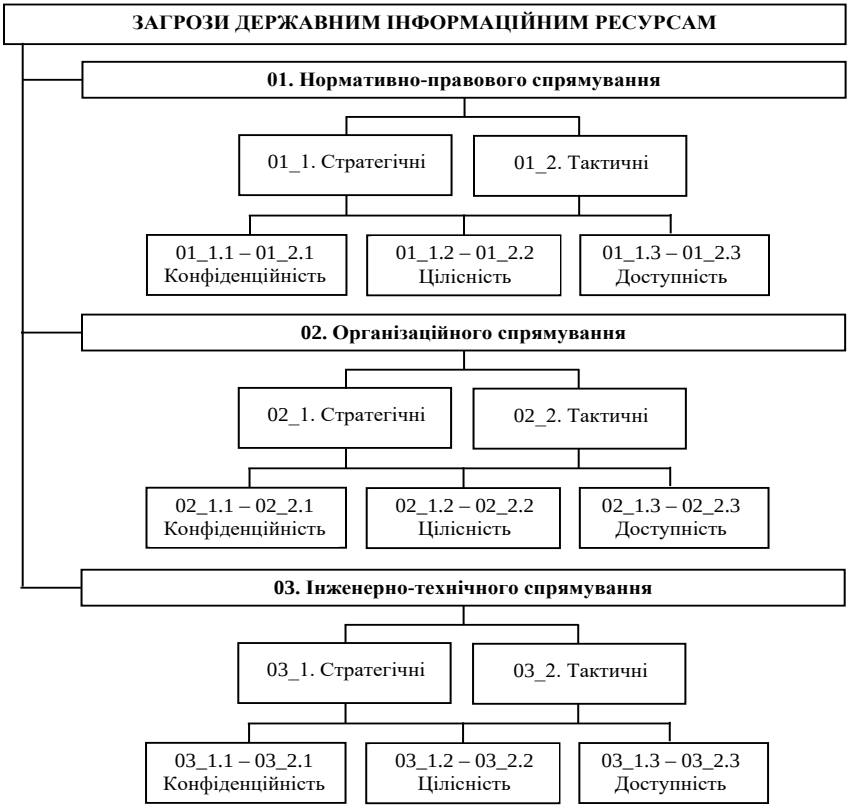

Рис. 2.15. Поділ загроз за видами спрямувань відповідно до основних властивостей інформації

Семантику класифікатора загроз з урахуванням поділу на стратегічні та тактичні загрози ДІР показано на рис. 2.16. Опис класифікатора складається з п’яти числових частин. Класифікатор включає: позначення спрямування загрози (01 — нормативно-правове, 02 — організаційне, 03 — інженерно-технічне); позначення, що характеризує рівень загроз (0х_1 — стратегічний, 0х_2 — тактичний); позначення, що характеризує тип загроз (0х_х.1 — конфіденційність, 0х_х.2 — цілісність , 0х_х.3 — доступність); позначення виду загрози залежно від типу (0х_х.1.х, 0х_х.2.х, 0х_х.3.х); додаткова інформація про направленість загрози. Всі частини класифікатора відділяються один від одного крапкою, лише рівень загроз нижнім підкреслюванням (рис. 2.16).

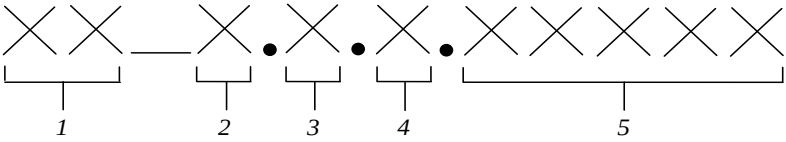

Рис. 2.16. Класифікатор загроз державним інформаційним ресурсам: *1* — спрямування; *2* — рівень; *3* — тип; *4* — вид; *5* — додаткова інформація

Таким чином, визначені основні напрями аналізу створення класифікації загроз ДІР, які полягають у аналізуванні існуючих доктрин та законів України, що регламентують питання інформаційної безпеки України чи захист інформації, де є інформаційні ресурси; аналізуванні оціночних стандартів, направлених на класифікацію інформаційних систем та засобів захисту за вимогами безпеки; аналізуванні технічних специфікацій, які регламентують різні аспекти реалізації засобів захисту; інших підходів.

Виходячи з цього, репрезентована початкова класифікація ДІР на основі трьох основних спрямувань захисту інформаційних ресурсів в АС (нормативно-правове спрямування, організаційне спрямування, інженерно-технічне спрямування).

Уперше розроблено методологію побудови класифікатора загроз, принципи та методику представлення, семантику і систему кодування різних класів загроз ДІР.

2.3.3. Класифікація загроз державним інформаційним ресурсам нормативно-правового спрямування в розрізі методології побудови їх класифікатора

Спираючись на дослідження, які були проведені авторами та опубліковані раніше [3; 9; 8], виникає необхідність у здійсненні (в деяких випадках уточнені та наведенні з точки зору розширеного визначення державних інформаційних ресурсів [10]) розкриття загроз державним інформаційним ресурсам (ДІР) як нормативно-правового спрямування (НПС), що є предметом розгляду даного розділу, так і організаційного та інженерно-технічного спрямування. Це у свою чергу обумовлює актуальність даної тематики.

Авторами здійснено ретельний аналіз проблеми створення методології побудови класифікатора загроз ДІР, основи якого закладені в роботах [10; 29], де викладено низку сучасних теоретичних

та практичних підходів до вирішення нормативно-правових та організаційно-технічних завдань для реалізації процесу захисту інформаційних ресурсів. Також основою для цього послужили роботи з нормативно-правового аналізу захисту ДІР [37], їх уразливості [38] та визначення переліку загроз [4]. У подальшому авторами визначено правові аспекти формування системи ДІР [3], уточнено деякі визначення, що відносяться до понять «загроза» ДІР та «атака» на ДІР [8] та, як результат, запропонована методологія побудови класифікатора загроз ДІР [9]. Узагальнений авторами аналіз їх досліджень та публікацій з даної тематики наведено на рис. 2.17.

Рис. 2.17. Узагальнений авторами аналіз
їхніх досліджень та публікацій

Виходячи з наведеного, необхідно здійснити визначення загроз державним інформаційним ресурсам нормативно-правового спрямування з урахуванням розробленої методології побудови їх класифікатора та подальшого удосконалення самого класифікатора [9].

Поділ загроз нормативно-правового спрямування відповідно до основних властивостей інформації показано на рис. 2.18.

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-правого спрямування [10; 32; 55; 56; 57; 58; 60; 62; 79–83]. Необхідно зазначити, що даний класифікатор повинен постійно оновлюватись залежно від розвитку інформаційного суспільства.

Рис. 2.18. Поділ загроз нормативно-правового спрямування відповідно до основних властивостей інформації

Отже, до *основних стратегічних загроз ДІР нормативно-правового спрямування (01_1.1_2_3)* можна віднести такі [89]:

Стратегічні 01_1.1_2_3

01_1.1_2_3.1 — загрози державній політиці України у сфері інформатизації та її безпеки [к,ц,д,01,02];

01_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];

01_1.1_2_3.3 — 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 (зокрема ДІР) [к,ц,д,01,02,03];

01_1.1_2_3.4 — недостатня координація діяльності органів державної влади з формування і реалізації єдиної державної політики в галузі забезпечення інформаційної безпеки України та захисту ДІР, а також низький організаційно-технічний рівень інформатизації органів державної влади [к,ц,д,01,02];

01_1.1_2_3.5 — недосконаліть нормативної правової бази, що регулює відносини в інформаційній сфері, а також недостатня практика застосування норм права [к,ц,д,01,02];

01_1.1_2_3.6 — нерозвиненість інститутів громадянського суспільства і недостатній державний контроль за розвитком ДІР та інформаційного ринку України [к,ц,д,01,02];

01_1.1_2_3.7 — відсутність Державних економічних програм та недостатнє фінансування заходів із забезпечення інформаційної

безпеки держави, а також недосконаліть системи страхування інформаційних ризиків фізичних і юридичних осіб[к,ц,д,01,02];

01_1.1_2_3.8 — зниження ефективності системи освіти і виховання, недостатня кількість кваліфікованих кадрів у галузі забезпечення інформаційної безпеки, а також зниження наукового потенціалу у галузі інформатизації та безпеки інформаційних технологій[к,ц,д,01,02];

01_1.1_2_3.9 — 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];

01_1.1_2_3.10 — 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];

01_1.1_2_3.11 — відсутність (або/чи часткова) діяльності державних органів виконавчої влади із застосування правових норм, включаючи попередження і припинення правопорушень в інформаційній сфері, а також виявлення, викриття і притягнення до відповідальності осіб, що скоїли злочини та інші правопорушення в цій сфері[к,ц,д,01,02];

01_1.1_2_3.12 — відсутність системи удосконалення процесів сертифікації інформаційно-телекомунікаційного обладнання, систем захисту інформації, а також програмного забезпечення автоматизованих систем обробки інформації на відповідність вимогам[к,ц,д,01,02].

Тактичні 01_2

До основних *тактичних загроз конфіденційності ДІР нормативно-правового спрямування (01_2.1)* можна віднести такі:

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

01_2.1.2 — невиконання вимог до впровадження (відсутність упровадження, повна/часткова) та реалізації організаційних заходів захисту ДІР згідно із законодавчою базою, державними стандартами, нормативними документами і інструкціями, іншими виробничими документами (у тому числі загрози безпеці інформації обмеженого доступу (ІзОД), зокрема державної таємниці)[к,ц,д,01,02];

01_2.1.3 — порушення встановленого законодавством режиму проектування, технічного обладнання та впровадження приміщень, призначених для обробки, зберігання, передавання і відображення ДІР ^{к,ц,д,01,02};

01_2.1.4 — відсутність (повна/часткова) правил та вимог (у тому числі відповідальність) до розподілу обов'язків осіб, що відповідають за процеси розробки, впровадження і супроводу інформаційних систем, а також комплексів засобів захисту ДІР ^{к,ц,д,01,02};

01_2.1.5 — порушення режиму охорони об'єкта (об'єкта інформаційної діяльності), а також несанкціоноване проникнення на територію та приміщення, де оброблюються й зберігаються ДІР ^{к,ц,д,01,02};

01_2.1.6 — порушення пропускного режиму безпосередньо до інформаційної системи (ІС) і технічних засобів обробки, зберігання, передавання і відображення ДІР ^{к,ц,д,01,02};

01_2.1.7 — відсутність системи підготовки кадрів (у тому числі підвищення кваліфікації), а також порушення процедур при підборі фахівців для роботи з ДІР ^{к,ц,д,01,02};

01_2.1.8 — невиконання договірних зобов'язань щодо захисту ДІР та правил доступу до даних і послуг третьою стороною ^{к,ц,д,01,02};

01_2.1.9 — 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};

01_2.1.10 — відсутність (повна/часткова) політики управління доступом до ДІР у розподіленому та об'єднаному інформаційному середовищі (або/чи узгодженості між політиками різних систем, що співпрацюють), а також відсутність класифікації інформації з обмеженим доступом (якщо ДІР до неї відноситься) та правил доступу до ІзОД ^{к,ц,д,01,02};

01_2.1.11 — використання неліцензійного програмного забезпечення (ПЗ), а також не атестованих (або/чи не сертифікованих) програмно-апаратних комплексів зберігання, обробки, передачі та захисту ДІР в автоматизованих (інформаційних) системах різних класів ^{к,ц,д,01,02};

01_2.1.12 — порушення або невиконання єдиної системи державних стандартів та правових норм криптографічного та технічного захисту інформації (безпосередньо захист ДІР) відповідно до чинного законодавства ^{к,ц,д,01,02};

01_2.1.13 — невиконання організаційно-технічних вимог та розпорядчих документів, що стосуються розробки, впровадження і реалізації політики безпеки інформаційних систем ДІР, Реєстру ЕлДІР та ДепозитаріюЕлДІР ^{к,ц,д,01,02};

01_2.1.14 — відсутність або порушення загальної встановленої системи розподілу доступу (моделі доступу, матриці доступу, атрибутів доступу, системи ідентифікації і автентифікації тощо), невиконання правил і вимог зміни паролів або ідентифікаторів до інформаційних ресурсів або/чи інформаційної системи ДІР ^{к,ц,д,01,02,03};

01_2.1.15 — 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, РеєструЕлДІР або ДепозитаріюЕл ДІР ^{к,ц,д,01,02,03};

01_2.1.16 — відсутність вимог та технічних характеристик моніторингу і контролю (корекції процесів) за робочими процесами ІС, а також невизначення оцінки ефективності щодо захисту ДІР^{к,ц,д,01,02,03};

01_2.1.17 — 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 РеєстромЕлДІР або ДепозитаріємЕлДІР)^{к,ц,д,01,02,03};

01_2.1.18 — відсутність (повна або часткова) процедур реалізації методів і засобів технічного та криптографічного захисту ДІР, а також контролю за цими процесами згідно з чинним законодавством^{к,ц,д,01,02,03};

01_2.1.19 — відсутність або порушення загальної встановленої системи розподілу доступу, зміни, збереження й управління криптографічними ключами при їх використанні згідно з чинним законодавством^{к,ц,д,01,02,03};

01_2.1.20 — відсутність (повна/часткова) внутрішніх стандартів, розпорядчих документів щодо впровадження, використання та регулярного оновлення антивірусних баз і ПЗ^{к,ц,д,01,02};

01_2.1.21 — 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 (у тому числі неправомірне підключення — «врізання» до комутативних або безкомутативних каналів зв'язку тощо), а також відсутність контролю за виконанням спеціальних вимог із захисту ДІР[к,ц,д,01,02,03];

01_2.1.22 — відсутність або/чи неналежне ведення журналів реєстрації або аудиту та інцидентів (у тому числі розслідування інцидентів) робочих процесів[к,ц,д,01,02];

01_2.1.23 — втрата, викрадення або несанкціоноване знищення журналів реєстрації або аудиту та інцидентів (у тому числі розслідування інцидентів) робочих процесів[к,ц,д,01,02];

01_2.1.24 — відсутність програми і порядку фінансування, що стосуються розробки, впровадження та супроводу засобів (комплексів) захисту ДІР[к,ц,д,01,02];

01_2.1.25 — відсутність (невиконання) *затвердженої інформаційної політики безпеки організації* як сукупності вимог і керівних принципів у галузі інформаційної безпеки, якими керується у своїй діяльності організація[к,ц,д,01,02];

01_2.1.26 — відсутність (невиконання) *положення про відділ захисту інформації Управління безпеки організації*, яке визначає порядок діяльності відділу захисту інформації Управління безпеки, його структуру, основні завдання, функції, права, обов'язки та порядок взаємодії з іншими підрозділами організації[к,ц,д,01,02];

01_2.1.27 — відсутність (невиконання) *положення про відділ режиму та захисту об'єктів Управління безпеки організації*, яке визначає порядок діяльності відділу режиму та захисту об'єктів Управління безпеки, його структуру, основні завдання, функції, права, обов'язки та порядок взаємодії з іншими підрозділами організації[к,ц,д,01,02];

01_2.1.28 — відсутність (невиконання) *положення про забезпечення захисту інформації в інформаційно-телекомунікаційних системах*, яке визначає загальні вимоги, організаційні засади забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах організації та виконавців цих робіт[к,ц,д,01,02];

01_2.1.29 — відсутність (невиконання) *положення про службу безпеки організації в цілому та її підрозділів*, яке визначає порядок підпорядкованості та діяльності служби безпеки організації (підрозділів), її структуру, основні завдання, функції, права, обов'язки та порядок взаємодії з іншими підрозділами [к,ц,д,01,02];

01_2.1.30 — відсутність (невиконання) *положення про інформаційно-аналітичний відділ Управління безпеки організації*, яке визначає порядок діяльності інформаційно-аналітичного відділу Управління безпеки організації, його структуру, основні завдання, функції, права, обов'язки та порядок взаємодії з іншими підрозділами організації[к,ц,д,01,02];

01_2.1.31 — відсутність (невиконання) *регламентованого порядку доступу до інформаційних ресурсів організації*, яке визначає регламент замовлення працівниками організації та погодження й затвердження прав доступу на використання інформаційних ресурсів, що використовуються в організації [к,ц,д,01,02];

01_2.1.32 — відсутність (невиконання) *інструкції з пропускного і внутрішньооб'єктового режиму*, яка визначає порядок пропускного та внутрішньооб'єктового режиму, регламентує дії працівників організації у штатних і позаштатних ситуаціях[к,ц,д,01,02];

01_2.1.33 — відсутність (невиконання) *положення про інформаційну політику організації*, визначає основні принципи інформаційної політики організації, перелік інформації та документів, які можуть бути розголошені перед громадськістю (зацікавленими особами), а також встановлює порядок надання такої інформації та документів і порядок взаємодії організації та зацікавлених осіб[к,ц,01,02];

01_2.1.34 — відсутність (невиконання) *положення про організацію доступу до мережі Інтернет*, яке призначено для вдосконалення захисту інформації організації під час роботи в мережі Інтернет та підвищення ефективності використання Інтернет [к,д,01,02];

01_2.1.35 — відсутність (невиконання) *положення про антивірусний захист інформації*, яке визначає перелік робіт і розподіл обов'язків працівників організації в процесі організації антивірусного захисту інформації на серверах та робочих станціях організації[к,д,01,02].

До основних *тактичних загроз цілісності ДІР нормативно-правового спрямування (01_2.2)* можна віднести такі:

01_2.2.1–01_2.2.32 (*див. загрози 01_2.1.1–01_2.1.32*);

01_2.2.33 (*див. загрози 01_2.1.33*);

01_2.2.34 — несанкціонована модифікація процедур штатного функціонування або не авторизоване внесення змін у 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];

01_2.2.35 — несанкціонована модифікація процедур штатного функціонування або не авторизоване внесення змін у 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];

01_2.2.36 — несанкціонована модифікація процедур штатного функціонування або не авторизоване внесення змін у 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];

01_2.2.37 — несанкціонована модифікація процедур штатного функціонування або не авторизоване внесення змін у ПЗ системи електронного документообігу (у тому числі електронної комерції) ІС ДІР, РеєстрЕлДІР або ДепозитарійЕлДІР (несанкціонована фальсифікація та модифікація текстів та функцій ПЗ, нехтування проектами змін, відсутність документального оформлення порушень або змін тощо)[ц,д,01,02,03];

01_2.2.38 — подання власником або/чи адміністратором інформаційного ресурсу (власником інформаційної системи, адміністратором безпеки, авторизованими користувачами тощо) недостовірних відомостей (даних) до інформаційної системи ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР та їх навмисна (не навмисна) фальсифікація й модифікація[01,02,03].

До основних *тактичних загроз доступності ДІР нормативно-правового спрямування (01_2.3)* можна віднести такі:

01_2.3.1–01_2.3.32 (*див. загрози 01_2.1.1–01_2.1.32, 01_2.2.1–01_2.2.32*);

01_2.3.33–01_2.3.36 (*див. загрози 01_2.2.34–01_2.2.37*);
01_2.3.37–01_2.3.38 (*див. загрози 01_2.1.34–01_2.1.35*).

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'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).

На основі вищенаведеного та з урахуванням запропонованого авторами підходу щодо класифікатора загроз ДІР [9] можна скласти класифікацію функціональних профілів загроз ДІР нормативно-правового спрямування, приклади яких наведено в дод. 1.

2.3.4. Класифікація загроз державним інформаційним ресурсам організаційного спрямування в розрізі методології побудови їх класифікатора

Визначення організаційної складової з урахуванням захисту інформаційних ресурсів є обов'язковим процесом при розробці комплексних систем захисту інформації згідно з вітчизняними та міжнародними вимогами і стандартами. Організаційна складова — це частка базової платформи інформаційної безпеки державних інформаційних ресурсів: нормативно-правове, організаційне та технічне забезпечення. Даному питанню приділяють значну увагу багато професійно спрямованих організацій та вчених. Так, цей елемент є обов'язковою складовою законодавчої та нормативно-правової бази країни з умов створення міжнародних, державних, галузевих стандартів, нормативних документів технічного й криптографічного захисту інформації (НД ТЗІ, НД КЗІ), інструкцій операторів робочих станцій тощо.

Прикладом упровадження організаційної складової в розбудову системи менеджменту інформаційної безпеки може слугувати класифікатор загроз інформаційної безпеки DSECCT (*Digital Security*

Classification of Threats), розроблений фахівцями компанії Digital Security [59]. Показано, що на базі встановленої моделі загроз організаційного характеру впроваджується безпосередньо сама система регламентації процесів функціонування АС та коригується діяльність персоналу з метою максимального утруднення або повного виключення процедур реалізації загроз інформаційним ресурсам.

Виходячи з наведеного, необхідно розробити та вдосконалити методологію побудови класифікатора загроз державним інформаційним ресурсам на основі платформи організаційного спрямування. Також необхідно базові приклади кодифікації за розробленою методологією «подвійної трійки» та описати основні загрози організаційного спрямування.

Авторами здійснено ретельний аналіз світових тенденцій організаційно-правової систематизації різних класів моделей у політику безпеки інформаційних систем. Раніше викладено основні розробки та запропоновано низку сучасних теоретичних та практичних підходів до вирішення нормативно-правових та організаційно-технічних завдань реалізації процесу взаємопов'язаної процедури кодифікації й формування стандартизованого класифікатора загроз [3; 9; 10; 29].

Актуальність дослідження обумовлена необхідністю введення чіткої системи класифікації ЗДІР за організаційним спрямуванням. Даний напрям досліджень є подальшим розвитком теорії створення реєстру ДІР, а також встановлює концептуальні підходи до побудови сучасних моделей порушника й загроз ДІР [3; 9].

Досліджуючи підхід, розроблений С. В. Віхоревим [57], під час класифікації загроз інформаційній безпеці спостерігається відсутність прямих посилань на клас організаційних загроз як складової загальної моделі. Основою його класифікації є так звана категорія класифікації загроз як збиток інформаційним ресурсам або бізнес-процесам організації.

Звертаючись до переліку типових загроз інформаційної безпеки, пов'язаних з міжнародним стандартом ISO/IEC 27002:2005, можна побачити відсутність у прямій постановці класифікації загроз організаційного спрямування (наприклад, присутні фізичні загрози, юридичні загрози, загрози антропогенних та природних катастроф, загрози нецільового використання комп'ютерного обладнання та мережі, порушення правил безпеки та витоку інформації через співробітників організації і т. д.).

Дедалі поширюється практика вирішення питання класифікації загроз інформаційним ресурсам, що тісно пов'язана з теорією управління ризиками. Так, професор О. М. Астахов у своєму підході до класифікації загроз також окремо не виділяє і не посилається на категорію загроз організаційного спрямування. Його підхід заснований на міжнародних стандартах системи менеджменту інформаційної безпеки з умов організації безперервності бізнеспроцесів і мінімізації ризиків [90].

Класифікація загроз інформаційній безпеці запропонована професором А. Г. Корченком, виконана за такими основними базовими ознаками, як вплив та порушення основних властивостей інформації: конфіденційності (К-тип); цілісності (Ц-тип); доступності (Д-тип) або їх комбінації (КЦ-тип; КД-тип; ЦД-тип; КЦД-тип), а також за природою джерела (об'єктивна і суб'єктивна). У вказаній постановці до класифікації не визначені загрози організаційного спрямування [91].

У нормативному документі Адміністрації Держспецзв'язку НД ТЗІ 1.4-001–2000 «Типове положення про службу захисту інформації в автоматизованій системі» (затверджено наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04.12.2000 р. № 53, із змінами згідно з наказом Адміністрації Держспецзв'язку від 28.12.2012 р. № 806) наведені основні загрози для інформації в АС та вказано, що основою для проведення аналізу ризиків і формування вимог до КСЗІ є розробка моделі загроз та моделі порушника. Дана класифікація загроз побудована за загальноприйнятою формою і ознаками. Зокрема, загрози для інформації, що обробляється в АС, залежать від характеристик 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 попередніх дослідженнях, не визначено.

Отже, можна дійти висновку: формування моделей загроз, методика опису та їх класифікація представлення, що ґрунтується на різноманітті загроз інформації організаційного спрямування, як безпосередньо визначений клас загроз ДІР відсутній. Авторами досліджень встановлено, що наведена методологія формування кла-

сифікатора загроз ДІР за відповідним спрямуванням платформ «подвійної трійки захисту» (нормативно-правовим, організаційним, інженерно-технічним) не розглядалась та даний напрям не вирізнявся зовсім [9].

Поділ загроз організаційного спрямування, принципи їх класифікації і кодифікації відповідно до першої платформи основних властивостей інформації наведено на рис. 2.19.

Рис. 2.19. Поділ загроз організаційного спрямування відповідно до основних властивостей інформації

Таким чином, до *основних стратегічних загроз ДІР за організаційним спрямуванням (02_1.1_2_3)* можна віднести такі [92]:

Стратегічні 02_1.1_2_3

02_1.1_2_3.1 — загрози державній політиці України у сфері інформатизації та її безпеки[к,ц,д,01,02];

02_1.1_2_3.2 — 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];

02_1.1_2_3.3 — діяльність іноземних політичних, економічних і військових розвідувальних та інформаційних структур, спрямована проти інтересів України в інформаційній сфері[к,ц,д,01,02,03];

02_1.1_2_3.4 — 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 (у тому числі ДІР)[к,ц,д,02,03];

02_1.1_2_3.5 — організація діяльності космічних, повітряних, морських і наземних технічних та інших засобів (видів) розвідки іноземних держав[к,ц,д,02,03];

02_1.1_2_3.6 — 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 (у тому числі ДІР)[к,ц,д,01,02,03];

02_1.1_2_3.7 — створення несприятливої криміногенної обстановка, що супроводжується збільшенням державних і кримінальних структур в інформаційній сфері, одержання кримінальними структурами права доступу до інформації (у тому числі 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];

02_1.1_2_3.8 — недостатня координація діяльності органів державної влади з формування і реалізації єдиної державної політики в галузі забезпечення інформаційної безпеки України та захисту ДІР, а також низький організаційно-технічний рівень інформатизації органів державної влади[к,ц,д,01,02];

02_1.1_2_3.9 — недосконаліть нормативної правової бази, що регулює відносини в інформаційній сфері, а також недостатня практика застосування норм права[к,ц,д,01,02];

02_1.1_2_3.10 — нерозвиненість інститутів громадянського суспільства і недостатній державний контроль за розвитком ДІР та інформаційного ринку України[к,ц,д,01,02];

02_1.1_2_3.11 — відсутність державних економічних програм та недостатнє фінансування заходів із забезпечення інформаційної безпеки держави, а також недосконаліть системи страхування інформаційних ризиків фізичних і юридичних осіб[к,ц,д,01,02];

02_1.1_2_3.12 — зниження ефективності системи освіти і виховання, недостатня кількість кваліфікованих кадрів у галузі забезпечення інформаційної безпеки, а також зниження наукового потенціалу в галузі інформатизації та безпеки інформаційних технологій[к,ц,д,01,02];

02_1.1_2_3.13 — 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];

02_1.1_2_3.14 — 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];

02_1.1_2_3.15 — відсутність (або/чи часткова) діяльності державних органів виконавчої влади із застосування правових норм, включаючи попередження і припинення правопорушень в інформаційній сфері, а також виявлення, викриття і притягнення до відповідальності осіб, що скоїли злочини та інші правопорушення в цій сфері[к,ц,д,01,02];

02_1.1_2_3.16 — відсутність системи моніторингу показників і характеристик інформаційної безпеки України та її застосування у найважливіших сферах діяльності суспільства і держави [к,ц,д,02,03];

02_1.1_2_3.17 відсутність системи удосконалення процесів сертифікації інформаційно-телекомунікаційного обладнання, систем захисту інформації, а також програмного забезпечення автоматизованих систем обробки інформації на відповідність вимогам[к,ц,д,01,02].

Тактичні 02_2.1

До *основних тактичних загроз конфіденційності ДІР за організаційним спрямуванням (02_2.1)* можна віднести такі:

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

02_2.1.2 — невиконання вимог до впровадження (відсутність впровадження, повна/часткова) та реалізації організаційних заходів захисту ДІР згідно з законодавчою базою, державними стандартами, нормативними документами і інструкціями, іншими виробничими документами (у тому числі загрози безпеці інформації обмеженого доступу (ІзОД), зокрема державної таємниці)[к,ц,д,01,02];

02_2.1.3 — порушення встановленого законодавством режиму проектування, технічного обладнання та впровадження приміщень, призначених для обробки, зберігання, передавання і відображення ДІР[к,ц,д,01,02];

02_2.1.4 — втрата, викрадення або несанкціоноване знищення проектної, виробничої документації щодо обробки, зберігання, передачі і відображення ДІР^{к,ц,д};

02_2.1.5 — відсутність (повна/часткова) правил та вимог (у тому числі відповідальність) до розподілу обов'язків осіб, що відповідають за процеси розробки, впровадження і супроводу інформаційних систем, а також комплексів засобів захисту ДІР^{к,ц,д,01,02};

02_2.1.6 — порушення режиму охорони об'єкта (об'єкта інформаційної діяльності), а також несанкціоноване проникнення на територію та приміщення, де оброблюються й зберігаються ДІР^{к,ц,д,01,02};

02_2.1.7 — порушення пропускного режиму безпосередньо до інформаційної системи (ІС) і технічних засобів обробки, зберігання, передавання і відображення ДІР^{к,ц,д,01,02};

02_2.1.8 — відсутність системи підготовки кадрів (у тому числі підвищення кваліфікації), а також порушення процедур при підборі фахівців для роботи з ДІР^{к,ц,д,01,02};

02_2.1.9 — невиконання договірних зобов'язань щодо захисту ДІР та правил доступу до даних і послуг третьою стороною^{к,ц,д,01,02};

02_2.1.10 — неповідомлення (несвоєчасне повідомлення) спеціально уповноваженого центрального органу виконавчої влади з питань організації спеціального зв'язку та захисту інформації (або підпорядкованого йому регіонального органу) про спроби та/або факти несанкціонованих дій у системі щодо інформації, яка є власністю держави (згідно з вимогами встановленими чинним законодавством)^{к,ц,д};

02_2.1.11 — 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};

02_2.1.12 — відсутність (повна/часткова) політики управління доступом до ДІР у розподіленому та об'єднаному інформаційному середовищі (або/чи узгодженості між політиками різних систем, що співпрацюють), а також відсутність класифікації інформації з обмеженим доступом (якщо ДІР до неї відноситься) та правил доступу до ІзОД^{к,ц,д,01,02};

02_2.1.13 — використання неліцензійного програмного забезпечення (ПЗ), а також не атестованих (або/чи не сертифікованих) програмно-апаратних комплексів зберігання, обробки, передачі та

захисту ДІР в автоматизованих (інформаційних) системах різних класів[к,ц,д,01,02];

02_2.1.14 — порушення або невиконання єдиної системи державних стандартів та правових норм криптографічного та технічного захисту інформації (безпосередньо захист ДІР) відповідно до чинного законодавства[к,ц,д,01,02];

02_2.1.15 — невиконання організаційно-технічних вимог та розпорядчих документів, що стосуються розробки, впровадження і реалізації політики безпеки інформаційних систем ДІР, РеєструЕлДІР та ДепозитаріюЕлДІР[к,ц,д,01,02];

02_2.1.16 — втрата контролю за діями користувачів ІС, використання та вплив (психологічний, фізичний, тощо) на персонал, який має доступ до ДІР з корисною метою[к,ц,д];

02_2.1.17 — відсутність або порушення загальної встановленої системи розподілу доступу (моделі доступу, матриці доступу, атрибутів доступу, системи ідентифікації і автентифікації тощо), невиконання правил і вимог зміни паролів або ідентифікаторів до інформаційних ресурсів або/чи інформаційної системи ДІР[к,ц,д,01,02,03];

02_2.1.18 — 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, РеєструЕлДІР або Депозитарію ЕлДІР[к,ц,д,01,02,03];

02_2.1.19 — відсутність вимог та технічних характеристик моніторингу і контролю (корекції процесів) за робочими процесами ІС, а також невизначення оцінки ефективності щодо захисту ДІР[к,ц,д,01,02,03];

02_2.1.20 — 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 РеєстромЕлДІР або ДепозитаріємЕлДІР)[к,ц,д,01,02,03];

02_2.1.21 — відсутність (повна або часткова) процедур реалізації методів і засобів технічного та криптографічного захисту ДІР, а також контролю за цими процесами згідно з чинним законодавством[к,ц,д,01,02,03];

02_2.1.22 — відсутність або порушення загальної встановленої системи розподілу доступу, зміни, збереження й управління криптографічними ключами при їх використанні згідно з чинним законодавством[к,ц,д,01,02,03];

02_2.1.23 — відсутність (повна/часткова) внутрішніх стандартів, розпорядчих документів щодо впровадження, використання та регулярного оновлення антивірусних баз і ПЗ[к,ц,д,01,02];

02_2.1.24 — 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 (у тому числі неправомірне підключення — «врізання» до комутативних або безкомутативних каналів зв'язку тощо), а також відсутність контролю за виконанням спеціальних вимог із захисту ДІР[к,ц,д,01,02,03];

02_2.1.25 — відсутність або/чи неналежне ведення журналів реєстрації або аудиту та інцидентів (у тому числі розслідування інцидентів) робочих процесів[к,ц,д,01,02];

02_2.1.26 — втрата, викрадення або не санкціоноване знищення журналів реєстрації або аудиту та інцидентів (у тому числі розслідування інцидентів) робочих процесів[к,ц,д,01,02];

02_2.1.27 — крадіжки носіїв інформації, виробничих відходів (роздруків, записів тощо)[к,ц,д];

02_2.1.28 — відсутність програми і порядку фінансування, що стосуються розробки, впровадження та супроводу засобів (комплексів) захисту ДІР [к,ц,д,01,02].

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

До *основних загроз цілісності ДІР організаційного спрямування (02_2.2)* можна віднести такі:

02_2.2.1 – 02_2.2.28 (*див. загрози 02_2.1.1 – 02_2.1.28*);

02_2.2.29 — несанкціонована модифікація процедур штатного функціонування або неавторизоване внесення змін у 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];

02_2.2.30 — несанкціонована модифікація процедур штатного функціонування або не авторизоване внесення змін у 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];

02_2.2.31 — несанкціонована модифікація процедур штатного функціонування або неавторизоване внесення змін у 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];

02_2.2.32 — несанкціонована модифікація процедур штатного функціонування або неавторизоване внесення змін у ПЗ системи електронного документообігу (у тому числі електронної комерції) ІС ДІР, РеєстрЕлДІР або ДепозитарійЕлДІР (несанкціонована фальсифікація та модифікація текстів та функцій ПЗ, нехтування проектами змін, відсутність документального оформлення порушень або змін тощо)[ц,д,01,02,03];

02_2.2.33 — 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, РеєструЕлДІР або ДепозитаріюЕлДІР зі зловмисною метою[ц,д,02,03];

02_2.2.34 — навмисно або/чи ненавмисно залишені адміністратором ІС ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР (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];

02_2.2.35 — навмисно або/чи не навмисно залишені адміністратором ІС ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР (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];

02_2.2.36 — відсутність (повна/часткова) процедур щодо впровадження, використання та регулярного оновлення антивірусних баз і ліцензованого ПЗ, а також загального репозитарію ДІР[ц,д,02,03];

02_2.2.37 — відсутність ПЗ або програмно-апаратних засобів і методів резервування та архівації важливих критичних даних [ц,д,02,03];

02_2.2.38 — порушення режимів функціонування (виведення з ладу тощо) систем життєзабезпечення ІС ДІР (електроживлення, заземлення, охоронної сигналізації, вентиляції та ін.)[ц,д,02,03];

02_2.2.39 — подання власником або/чи адміністратором інформаційного ресурсу (власником інформаційної системи, адміністратором безпеки, авторизованими користувачами тощо) недостовірних відомостей (даних) до інформаційної системи ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР та їх навмисна (ненавмисна) фальсифікація й модифікація[01,02,03].

До *основних загроз доступності ДІР організаційного спрямування (02.3)* можна віднести такі:

02_2.3.1–02_2.3.28 (*див. загрози 02_2.1.1 – 02_2.1.28; 02_2.2.1 – 02_2.2.28*);

02_2.3.29–02_2.3.39 (*див. загрози 02_2.2.29 – 02_2.2.39*);

02_2.3.40 — відсутність (повна/часткова) процедур перевірки технічного стану й контролю за ним, встановлення оцінки ефективності роботи, а також невиконання системи вимог та обмежень на технічні характеристики, які відображують штатні режими роботи ІС ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР[02,03];

02_2.3.41 — відсутність (повна/часткова) процедур перевірки технічного стану і контролю за ним, встановлення оцінки ефективності роботи, а також невиконання системи вимог та обмежень на технічні характеристики, які відображують штатні режими роботи комплексів засобів захисту ІС ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР[02,03];

02_2.3.42 — відсутність (повна/часткова) процедури перевірки засобів обслуговування, ремонту й ефективності надання послуг (у тому числі третіми особами) користувачам ІС ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР[02,03];

02_2.3.43 — відсутність (повна/часткова) керування потоками та/чи зміна їх напряму (у тому числі 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];

02_2.3.44 — 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];

02_2.3.45 — несанкціоновані 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, РеєструЕлДІР або ДепозитаріюЕлДІР[02,03];

02_2.3.46 — несанкціоноване обмеження або порушення здатності продовжувати функціонування процесів в умовах виникнення збоїв і відмов окремих компонентів ІС ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР[02,03];

02_2.3.47 — несанкціоновані дії (процеси), які обмежують (повна/часткова) можливість встановлення (інсталяції) ІС ДІР, РеєстрЕлДІР або ДепозитаріюЕлДІР або інформаційного об'єкта у відомий чи визначений штатний стан (режим)[02,03];

02_2.3.48 — несанкціоноване обмеження або порушення здатності продовжувати функціонування процесів надання встановлених послуг (різних типів) ІС ДІР, РеєструЕлДІР або Депозитарію ЕлДІР[02,03];

Загрози доступності ДІР організаційного спрямування 02_2.3.45 та 02_2.3.46 можна визначити, як:

загроза порушення квоти 02_2.3.45 — несанкціоновані дії (процеси), які обмежують (повна/часткова) можливості використання певного інформаційного ресурсу (програмного або/чи про-

грамно-апаратного) АС ДІР різних класів адміністратором (власником інформаційної системи, адміністратором безпеки, авторизованими користувачами, третьою стороною тощо) ІС ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР (порушення квоти);

загроза порушення послуги стійкості до відмов 02_2.3.46 — несанкціоноване обмеження або порушення здатності продовжувати функціонування процесів в умовах виникнення збоїв і відмов окремих компонентів ІС ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР.

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'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).

Приклади функціональних профілів загроз ДІР організаційного спрямування на основі вищенаведеного та з урахуванням запропонованого авторами підходу щодо класифікатора загроз ДІР [9], наведено в дод. 2.

2.3.5. Класифікація загроз державним інформаційним ресурсам інженерно-технічного спрямування в розрізі методології побудови їх класифікатора

Ретельний аналіз проблеми створення методології побудови класифікатора загроз ДІР авторами наведено в роботах [3; 9; 10; 29], де викладено низку сучасних теоретичних та практичних підходів до вирішення нормативно-правових, організаційних та інженерно-технічних завдань для реалізації процесу захисту інформаційних ресурсів держави.

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

У класифікаторі загроз інформаційній безпеці DSECCT (*Digital Security Classification of Threats*), розробленому фахівцями компанії Digital Security [59], загрози інформаційній безпеці поділяються на технологічні та організаційні. У 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 тощо).

У підході С. В. Віхорева [57] загрозами безпеці інформації визначено: розкрадання (копіювання) інформації; знищення інформації; модифікація (викривлення) інформації; порушення доступності (блокування) інформації; заперечення автентичності інформації; нав'язування хибної інформації. В 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 інформаційній безпеці, пов'язаних з міжнародним стандартом ISO/IEC 27002:2005, можна констатувати відсутність у прямій постановці класифікації загроз інженерно-технічного спрямування (в перелік типових загроз інформаційній безпеці згідно з наведеним стандартом входять: фізичні загрози; нецільове використання комп'ютерного обладнання в мережі Інтернет співробітниками організації; загрози витоку конфіденційної інформації; загрози витоку інформації по технічних каналах; 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 з успішним вирішенням питання класифікації загроз інформаційним ресурсам. У своєму підході до класифікації загроз О. М. Астахов [90] окремо не виділяє загрози інженерно-технічного спрямування. Його підхід заснований на міжнародних стандартах з інформаційної безпеки.

Класифікація загроз інформаційній безпеці А. Г. Корченка [91] виконана за такими основними базовими ознаками: за дією на ха-

рактеристики безпеки інформації (К-тип; Ц-тип; Д-тип; КЦ-тип; КД-тип; ЦД-тип; КЦД-тип, де К-конфеденційність, Ц-цілісність, Д-доступність наприклад, КЦ-тип являє собою загрозу конфіденційності та цілісності) та за природою джерела (об'єктивна і суб'єктивна). У вказаній класифікації також у прямій постановці не визначені загрози інженерно-технічного спрямування.

У системній класифікації загроз безпеці інформації, яка запропонована А. А. Малюком [93; 94], вона здійснюється за параметрами класифікації, значенням параметрів та змістом значення параметра (табл. 2.6). Отже, у даній класифікації також відсутня пряма постановка визначення загроз інженерно-технічного спрямування.

Таблиця 2.6

Системна класифікація загроз безпеці інформації

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

У НДТЗІ 1.4-001-2000 «Типове положення про службу захисту інформації в автоматизованій системі», затвердженому наказом Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 04 грудня 2000 року № 53 із змінами згідно з наказу Адміністрації Держспецзв'язку від 28.12.2012 р. № 806 наведені основні загрози для інформації в АС та вказано, що основою для проведення аналізу ризиків і формування вимог до 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 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 праці [9] немає.

Отже, із проведеного аналізу видно, що технічному напряму захисту інформаційних ресурсів завжди приділялась значна увага, але в запропонованому авторами класифікаторі загроз [9] інженерно-технічне спрямування не вирізнялось у прямій постановці.

Виходячи з наведеного, необхідно розробити класифікатор загроз державним інформаційним ресурсам інженерно-технічного спрямування з урахуванням розробленої методології побудови їх класифікатора [9].

Поділ загроз інженерно-технічного спрямування, принципи їх класифікації і кодифікації відповідно до першої платформи основних властивостей інформації подано на рис. 2.20.

Рис. 2.20. Поділ загроз інженерно-технічного спрямування відповідно до основних властивостей інформації

Таким чином, до *основних стратегічних загроз ДІР за інженерно-технічним спрямуванням (03_1.1_2_3)* можна віднести такі [95]:

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 (у тому числі 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 (у тому числі ДІР)[к,ц,д,01,02,03];

03_1.1_2_3.6 — створення несприятливої криміногенної обстановка, що супроводжується збільшенням державних і кримінальних структур в інформаційній сфері, одержання кримінальними структурами права доступу до інформації (у тому числі 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 (невиконання) 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), невиконання 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, РеєструЕлДІР або ДепозитаріюЕл ДІР[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 невизначення 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 ко-

рекція процесів, своєчасне оновлення інформаційного ресурсу та належного ПЗ, інші роботи, пов'язані з РеєстромЕлДІР або ДепозитаріємЕлДІР)[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 з чинним законодавством[к,ц,д,01,02,03];

03_2.1.8 — відсутність або порушення загальної встановленої системи розподілу доступу, зміни, збереження й управління криптографічними ключами під час їх використання згідно з чинним законодавством[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 (у тому числі неправомірне підключення — «врізання» до комутативних або безкомутативних каналів зв'язку тощо), а також відсутність контролю за виконанням спеціальних вимог із захисту ДІР[к,ц,д,01,02,03];

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

До *основних загроз цілісності ДІР за інженерно-технічним спрямуванням (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 неавторизоване внесення змін у 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 неавторизоване внесення змін у 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 неавторизоване внесення змін у 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 неавторизоване внесення змін у ПЗ системи електронного документообігу (у тому числі електронної комерції) ІС ДІР, РеєстрЕлДІР або ДепозитарійЕлДІР (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, РеєструЕлДІР або ДепозитаріюЕлДІР зі зловмисною метою[ц,д,02,03];

03_2.2.15 — навмисно або/чи ненавмисно залишені адміністратором ІС ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР (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 ненавмисно залишені адміністратором ІС ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР (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, РеєструЕлДІР або ДепозитаріюЕлДІР та їх навмисна (ненавмисна) фальсифікація й модифікація[01,02,03].

До *основних загроз доступності ДІР* за *інженерно-технічним спрямуванням (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 невиконання системи вимог та обмежень на технічні характеристики, які відображують штатні режими роботи ІС ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР[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, РеєструЕлДІР або ДепозитаріюЕлДІР[02,03];

03_2.3.22 — відсутність (повна/часткова) процедури перевірки засобів обслуговування, ремонту й ефективності надання послуг (у тому числі третіми особами) користувачам ІС ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР[02,03];

03_2.3.23 — відсутність (повна/часткова) керування потоками та/чи зміна їх напряму (у тому числі 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 — несанкціоновані 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, РеєструЕлДІР або ДепозитаріюЕлДІР[02,03];

03_2.3.26 — несанкціоноване обмеження або порушення здатності продовжувати функціонування процесів в умовах виникнення збоїв і відмов окремих компонентів ІС ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР[02,03];

03_2.3.27 — несанкціоновані дії (процеси), які обмежують (повна/часткова) можливість встановлення (інсталяції) ІС ДІР, РеєстрЕлДІР або ДепозитаріюЕлДІР або інформаційного об'єкта у відомий чи визначений штатний стан (режим)[02,03];

03_2.3.28 — несанкціоноване обмеження або порушення здатності продовжувати функціонування процесів надання встановлених послуг (різних типів) ІС ДІР, РеєструЕлДІР 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'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).

Приклади функціональних профілів загроз ДІР інженерно-технічного спрямування на основі вищенаведеного та з урахуванням запропонованого авторами підходу щодо класифікатора загроз ДІР [9] наведено в дод. 3.

Оцінювання ФП ЗДІР здійснено згідно з методикою експертного оцінювання, яка наведена в дод. 4.

Розділ 3

УКРАЇНСЬКИЙ СЕГМЕНТ ІДЕНТИФІКАТОРІВ ОБ'ЄКТІВ

3.1. Світовий простір ідентифікаторів об'єктів: аналіз, перспективи розвитку, місце українського сегмента

У підрозділі 1.3 вказувалось, що сучасний розвиток держави, зростання її економіки у світовому просторі, формування зовнішньополітичних стосунків з іншими країнами неможливо реалізувати без так званих п'яти літер «і»: інформація, інфраструктура, інтелектуальний капітал, інвестиції, інновації. Також, згідно з заявами Всесвітнього економічного форуму, інформація на сьогодні є сировиною і має відповідні їй активи. Для забезпечення функціонування різних класів систем, інформація слугує кількісною мірою для прийняття будь-яких рішень. Таку сировину, як і будь-яку іншу, слід добути, переробити і доставити в зазначені терміни до кінцевого користувача інформаційних послуг. Організацію процесів зберігання та обробки інформації, її поповнення і висвітлення, а також надання послуг клієнтам, відповідно до їх запитів, безпосередньо виконує інформаційна система.

У цьому ж підрозділі було наведено одне із найбільш вживаних визначень інформаційної системи, яке дав М. Р. Когаловський [44]: «інформаційною системою називається комплекс, що включає обчислювальне і комунікаційне обладнання, програмне забезпечення, лінгвістичні засоби і *інформаційні ресурси*, а також системний персонал, що забезпечує підтримку динамічної інформаційної моделі деякої частини реального світу для задоволення інформаційних потреб користувачів».

З організаційно-технічного погляду, на сучасному етапі розвитку інфраструктури світових сегментів ІС найбільший інтерес становлять науково-дослідницькі та практичні роботи, що проводить управління перспективних досліджень МО США (*Defense Advanced Research Projects Agency* — DARPA). Один із найбільш перспективних напрямів — це створення глобальної інформаційної решітки, що являє собою інтегровану безпровідну мережу таких поколінь (The Wireless Network after Next — WnaN, Global Information Grid — GIG) [96].

Планування і реалізація операцій у глобальних інформаційно-комунікаційних системах такого класу здійснюються відповідно до концепції «Мережоцентричної операції» (Net — Centric Operations). Основою для мережоцентричних операцій є глобальна інформаційна система, або так звана *глобальна інформаційна решітка* (GIG, Global Information Grid) міністерства оборони США. За своєю суттю GIG є набором взаємозв'язаних високозахищених мережевих сегментів глобальної інформаційної системи. Вона оптимізує процеси управління, збору, обробки, зберігання та розподілу інформаційних ресурсів, а також забезпечує процеси доведення інформаційних потоків до споживачів міністерства оборони і його клієнтів. За допомогою GIG здійснюється як адміністративне, так і оперативне управління Збройними силами США. Головним відомством, що відповідає за працездатність і захист глобальної інформаційної системи військового відомства, призначено об'єднане стратегічне командування американських Збройних сил [97].

З 2010 р. діє кібернетичне командування, що знаходиться у веденні стратегічного командування, яке безпосередньо керує роботою глобальної інформаційної мережі GIG Збройних сил США. Вартість такої системи, згідно з офіційними даними, становить понад 200 млрд доларів США [98].

Складність та різноманітність даних, типу протоколів, розгалуженість стандартів побудови ІС викликали необхідність появи нотацій високого рівня для їх формалізованого опису. Як така нотація, Міжнародний консультативний комітет з телефонії і телеграфії (МККТТ сьогодні це ITU-T) запропонував використовувати абстрактно-синтаксичну нотацію версії 1 (ASN.1) [98], яка відноситься до рекомендацій ITU-T серії X «Мережі передачі даних і взаємозв'язок відкритих систем».

ASN.1 (Abstract Syntax Notation One) є сумісним описом вимог зі стандартами серії ISO і ITU-T, а також являє собою мову для представлення абстрактного синтаксису даних (ASN.1) у сфері інформаційно-комунікаційних систем та мереж. Зазначений документ використовує базову модель взаємодії відкритих систем (OSI) для побудови ієрархії обміну даними. Більш докладно можна зазначити, що ASN.1 є стандартом, який описує структури даних для представлення, обробки, кодування (шифрування), передачі та декодування (розшифрування) інформаційних потоків. Він забезпечує на-

бір формальних правил організації структури об'єктів, які не залежать від конкретної ІС [100].

Історія розвитку стандарту ASN.1 починається в рамках CCITT X.409:1984. Враховуючи його широке практичне застосування, було сформовано наступний клас стандартів X.208. та X.680 [101].

Із розвитком сучасних інформаційних технологій та стрімким розширенням кількості елементарних сегментів глобальної інформаційної системи (інформаційні ресурси рознесені не тільки територіально, але і географічно) перед суспільством постала достатньо велика наукова проблема щодо створення чіткої організаційно-технічної системи обліку та ідентифікації інформаційних об'єктів різних класів. Питання створення міжнародних реєстрів інформаційних ресурсів та їх ідентифікація в глобальному світовому просторі стала часткою інформаційної культури кожної держави.

У 2001 р. Міжнародна організація ITU в рамках проекту ITU-T SG-17 відкрила процедуру сприяння використанню стандарту ASN.1 у широкому спектрі галузей промисловості і органів стандартизації різних країн з умов забезпечення процесів ідентифікації об'єктів.

Отже, здійснення аналізу та виділення напрямів і перспектив розвитку світового простору ідентифікаторів об'єктів (IOD), а також визначення місця Українського сегмента ідентифікаторів є актуальним.

Аналізуючи питання, пов'язані з ідентифікаторами об'єктів, можна констатувати факт, що даний напрям є слаборозвиненим на теренах України з нормативно-правової, організаційно-технічної точки зору, а також у найближчому зарубіжжі загалом.

Окремі публікації подано в презентаційному вигляді [102; 103], решта — загальні статті, що наведені в мережі Інтернет [104; 105] і звичайно міжнародні стандарти [99; 101; 106], державні стандарти України [107; 108], окремі нормативно-правові акти [11; 109]. Звичайно найкращим чином сучасне дерево OID можна вивчити в інтерактивному режимі за допомогою будь-якого Web браузера.

Такий архів OID наведено в праці [110].

Яким же чином досягається унікальність ідентифікації об'єктів у світовому просторі? В основу вирішення цього питання на міжнародному рівні були покладені міжнародні рекомендації, вимоги та стандарти серії X.208 «Abstract Syntax Notation One» (потім серія

X.680), розроблені спільно МСЭ-Т і ИСО/МЭК. Уперше в цих документах були визначені правила створення ієрархічної деревоподібної моделі ідентифікації об'єктів на основі побудови загального дерева ідентифікаторів об'єктів (OID — tree, Д — OID) і безпосередньо Object Identifier (OIDs).

Ідентифікатори об'єктів — це певна схема ідентифікації для фізичних або віртуальних одиниць, яка заснована на деревоподібній структурі атрибутів ідентифікації, яку називають «Деревом міжнародного ідентифікатора об'єктів». Дерево складається з набору вузлів, починаючи з кореневого вузла. Від кожного вузла відходить довільна множина дуг, кожна з яких з'єднана з єдиним дочірнім вузлом на наступному рівні.

Кількість рівнів дерева не обмежується [111].

Рекомендація ITU-T X.660|ISO/ISO 9834-1, а також вітчизняні нормативно-правові акти дають визначення *ідентифікатора об'єкта*. Так, наприклад, рішенням Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації від 18 квітня 2013 р. № 227 введене на території України таке тлумачення даного поняття (розд. II. Терміни, визначення та скорочення).

Ідентифікатор об'єкта (далі — ІО) — значення, що відрізняється від інших подібних значень, яке пов'язується з інформаційним об'єктом і є упорядкованим списком первинних цілочислових значень від кореня (Root) міжнародного дерева ІО до вершини, який однозначно ідентифікує цю вершину.

Однак на жаль, для пересічного громадянина, а також і для фахівців, це визначення важко сприймається. Автори пропонують свою скориговану пропозицію для визначення і тлумачення ІО [12].

Ідентифікатор об'єкта (object identifier) *— значення вузла, що відрізняється від інших подібних значень та логічно пов'язується з інформаційним об'єктом, унікально його визначає та однозначно ідентифікує як вузол дерева міжнародних ідентифікаторів об'єктів. Список значень вузлів дерева (Root) є впорядкованою послідовністю первинних цілих значень, що починаються від кореня міжнародного дерева до вершини або/чи вузла ідентифікації.*

Міжнародний стандарт також наводить визначення поняття дерева міжнародних ідентифікаторів об'єктів (*international object identifier tree*) — дерево, корінь якого відповідає дійсній рекомендації Міжнародного стандарту і вузли якого відповідають органам реєстрації, відповідальним за розподіл дуг із батьківського вузла [106].

Дане визначення не дуже зрозуміло й коректне з точки зору тлумачення організаційної структури.

Спробуємо обґрунтувати сутність ієрархії побудови дерева ідентифікаторів.

Починаючи з 2000 р., дозволено використовувати ASCII символи (коди).

Нині під час використання Юнікод-позначок дерево отримало назву — «Міжнародне OID – tree».

Повний шлях від вузла головного кореня до вузла ідентифікації описується рядком з Юнікод-позначок та його кінцеве значення називається OID-TRI формою ідентифікації. Таким чином досягається відповідність між позначками Юнікоду (Unicode label) і описом ASN.1.

Консультативний Комітет з телефонії і телеграфії в рамках ASN.1 проекту створив репозитарій, який містить відомості про різні класи та сховища OID (у тому числі усіх тих, які визначені в будь-якій рекомендації ITU-T).

Приклад організації сховища на основі ASN.1, яке фіксує організаційну структуру збору відомостей про OID наведено на рис. 3.1. Сьогодні в цьому репозиторії зберігається приблизно 895,445 ідентифікаторів [110].

Метою будь-якої інформаційної системи незалежно від сфери її застосування, програмного і апаратного забезпечення є надання повної, достовірної і своєчасної інформації кінцевим клієнтам послуг. Тому актуальною стає проблема ідентифікації даних різних класів інформаційних об’єктів світового простору.

Ідентифікація — (от середньолат. *identifico* — ототожнюю) — ототожнення, уподібнення (визнання тотожності, ототожнення об’єктів розпізнання) [112].

Під ідентифікацією в інформаційних системах будемо розуміти процес привласнення суб’єктам і об’єктам інформаційної (або/чи інформаційно-правової) діяльності особистого ідентифікатора (значення, числа, номера, та ін.) та реалізація процесів його порівняння й ототожнення з переліком існуючих ідентифікаторів дерева.

Термін «Ідентифікатор об’єкта (ІО)» іноді використовується для інших схем і процедур ідентифікації, тому зазвичай зазначену систему називають «ASN.1 Object Identifiers (ідентифікатори об’єктів)» [105].

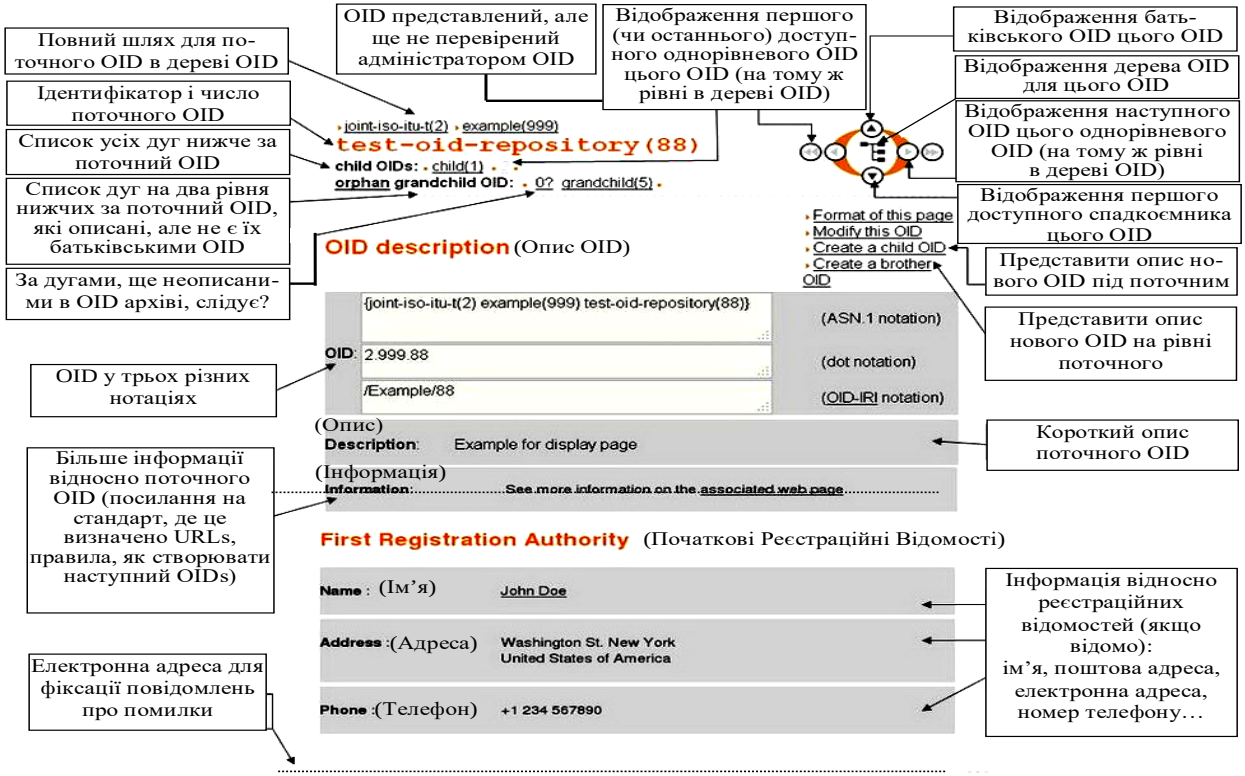

Рис. 3.1. Структурно-логічна схема організації сховища OID на основі ASN.1

Приклад інтерфейсу, що відображає три верхніх лінії дерева ідентифікації об'єктів ASN.1 наведено на рис. 3.2 [110].

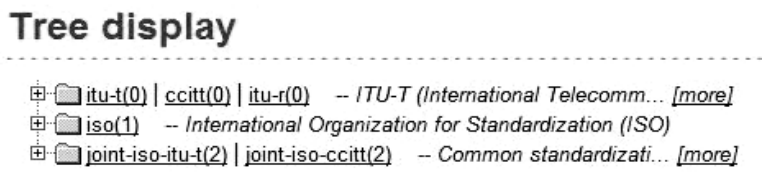

Рис. 3.2. Представлення трьох верхніх ліній дерева ідентифікації об'єктів ASN.1

Отже, відповідно до стандарту ASN.1, опис світового дерева від кореневого вузла має три базові організаційно-технічні гілки (дуги): перша гілка організаційно формується й керована міжнародним комітетом ITU-T з привласненим значенням індексу вузла — 0; друга гілка, керована міжнародною організацією стандартизації ISO, має привласнений індекс — 1; третя гілка, керована спільно ITU-T і ISO та означена індексом — 2. У зв'язку з цим у загальному вигляді світове дерево OIDs може бути проілюстровано як на рис. 3.3.

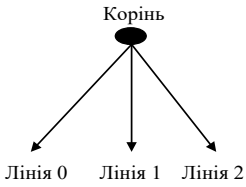

Рис. 3.3. Загальний вигляд світового дерева OIDs згідно з організаційним розподілом базових індексів

Гілки дерева, що організаційно формуються й керовані комітетом ITU-T, а також знаходяться нижче вузла 0, відображені на рис. 3.4. Даний напрям дерева ідентифікаторів має гілки з числовими значеннями від 0 до 5 та додаткову лінію вторинних ідентифікаторів даних з числовим значенням 9, згідно з вимогами і рекомендаціями ITU-T.

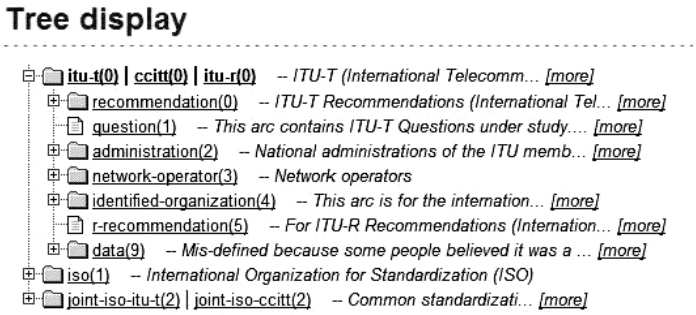

Рис. 3.4. Лінії нижче лінії 0

Лінії нижче вузла 1 відображені на рис. 3.5. Гілки вузла 1 забезпечують область імен ідентифікаторів для позначок серії стандартів ISO та IEC, а також для інших національних органів системи ISO та міжнародних організацій, так звані «Вказівники Міжнародного Коду» [105].

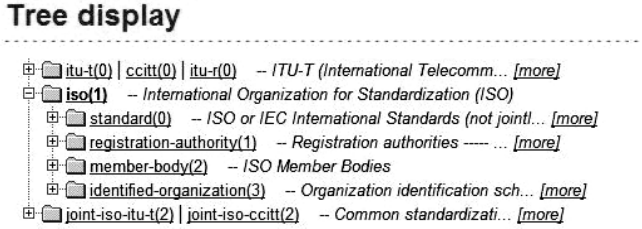

Рис. 3.5. Лінії нижче лінії 1

Розглядаючи лінії нижче базових вузлів 0 і 1, можна зробити висновок, що вони відносно постійні, в них зміни відбуваються не часто, на відміну від гілок нижче значення позначки 2 (рис. 3.6).

Схема ідентифікації OID часто застосовується в галузях промисловості, органах стандартизації, а також у діяльності національних урядів. Метою введення дерева ідентифікаторів є використання чіткої технології розподілення інформаційних ресурсів держави на базі гнучкої системи ідентифікації об'єктів в інформаційному середовищі країни.

Основні типи об'єктів, які можуть ідентифікуватися за допомогою міжнародних OID [105; 110; 111] такі:

- країни, державні та недержавні організації в країні, проекти;
- система побудови сертифікатів ключів, електронних підписів відповідно до рекомендацій міжнародного комітету Rec. ITU-T X.509, включаючи політику і технології застосування сертифікатів (*certificate policy*);
- алгоритми шифрування (наприклад, SHA-1 або RSA);
- протоколи сповіщення (Common Alerting Protocol (CAP) emergency message identification ([WMO-alerting-OIDs]);
- схеми ідентифікації для застосувань tag-based об'єктів (also [X.668]);
- система та правила визначення імен атрибутів (*distinguished name attributes* [X.509]);

- системи відображення модулів типу ASN.1, наприклад, BioAPI (Biometrics) Interworking Protocol;
- технології, алгоритми та правила кодування/декодування ASN.1 модулів, наприклад, ASN.1 Basic Encoding Rules;
- змістовні та практичні об'єкти MIB для управління мережами на основі різних типів протоколів;
- модулі електронного документообігу із застосуванням у державній (недержавній) системі охорони здоров'я, наприклад, HL7 (*international*) tree of allocations;
- різні класи інформаційних об'єктів на основі ASN.1 (див. [X.681]);
- системи та мережі авіаційного електрозв'язку (ATN) з використанням ISO/OSI стандартів і протоколів;
- модулі провайдерів й операторів мережевих послуг;
- вузли модулів обміну інформаційними ресурсами з кібербезпеки;
- інші об'єкти.

Є декілька можливостей отримання свого вузла та його ідентифікаційного коду в розподіленому дереві OID.

Якщо ваша організація є розробником стандартів ISO або IEC або рекомендацій ITU-T, ви автоматично маєте привласнений вам вузол і позначку.

Якщо вам тільки необхідно отримати класифікацію інформаційного ресурсу (об'єкта) у будь-якій державі, то для подальшої роботи є лінія дуги з позначкою 2.16.xx. Зазначена гілка вузлів використовується для багатьох держав.

Стандартом X.660|ISO/IEC 9834-1 передбачається, що національний адміністратор OID — tree має бути визначений спільним рішенням адміністрації (ITU) зв'язку і національним органом зі стандартизації (ISO).

Так, відповідно до спільного рішення міжнародних органів та згідно з Положенням «Про порядок формування простору ідентифікаційних кодів об'єктів українського сегмента світового простору ідентифікаторів об'єктів», затвердженого рішенням національної комісії державного регулювання у сфері зв'язку та інформатизації, в Україні встановлено коди вузлів гілок IO : *{iso(1) member-body(2) ua(804)}* та *{joint-iso-itu-t(2) country(16) ua(804)}* [11].

Рис. 3.6. Гілки дерева нижче базового вузла із значенням позначки 2

На підставі спільного рішення адміністрації зв'язку (ITU) і національного органу зі стандартизації (ISO), а також спільної робочої групи ITU-T SG-17 і ISO/IEC JTC 1/SC 6 з 2013 р. в Україні визначений орган реєстрації (HPO) ідентифікаторів об'єктів.

Під час розробки структури національного дерева ідентифікаторів об'єктів повинні враховуватися:

- міжнародна практика застосування, розробки і опису інформаційних об'єктів;
- стандартні міжнародні OID в окремих сферах застосування;
- національні OID та правила опису синтаксису об'єктів;
- відсутність перетинання з раніше розробленими стандартними OID тощо.

Структурно-логічну схему Українського сегмента міжнародного дерева ідентифікаторів об'єктів OID – tree показано на рис. 3.7.

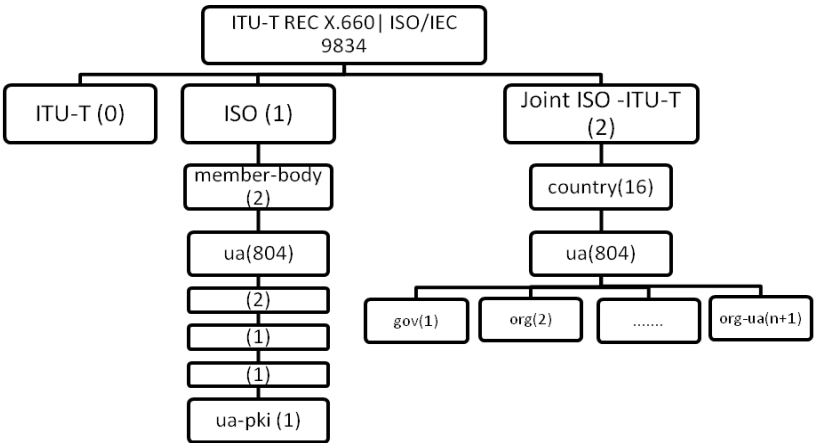

Рис. 3.7. Український сегмент міжнародного дерева ідентифікаторів об'єктів OID – tree

Національне дерево України повинно починатися з головного вузла OID-TREE, що має код-позначку 2.16.804 і лексику {joint-iso-itu-t (2) країна (16) ua (804)}/JOINT-ISO-ITU-T/16/804, значення якого привласнене відповідно до міжнародних рекомендацій (рис. 3.8).

Для реєстрації об'єктів у сфері державного управління створено гілку з лексикою — {joint-iso-itu-t (2) країна(16) ua (804) gov(1)}.

Рис. 3.8. Структура національного дерева OID – tree України

Для реєстрації об’єктів у сфері бізнесу та недержавними структурами створено гілку — {joint-iso-itu-t (2) country (16) ua (804) org (2)}.

Як визначено у вітчизняному нормативному акті, подальший розвиток 1-го рівня національного дерева ідентифікаторів повинен визначатися шляхом внесення відповідних змін до нормативних документів, що регламентують структуру національного дерева українського сегмента світового простору ІО за поданням НРО [11].

На жаль, автори констатують, що питанню ідентифікації об'єктів в Україні приділяється мало уваги, виникає ціла низка непорозумінь відносно необхідності організаційно-правового визначення цього напряму. В Україні на сьогодні існує тільки декілька правових актів. Відсутні роз'яснення органу реєстрації й інших державних структур щодо питань: фінансової складової процедури реєстрації, обов'язковості процесу призначення ідентифікаторів, класифікації інформаційних ресурсів (у тому числі державних), що підлягають реєстру тощо. Дана робота, на жаль, відсутня в масштабах України в цілому [12].

Крім затвердження нормативно-правового акту, який регламентує порядок формування простору ідентифікаційних кодів об'єктів українського сегмента світового простору ідентифікаторів, робота з цього питання майже не ведеться [11]. Розглядаючи Національний реєстр електронних інформаційних ресурсів, можна спостерігати невелику кількість об'єктів, що мають національні ідентифікатори.

У сучасних умовах розвитку інформаційного суспільства держави особливого значення набувають її ресурси, система організації і вільного доступу до них всіх категорій суб'єктів інформаційної діяльності [3]. Державні інформаційні ресурси набувають базової значущості при реалізації процесів глобалізації інфраструктур.

Виходячи з цього, необхідно активізувати ці питання та впровадити досвід, накопичений міжнародними організаціями й країнами світу. Також, виходячи із запропонованої авторами класифікації загроз ДІР [3; 4] доцільним є подальше визначення можливості розробки репозитарію на основі нотацій ASN.1 з узагальненою класифікацією загроз державним інформаційним ресурсам на рівні окремої гілки OID українського сегмента. Прикладом такої роботи є структура світового дерева відповідно до міжнародних вимог. Гілки вузлів зазначеного рівня відбивають ієрархічну структуру об'єктних ідентифікаторів для існуючих криптографічних алгоритмів та методів шифрування даних, що є державними стандартами для різних країн (Object identifier — OID) [109].

Прикладом може бути «Інфраструктура відкритих ключів» — ua-pki з кодом-позначкою вузла 1.2.804.2.1.1.1. Змістом даного вузла є об'єктні ідентифікатори криптографічних алгоритмів, об'єктні ідентифікатори політики сертифікації, об'єктні ідентифікатори уточненого призначення відкритого ключа, об'єктні ідентифікатори організацій — розробників засобів інфраструктури відкритих ключів, об'єктні ідентифікатори національних реквізитів у розширенні «Персональні дані підписувача».

Отже, важливо в сучасних умовах інтеграції інфраструктури країни до світового простору застосовувати міжнародну практику та попит ідентифікації ресурсів у різних областях діяльності суспільства. Необхідно забезпечити процеси розробки та впровадження переліку нових національних ідентифікаторів, правил їх опису і синтаксису в умовах ефективного функціонування інтегрованих інформаційних систем українського сегмента [12].

3.2. Реєстр електронних інформаційних ресурсів. Нормативно-правовий аналіз, зміст та визначення

В умовах стрімкого зростання новітніх технологій подальшого розвитку інформаційного суспільства держави провідну роль відіграють її ресурси, а також система організації і вільного доступу до них всіх категорій суб'єктів інформаційної діяльності. ДІР набувають базової значущості при реалізації процесів глобалізації інфраструктур, а також в умовах інтеграції України до світового інформаційного простору [3]. На сучасному етапі інформатизації світового простору виникає нова загрозлива тенденція дезінтеграції або поділу країн за ознакою рівня розвитку інформаційної сфери на так звані: «інформаційно багаті» та «інформаційно бідні» [113]. Стримування процесів законодавчого, організаційно-технічного забезпечення сучасної інфраструктури держави, їх відставання від світового рівня може призвести до ситуації, коли Україна поступово буде віднесена до негативних.

Створення реєстру електронних інформаційних ресурсів (РЕІР) тісно пов'язане з курсом України у напрямку розбудови європейського інформаційного простору. Основу НПЗ формування, використання та захисту національних ресурсів у цілому становлять Закони України «Про Національну програму інформатизації», «Про ін-

формацію», «Про захист інформації в автоматизованих системах» та ціла низка інших законодавчих актів. Основні положення державної політики у сфері національних інформаційних ресурсів також визначає Концепція формування системи національних інформаційних ресурсів, затверджена розпорядженням Кабінету Міністрів України від 18.05.2003 р. № 259-р. Постановою КМ України від 17.03.2004 р. № 326 затверджено Положення про Національний реєстр електронних інформаційних ресурсів. Згідно з цим Положенням до Національного реєстру включаються web-сайти, бази даних та реєстри в електронній формі [114]. Іншою Постановою КМ України від 03.08.2005 р. № 688, затверджено Положення про реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління. Таким чином, вирішення питання забезпечення формування системи державних інформаційних ресурсів, одним із завдань якого є удосконалення роботи та наповнення Національного реєстру електронних інформаційних ресурсів, розробка та удосконалення його НПЗ та системи в цілому, є актуальним завданням.

Питанням методології створення реєстрів електронних інформаційних ресурсів у світі займаються вже доволі давно, в Україні ж це питання стало актуальним і відповідно почало широко обговорюватися з появою Концепції формування системи національних інформаційних ресурсів у 2003 р., де запроваджені основні визначення, що стосуються даного напряму, а саме: національний, державний, комунальний, приватний ресурс, поняття власника та упорядника електронних ресурсів, система національних ресурсів, а також безпосередньо — реєстр інформаційних електронних ресурсів. У роботах О. Г. Додонова, О. В. Нестеренка, А. В. Бойченка [114; 115], А. І. Марущака [32; 42], А. Б. Антопольського [116] широко обговорювались питання як створення реєстрів електронних інформаційних ресурсів, так і в цілому поняття інформаційного ресурсу та його складових. Але подальшому прискоренню роботи щодо створення нормативної бази, впровадження та покращення системи електронних інформаційних ресурсів відповідно до Концепції формування системи національних електронних ресурсів, приведення даної системи відповідної до міжнародних стандартів приділялося недостатньо уваги на правових теренах нашої країни.

Це, у свою чергу, віддзеркалюється у питанні формування реєстрів електронних інформаційних ресурсів у державі з умов входження до загального світового дерева реєстрації та накопичення електронних ресурсів.

Виходячи з наведеного, необхідно провести аналіз існуючого НПЗ, міжнародного досвіду у галузі інформатизації суспільства і держави. На основі проведених досліджень необхідно визначити основні напрями щодо організації подальших процесів розробки і впровадження реєстру електронних інформаційних ресурсів в Україні. В результаті проведення досліджень необхідно визначити місце реєстру в загальній системі національних інформаційних ресурсів держави.

Під час розгляду актуальності дослідження були вказані основні НПА, що регламентують роботу реєстру електронних інформаційних ресурсів. Наведемо як узагальнений підхід основну порівняльну характеристику з даного питання відповідно до відомостей НПА (табл. 3.1).

Таблиця 3.1

Порівняльна характеристика основних положень щодо питання реєстру електронних інформаційних ресурсів в Україні

Положення про Національний реєстр електронних інформаційних ресурсів	Положення про реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління
Визначення	
Національний реєстр електронних інформаційних ресурсів — це інформаційно-телекомунікаційна система, призначена для реєстрації, обліку, накопичення, оброблення і зберігання відомостей про склад, зміст, розміщення, умови доступу до електронних інформаційних ресурсів та задоволення потреб юридичних і фізичних осіб в інформаційних послугах	***Реєстр*** — інформаційна система, призначена для накопичення, обліку, оброблення і зберігання відомостей про склад, структуру, розміщення, умови функціонування, призначення, стан захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, що містять державні електронні інформаційні ресурси або

Продовження табл. 3.1

Положення про Національний реєстр електронних інформаційних ресурсів	Положення про реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління
	плануються для цього, органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління
Мета реєстру	
Запровадження єдиної системи обліку електронних інформаційних ресурсів держави	Запровадження єдиної системи обліку відомостей, визначених переліком відомостей про інформаційну, телекомунікаційну та інформаційно-телекомунікаційну систему органу виконавчої влади, а також підприємства, установи і організації, що належить до сфери його управління; проведення аналізу стану захисту державних електронних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах надання методичної допомоги і координація діяльності міністерств та інших центральних органів виконавчої влади, пов'язаної із захистом державних електронних інформаційних ресурсів в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах
Реєстр містить	
Веб-сайти, бази даних та реєстри в електронній формі (е-ресурси органів державної влади, органів місцевого самоврядування	Відомості про інформаційну, телекомунікаційну та інформаційно-телекомунікаційну систему органів виконавчої влади, а також

Закінчення табл. 3.1

Положення про Національний реєстр електронних інформаційних ресурсів	Положення про реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління
та інших юридичних осіб публічного права)	підприємства, установи і організації, що належать до сфери його управління
Склад реєстру	
Еталонний фонд, робочий фонд, страховий фонд та інформаційний фонд	Інформаційний фонд (складається з робочого фонду, еталонного фонду, страхового фонду), комп'ютерне обладнання, електронні носії інформації, програмне забезпечення, експлуатаційна документація, комплексна система захисту інформації
Інформація, яка міститься в інформаційному фонді реєстру, є *державним електронним інформаційним ресурсом*	
Управління реєстром	
Державне агентство з питань науки, інновацій та інформатизації України (Держкомінформнауки)	Адміністрація Держспецзв'язку України

Також необхідно зазначити, що питання подальшого удосконалення реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем знайшли своє відображення в Наказі Адміністрації державної служби спеціального зв'язку та захисту інформації України від 24.04.2007 р. № 72 «Про затвердження Порядку формування й користування інформаційним фондом реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління», який визначає види та форми надання відомостей до інформаційного фонду Реєстру інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління органами виконавчої влади, а також правила користування ним.

Автори приділяли достатньо уваги зазначеним питанням, а саме основним визначенням і змістовним наповненням таких понять, як: державні інформаційні ресурси, державні електронні інформаційні ресурси, реєстр державних електронних ресурсів, депозитарій електронних державних інформаційних ресурсів, розширене визначення поняття державної системи, що їх поєднує [3; 15].

Однак, розглядаючи питання, пов'язані з Національним реєстром електронних інформаційних ресурсів, реєстром інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем не можливо уявити без їх відповідності до світового простору ідентифікаторів об'єктів. Нині, український сегмент наявний [11], але він тільки конструктивно зазначений, наявність ідентифікаторів об'єктів українського сегмента доволі незначна [15]. Подібні процеси спостерігаються і при наповненні Національного реєстру та реєстру інформаційних систем. Обидва реєстри мають фонд, який містить інформацію про ***державні електронні інформаційні ресурси***. Однак з цього напряму повністю відсутня система та рекомендації щодо процедур обов'язкової реєстрації державних електронних ресурсів. Проблема полягає і в тому, що функції управління основних реєстрів за нормативно-організаційними вимогами здійснюють різні структури, що свідчить про неузгодженість нормативно-правової бази. Є гостра необхідність зосередження системи державного управління на базі одного органу. На думку авторів та відповідно до законодавчої та нормативно-правової бази, враховуючи функціональні можливості і обов'язки — це адміністрація Держспецзв'язку України. Дійсно, актуальним є завдання реєстрації, накопичення й відображення систематизованої інформації про державні інформаційні ресурси, як у Національному реєстрі, реєстрі інформаційних систем, так і в реєстрі світового простору ідентифікаторів об'єктів, гілка якого визначена для українського сегмента [11].

Як було зазначено в підрозд. 3.1 для реєстрації інформаційних об'єктів у сфері державного управління створено гілку — {joint-iso-itu-t (2) країна(16) ua (804) gov(1)}. Для реєстрації об'єктів у сфері бізнесу та недержавних структур створено гілку українського сегмента з кодом-позначкою вузла дерева ідентифікаторів — {joint-iso-itu-t (2) country (16) ua (804) org (2)}. Положення про порядок формування простору ідентифікаційних кодів об'єктів українського

сегмента визначає подальший розвиток 1-го рівня національного дерева ІО. Національна комісія у сфері зв'язку та інформатизації України повинна здійснювати процеси державного регулювання цих питань шляхом внесення відповідних змін до нормативних документів, що регламентують організаційну структуру національного дерева українського сегмента світового простору ідентифікаторів об'єктів (OID) [11; 12; 15].

Розглядаючи міжнародні рекомендації та стандарти серії ASN.1, результатом яких повинно бути створення державного репозитарію, який збирає відомості про OID [110], на жаль, ми не можемо констатувати великої кількості зареєстрованих об'єктів українського сегмента (рис. 3.9).

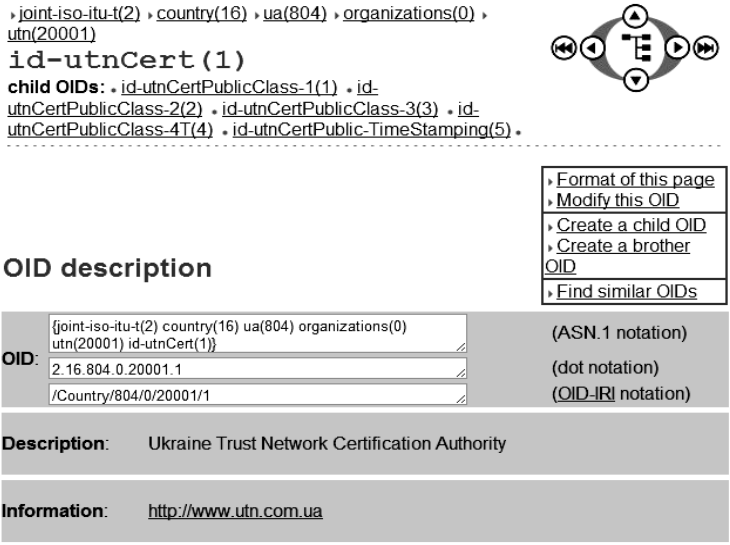

Рис. 3.9. Приклад зареєстрованих об'єктів українського сегмента міжнародного дерева ідентифікаторів об'єктів OID – tree

Досліджуючи реєстр за посиланням у розділі **Information**, можна визначити інформаційний ресурс посвідчувального центру сертифікатів цифрового підпису (рис. 3.10).

Враховуючи наведений вище матеріал стосовно недоліків організаційної системи в країні з даного напряму, констатуємо, що робота майже не проводиться, немає узгодженості між наповненням реєстрів та єдиним органом управління [117].

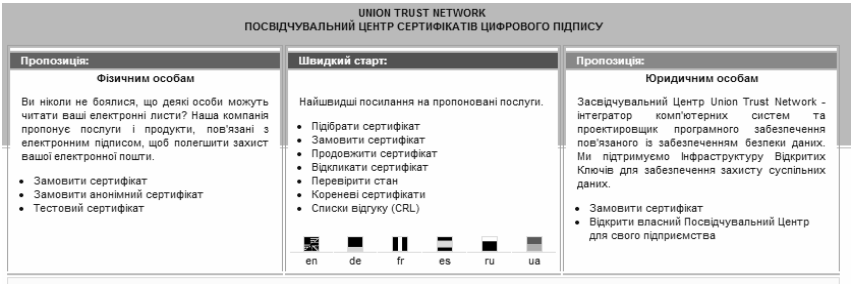

Рис. 3.10. Інформаційний ресурс посвідчувального центру сертифікатів цифрового підпису

3.3. Ієрархічна гілка кодів вузлів українського сегмента міжнародного дерева ідентифікаторів об’єктів на базі структури системи судів загальної юрисдикції

Розглянемо приклад та спробуємо описати ієрархічну гілку кодів вузлів для наповнення Національного реєстру українського сегмента міжнародного дерева ідентифікаторів об’єктів на базі структури системи судів загальної юрисдикції (рис. 3.11) [118].

Відповідно до ст. 6 Конституції України державна влада здійснюється на засадах її поділу на *законодавчу, виконавчу* та *судову*. У зв’язку з цим є доречним визначати корені дерева (root) ідентифікаторів об’єктів українського сегмента для державних органів влади з урахуванням такого поділу. Нормативно-правовий акт «Положення про порядок формування простору ідентифікаційних кодів об’єктів українського сегмента» є чинним, однак його наповнення відповідно структури системи судів не здійснюється.

Згідно з положенням, національні реєструючи організації повинні забезпечувати унікальність значень ідентифікаторів об’єктів у реєстрі. Сама реєстрація полягає в призначенні національною реєструючою організацією (НРО) ідентифікатора вузла ІО на підставі заяви замовника, а також повинна забезпечити підтримку і публікацію в реєстрах на національному та міжнародному рівнях.

Так, наприклад, ІО Республіки Казахстан у світовому телекомунікаційному просторі показано на рис. 3.12 [119]. Уповноважений орган публікує та здійснює актуалізацію ІО на вказаному веб-сайті. В Україні це питання не вирішено.

Рис. 3.11. Структура системи судів загальної юрисдикції України

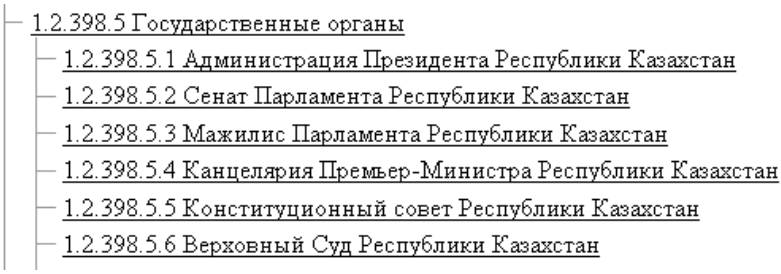

Рис. 3.12. Державний реєстр ІО Республіки Казахстан у світовому телекомунікаційному просторі

У зв'язку з проведеним аналізом пропонуємо як приклад визначати гілки щодо структури судів загальної юрисдикції [117]. Для цього всі державні органи визначатимуться гілкою gov(1) (як це вказано в [11]). Надалі група ІО, які будуть певним чином відноситися до законодавчої влади, позначатиметься *low* (закон), виконавчої — *executive* (виконавча), судової — *court* (суд). Окремо визначаєтиметься ІО Адміністрації Президента України — *president* (президент), Конституційного Суду України — *court-constitution*, прокуратура — *prosecutor* (обвинувач), *other-gov* — інших державних органів (рис. 3.13).

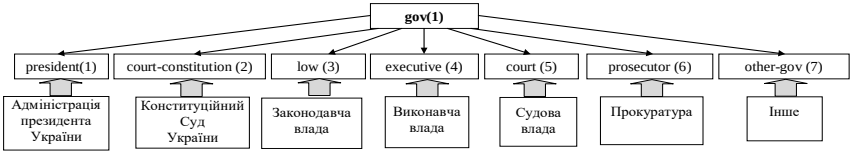

Рис. 3.13. Пропозиції щодо подальшої класифікації ІО державних органів (після визначеної гілки gov(1))

Надалі розглянемо гілку (дугу) court(5), що має містити вузли дерева ІО, які зареєстровані згідно з рис. 3.11. Так, ІО для Верховного Суду України може бути записаний у вигляді кодів-позначок:

{joint-iso-itu-t(2) country(16) ua(804) gov(1) court(5) s-court(1)}	ASN.1 notation
2.16.804.1.5.1	dot notation
/Joint-ISO-ITU-T/16/804/1/5/1	OID-IRI notation

ІО для Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ:

{joint-iso-itu-t(2) country(16) ua(804) gov(1) court(5) s-court(1) sc-court(1)}	ASN.1 notation
2.16.804.1.5.1.1	dot notation
/Joint-ISO-ITU-T/16/804/1/5/1/1	OID-IRI notation

ІО для Вищого господарського суду України:

{joint-iso-itu-t(2) country(16) ua(804) gov(1) court(5) s-court(1) arbitr-court(2)}	ASN.1 notation
2.16.804.1.5.1.2	dot notation
/Joint-ISO-ITU-T/16/804/1/5/1/2	OID-IRI notation

ІО для Вищого адміністративного суду України:

{joint-iso-itu-t(2) country(16) ua(804) gov(1) court(5) s-court(1) vasu-court(3)}	ASN.1 notation
2.16.804.1.5.1.3	dot notation
/Joint-ISO-ITU-T/16/804/1/5/1/3	OID-IRI notation

Побудуємо як приклад гілку позначок вузлів ІО для Житомирського апеляційного адміністративного суду з урахуванням міжнародного дерева:

{joint-iso-itu-t(2) country(16) ua(804) gov(1) court(5) s-court(1) vasu-court(3) zaas-court(4)}	ASN.1 notation
2.16.804.1.5.1.3.4	dot notation
/Joint-ISO-ITU-T/16/804/1/5/1/3/4	OID-IRI notation

та ІО для Житомирського окружного адміністративного суду:

{joint-iso-itu-t(2) country(16) ua(804) gov(1) court(5) s-court(1) vasu-court(3) zaas-court(4) adm-zt-court(8)}	ASN.1 notation
2.16.804.1.5.1.3.4.8	dot notation
/Joint-ISO-ITU-T/16/804/1/5/1/3/4/8	OID-IRI notation

З наведених вище прикладів видно, що для спрощення визначення певного значення вузла ІО можна використовувати частину з його посилання на е-ресурс у мережі Internet.

Подальше здійснення визначення ІО для решти об'єктів, які входять до системи судів загальної юрисдикції (див. рис. 3.11) не складне.

Отже, проведено аналіз існуючого нормативно-правового забезпечення і міжнародного досвіду в галузі інформатизації суспільства та держави. На основі проведених досліджень визначено основні напрями щодо організації подальших процесів розробки і впровадження реєстру державних електронних інформаційних ресурсів в Україні.

У результаті проведення досліджень визначено місце судової гілки реєстру в загальній системі національних інформаційних ресурсів держави.

Під час цього аналізу можна дійти висновку, що наповнення Національного реєстру та українського сегмента ІО йде дуже повільно, особливо це стосується частини українського сегмента державних вузлів дерева ідентифікаторів.

Констатовано відсутність процесів і вимог до обов'язкової реєстрації державних електронних ресурсів.

Визначено стан децентралізації функцій управління різними структурами, що свідчить про неузгодженість нормативно-правової бази та необхідності подальшого зосередження управління в одному державному органі (на думку авторів це — адміністрація Держспецзв'язку України) [117].

СПИСОК ЛІТЕРАТУРИ

1. *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.

2. *Про Державну* службу спеціального зв'язку та захисту інформації України: Закон України від 23 лютого 2006 р. № 3475-IV-ВР//ВВР. — 2006. — № 30 (в редакції Закону № 1194-VII від 09.04.2014). — С. 258.

3. *Юдін О. К*. Правові аспекти формування системи державних інформаційних ресурсів [Електронний ресурс] / О. К. Юдін, С. С. Бучик // Безпека інформації. — 2014. — Т. 20 (1). — С. 76–82. — Режим доступу:

http://jrnl.nau.edu.ua/index.php/Infosecurity/article/view/6578. (Журнал індексується у наукометричних базах даних)

4. *Юдін О. К.* Аналіз загроз державним інформаційним ресурсам [Електронний ресурс] / О. К. Юдін, С. С. Бучик // Проблеми інформатизації та управління. — 2013. — № 4 (44). — С. 93–99. — Режим доступу:
http://jrnl.nau.edu.ua/index.php/PIU/article/view/6404. (Журнал індексується у наукометричних базах даних)

5. *Концепції* формування системи національних електронних інформаційних ресурсів: розпорядження Кабінету Міністрів України від 5 травня 2003 р. № 259-р. [Електронний ресурс]. — Режим доступу: http://zakon2.rada.gov.ua/laws/show/259-2003-р

6. *Положення* про Реєстр інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем органів виконавчої влади, а також підприємств, установ і організацій, що належать до сфери їх управління : затверджено Постановою Кабінету Міністрів України від 3 серпня 2005 р. № 688 (у редакції від 07.09.2011 р. № 938) [Електронний ресурс]. — Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/KP050688.html.

7. *Положення* про Національний реєстр електронних інформаційних ресурсів : затверджено Постановою Кабінету Міністрів України від 17 березня 2004 р. № 326 (у редакції від 21.07.2010 р. № 675) [Електронний ресурс]. — Режим доступу: http://zakon4.rada.gov.ua/laws/show/326-2004-п.

8. *Юдін О. К.* Загрози державним інформаційним ресурсам: терміни та визначення [Електронний ресурс] / О. К. Юдін, С. С. Бучик // Захист інформації. — 2014. — Т. 16 (2). — С. 121–125. — Режим доступу:
http://jrnl.nau.edu.ua/index.php/ZI/article/view/6930. (Журнал індексується у наукометричних базах даних).

9. *Методологія* побудови класифікатора загроз державним інформаційним ресурсам [Електронний ресурс] / О. К. Юдін, С. С. Бучик, А. В. Чунарьова, О. І. Варченко // Наукоємні технології. — 2014. — № 2 (22). — С. 200–210. — Режим доступу: http://jrnl.nau.edu.ua/index.php/SBT/article/view/6820. (Журнал індексується у наукометричних базах даних)

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

11. *Положення* про порядок формування простору ідентифікаційних кодів об'єктів Українського сегмента світового простору ідентифікаторів об'єктів. Затверджено Рішенням Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації 18 квітня 2013 року № 227.

12. *Юдін О. К.* Світовий простір ідентифікаторів об'єктів: аналіз, перспективи розвитку, місце українського сегмента [Електронний ресурс] / О. К. Юдін, С. С. Бучик, О. В. Фролов // Наукоємні технології. — 2014. — № 3 (23). — С. 295 — 302. — Режим доступу:
http://jrnl.nau.edu.ua/index.php/SBT/article/view/7406. (Журнал індексується у наукометричних базах даних)

13. *Бучик С. С.* Аналіз нормативно-правового забезпечення захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах. Materialy IX mezinarodni vedecko-prakticka conference "Predni vedecke novinky — 2013". Dil 9. Moderni informacni technologie. Matematika. Fyzika. Televychova a sport: Pracha. Publishing House "Education and Science". — Stran. 43–46.

14. *Бучик С. С.* Концептуальний аналіз уразливості державних інформаційних ресурсів. Материали за 9-а международна научна практична конференция, «Новини на научния прогрес», — 2013. Том 9. Технологии. Съвременни технологии на информации. Математика. София. «Бял ГРАД-БГ» ООД. — Стр.46–49.

15. *Юдін О. К.* Український сегмент ідентифікаторів електронних ресурсів / О. К. Юдін, С. С. Бучик, О. М. Весельська // Матеріали IV міжнар. науково-технічної конференції ITSEC. — К. : НАУ. — 2014. — С. 166–169.

16. *Юдін О. К.* Система державних інформаційних ресурсів. Нормативно-правовий аналіз, зміст та визначення [Електронний ресурс] / С. С. Бучик, В. В. Матвійчук // Актуальные научные достижения : междунар. науч.-техн. конф., 27–30 июня 2014 г. : тези докл. — Прага, 2014. — С. 78–81. — Режим доступу до тез: http://www.rusnauka.com/20_AND_2014/Informatica/4_174617.doc.htm.

17. *Юдін О. К.* Класифікатор загроз державним інформаційним ресурсам. Методологія побудови [Електронний ресурс] / С. С. Бучик, О. І. Варченко // Динамика научных исследований : междунар. науч.-техн. конф., 07–15 июля 2014 г.: тезисы докл. — Перемышль, 2014. — С. 93–97. — Режим доступу до тез: http://www.rusnauka.com/22_DNI_2014/Informatica/4_174619.doc.htm.

18. *Юдін О. К.* Правові аспекти формування термінології загроз державним інформаційним ресурсам [Електронний ресурс] / С. С. Бучик, Р. В. Зюбина // Современная европейская наука: междунар. науч.-техн. конф., 30 июня–07 июля 2014 г.: тези докл. — Шеффилд, 2014. — С. 38–41. — Режим доступу до тез: http://www.rusnauka.com/21_SEN_2014/Informatica/4_174618.doc.htm.

19. *Юдін О. К.* Подання автоматизованої системи як об'єкта «триєдиної» системи захисту інформації / С.С. Бучик, Б. С. Коновал // Проблеми створення, розвитку та застосування високотехнологічних систем спеціального призначення: XX Всеукр. наук.-практ. конф., 28 лист. 2014 р. : тези доповідей. — Житомир : ЖВІ ДУТ, 2014. — С. 154–155.

20. *Юдін О. К.* Аналіз, перспективи розвитку, місце українського сегмента в світовому просторі ідентифікаторів об'єктів [Електронний ресурс] / О. К. Юдін, С. С. Бучик, О. В. Фролов // Фундаментальная и прикладная наука: междунар. науч.-техн. конф., 30.10–07.11.2014 г.: тезисы докл. — Великобритания, 2014. — С. 93–97. — Режим доступу до тез: http://www.rusnauka.com/35_FPN_2014/Informatica/4_179968.doc.htm.

21. *Юдін О. К.* Нормативно-правовий аналіз, зміст та ієрархія реєстру електронних державних інформаційних ресурсів [Електронний ресурс] / О. К. Юдін, С. С. Бучик, О. В. Фролов // Перспективные разработки науки и техники: междунар. науч.-техн. конф., 07–15.11.2014 г.: тезисы докл. — Польша, 2014. — С.44–50. — Режим доступу до тез: http://www.rusnauka.com/36_PWMN_2014/Informatica/4_179969.doc.htm.

22. *Юдін О. К.* Класифікація загроз державним інформаційним ресурсам організаційного спрямування. Методологія побудови класифікатора [Електронний ресурс] / О. К. Юдін, С. С. Бучик // Перспективные вопросы современной науки: междунар. науч.-техн. конф., 15–22.12.2014 г.: тезисы докл. — Болгария, 2014. — С. 72–78. — Режим доступу до тез: http://www.rusnauka.com/41_PWSN_2014/Informatica/4_182685.doc.htm.

23. *Юдін О. К.* Український сегмент дерева ідентифікаторів державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Інформаційна безпека України: наук.-техн. конф., 12–13.03.2015 р.: тези доп. — К. : КНУ ім. Тараса Шевченко, 2015. — С. 35–36.

24. *Бучик С. С.* Методологія побудови класифікатора загроз державним інформаційним ресурсам. Загрози нормативно-правового спрямування [Електронний ресурс] / С. С. Бучик // АВІА-2015: XII міжнар. наук.-техн. конф., 28–29.04.2015 р.: тези доп. — К. : НАУ, 2015. — С. 5.5–5.8. — Режим доступу: http://avia.nau.edu.ua/doc/2015/AVIA_2015.pdf.

25. *Юдін О. К.* Класифікатор загроз державним інформаційним ресурсам: нормативно-правове, організаційне, інженерно-технічне спрямування / О. К. Юдін, С. С. Бучик // Безпека інформації в інформаційно-телекомунікаційних системах: XVII міжнар. наук.-практ. конф., 26–28.05.2015 р.: тези доп. — К. : Державна служба спеціального зв'язку та захисту інформації України, 2015. — С. 95–96.

26. *Юдін О. К.* Класифікація загроз державним інформаційним ресурсам інженерно-технічного спрямування. Методологія побудови класифікатора [Електронний ресурс] / О. К. Юдін, С. С. Бучик // Захист інформації і безпека інформаційних систем: IV міжнар. наук.-техн. конф., 04–05.06.2015 р.: тези доп. — Л. : Національний університет «Львівська політехніка», 2015. — С. 83–84.

27. *Чунарьова А. В.* Аналіз нормативно-правового забезпечення захисту інформації сучасних ІКСМ [Електронний ресурс] / А. В. Чунарьова, А. В. Чунарьов // Захист інформації. — 2012. — Т. 14, № 2 (55). — С. 5–8. — Режим доступу: http://jrnl.nau.edu.ua/index.php/ZI/article/view/2185/2177.

28. *Юдін О. К.* Захист інформації в мережах передачі даних: підручник / О. К. Юдін, О. Г. Корченко, Г. Ф. Конахович. — К. : Вид-во ТОВ НВП «ІНТЕРСЕРВІС», 2009. — 716 с.

29. *Богуш В. М.* Інформаційна безпека держави : навч. посіб. / В. М. Богуш, О. К. Юдін. — К. : «МК-Прес», 2005. — 432 с.

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

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

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

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

34. *Ліпкан В. А.* Інформаційна безпека України в умовах Євроінтеграції [Електронний ресурс] / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. — К. : КНТ, 2006. — 280 с. — Режим доступу: http://pidruchniki.com/1584072028356/politologiya/informatsiyna_bezpeka_ukrayini_v_umovah_yevrointegratsiyi.

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

36. *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.

37. *Yudin O.* The analysis of normatively-legal providing of defence of state informative resources in information-telecommunication systems [Електронний ресурс] / O. Yudin, S. Buchyk // Science-based technologies. — 2013. — №2 (18). — P. 202–206. — Режим доступу:
http://jrnl.nau.edu.ua/index.php/SBT/article/view/4938/5035. (Журнал індексується у наукометричних базах даних).

38. *Юдін О. К.* Концептуальний аналіз уразливості державних інформаційних ресурсів / О. К. Юдін, С. С. Бучик // Наукоємні технології. — 2013. — № 3 (19). — С. 299–304. — Режим доступу:
http://jrnl.nau.edu.ua/index.php/SBT/article/view/5571/6309. (Журнал індексується у наукометричних базах даних).

39. *Миндалёв И. В.* Мировые информационные ресурсы. Государственные информационные ресурсы / И. В. Миндалёв [Електронный ресурс]. — Режим доступа:
http://www.kgau.ru/istiki/umk/mir/index.html.

40. *Арістова І. В.* Державна інформаційна політика та її реалізація в діяльності органів внутрішніх справ України: організаційно-правові засади: дис. … д-ра юрид. наук: 12.00.07 / І. В. Арістова. — К., 2002. — 476 с.

41. *Олійник О. В.* Організаційно-правові засади захисту інформаційних ресурсів України: дис. … канд. юрид. наук: 12.00.07 / О. В. Олійник. — К., 2006. — 201 с.

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

43. *Кабашов С. Ю.* Делопроизводство и архивное дело в терминах и определениях: учеб. пособие / С. Ю. Кабашов, И. Г. Асфандиярова. — М. : Изд-во Флинта; Наука, 2009. — 296 с.

44. *Когаловский М. Р.* Перспективные технологии информационных систем / М. Р. Когаловский. — М. : ДМК Пресс; Компания АйТи, 2003. — 288 с.

45. *Мельников В. П.* Информационная безопасность и защита информации / В. П. Мельников. — М. : Издательский центр «Академия», 2008. — 336 с.

46. *Завгородний В. И.* Комплексная защита информации в компьютерных системах: учеб. пособие / В. И. Завгородний. — М. : Логос, 2001. — 264 с.

47. *Горбенко І. Д.* Захист інформації в інформаційно-телекомунікаційних системах: навч. посібник. Ч. 1. Криптографічний захист інформації / І. Д. Горбенко, Т. О. Гриненко. — Х. : ХНУРЕ, 2004. — 368 с.

48. *Корченко О. Г.* Оценка безопасности компьютерных систем на базе методов и моделей нечетких множеств / О. Г. Корченко // Сборник научных трудов «Защита информации». — К. : КМУГА, 1998. — 232 с.

49. *Термінологічний* словник з інформаційної безпеки / В. Б. Дудикевич, А. В. Зачепило, Л. Т. Пархуць, В. В. Хома, О. В. Яструбецький [Електронний ресурс]. — Режим доступу: http://megalib.com.ua/content/8805_Terminologichnii_slovnik.html.

50. *Доктрина* інформаційної безпеки України: затв. Указом Президента України від 8 липня 2009 р. № 514/2009 [Електронний ресурс] // Офіц. вісн. України. — 2009. — № 52. — Ст. 1783 (Проект Указу Президента України «Про Доктрину інформаційної безпеки України» від 2014 року у зв'язку з втратою чинності вищенаведеного Указу на підставі Указу Президента № 504/2014 від 06.06.2014. — Режим доступу: http://comin.kmu.gov.ua/control/uk/publish/article?art_id=113319&cat_id=61025).

51. *Юдін О. К.* Автоматизована система як об'єкт «триєдиної» системи захисту інформації / О. К. Юдін, С. С. Бучик, О. І. Варченко // Вісник інженерної академії України. — 2014. — № 2. — С. 146–148.

52. *Гармонизированные* критерии Европейских стран ITSEC [Електронный ресурс]. — Режим доступа: http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/garmonizirovannye_kriterii_evropejskix_stran_itsec/?all.

53. *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).

54. *Про захист* інформації в автоматизованих системах: Закон України від 05.07.1994 р. № 81/94-ВР//ВВР. — 1994. — № 31. — С. 287.

55. *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).

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

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

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

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

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

61. *Элвис-Плюс.* Информаториум. Персональные данные [Електронный ресурс]. — Режим доступа:
http://www.elvis.ru/competency/informatorium/40/.

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

63. *Анализ* подходов к классификации угроз информационной безопасности [Електронный ресурс]. — Режим доступа: http://infocom.uz/2013/05/01/analiz-podxodov-k-klassifikacii-ugroz-informacionnoj-bezopasnosti.

64. *Общие* критерии, основные изменения [Електронный ресурс]. — Режим доступа: http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/obschie_kriterii_osnovnye_izmenenija/?all.

65. *Общие* критерии оценки безопасности информационных технологий [Електронный ресурс]. — Режим доступа: http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/obschie_kriterii_otsenki_bezopasnosti_informatsionnyx_texnol/?all.

66. *Федеральные* критерии безопасности информационных технологий [Електронный ресурс]. — Режим доступа: http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/federalnye_kriterii_bezopasnosti_informatsionnyx_texnologij/?all.

67. *Канадские* критерии безопасности компьютерных систем CTCPEC [Електронный ресурс]. — Режим доступа: http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/kanadskie_kriterii_bezopasnosti_kompjuternyx_sistem_ctcpec/?all.

68. *Профили* защиты на основе «Общих критериев». Аналити-ческий обзор / В. Б. Бетелин, В. А. Галатенко, М. Т. Кобзарь, А. А. Сидак, И. А. Трифаленков [Електронный ресурс]. — Режим доступа: http://citforum.ru/security/criteria.

69. *Россия* перешла на «Общие критерии» (ГОСТ Р 15408-2002) [Електронный ресурс]. — Режим доступа: http://www.securitylab.ru/informer/240673.php.

70. *Информационная* технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий: ГОСТ Р ИСО/МЭК 15408-1-2002. Ч. 1. Введение и общая модель. — М. : ИПК Издательство стандартов, 2002.

71. *Информационная* технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий: ГОСТ Р ИСО/МЭК 15408-2–2002. Ч. 2. Функциональные требования безопасности. — М. : ИПК Издательство стандартов, 2002.

72. *Информационная* технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий: ГОСТ Р ИСО/МЭК 15408-3-2002. Ч. 3.

Требования доверия к безопасности. — М. : ИПК Издательство стандартов, 2002.

73. *Петров О. С.* Критерії оцінки захищеності інформації в комп'ютерних системах: порівняння єдиних критеріїв та критеріїв України / О. С. Петров, О. А. Таликін, А. В. Мінін // Вісник Східноукраїнського національного університету ім. В. Даля, 2005. — С. 92–96.

74. *Рекомендации* X.800 для распределенных систем [Електронный ресурс]. — Режим доступа: http://dehack.ru/mezhdunarodnye_standarty_po_otsenke_bezopasnosti_informatsio/rekomendatsii_x_800_dlja_raspredelennyx_sistem/?all.

75. [Електронний ресурс]. — Режим доступу: http://www.dsec.ru/products/grif.

76. *Шаньгин В. Ф.* Информационная безопасность / В. Ф. Шаньгин. — М. : ДМК Пресс, 2014. — 702 с.

77. *Чунарьова А. В.* Принципи організації захисту інформації в сучасних інформаційно-комунікаційних системах і мережах [Електронний ресурс] / А. В. Чунарьова, А. В. Чунарьов. — Режим доступу: http://www.rusnauka.com/16_ADEN_2010/Informatica/68642.doc.htm.

78. *Загрози* безпеці інформації [Електронний ресурс]. — Режим доступу: http://wiki.tntu.edu.ua/Загрози_безпеці_інформації.

79. *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).

80. *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).

81. *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).

82. *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).

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

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

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

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

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

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

89. *Юдін О. К.* Класифікація загроз державним інформаційним ресурсам нормативно-правового спрямування. Методологія побудови класифікатора / О. К. Юдін, С. С. Бучик // Захист інформації. — 2015. — Т. 18 (2). — С. 108–118.

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

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

92. *Юдін О. К.* Класифікація загроз державним інформаційним ресурсам організаційного спрямування. Методологія побудови класифікатора / О. К. Юдін, С. С. Бучик // Спеціальні теле-

комунікаційні системи та захист інформації. — 2014. — № 2(26). — С. 43– 49.

93. *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.

94. *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.

95. *Юдін О. К*. Класифікація загроз державним інформаційним ресурсам інженерно-технічного спрямування. Методологія побудови класифікатора / О. К. Юдін, С. С. Бучик // Наукоємні технології. — 2015. — № 2 (26). — С. 188–195.

96. *The Global* Information Grid (GIG) 2.0. Concept of Operations. Version 1.1. Washington, D.C. 20318-6000, 2009.

97. *Пашков В*. Информационная безопасность США [Електронный ресурс] / В. Пашков // Зарубежное Военное Обозрение. — 2010. — № 10. — С. 3–13. — Режим доступа: http://elibrary.az/docs/jurnal-10/1164.doc.

98. *Васильев Андрей*. Первая сетецентрическая война [Електронный ресурс]. — Режим доступа: http://topwar.ru/34855-pervaya-setecentricheskaya-voyna.html.

99. *Рекомендация* МСЭ-Т X.694. Сетевые и системные аспекты ВОС — Система абстрактных синтаксических нотаций Один (ASN.1). — Женева, 2005. — 70 с.

100. *ASN 1* [Електронний ресурс]. — Режим доступу: http://ru.wikipedia.org/wiki/ASN.1.

101. *X.680*: ITU-T Recommendation X.680 (1994) | ISO/IEC 8824-1: 1995, Abstract Syntax Notation One (ASN.1): Specification of Basic Notation.

102. *Кликич Анатолий*. Идентификаторы цифровых объектов (OID). Назначение, структура, применение [Електронный ресурс]. — Режим доступа: (Український науковий центр розвитку інформаційних технологій) http://www.itdev.org.ua/index.php?option=com_content&view=article&id=272&Itemid=220&lang=uk.

103. *Державний* університет телекомунікацій. Презентація щодо наукової та науково-технічної діяльності за 2013 рік [Електронний ресурс]. — Режим доступу: (Офіційний веб-сайт Міністерства освіти і науки України. Звітування та презентації вищих навчальних закладів та наукових установ щодо наукової та науково-технічної діяльності за 2013 рік. 20.03.2014. Державний університет телекомунікацій)
http://mon.gov.ua/ua/activity/63/64/2612/1390998643/1390998758/1394611213/.

104. *Затверджено* порядок формування простору ідентифікаційних кодів // Зв'язок. — 2013. — № 15 — 16. — С. 3.

105. *Лармус Джон*. Идентификация объектов (Идентификаторы объектов ASN.1) [Електронный ресурс] / Джон Лармус // Документальная электросвязь, № 20, 2010. — С. 41–44. — Режим доступа:
http://www.aciso.ru/files/docs/Kostrov_ADE_fraud.pdf.

106. *Международный* стандарт ISO/IEC 9834-1. Рекомендация МСЭ-Т X.660. Информационные технологии — процедуры для работы органов регистрации идентификаторов объектов: Общие процедуры и верхние дуги дерева международных идентификаторов объектов. — Женева, 2013. — 26 с.

107. *Інформаційні* технології. Нотація абстрактного синтаксису 1 (ASN.1): ДСТУ ISO/IEC 8824:2009.

108. *Коди* назв країн світу: ДСТУ ISO 3166-1:2009 (ISO 3166-1:2006, IDT). Затверджений наказом Державного комітету України з питань технічного регулювання та споживчої політики від 23 грудня 2009 року. — № 471.

109. *Вимоги* до структури об'єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами. Наказ Міністерства юстиції України, Адміністрації Державної служби спеціального зв'язку та захисту інформації України 20.08.2012 р. № 1236/5/453.

110. *OID Repository* [Електронний ресурс]. — Режим доступу: http://www.oid-info.com.

111. *OID* [Електронний ресурс]. — Режим доступу: http://www.itu.int/itu-t/studygroups

112. *Словник* іншомовних слів: 23 000 слів та термінологічних словосполучень / уклад.: Л. О. Пустовіт, О. І. Скопненко, Г. М. Сюта, Т. В. Цимбалюк. — К. : Довіра, 2000. — 1018 с.

113. *Иноземцев В. Л.* Современное постиндустриальное общество: природа, противоречия, перспективы / В. Л. Иноземцев. — М. : Логос, 2004. — 304 с.

114. *Додонов О. Г.* Методологія створення Національного реєстру електронних інформаційних ресурсів / О. Г. Додонов, О. В. Нестеренко, А. В. Бойченко // Реєстрація, зберігання і обробка даних. — 2005. — Т. 7. — № 3. — С. 88–97.

115. *Нестеренко О. В*. Єдина державна система електронних інформаційних ресурсів / О. В. Нестеренко // Науково-технічна інформація. — 2006. — № 4. — С. 3–9.

116. *Антопольский А. Б.* Проблемы учёта и регистрации информационных ресурсов / А. Б. Антопольский // Проблемы информатизации. — 2008. — № 2. — С. 33–40.

117. *Юдін О. К.* Реєстр електронних інформаційних ресурсів. Нормативно-правовий аналіз, зміст та ієрархія / О. К. Юдін, С. С. Бучик, О. В. Фролов // Вісник інженерної академії України. — 2014. — № 3–4. — С. 135–141.

118. *Офіційний* веб-портал судової влади України [Електронний ресурс]. — Режим доступу: http://court.gov.ua/sudy.

119. *Корневой* удостоверяющий центр республіки Казахстан [Електронный ресурс]. — Режим доступа: http://www.oid.pki.gov.kz.

120. *Бучик С. С*. Системи підтримки прийняття рішень : конспект лекцій / С. С. Бучик, С. О. Кондратенко, О. О. Писарчук. — Житомир : ЖВІРЕ, 2006. — 168 с.

121. *Постников В. М*. Анализ подходов к формированию состава экспертной группы, ориентированной на подготовку и принятие решений / В. М. Постников // Наука и образование. — 2012. — № 5 [Електронный ресурс]. — Режим доступа: http://technomag.bmstu.ru/doc/360728.html.

122. *Чернышева Т. Ю*. Иерархическая модель оценки и отбора экспертов [Електронный ресурс] // Доклады ТУСУР. Управления, вычислительная техника и информатика. — 2009. — № 1(19). — Часть 1. — С. 168–173. — Режим доступа: http://tusur.ru/filearchive/reports-magazine/2009-1-1/168-173.pdf.

123. *Лукичева Л. И.* Управленческие решения : учеб. по спец. «Менеджмент организации» / Л. И. Лукичева, Д. Н. Егорычев; под ред. Ю. П. Анискина. — М. : «Омега-Л», 2009. — 383 с.

124. *Каратанов А. В.* Информационные технологии экспертного оценивания проектных решений при формировании единого информационного пространства // А. В. Каратанов, Е. А. Дружинин // Збірник наукових праць Харківського університету повітряних сил. — 2014. — №3(40). — С. 155–160.

125. *Постников В. М.* Подход к расчёту весовых коэффициентов ранговых оценок экспертов при выборе варианта развития информационной системы // В. М. Постников, С. Б. Спиридонов // Наука и образование. — 2013. — № 8 [Електронный ресурс]. — Режим доступа: http://technomag.edu.ru/doc/580272.html.

Додаток 1

Приклади функціональних профілів загроз державним інформаційним ресурсам нормативно-правового спрямування

Спрямування загроз	Рівень загроз	Вид загроз	Функціональний профіль загроз	Джерело загроз			Відносно до інформаційного об'єкта		Характер загроз		Загрози за структурою впливу			Рівні впливу загроз				
				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	Системи управління базами даних
01 Нормативно-правового спрямування	01_1	01_1.1_2_3 Конфіденційність Цілісність Доступність	01_1.1_2_3.1 — загрози державній політиці України у сфері інформатизації та її безпеки к,ц,д,01,02	1	0	0	1	1	1	1	1	0	0	1	0	0	0	1
	01_2	01_2.1	.....	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
		Конфіденційність	01_2.1.3 — порушення встановленого законодавством режиму проектування, технічного обладнання та впровадження приміщень, призначених для обробки, зберігання, передавання і відображення ДІР к,ц,д,01,02	1	1	0	1	0	1	1	0	1	1	1	1	1	1	1
			01_2.1.4 — відсутність (повна/часткова) правил та вимог (у тому числі відповідальність) до розподілу обов'язків осіб, що відповідають за процеси розробки, впровадження і супро-воду інформаційних систем, а також комплексів засобів захисту ДІР к,ц,д,01,02	1	0	0	1	0	1	0	1	1	1	0	0	0	0	1
		01_2.2 Цілісність	…….	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Закінчення дод. 1

Спрямування загроз	Рівень загроз	Вид загроз	Функціональний профіль загроз	Джерело загроз			Відносно до інформаційного об'єкта		Характер загроз		Загрози за структурою впливу			Рівні впливу загроз				
				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	Системи управління базами даних
			01_2.2.34 — несанкціонована модифікація процедур штатного функціонування або неавторизоване внесення змін у 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]	1	1	0	1	1	1	0	1	1	1	0	0	1	1	1
			……...	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Додаток 2

Приклади функціональних профілів загроз державним інформаційним ресурсам організаційного спрямування

Спрямування загроз	Рівень загроз	Вид загроз	Функціональний профіль загроз	Джерело загроз			Відносно до інформаційного об'єкта		Характер загроз		Загрози за структурою впливу			Рівні впливу загроз				
				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	Системи управління базами даних
01 Організаційного спряму-вання	02_1	02_1.1_2_3 Конфіденційність Цілісність Доступність	……	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Спрямування загроз	Рівень загроз	Вид загроз	Функціональний профіль загроз	Джерело загроз			Відносно до інформаційного об'єкта		Характер загроз		Загрози за структурою впливу			Рівні впливу загроз				
				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	Системи управління базами даних
			02_1.1_2_3.4 — 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 (у тому числі ДІР)[к,ц,д,02,03]	1	1	0	0	1	1	0	1	0	0	0	0	0	0	1
	02_2	02_2.1 Конфіденційність	……..	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
			02_2.1.4 — втрата, викрадення або несанкціоноване знищення проектної, виробничої документації щодо обробки, зберігання, передачі і відображення ДІР[к,ц,д]	1	0	0	1	1	1	0	1	1	1	0	0	0	0	1
		02_2.2 Цілісність	……	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
			02_2.2.37 — 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	0	0	1
		02_2.3 Доступність	……	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
			02_2.3.47 — несанкціоноване обмеження або порушення здатності продовжувати функціонування процесів надання встановлених послуг (різних типів) ІС ДІР, РеєструЕлДІР або ДепозитаріюЕлДІР[02,03]	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Додаток 3

Приклади функціональних профілів загроз державним інформаційним ресурсам інженерно-технічного спрямування

Спрямування загроз	Рівень загроз	Вид загроз	Функціональний профіль загроз	Джерело загроз			Відносно до інформаційного об'єкта		Характер загроз		Загрози за структурою впливу			Рівні впливу загроз				
				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	Системи управління базами даних
03 Інженерно-технічного спрямування	03_1	03_1.1_2_3 Конфіденційність Цілісність Доступність	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]	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	1
			……..	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
	03_2	03_2.1 Конфіденційність	03_2.1.1 — відсутність (невиконання) сформо-ваної політики безпеки при зберіганні, оброб-ці, передачі та відображенні ДІР в автомати-зованих (інформаційній) системах різних класів[к,ц,д,01,02,03]	1	0	0	1	0	1	1	1	1	1	1	1	1	1	1	1
			……..	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
		03_2.2 Цілісність	……..	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
			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]	1	1	0	1	1	1	0	1	1	1	0	0	1	1	1
			……..	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…
			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	1	0	1	0	1	0	1	0	0	0	0	0	0	0	1
			……..	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…	…

Додаток 4

МЕТОДИКА ЕКСПЕРТНОГО ОЦІНЮВАННЯ ФУНКЦІОНАЛЬНИХ ПРОФІЛІВ ЗАГРОЗ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

Дана методика призначена для уточнення функціональних профілів (ФП) загроз державним інформаційним ресурсам (ЗДІР), які були визначені в розрізі побудови класифікатора загроз у роботах [89; 92; 95]. Безпосередньо методологія побудови класифікатора ЗДІР була розглянута в праці [9].

Як зазначалося в роботах [89; 92; 95], авторами була розглянута класифікація ЗДІР нормативно-правового, організаційного та інженерно-технічного спрямування. Надалі кожна загроза була віднесена: 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). Загалом це складає ФП ЗДІР за відповідним спрямуванням.

Нижче наведена безпосередньо методика експертного оцінювання ФП ЗДІР, яка полягає в такому:

1. Складання таблиць опитування експертів, які відповідають будові класифікаторів загроз ДІР нормативно-правового, організаційного та інженерно-технічного спрямування (були наведені в роботах [89; 92; 95]).

2. Формування складу експертної групи.

3. Проведення експертизи (заповнення таблиць опитування).

4. Аналіз експертної інформації (аналіз узгодженості відповідей експертів).

5. Прийняття рішення щодо оцінювання ФП ЗДІР з урахуванням експертного оцінювання.

Розглянемо докладніше кожен із етапів методики.

1. *Складання таблиць опитування експертів.*

Для складання таблиць опитування експертів використаємо анкетування, що припускає письмову відповідь експерта на систему запитань [120]. Приклад таблиці опитування для одного експерта наведено в табл. Д4.1.

Таблиця Д4.1

Таблиця опитування

Функціональний профіль загроз	Джерело загроз			Відносно до інформаційного об'єкта		Характер загроз		Загрози за структурою впливу			Рівні впливу загроз				
	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	Системи управління базами даних
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Пропонується використовувати закриті питання, а саме відповіді у формі «так» — експерт ставить 1, або «ні» — експерт ставить 0.

У даному випадку експерти добре розуміють питання, експертиза проводиться оперативно, експерти добре розуміють поставлене завдання та впевнено працюють.

Ця форма використовується у зв'язку з тим, що набір альтернатив достатньо очевидний.

2. *Формування складу експертної групи.*

Є різні підходи до обирання кількості експертів у складі робочої групи. Розглянемо деякі загальноприйняті підходи [121; 122]:

– кількість експертів (m) повинна бути не менше числа факторів (n) або варіантів, які необхідно оцінити експертним шляхом ($m \geq n$). Даний підхід не підходить, оскільки кількість альтернативних відповідей, запропонованих експерту, всього дві: так чи ні;

– кількість експертів можна визначати за такою формулою:

$$m \geq 0{,}5(0{,}33/b + 5), \qquad (Д1)$$

де b — помилка результату експертного аналізу або допустима ймовірність помилки ($0 < b < 1$) [121].

У праці [122] наведено іншу формулу:

$$m = 0{,}5(3/\alpha + 5), \qquad (Д2)$$

тут α — параметр, який задає мінімальний рівень помилки експертизи (допустима ймовірність помилки) та лежить у межах $0 < \alpha \leq 1$.

У формулах (Д1) та (Д2) параметр b та α визначають відсутність помилки (значення дорівнюються нулю), 100 % помилка (значення дорівнює одиниці).

При цьому повинна спостерігатися стабілізація середньої оцінки характеристики, що прогнозується.

Про досягнення цієї стабілізації свідчить той факт, що включення або виключення експерта із групи не змінює відносну оцінку вихідної величини більш ніж на b (α) [123].

Як бачимо дані формули схожі, але дають різні результати (табл. Д4.2, Д4.3).

Таблиця Д4.2

Таблиця розрахунку кількості експертів за формулою (Д1)

Помилка	0,05	…	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1
Кількість експертів	5,8	…	4,15	3,33	3,05	2,91	2,83	2,78	2,74	2,71	2,69	2,67

Таблиця Д4.3

Таблиця розрахунку кількості експертів за формулою (Д2)

Помилка	0,05	…	0,1	0,2	0,3	0,4	0,5	0,6	0,7	0,8	0,9	1
Кількість експертів	32,5	…	17,5	10	7,5	6,25	5,5	5	4,64	4,38	4,17	4

Так, за допустимої помилки експертного аналізу в 5 % ($b = 0{,}05$ або $\alpha = 0{,}05$) до складу робочої групи має входити не менше шести осіб за формулою (Д1) і не менше 33 за формулою (Д2). Але під час перевірки посилання в праці [121] щодо правильності формули (Д1) виявляється, що була допущена помилка. Посилаючись на працю [123, стор. 158], формула ідентична (Д2). Та сама помилка і в праці [122, стор. 156], де також наведена формула (Д1), але посилання йде на працю [123].

Таким чином, кількість експертів необхідно визначати виходячи із формули (Д2). У зв'язку з достатньо очевидним набором альтернатив обмежимось мінімальним рівнем помилки експертизи на рівні 10 % та оберемо групу експертів у складі 17 осіб.

Надалі необхідно, знаючи категорію експертів, врахувати їх компетентність. Рівень компетентності експертів робочої групи M повинен відповідати таким вимогам [124]:

$$0{,}67 \le M \le 1{,}00\,. \qquad (Д3)$$

При цьому значення M розраховується за такою формулою:

$$M = \frac{1}{m} \cdot \sum_{j=1}^{m} K_j\,, \qquad (Д4)$$

де m — кількість експертів у складі робочої групи; K_j — рівень компетентності j-го експерта.

Для проведення експертизи були задіяні експерти з кафедри комп'ютеризованих систем захисту інформації Інституту комп'ютерних інформаційних технологій Національного авіаційного університету. Отже, знаючи категорії задіяних експертів, можна їх компетентність визначити таким чином (табл. Д4.4).

Таблиця Д4.4

Визначення коефіцієнта компетентності експертів з урахуванням їх категорії (рівня професійної підготовки та інформованості)

Номер з/п	Кваліфікація експертів	Значення коефіцієнта компетентності, k	Кількість задіяних експертів
1	Доктор технічних наук	1	2
2	Докторант (здобувач наукового ступеня д-р техн. наук)	0,95	2
3	Кандидат технічних наук	0,9	3
4	Аспірант (здобувач наукового ступеня канд. техн. наук)	0,85	5
5	Інженер зі стажем роботи більше 20 років	0,8	1
6	Інженер зі стажем роботи від 15 до 20 років	0,7	1
7	Інженер зі стажем роботи від 10 до 15 років	0,6	1
8	Інженер зі стажем роботи від 5 до 10 років	0,5	2

Отримаємо за формулою (Д4) значення рівня компетентності робочої групи. Виходячи із кількості експертів ($m = 17$), які розбиті за категоріями коефіцієнтів компетентності експертів (табл. Д4.4) значення $M = 0{,}76$, що відповідає умові (Д3).

Перевіримо кількість визначених експертів способом, наведеним в праці [121]. Відповідно до нього кількість експертів рекомендується визначати за формулою:

$$m \le \frac{3}{2 \cdot Q_{\max}} \cdot \sum_{i=1}^{m^*} Q_i \,, \qquad \text{(Д5)}$$

де $Q_{\max}$ — максимально можлива компетентність i-го експерта; m^* — кількість експертів у попередньо сформованій групі; Q_i — компетентність i-го експерта, яка оцінюється в балах (рекомендується від 1 до 5).

Для цього значення коефіцієнтів компетентності, які наведені в табл. Д4.4 нормуємо в межах від 1 до 5 (табл. Д4.5).

Таблиця Д4.5

Нормовані коефіцієнти компетентності експертів

Номер з/п	Кваліфікація експертів	Нормоване значення коефіцієнта компетентності, Q_i	Кількість задіяних експертів
1	Доктор технічних наук	5	2
2	Докторант (здобувач наукового ступеня д-р техн. наук)	4,75	2
3	Кандидат технічних наук	4,5	3
4	Аспірант (здобувач наукового ступеня канд. техн. наук)	4,25	5
5	Інженер зі стажем роботи більше 20 років	4	1
6	Інженер зі стажем роботи від 15 до 20 років	3,5	1
7	Інженер зі стажем роботи від 10 до 15 років	3	1
8	Інженер зі стажем роботи від 5 до 10 років	2,5	2

Розраховуючи за формулою (Д5) отримаємо значення $m \le 20{,}925$, тобто кількість експертів у нашому випадку може знаходитися в інтервалі від 17 до 21, що не суперечить раніше визначеній кількості.

У праці [121] наведено підхід з використанням теорії ймовірності та математичної статистики. Згідно з даним підходом склад експертної групи має бути в межах від 11 до 21 особи, що також не суперечить раніше визначеній кількості експертів.

Необхідно зауважити, що підбір кількісного та якісного складу експертів здійснюється на основі масштабів проблеми, що вивчається, достовірності оцінок, характеристик експертів та витрат ресурсів. Отже, мінімальна кількість експертів визначається кількістю різних аспектів, спрямувань, які необхідно врахувати. У зв'язку із цим, не завжди є правильним судження, що як видно з табл. Д4.3 при обиранні групи експертів з чотирьох осіб допустима ймовірність помилки буде становити 1. В разі призначення коефіцієнта компетентності всім чотирьом експертам, чи ще меншій кількості експертів значення 1 (найбільше значення), можна стверджувати, що допустима ймовірність помилки буде прагнути до 0.

3. Проведення експертизи (заповнення таблиць опитування).

Під час заповнення таблиць опитування необхідно встановити рівень взаємодії між експертами. Відповідно до праці [120], виділяють три рівні взаємодії:

1. Експерти можуть вільно обмінюватися інформацією один з одним.

2. Обмін інформацією між експертами регламентований.

3. Експерти ізольовані один від одного.

Для проведення експертизи оцінювання функціональних профілів загроз державних інформаційних ресурсів з урахуванням категорій експертів, наведених в табл. Д4.4, доцільно ізолювати експертів один від одного. Як уже зазначалося, таблиці заповнюються шляхом віднесення (1) чи невіднесення (0) вказаного параметра до визначеного функціонального профілю загроз ДІР (приклад заповнення для функціонального профілю ЗДІР нормативно-правового спрямування наведено в табл. Д4.6).

Категорія експерта вказується обов'язково. Для подальшого визначення коефіцієнта компетентності.

Таблиця Д4.6

Таблиця опитування експерта (вказується категорія експерта) ФПЗ ДІР НПС

Функціональний профіль загроз	Джерело загроз			Відносно до інформаційного об'єкта		Характер загроз		Загрози за структурою впливу			Рівні впливу загроз				
	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	Системи управління базами даних
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
01_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	0	0	1	1	1	1	1

4. Аналіз експертної інформації.

Є три основні групи методів обробки експертної інформації: статистичні методи, алгебричні методи та методи шкалірування [120]. Аналіз найбільш розповсюджених методів аналізу експертних оцінок наведено в праці [125]. Здійснюючи оцінювання ФП ЗДІР, доцільно використати статистичні методи. В даному випадку достатньо застосувати метод чисельної оцінки, результуючі оцінки, за яким визначаються за формулою методу середньозважених.

Оскільки результатами опитування експертів є декілька думок x_i, $i=\overline{1,m}$, то результуюча оцінка визначається за формулою:

$$\varphi(x_1, x_2, ..., x_m) = \frac{\sum_{i=1}^{m} x_i k_i}{\sum_{i=1}^{m} k_i}, \qquad (Д6)$$

де $\varphi(x_1, x_2, ..., x_m)$ — результуюча оцінка; m — кількість експертів (визначено під час формування складу експертної групи);
x_i — оцінка i-го експерта; k_i — вага i-го експерта (визначено під час формування складу експертної групи).

Ступенем узгодженості думок експертів є дисперсія результуючої оцінки, яка визначається згідно з виразом:

$$\sigma_x^2 = \frac{\sum_{i=1}^{m} \left(\varphi(x_1, x_2, ..., x_m) - x_i\right)^2 k_i}{\sum_{i=1}^{m} k_i}. \qquad (Д7)$$

Визначимо статистичну значимість отриманих результатів. Якщо задатись імовірністю помилки $P_{\text{пом}}$, то інтервал, у який оцінювана величина потрапить з імовірністю $1-P_{\text{пом}}$, становитиме:

$$\overline{\varphi(x_1, x_2, ..., x_m)} - \Delta \le \varphi(x_1, x_2, ..., x_m) \le \overline{\varphi(x_1, x_2, ..., x_m)} + \Delta, \quad (Д8)$$

рахується, що величина $\varphi(x_1, x_2, ..., x_m)$ розподілена нормально з центром $\overline{\varphi(x_1, x_2, ..., x_m)}$ та дисперсією (Д6).

Тоді

$$\Delta = t\sqrt{\frac{\sigma^2}{m}}, \qquad (Д9)$$

де величина t має розподіл Стьюдента з $m-1$ степенями вільності. Її визначають за таблицею, задавши величину $P_{\text{пом}}$.

Розглянемо приклад розрахунку за одним із показників елементу функціонального профілю.

Нехай експерти провели оцінювання ФП ЗДІР НПС за відношенням до антропогенного джерела загрози (табл. Д4.7). Результуюча оцінка, яка розрахована за формулою (Д6) становить $\varphi(x_1, x_2, ..., x_m) = 0,83$, з дисперсією $\sigma_x^2 = 0,14$. Задавши ймовірність помилки $P_{\text{пом}} = 0,01$, за таблицями розподілу Стьюдента визначимо величину t: кількість степенів вільності дорівнює 16; $t = 1,7458837$. За формулою (Д9) $\Delta = 0,16$. Отже, з імовірністю 0,9 величина $\varphi(x_1, x_2, ..., x_m)$ знаходиться в інтервалі [0,67; 0,99], що характеризує ймовірність результату.

Таблиця Д4.7

Приклад узагальнення оцінок, отриманих від експертів

Номер з/п	Категорія експерта (за табл. Д4.4)	Коефіцієнт компетентності (за табл. Д4.4)	Оцінка відношення ФП до антропогенного джерела загроз
1	Доктор технічних наук	1	1
2	Доктор технічних наук	1	1
3	Докторант (здобувач наукового ступеня д-ра техн. наук)	0,95	1
4	Докторант (здобувач наукового ступеня д-ра техн. наук)	0,95	1
5	Кандидат технічних наук	0,9	1
6	Кандидат технічних наук	0,9	1
7	Кандидат технічних наук	0,9	1
8	Аспірант (здобувач наукового ступеня канд. техн. наук)	0,85	1

Номер з/п	Категорія експерта (за табл. Д4.4)	Коефіцієнт компетентності (за табл. Д4.4)	Оцінка відношення ФП до антропогенного джерела загроз
9	Аспірант (здобувач наукового ступеня канд. техн. наук)	0,85	1
10	Аспірант (здобувач наукового ступеня канд. техн. наук)	0,85	0
11	Аспірант (здобувач наукового ступеня канд. техн. наук)	0,85	1
12	Аспірант (здобувач наукового ступеня канд. техн. наук)	0,85	1
13	Інженер зі стажем роботи більше 20 років	0,8	0
14	Інженер зі стажем роботи від 15 до 20 років	0,7	0
15	Інженер зі стажем роботи від 10 до 15 років	0,6	1
16	Інженер зі стажем роботи від 5 до 10 років	0,5	1
17	Інженер зі стажем роботи від 5 до 10 років	0,5	1

5. Прийняття рішення щодо оцінювання ФП ЗДІР з урахуванням експертного оцінювання.

Для прийняття рішення використаємо ступінь узгодженості думок експертів — дисперсію, величина якої не повинна перевищувати 0,3 та мінімальне значення граничної інтервальної оцінки, величина якої повинна відповідати $\overline{\varphi(x_1, x_2, ..., x_m)} - \Delta \geq 0,5$. Отже, повертаючись до розглянутого вище прикладу, можна стверджувати, що оцінку відношення ФП до антропогенного джерела загроз буде визначено 1, оскільки $\sigma_x^2 \leq 0,14$ та $\overline{\varphi(x_1, x_2, ..., x_m)} - \Delta = 0,67$ більше ніж 0,5. Наведемо приклад для оцінювання всього ФП ЗДІР. Розрахунок результуючих оцінок здійснювався в MS Office Excel. У табл. Д4.8 наведено приклад визначення результуючих оцінок за розробленою методикою для ФП ЗДІР 01_1.1_2_3.1 – загрози державній політиці України у сфері інформатизації та її безпеки^{к,ц,д,01,02}.

Таблиця Д4.8

Приклад визначення результуючих оцінок для ФП ЗДІР 01_1.1_2_3.1

Категорія експерта	Коефіцієнт компетентності	Джерело загроз			За відношенням до інформаційного об'єкта		Характер загроз		Загрози за структурою впливу			Рівні впливу загроз				
		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	Системи управління базами даних
Доктор технічних наук	1	1	1	1	1	1	1	0	1	1	1	1	0	0	0	1
Доктор технічних наук	1	1	0	0	0	1	1	0	1	0	0	1	1	1	0	1
Докторант	0,95	1	1	0	1	1	1	1	1	1	1	1	0	0	0	1
Докторант	0,95	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1
Кандидат технічних наук	0,9	1	1	0	1	0	1	1	1	0	0	1	1	0	0	1
Кандидат технічних наук	0,9	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Кандидат технічних наук	0,9	1	0	0	1	0	1	1	1	0	1	0	1	1	1	1

Продовження дод. 4
Продовження табл. Д4.8

Категорія експерта	Коефіцієнт компетентності	Джерело загроз			За відношенням до інформаційного об'єкта		Характер загроз		Загрози за структурою впливу			Рівні впливу загроз				
		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	Системи управління базами даних
Аспірант	0,85	1	0	0	1	0	0	1	1	1	0	0	1	1	0	0
Аспірант	0,85	1	0	0	1	0	0	1	1	1	0	0	1	1	0	0
Аспірант	0,85	0	1	0	0	1	1	0	1	1	0	1	1	1	1	1
Аспірант	0,85	1	1	0	1	1	0	0	1	1	1	1	0	1	1	0
Аспірант	0,85	1	0	1	0	1	0	1	0	1	1	0	1	0	1	0
Інженер більше 20 років	0,8	0	1	0	1	1	1	1	1	1	0	1	0	0	0	1
Інженер від 15 до 20 років	0,7	0	1	0	1	1	1	1	1	1	0	1	0	0	0	1
Інженер від 10 до 15 років	0,6	1	0	0	1	1	1	1	1	0	0	1	1	0	1	1
Інженер від 5 до 10 років	0,5	1	0	0	1	1	1	1	0	0	0	0	1	0	1	0

Закінчення дод. 4

Закінчення табл. Д4.8

Категорія експерта	Коефіцієнт компетентності	Джерело загроз			За відношенням до інформаційного об'єкта		Характер загроз		Загрози за структурою впливу			Рівні впливу загроз				
		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	Системи управління базами даних
Інженер від 5 до 10 років	0,5	1	1	1	1	1	1	0	1	0	0	1	0	0	0	1
Результат		**1**	**0**	**0**	**1**	**1**	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**1**
Результуюча оцінка		0,83	0,60	0,30	0,81	0,75	0,76	0,70	0,84	0,68	0,46	0,72	0,66	0,51	0,46	0,72
Дисперсія		0,14	0,24	0,21	0,16	0,19	0,18	0,21	0,14	0,22	0,25	0,20	0,23	0,25	0,25	0,20
min		0,67	0,39	0,11	0,64	0,57	0,57	0,50	0,68	0,49	0,25	0,53	0,45	0,30	0,25	0,53
max		0,99	0,81	0,50	0,97	0,93	0,94	0,89	0,99	0,88	0,67	0,91	0,86	0,72	0,67	0,91
Відхилення в інтервалі		0,16	0,21	0,19	0,17	0,18	0,18	0,19	0,16	0,20	0,21	0,19	0,20	0,21	0,21	0,19

Навчальне видання

ЮДІН Олександр Константинович,
Бучик Сергій Степанович

ДЕРЖАВНІ ІНФОРМАЦІЙНІ РЕСУРСИ. МЕТОДОЛОГІЯ ПОБУДОВИ КЛАСИФІКАТОРА ЗАГРОЗ

Монографія

Редактор
Технічний редактор *А. І. Лавринович*
Художник дизайну О. О. Зайцева
Коректор *О. О. Крусь*
Комп'ютерна верстка *Л. Т. Колодіної*

Підп. до друку.. Формат 60×84/16. Папір офс.
Офс. друк. Ум. друк. арк. . Обл.-вид. арк. .
Тираж пр. Замовлення № -1.

Видавець і виготівник
Національний авіаційний університет
03680. Київ-58, проспект Космонавта Комарова, 1

Свідоцтво про внесення до Державного реєстру ДК № 977 від 05.07.2002