УДК 346.1:347.775(477)

АРХИПОВ О.Є., *доктор технічних наук, професор,*
Національний технічний університет України “КПІ”
КАСПЕРСЬКИЙ І.П, *кандидат юридичних наук, старший науковий співробітник,*
Національна академія СБ України

МЕТОДИЧНІ АСПЕКТИ ФОРМУВАННЯ ПЕРЕЛІКУ ІНФОРМАЦІЇ, ЩО СТАНОВИТЬ КОМЕРЦІЙНУ ТАЄМНИЦЮ ОКРЕМОГО ПІДПРИЄМСТВА

Анотація. *У статті наведено можливості використання методичного досвіду віднесення даних до державної таємниці при формуванні переліку інформації, що становить комерційну таємницю окремого підприємства.*

Аннотация. *В статье приведены возможности использования методического опыта отнесения данных к государственной тайне при формировании перечня информации, составляющей коммерческую тайну отдельного предприятия.*

Summary. *The article presents the possibilities of use of methodological experience of allocating data to state secrets when forming the list of information constituting a commercial secret of a separate enterprise.*

Ключові слова*: інформація з обмеженим доступом, таємна інформація, конфіденційна інформація, комерційна таємниця, перелік інформації, що становить комерційну таємницю, звід відомостей, що становлять державну таємницю.*

Сучасне суспільство вже досить звично сприймає факт існування проблем, пов’язаних із сферою інформаційної безпеки, зокрема нагальну необхідність захисту інформації як ціннісного ресурсу в житті особи, суспільства і держави. На жаль, попри усвідомлення означених проблем, рівень розробки їх правового, організаційного та технічного забезпечення за окремими напрямами залишається недостатнім.

Оцінюючи рівень організаційно-правового забезпечення захисту інформації з обмеженим доступом, легко дійти висновку про нерівномірну увагу законодавця та інших уповноважених органів до забезпечення захисту різних її видів. У цьому контексті варто порівняти два види інформації з обмеженим доступом – комерційну та державну таємниці. Нагадаємо їх законодавчі визначення:

Державна таємниця (далі також – секретна інформація) – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою [1, ст. 30].	Комерційною таємницею є інформація, яка є секретною в тому розумінні, що вона в цілому чи в певній формі та сукупності її складових є невідомою та не є легкодоступною для осіб, які звичайно мають справу з видом інформації, до якого вона належить, у зв’язку з цим має комерційну цінність та була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію [2, ст. 505].

Зміст наведених визначень дає змогу зрозуміти, що стосовно державної таємниці держава встановлює порядок віднесення інформації до цього виду даних, а щодо комерційної таємниці питання віднесення до неї певної інформації віддано законодавцем на розсуд її власника.

Така диспозитивність регулювання віднесення інформації до комерційної таємниці викликає низку запитань та неузгодженостей.

По-перше, виходячи із загального визначення таємної інформації, даної Законом України “Про інформацію”, складно погодитись із належністю комерційної таємниці до класу таємних даних, бо таємна інформація “містить відомості, які становлять державну та іншу передбачену законом таємницю, розголошення якої завдає шкоди особі, суспільству і державі”, причому “порядок обігу таємної інформації та її захисту визначається відповідними державними органами” [3, ст. 30]. А у випадку коли сам власник на власний розсуд вирішує питання обмеження доступу до інформації, то відповідно до того ж Закону України “Про інформацію”, ці дані є не таємними, а конфіденційними, бо її власники не зобов’язані, а мають лише право “самостійно визначати режим доступу до неї, включаючи належність її до категорії конфіденційної, та встановлювати для неї систему (способи) захисту” [2, ст. 505]. На належності комерційної таємниці до класу конфіденційної інформації наполягають і інші дослідники [4, 5].

По-друге відсутність єдиних загальнодержавних стандартів формалізації рішення щодо віднесення інформації до комерційної таємниці ускладнює процес захисту прав власника комерційної таємниці, бо залишається незрозумілим, який саме обсяг заходів її захисту дозволить вважати, що конкретна комерційна таємниця за її визначенням “була предметом адекватних існуючим обставинам заходів щодо збереження її секретності, вжитих особою, яка законно контролює цю інформацію”. Знайти межу достатності цієї “адекватності” можливо лише встановленням належного правового порядку захисту комерційної таємниці.

В цілому погоджуючись із позицією Г.О. Сляднєвої стосовно того, що право суб’єкта господарювання на комерційну таємницю не може бути обмежене шляхом законодавчого встановлення переліку і змісту відомостей, що становлять комерційну таємницю [5], наполягаємо на необхідності встановлення законодавцем єдиного порядку формалізації рішення власника стосовно встановлення режиму охорони комерційної таємниці щодо належних йому даних. Достатнім рівнем цієї формалізації варто визнати можливість прийняття постанови Кабінету Міністрів України, якою встановити хоча б перелік мінімальних вимог стосовно закріплення наявності та режиму охорони комерційної таємниці окремим підприємством у своїх внутрішніх документах (статут, установчий договір, штатний розпис, трудові угоди, угоди про конфіденційність тощо, типові форми яких можливо передбачити додатками до постанови). А до встановлення такого порядку пропонуємо власне бачення методичних аспектів віднесення інформації до комерційної таємниці, основи яких, можливо, в майбутньому закріпити владним розпорядженням держави.

Виходячи з того, що зміст, послідовність етапів та сукупність заходів, які необхідні для забезпечення захисту комерційної таємниці, практично не відрізняються від загального алгоритму дій з побудови системи захисту будь-якої інформації з обмеженим доступом [6, 7], ми виносимо власні пропозиції щодо використання окремих аспектів досвіду організаційного та методичного забезпечення віднесення інформації до державної таємниці у створенні системи захисту комерційної таємниці на рівні окремого підприємства.

Втілення такої формальної схеми вимагає в першу чергу її адаптації до властивостей та умов функціонування комерційної таємниці як об’єкта захисту. Тут підлягає врахуванню суттєва різниця між комерційною та державною таємницею. Мета захисту державної таємниці настільки суттєва, що в ході віднесення інформації до державної таємниці при обрахунку рівня зниження ефективності функціонування об’єкта захисту

внаслідок розголошення інформації втрати на організацію та здійснення режимно-секретної діяльності взагалі не враховуються [8, п. 3.1], хоча і підлягають зазначенню у висновку про віднесення [1]. У випадку ж з комерційною таємницею необхідно враховувати баланс між вартістю заходів захисту комерційної таємниці і обсягом можливих втрат на захист цієї інформації, бо діяльність суб’єкта господарювання, в тому числі і щодо захисту власних інформаційних ресурсів, повинна бути економічно доцільною. Крім того, як справедливо стверджує С.О. Князєв, надмірне “утаємничування“ може викликати втрату клієнтів, а отже, прибутку, оскільки умови ринку потребують постійних клієнтів, широкої інформації про діяльність фірми [9].

Виходячи з таких орієнтирів власник інформації і повинен приймати рішення щодо можливості використання правового інституту комерційної таємниці на власному підприємстві взагалі та зокрема і щодо виду і обсягів тих даних, доступ до яких необхідно і економічно доцільно обмежувати.

Вихідним кроком на цьому шляху стають виявлення та регламентація складу відомостей, що становлять комерційну таємницю, її фіксація у спеціальному Переліку. Дослідники називають цей документ по-різному: Перелік відомостей, що становлять чи містять комерційну таємницю [9 – 13], або Перелік конфіденційних відомостей [14]. Окремі методичні рекомендації щодо вимог законодавства України до визначення інформації, яка містить комерційну таємницю, наведено в роботах Г.О. Андрощука, П.П. Крайнєва та Є.О. Степанова [12, 14]. В статті В.Ф. Шпака [15] розглянуто використання технології експертного опитування у формуванні Переліку. Основну увагу приділено технологічним питанням організації та проведення експертизи, методиці обробки отриманих експертних оцінок, класифікації загального масиву комерційної таємниці за рівнями її важливості.

На жаль, ні нормативні документи, ні наведені праці науковців цілісно не охоплюють методичні аспекти формування Переліку інформації, що становить комерційну таємницю окремого підприємства (далі – Перелік)

Зважаючи на суттєво індивідуалізований підхід у визначенні конкретних відомостей, що містять комерційну таємницю, значний інтерес становлять можливі узагальнення та типові прийоми, використання яких є корисним при укладанні Переліку. Тут знову-таки слід звернутися до правових аспектів [3], що обмежують коло відомостей, які не можна відносити до інформації з обмеженим доступом взагалі або тільки до комерційної таємниці зокрема [16].

В цій ситуації як аналог Переліку можливо використати Звід відомостей, що становлять державну таємницю (ЗВДТ), щодо якого накопичено значний досвід формування та використання. У цьому контексті врахуванню підлягає те, що ЗВДТ являє собою загальнодержавний акт, створення якого забезпечується через інститут державних експертів з питань таємниць та регламентується низкою нормативно-правових документів [17 – 19], в яких чітко визначено сфери існування відомостей, що становлять державну таємницю, єдиний порядок віднесення інформації до державної таємниці та її структурування за рівнем важливості.

Отже ЗВДТ поділено на чотири тематичні сфери, в яких функціонує державна таємниця: оборони; економіки, науки і техніки; зовнішніх відносин; державної безпеки та охорони правопорядку. У випадку з комерційною таємницею ми підтримуємо позицію Т.Ю. Ткачука, який на прикладі діяльності торговельного підприємства допускає внутрішню класифікацію переліку конфіденційної інформації за напрямами діяльності підприємства: (кадрова, фінансова політика, обсяги товарного запасу тощо) [20]. Тобто те-

матична класифікація Переліку цілком доцільна з огляду на специфіку діяльності як підприємства взагалі, так і його окремих підрозділів (філій) зокрема.

Із загальної структури ЗВДТ у Перелік можливо перенести найсуттєвіші складові, доповнивши їх складовими, які випливають із рівня регулювання (окреме підприємство), і зобразивши Перелік у вигляді таблиці, в якій фіксуються наступні параметри:

Зміст інформації, що становить комерційну таємницю	Перелік документів (інших носіїв), у яких дозволено фіксувати ці дані	Термін захисту даних	Перелік посадових осіб підприємства, яким можливо надавати доступ до цих даних	Перелік посадових осіб, які мають право надавати доступ до цих даних	з/п
1	2	3	4	5	

Додатковим аспектом, який можливо враховувати в даній таблиці, може бути гриф обмеження доступу до конкретного виду інформації – у випадку запровадження багатоступеневої внутрішньої класифікації інформації, що становить комерційну таємницю за важливістю, тобто обсягом можливої шкоди внаслідок розголошення цих даних, як це пропонує зробити Т.Ю. Ткачук, розділивши дані на два види: “особливо секретно” – відомості, оволодіння якими негативно відіб’ється на усій діяльності підприємства, та “секретно” – відомості, оволодіння якими може спричинити шкоду за окремим напрямом діяльності торговельного підприємства [20]

Третя колонка повинна корелювати із Інструкцією щодо діловодства чи іншими нормативними документами підприємства, якими встановлено порядок ведення документації.

Основним організаційним аспектом є забезпечення Переліком принципу розділення відомостей, що містять комерційну таємницю, на інформаційні фрагменти такого обсягу, який виключає можливість відновлення кожним із допущених вихідної інформації, на чому наголошує Є.О. Степанов [14]. За своєю суттю ця рекомендація – практичне втілення фундаментального організаційного принципу захисту інформації – розподілу обов’язків (separation of duties), сенс якого у цілеспрямованому подрібненні вихідної інформації з обмеженим доступом на окремі частини з наступним розподілом їх між виконавцями так, щоб жоден з них не міг мати достатньо повного уявлення про задачу чи проблему, що її містить повний вихідний масив інформації з обмеженим доступом.

Однак, якщо назване розділення інформації з обмеженим доступом є ефективним захисним заходом, його беззастережне застосування при складанні Переліку може привести до негативних наслідків. Комплекс інформації, утворений простим накопиченням первинної інформації, зважаючи на можливість її аналітичної обробки, має ймовірність отримати статус таємної, а якщо первинні інформаційні елементи вже мали його, то рівень важливості інформаційного комплексу може підвищитися. Подібна залежність цінності інформації від її обсягу відзначається кількома авторами [21, 22] і детально проаналізована нами [23] стосовно інформації, що містить державну таємницю.

За прикладом знову звертаємося до інституту державної таємниці. Так, первинною інформацією для віднесення можуть стати відомості про хімічні реагенти, що ввозяться на територію підприємства, про яке відомо, що воно належить до оборонного комплексу. Разом з певною додатковою інформацією (яким чином транспортують готову продукцію з підприємства, деталі та елементи зовнішнього вигляду транспортної тари, вид і тип транспортних засобів, інше), залежно від змісту та повноти всієї сукупної інформа-

ції наслідком її аналітичного осмислення може бути кілька варіантів висновку, різних за ступенем наближення до реального стану речей:

а) підприємство виробляє компоненти, які, можливо, застосовуються у спорядженні паливних систем військової техніки;

б) підприємство є виробником ракетного палива;

в) підприємство є виробником ракетного палива для ракет класу АА;

г) підприємство є виробником ракетного палива для ракет класу АА з приблизним обсягом виробництва YY тон на місяць.

Відповідно до важливості інформації, яка міститься в тому чи іншому варіанті отриманого аналітичного висновку, комплексу первинної секретної інформації слід надати певний ступінь секретності, який в деяких випадках (можливо, варіанти “в”, “г”) буде вищий за ступінь секретності елементів первинної інформації, тобто матиме місце якісне перетворення сукупного масиву інформації, що суттєво виходить за межі просто генетичного наслідування. Підтвердження можливості стрибкоподібного якісного перетворення накопиченої інформації, яке змушує підвищити ступінь її секретності, знаходимо в ЗВДТ [18]. Наприклад:

Номер статті ЗВДТ	Зміст відомостей, що становлять державну таємницю	Ступінь секретності
1.9.2.	Відомості за окремими показниками про відкриття, винаходи, науково-технічні рішення, які можуть бути використані для потреб оборони держави і мають принципове значення для розробки нових видів озброєння чи військової техніки	
	- у цілому по Україні	ОВ
	- щодо окремого відкриття, винаходу чи науково-технічного рішення: при засекречуванні ступінь секретності встановлюється і знімається за рішенням державного експерта з питань таємниць	ЦТ, Т

Як бачимо з цього витягу, сукупна інформація „у цілому по Україні” беззастережно отримує гриф “ЦТ”, тоді як її фрагменти можуть мати будь-який довільний статус, хоч би й несекретний, залежно від того, що вирішить у кожному конкретному випадку державний експерт з питань таємниць. Таким чином, саме зібрання і спільне представлення сукупної інформації обумовлює різке зростання її сукупної важливості.

Подібні ефекти достатньо просто інтерпретуються з позицій теорії систем та системного аналізу [24 – 26]: аналітична сумісна обробка всього комплексу інформації систематизує та впорядковує накопичені в ньому відомості і факти, дозволяє виявити і формалізувати сукупність зв’язків та співвідношень між базовими інформаційними елементами цього комплексу, тобто трансформувати вихідну неструктуровану сукупність відомостей у певним чином впорядковану систему взаємопов’язаних компонентів з більшменш складною структурою. Як відомо, система характеризується рядом властивостей, серед яких однією з головних є емерджентність – наявність у системи рис (властивостей), які не можуть бути безпосередньо виведені (отримані) через відомі характеристики окремих елементів, що складають систему [24 – 26]. Емерджентність – наслідок властивого складним системам синергізму [24], специфічного ефекту взаємопідсилюючих сукупних дій елементів системи, результат яких значно вищий за простий сумарний ефект від дії цих же елементів при їх взаємонезалежному функціонуванні. В нашому випадку наслідок ефекту емерджентності зведених у комплекс відомостей – це істотне зростання сукупної важливості секретної інформації всього комплексу (з огляду на існуючу мож-

ливість сукупної аналітичної обробки відомостей, що утворюють інформаційний комплекс) порівняно із простим сумарним накопиченням важливості окремих секретних складових комплексу при їх взаємонезалежному оцінюванні.

Слід наголосити, що рівень ефективності упорядкування та систематизації початкової розрізненої інформації, яка становить вихідний інформаційний комплекс, критично пов’язаний з рівнем знань та індивідуальних вмінь аналітика. Останнє означає, що за кожним випадком аналізу залежно від підготовки та здібностей аналітика матимемо певну множину можливих варіантів аналітичних рішень. Ця багатоваріантність ускладнює задачу визначення сукупної важливості відомостей, що складають інформаційний комплекс.

Однак при класифікації інформації з точки зору її можливої належності до комерційної таємниці, очевидно, слід виходити з розгляду варіанта, що веде до найбільш тяжких наслідків, обумовлених втратою інформації. Зазвичай, виникнення цього варіанта можливе за умов, коли аналітик, що працює з первинною інформацією, має найвищий рівень підготовки і використовує новітні технології та механізми обробки і аналізу даних, які дозволяють йому максимально якісно трансформувати первинні дані в сукупність систематизованої та впорядкованої вторинної інформації.

Ще одне слушне зауваження щодо рівня деталізації інформації при формуванні Переліку можна винайти з документів сфери технічного захисту інформації. У вимогах щодо захисту конфіденційної інформації від несанкціонованого доступу під час обробки в автоматизованих системах класу 2 [27] зазначається, що інформація в локальних обчислювальних мережах за рівнем інтеграції поділяється на сукупність сильно пов’язаних об’єктів, які потребують забезпечення своєї цілісності як сукупність, та на окремі слабко пов’язані об’єкти, для яких характерний широкий спектр засобів свого подання, зберігання, передавання і які тяжіють до забезпечення власної цілісності кожен окремо.

Таким чином, при укладанні Переліку разом з принципом максимальної деталізації вихідної інформації на базові інформаційні елементи слід передбачити можливість включення до його складу інформаційних комплексів (блоків) більшого обсягу, в які поєднуються природно пов’язані один з одним базові інформаційні елементи.

При цьому досить раціональним втіленням принципу розподілу обов’язків було б зазначення у запропонованій нами таблиці переліку розділених сегментів інформації, доступних окремій посадовій особі, навіть у тому випадку, коли ці окремі сегменти самі по собі не мають достатньої для віднесення до комерційної таємниці ваги, об’єднуючи їх у достатній для віднесення сукупності під одним пунктом, право надання допуску до яких належить одній-двом посадовим особам. Таким чином ця таблиця трансформується з простого переліку інформації, що становить комерційну таємницю підприємства, до схеми розмежування доступу до комерційної таємниці.

Певні труднощі при формуванні Переліку можуть виникати через необхідність врахування зв’язків між об’єктом, який безпосередньо пов’язаний з виникненням комерційної таємниці, та його зовнішнім оточенням. Так, одним з найважливіших чинників виробництва є матеріально-технічне забезпечення виробничого процесу. Розголошення відомостей в цій сфері може створити “вузькі місця” у постачанні сировини та комплектуючих, стимулювати зростання цін від постачальників, зриви постачання та розірвання контрактів, погіршення рівня взаємин з постачальниками й т.п., не кажучи вже про пряму загрозу компрометації комерційної таємниці, як це було наведено вище у прикладі з аналітичним осмисленням інформації про підприємство-виробника ракетного палива.

Очевидно, вийти із цієї ситуації можна було б шляхом укладання двосторонніх угод, які зобов’язували б сторони виконувати вимоги з нерозголошення комерційної таємниці. Однак такі угоди ефективні, коли в них зацікавлені в рівній мірі обидві сторони. В реаль-

них випадках для постачальника вимоги щодо виконання заходів із збереження комерційної таємниці можуть бути обтяжливими: вибіркове закриття маркетингової інформації (замовник, режим постачання, дані про обсяги та номенклатуру), додаткові вимоги до підбору персоналу, додаткові обов’язки для певних посадових осіб, нарешті, як наслідок, додаткові витрати. Для державної таємниці ці питання мали б беззастережно позитивне вирішення, обумовлене вимогами режиму секретності – встановленого законом єдиного порядку забезпечення охорони державної таємниці, однак у випадку із комерційною таємницею можливе виникнення конфліктних ситуацій, які потребують компромісних рішень, не виключаючи дій, що послаблюють захист комерційної таємниці.

Як бачимо, базовий досвід захисту державних інформаційних ресурсів з обмеженим досвідом дозволяє після його адаптації забезпечити організаційні і методичні аспекти захисту прав суб’єктів господарювання на їх комерційну таємницю. Завданнями науковців на цьому шляху є розробка універсальних механізмів прийняття і формалізації рішень щодо віднесення інформації до комерційної таємниці та заходів її захисту, які можливо закріпити на загальнодержавному рівні та ефективно застосовувати у всіх сферах господарської діяльності.

Використана література

1. Про державну таємницю : Закон України від 21.01.94 р. // Відомості Верховної Ради. –1999. – № 49.

2. Цивільний кодекс України // Офіційний вісник України. – 2003. – № 11. – Ст. 461.

3. Про інформацію : Закон України від 02.10.92 р. // Відомості Верховної Ради України. – 1992. – № 48.

4. Прокоф’єва Д.М. Дослідження змісту категорій інформації з обмеженим доступом відповідно до чинного законодавства України як підґрунтя розробки проекту Закону України “Про інформацію з обмеженим доступом, що не становить державної таємниці” : матеріали “круглого столу” [“Обговорення проекту закону України “Про інформацію з обмеженим доступом, що не становить державної таємниці”], Третя науково-технічна конференція “Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні”, 09.10.01 р. – К., 2001. – С. 28.

5. Сляднєва Г.О. Право суб’єкта господарювання на комерційну таємницю та його захист : автореф. дис. на здобуття канд. юрид. наук : 12.00.04. – Донецьк, 2005. – С. 7.

6. Галатенко В.А. Стандарты информационной безопасности / В.А. Галатенко. – М.: ИНТУИТ.РУ, 2004. –238 с.

7. Международный стандарт безопасности информационных систем : ISO 17799, 2002.

8. Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня її секретності : наказ Держкомсекретів України від 09.11.98 р. № 22.

9. Князєв С.О. Комерційна таємниця в Україні: особливості організаційно-правового впровадження // Юридичний журнал. – 2006. – № 6.

10. С.А. Нікіфоров. Підприємництво та правовий захист комерційної таємниці / С.А. Нікіфоров, С.С. Нікіфоров. – К. : Олан, 2001. – 208 с.

11. Чернявський А.А. Безпека підприємницької діяльності / А.А. Чернявський. – К. : МАУП, 1998.– 124 с.

12. Андрощук Г.А. Экономическая безопасность предприятия: защита коммерческой тайны / Г.А. Андрощук, П.П. Крайнев. – К. : Изд. дом “Ін Юре”, 2000. – 400 с.

13. Ткачук Т. Удосконалення системи захисту комерційної таємниці // Бизнес и безопасность. – 2007. – № 6. – С. 34-37.

14. Степанов Е.А. Управление персоналом / Е.А. Степанов. – М.: Инфра-М, 2002. – 228 с.

15. Шпак В.Ф. Коммерческая тайна и экономическая безопасность бизнеса // Защита информации – Конфидент. – 2003. – № 2 (50). – С.20-26.

16. Перелік відомостей, що не становлять комерційної таємниці : Постанова Кабінету Міністрів України від 09.08.93 р. № 611.

17. Про державну таємницю : Закон України від 21.01.94 р. // Відомості Верховної Ради. –1999. – № 49.

18. Звід відомостей, що становлять державну таємницю : Наказ Служби безпеки України від 12.08.05 р. № 440. – (Зареєстровано в Міністерстві юстиції України 17.08.05 р. за № 902/11182) // Офіційний вісник України. – 2005. – № 5. – Ст. 107.

19. Методичні рекомендації державним експертам з питань таємниць щодо визначення підстав для віднесення відомостей до державної таємниці та ступеня її секретності : Наказ Держкомсекретів України від 09.11.98 р. № 22.

20. Ткачук Т. Удосконалення системи захисту комерційної таємниці // Бизнес и безопасность. – 2007. – № 6. – С. 34-37.

21. Мельников В.В. Защита информации в компьютерных системах / В.В. Мельников. – М. : Финансы и статистика (Электронинформ), 1997. – 368 с.

22. Кононович В., Тардаскін М., Тардаскіна Т. Моделі цінності інформації з позицій інформаційної безпеки інформаційно-телекомунікаційних систем // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, 2004. – [Вип. 9]. – С. 30-38.

23. Архипов О.Е., Ворожко В.П. Системні аспекти оцінювання рівня важливості секретної інформації // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні, 2007. – [Вип. 15].

24. Катренко А.В. Системний аналіз об’єктів та процесів комп’ютеризації / А.В. Катренко. – Львів : “Новий світ-2000”. – 424 с.

25. Коломоец Ф.Г. Основы системного анализа и теории принятия решений / Ф.Г. Коломоец. – Минск : Тесей, 2006. – 320 с.

26. Сурмин Ю.П. Теория систем и системный анализ / Ю.П. Сурмин. – К. : МАУП, 2003. – 368 с.

27. Вимоги щодо захисту конфіденційної інформації від несанкціонованого доступу під час обробки в автоматизованих системах класу 2 : НД ТЗІ 2.5 – 008-2002.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~