УДК 681.06

Ю.І. Хлапонін

НЕОДНОЗНАЧНІСТЬ ТРАКТУВАННЯ ТА ПРОТИРІЧЧЯ ДЕЯКИХ ВИЗНАЧЕНЬ В НОРМАТИВНИХ ДОКУМЕНТАХ СИСТЕМИ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

Розглядаються питання відмінності тлумачень визначень „автоматизована система", „інформаційна система", „інформаційно-телекомунікаційна система" різними документами із діючої нормативної бази з технічного захисту інформації. Обґрунтовано роль, яку відіграє політика безпеки в установі, організації, на підприємстві, щодо інформаційної безпеки. Розглянуто питання визначення моделі загроз для інформації. Обґрунтовано, що категоріювання повинні підлягати об'єкти обчислювальної техніки разом з приміщеннями, в яких вони розміщені.

Ключові слова: інформаційно-телекомунікаційна система, інформаційна система, автоматизована система, технічний захист інформації, нормативна база, політика безпеки, інформаційна безпека, модель загроз, категоріювання, обчислювальна система.

Технічний захист інформації займає особливо важливе місце в загальному комплексі заходів щодо забезпечення національної безпеки України в інформаційній сфері та безпосередньо призначений для забезпечення організаційними, інженерними та технічними заходами, методами і засобами конфіденційності, цілісності та доступності інформації, яка обробляється в інформаційно-телекомунікаційних системах (ІТС), циркулює на об'єктах інформаційної діяльності та становить державну та іншу встановлену законом таємницю, віднесена до службової інформації або є відкритою, вимога щодо захисту якої встановлена законом.

Система технічного захисту інформації як кожна організаційно-технічна система складається з трьох основних компонентів: **нормативно-правової бази, організаційної інфраструктури та матеріально-технічної бази.**

Безперечним є те, що головною складовою системи, яка впливає надвііншієнормативно-правова база, оскількисамевонавизначаєїїправові та організаційні засади, норми та вимоги з технічного захисту інформації. В цілому, створена в Україні нормативно-правова база забезпечує функціонування системи технічного захисту інформації.

Але справа в тім, що в Україні є дійсними (діючими) як державні стандарти та нормативні документи ще радянського періоду так і нормативно-правові акти, видані вже Адміністрацією Держспецзв'язку України (або ще їх попередниками). Різноманітність цих документів, неузгодженість між собою окремих положень, що в них містяться, не дозволяє у повному обсязі реалізувати єдину політику в проектуванні та експлуатації систем технічного захисту інформації, ускладнює роботу виконавців та експертів, а отже створює передумови для можливих невиправданих інтелектуальних й економічних витрат.

Вимоги зазначених документів в деяких питаннях можуть суперечити один одному. Прикладом різного тлумачення нормативної бази може бути наступне.

Так, в енциклопедії [1] автоматизо́вана систе́ма (*АС*) (англ. *automated system*) — сукупність керованого об'єкта й автоматичних керуючих пристроїв, у якій частину функцій керування виконує людина. Звісно, що енциклопедія не є нормативним документом системи ТЗІ, але дане визначення є логічним і найбільш чітко визначає суть.

В [2] **автоматизована система** — організаційно-технічна система, що складається із засобів автоматизації певного виду чи кількох видів діяльності людей та персоналу, що здійснює цю діяльність.Дійсно, складається чітке уявлення , що АС – це на кшталт пристроїв з числовим програмним управлінням, де більшість процесу виробництва певного виду продукції здійснюється автоматично, а сировина подається для завантаження системи (вхід) та готова продукція відвантажується (вихід) за участі людини.

В [3] дається визначення автоматизованої системи (АС – automated system) як організаційно-технічної системи, що реалізує інформаційну технологію і об'єднує

обчислювальну систему, фізичне середовище, персонал і інформацію, яка обробляється. Дане визначення не відповідає [4], який встановлює терміни та визначення в галузі АС.

Законом України [5] вводиться поняття інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів.

Виходячи з цих визначень, виникає питання чи входить до складу інформаційної системи обчислювальна система (ОС), фізичне середовище, персонал і інформація, яка обробляється як вказано в [3].

В [6] подано терміни та визначення інформаційної, телекомунікаційної та інтегрованої систем як видів автоматизованих систем.

Поняття інформаційної системи викладене якорганізаційно-технічна система, що реалізує технологію обробки інформації за допомогою засобів обчислювальної техніки та програмного забезпечення, тобто поняття обчислювальної системи [3] або обчислювальної техніки [6] в складі ІС знову має місце.

Вказано також, що під інформаційно-телекомунікаційною системою (ІТС) розуміється будь-яка система, яка відповідає одному з трьох наведених вище видів автоматизованих систем. Але, наприклад, як може інформаційна (автоматизована) система класу 1 (одномашинний однокористувачевий комплек) бути інформаційно-телекомунікаційною (ІТС) не виконуючи при цьому функції „обміну інформацією шляхом передавання, випромінювання або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб”[6]? Визначення ж класів АС в [7] стає не актуальним (некоректним), з введенням Закону [5].

Діючим є також [9], в якому використовується поняття комп’ютерної системи (КС), яка в найбільш загальному випадку являє собою АС або її частину.

В ДСТУ [10] є визначення — **інформаційна система** (англ. *Information system*) — сукупність організаційних і технічних засобів для збереження та обробки інформації з метою забезпечення інформаційних потреб користувачів, та інформаційна система — комунікаційна система, що забезпечує збирання, пошук, оброблення та пересилання інформації. Останнє визначення дає розуміння, що інформаційна система не є такою, що автоматизує частину людської праці і результатом її роботи є щось матеріальне (виріб, продукція).

В [11] автори надають наступне визначення:

Інфокомунікації — сукупність засобів телекомунікації (електрозв’язку) та інформатики, що забезпечує доставляння сигналів електрозв’язку від джерел до споживачів, уможливлюючи ідентифікацію інформаційного змісту цих сигналів і використання оптимальних методів їх обробки, зокрема передавання маршрутизації, перетворення, програмування.

Інфокомунікаційна мережа — результат інтеграції засобів зв’язку й ЕОМ.

На мій погляд, дане визначення нарешті розмежовує поняття АС та ІТС і інфокомунікаційна система (мережа) призначена саме для обробки та передачі інформації.

Має місце також визначення системи автоматичного управління (САУ) як сукупності обєкту управління (ОУ) та автоматичного управляючого пристрою (АУП), відповідним чином взаємодіючих між собою [12].

Виходячи з даного визначення та враховуючи визначення АС в [1] можна зробити висновок, що **автоматизо́вана систе́ма** - цесистема автоматичного управління, у якій частину функцій керування виконує людина.

Таким чином, зрозуміло, що починаючи вже з ключових термінів (АС, ІС, ІТС) немає однозначних визначень цих понять, діюча нормативна база з ТЗІ потребує доопрацювання та впровадження єдиної термінології. Деякі автори навіть вважають, що захисту інформації в ІТС властива специфічна термінологія, професійна та жаргонна [13]. Насправді ж, термінологія має відображати концептуальні підходи до вирішення проблеми, а роблячи

посилання на те чи інше визначення (термін) доцільно вказувати згідно яких нормативно-правових документів вживаються визначення в тому чи іншому випадку.

Наступне питання. В [3] надається визначення політики безпеки інформації (information security policy) як сукупності законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації. В [6] визначено, що політика безпеки розробляється згідно з положеннями [8] та рекомендаціями [13]. Політику безпеки рекомендується оформляти у вигляді окремого документа Плану захисту. В той же час згідно [8] політика безпеки інформації в АС має бути окремим розділом Плану захисту інформації в АС та враховувати вимоги п. 5.6 Додатку [8], який, в свою чергу, посилається на [4]. В результаті, взаємні посилання з одного документа на інший ускладнюють роботу виконавців робіт з ТЗІ.

Що ж стосується світового досвіду то, на міжнародному рівні політика безпеки розглядається набагато ширше. Як приклад, міжнародні стандарти в області інформаційної безпеки, частково в *ISO/IEC 17799:2000*. Керування інформаційною безпекою – Інформаційні технології [14], який був прийнятий в 2000 р. та з часом переглядався і доповнювався (*ISO/IEC 27001:2005* [15]. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги). Згідно міжнародних стандартів відпрацьовується політика безпеки підприємства, яка включає в тому числі і інформаційну безпеку. Також надається перелік документів, які повинні бути відпрацьовані разом з політикою безпеки (положення, інструкції, рекомендації та ін.).

В цілому, ***політика безпеки*** – сукупність програмних, апаратних, організаційних, адміністративних, юридичних, фізичних заходів, методів, засобів, правил і інструкцій, чітко регламентуючих всі аспекти діяльності компанії, включаючи інформаційну систему і, забезпечуючи їхню безпеку. Політика безпеки є одним з найважливіших документів компанії.

Переваги для установ, організацій, підприємств, які будують системи управління інформаційною безпекою відповідно до міжнародних стандартів та в подальшому отримують сертифікати на відповідність ISO/IEC 27001: 2005 наступні:

– підвищення керованості та надійності;
– підвищення захищеності ключових напрямків діяльності;
– спрощення процедури виходу на міжнародний рівень;
– міжнародне визнання та підвищення авторитету;
– систематизація процесів управління безпекою інформації та ін.

Загалом, міжнародні стандарти в області інформаційної безпеки в Україні не є обов'язковими для виконання та носять лише рекомендаційний характер, хоча, наприклад, Національним банком України міжнародний стандарт [15] прийнятий в 2010 році в якості галузевого *ГСТУ СУІБ 1.0/ISO/IEC 27001:2010*.

Як бачимо із зазначеного, політика безпеки є одним із першочергових документів, які розробляються в установі, організації, на підприємстві, щодо інформаційної безпеки, а наприклад, план захисту інформації відпрацьовується на її основі. Це суттєво відрізняється від положень нормативних документів системи технічного захисту інформації в Україні, в яких політиці безпеки надається не достатня увага, хоча згідно п 5.1 Додатку [13] політика безпеки інформації в АС є частиною загальної політики безпеки організації і повинна успадковувати основні її принципи. На практиці, в Україні розробка політики безпеки організації зводиться до відпрацювання вимог до політики безпеки інформації в АС, складовими частинами якої мають існувати політики забезпечення конфіденційності, цілісності і доступності оброблюваної інформації [8].

В той же час в [17] п. 19 визначається, що План захисту інформації в системі містить:

– завдання захисту, класифікацію інформації, яка обробляється в системі, опис технології обробки інформації;

– визначення моделі загроз для інформації в системі;

– основні вимоги щодо захисту інформації та правила доступу до неї в системі;

– перелік документів, згідно з якими здійснюється захист інформації в системі;

– перелік і строки виконання робіт службою захисту інформації.

Як бачимо, мова про *політику безпеки* тут вже не ведеться.

Далі виникає питання стосовно визначення моделі загроз для інформації. Як відомо, відповідно до [17] розробляється модель загроз для інформації з обмеженим доступом (загрози від витоку ІзОД технічними каналами).

В [8] виділяють два основних напрями ТЗІ в АС – це захист АС і оброблюваної інформації від несанкціонованого доступу та захист інформації від витоку технічними каналами (оптичними, акустичними, захист від витоку каналами побічних електромагнітних випромінювань і наведень). Виникає питання, якщо в АС обробляється відкрита інформація, то згідно [16] вимоги до захисту інформації від витоку технічними каналами не є обов'язковими, і висуваються у відповідності до рішення власника (розпорядника) інформації. Вимоги щодо захисту інформації від несанкціонованих дій, у тому числі від комп'ютерних вірусів, висуваються для всіх систем, відповідно, модель загроз для інформації відпрацьовується згідно вимог [8]. Загрози оброблюваної в АС інформації залежать від характеристик ОС, фізичного середовища, персоналу і оброблюваної інформації. Загрози можуть мати або об'єктивну природу, наприклад, зміна умов фізичного середовища (пожежі, повені і т. ін.) чи відмова елементів ОС, або суб'єктивну, наприклад, помилки персоналу чи дії зловмисника. Із всієї множини способів класифікації загроз найпридатнішою для аналізу є класифікація загроз за результатом їх впливу на інформацію, тобто порушення конфіденційності, цілісності і доступності інформації [8].

Проектування систем захисту інформації починається з відпрацювання технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

В технічному завданні на КСЗІ, висуваючи вимоги до захисту АС і оброблюваної інформації від несанкціонованого доступу необхідно встановити функціональний профіль захищеності цієї інформації згідно [7, 17] (на основі моделі загроз для інформації).

Наступне питання, в якому криється неоднозначність, що, власне, категоруємо?

Відповідно до п. 6.5 [18] для забезпечення захисту інформації від витоку технічними каналами провести аналіз технології оброблення інформації в АС, архітектури та розташування елементів АС; за його результатами визначити зони безпеки інформації та провести у відповідності з вимогами НД ТЗІ категоріювання приміщень АС і засобів обчислювальної техніки.

У відповідності до вимог чинних нормативних документів системи ТЗІ провести заходи щодо блокування витоку інформації та впливу на неї технічними каналами.

Але ж, ЕОМ характеризуються рівнями ПЕМВН, за вимірюваннями яких визначають зону можливого перехоплення інформації (зону R2), і не повинні підлягати категоруванню.

Категоруванню повинні підлягати об'єкти обчислювальної техніки, тобто ЕОМ разом з приміщеннями, в яких вони розміщені. Об'єкти характеризуються контрольованими зонами (організаційними заходами).

ЕОМ можуть бути в захищеному чи в не захищеному виконанні, що залежить від того - відповідають чи не відповідають їх параметри вимогам ГОСТ 29339-92 в цілому, тому вираз "ЕОМ II категорії"' взагалі не визначає ступеня захищеності ЕОМ від витоку інформації по ПЕМВН.

Наступна думка. Згідно [7], в межах кожного класу АС класифікуються на підставі вимог до забезпечення певних властивостей інформації. З точки зору безпеки інформація характеризується трьома властивостями: конфіденційністю, цілісністю і доступністю. В зв'язку з цим, в кожному класі АС виділяються такі підкласи.

Приклад…автоматизована система, в якій підвищені вимоги до — забезпечення конфіденційності, цілісності і доступності оброблюваної інформації (підкласи «х.КЦД»).

2.КЦД.3 = { КД-2, КА-2, КО-1, КК-1, ЦД-1, ЦА-3, ЦО-2, ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2 }.

Але ж, відповідно до п. 6.3 [19] комісія з категоріювання визначає ступень обмеження доступу до інформації, яка оброблятиметься технічними засобами та/або озвучуватиметься на об'єкті, та з урахуванням цього ступеня встановлює категорію об'єкта.

Чи не достатнім є категоріювання обєкту та засобу ЕОТ і треба вводити поняття … підвищені вимоги до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації (підкласи «х.КЦД»).

Зрозуміло, що якщо мова йде про ІзОД, то підвищеними є вимоги до забезпечення конфіденційності, цілісності і доступності оброблюваної інформації (х.КЦД), якщо відкрита інформація, що належить до державних інформаційних ресурсів, то підвищеними є вимоги до забезпечення цілісності і доступності (х.ЦД).

Таким чином, видно, що виконавець робіт з ТЗІ має керуватися нормативно-правовими документами з захисту інформації, які мають взаємні посилання один на одного, в одному випадку мають дещо відмінні вимоги, а в іншому дублюють один одного. Це ускладнює роботу щодо створення систем захисту інформації, призводить до відпрацювання відповідних організаційно-розпорядчих документів, які цілими розділами (або частинами) повторюють один одного та невиправданих витрат часу виконавцем робіт з ТЗІ та фінансових витрат замовника, і як наслідок може зводитись до формального виконання вимог з захисту інформації.

Впроваджені в останні роки закони, що стосуються інформації та її захисту, а також внесення змін та доповнень до діючих потребує вжиття певних заходів з метою приведення нормативної бази системи технічного захисту інформації у відповідність до вимог цих законів. Діюча нормативна база з питань ТЗІ потребує доопрацювання з метою підвищення ефективності захисту інформації, впровадження єдиного порядку виконання заходів та упорядкування процедури. І в будь-якому разі, без якісної нормативно-правової бази навряд чи можливе ефективне впровадження інших (організаційних та технічних) заходів захисту інформації.

Література

1. Українська радянська енциклопедія: у 12 томах/ за ред. М. Бажана.— 2-ге вид.—К.: Головна редакція УРЕ, 1974–1985.

2. ДСТУ 2960-94. Організація промислового виробництва. Основні поняття. Терміни та визначення.

3. НД ТЗІ 1.1-003-99. Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.

4. ДСТУ 2226-93. Автоматизовані системи. Терміни та визначення.

5. Закон України від 5.07.1994 року № 80/94-ВР. Про захист інформації в інформаційно-телекомунікаційних системах.

6. НД ТЗІ 3.7-003-05. Порядок проведення робіт із створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі.

7. НД ТЗІ 2.5-005-99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу.

8. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.ДСТУ 2392-94 Інформація та документація. Базові поняття.

9. Кривуца В.Г., Беркман Л.Н., Лапинский В.В. Основи інфокомунікацій. За ред. В. Г. Кривуци — К.:ДУІКТ, 2011.— 276 с.

10. Енциклопедія кібернетики. тт. 1, 2. — К.: Головна редакція УРЕ, 1973. — 584 с.

11. Грайворонський М.В., Новіков О.М. Безпека інформаційно-комунікаційних систем. – Київ, Видавнича група BHV, 2009. – 608 с.

12. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі.

13. ISO 17799:2000. Керування інформаційною безпекою – Інформаційні технології.

14. ISO/IEC 27001:2005. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги.

15. Постанова Кабінету Міністрів України від 29 березня 2006 р. N 373. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах.

16. НД ТЗІ 1.6-003-04**.** Створення комплексів технічного захисту інформації на об’єктах інформаційної діяльності. Правила розроблення, побудови, викладення та оформлення моделі загроз для інформації.

17. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп’ютерних системах від несанкціонованого доступу.

18. НД ТЗІ 3.7-001-99. Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі.

19. НД ТЗІ 1.6-005-2013.Захист інформації на об’єктах інформаційної діяльності. Положення про категоріювання об’єктів, де циркулює інформація з обмеженим доступом, що не становить державної таємниці.

Надійшла 16.11.2015 р. Рецензент: д.т.н., проф. Єрохін В.Ф.