Розділ 8. Інформаційна безпека як об'єкт інформаційного права

8.1. Вступ до основ інформаційної безпеки

Масове впровадження нових технічних засобів, на основі яких здійснюється інформатизація у всьому світі, робить прозорими державні кордони і формує нові геополі-тичні парадигми у розумінні глобальних соціотехнічних систем. Міжнародна інформаційна сфера стає не тільки однією з важливих сфер співробітництва, а й середовищем конкуренції між окремими особами, державами, міждержавними політичними та економічними угруповуваннями. Електронно-комунікаційна інфраструктура, як і інші інформаційні ресурси, стає об'єктом міждержавної боротьби за світове лідерство або об'єктом недобросовісної конкуренції у підприємницькій діяльності чи інших суспільних інформаційних відносин.

Все це зумовлює необхідність формування такого аспекту інформаційної культури, як культура інформаційної безпеки, культура організації інформаційної безпеки. Зазначений аспект розвитку інформаційної культури набуває відображення у такій прикладній науковій дисципліні, як теорія організації (тектологія) інформаційної безпеки.

8.2. Елементи формування основ тектології інформаційної безпеки

Питання культури інформаційної безпеки широко висвітлюються у спеціальній літературі. Сьогодні критична маса науково-практичних знань щодо розвитку суспільних інформаційних відносин у такому аспекті дає змогу сформувати на теоретичному рівні елементи загальної теорії організації інформаційної безпеки в умовах формування інформаційного суспільства — захисту інформації в автоматизованих комп'ютерних системах.

Зазначений аспект теорії має зворотний зв'язок з культурою практики: формування організаційних підходів, методів, засобів систем захисту комп'ютеризованих соціальних інформаційних систем; формування змісту навчальних дисциплін у навчальних закладах, а також формування комплексу знань фахівців, які спеціалізуються на організації захисту інформації, її безпеки у відповідних соціальних структурах (установах, організаціях, підприємствах тощо).

Аналіз наукової думки та емпіричного матеріалу дає змогу визначити такі принципові положення організації захисту інформації в умовах інформатизації у контексті інформаційної безпеки.

1. Культура інформаційної безпеки як наукове явище сьогодні формується на рівні міжгалузевого комплексного соціоінженерного інституту (наукової дисципліни), який утворився на межі поєднання технічних і гуманітарних наук: правової інформатики, інформаційного права та тектології (теорії організації соціальних систем).
2. За природою походження культура інформаційної безпеки в умовах інформаційного суспільства має триєдиний зміст: організаційний, інженерно-технічний (у тому числі програмно-математичний) та правовий.
3. У перспективі сутність інформаційної безпеки, у тому числі щодо захисту інформації у соціотехнічних системах, буде доповнюватися спеціальними знаннями з інших галузей, підгалузей, інституцій технічних та суспільних наук.

З погляду теорії організації і теорії систем, у науковому синтезі їх — теорії організації систем управління — формування цілеспрямованих, керованих систем (у тому числі будь-яких практичних заходів) передбачає визначення елементів системи та осмислення проблематики предметної галузі (її природу) в цілому.

На нашу думку, провідними елементами системи інформаційної безпеки, у тому числі

щодо захисту інформації в автоматизованих комп'ютерних системах, є такі найважливіші чинники.

Суб'єкти — окремі люди, спільноти їх, різного роду організації, суспільство, держава, інші держави, союзи їх, світове співтовариство.

Об'єкт — правовідносини між суб'єктами (суспільні відносини), які визначаються за певними об'єктивно існуючими критеріями.

Провідний предмет суспільних правовідносин — інформація в автоматизованих (комп'ютерних) системах (у тому числі електронних телекомунікаціях, зокрема в Інтернеті).

8.2.1. Сутність теорії інформаційної безпеки

Наступне, що потрібно з'ясувати, — сутність теорії інформаційної безпеки щодо захисту інформації в автоматизованих (комп'ютерних) системах. Відповідно до положень теорії гіперсистем визначимо підсистеми нижчих порядків.

Перш за все — це класифікація суб'єктів суспільних відносин, яку можна розширювати залежно від потреб дослідження предметної галузі. Суб'єктів щодо інформаційної безпеки можна поділити на кілька категорій:

- щодо правового статусу регулювання відносин: суб'єкти регулювання відносин та учасників відносин;
- щодо мети учасників правовідносин: правомірні учасники та правопорушники тощо.

Класифікація суспільних відносин щодо безпеки інформації має багатоаспектний зміст, який визначається залежно від галузей знань. Але все ж їх можна поділити на такі загальні види: соціальні, технічні та соціотехнічні.

Визначальними також є тектологічні (організаційні) критерії: організаційно-управлінські, організаційно-правові та організаційно-технічні (у числі останніх виокремлюють ще організаційно-технологічні).

У суспільно-правовому змісті правовідносини інформаційної безпеки щодо захисту інформації мають сутність організовування нормального (безпечного) функціонування інформаційних систем, у тому числі тих, технічну основу яких становлять засоби комп'ютерної техніки та базовані на них електронні інформаційні технології (у тому числі технології телекомунікації).

Провідна системна мета правовідносин — захист суспільних інформаційних відносин від негативних впливів соціальних, техногенних та природних (стихійних) впливів.

Важливим аспектом загальних положень інформаційної безпеки щодо захисту

інформації в автоматизованих системах є наукове визначення і формулювання принципів її реалізації.

Зазначені принципи повинні мати чітку ієрархічну структуру і критерії. Виходячи з положень природи інформаційної безпеки як тектологічного явища, пропонується поділ принципів на такі групи першого порядку: організащино-правові; оргашзацшно-управлшські; організащино-технічні.

Залежно від науково-практичних потреб організаційної діяльності (організовування) принципи інформаційної безпеки можуть поділятися на групи другого та наступних порядків.

8.2.2. Напрямки інформаційної безпеки

Визначальним у проблематиці теорії організації інформаційної безпеки є з'ясування її напрямків на засадах комплексного підходу щодо методів захисту. Умовно можна визначити такі напрямки організації захисту: правові, управлінські, інженерно-технологічні. У складі останніх як автономні визначаються програмно-математичні (комп'ютерні програмні продукти захисту).

Формування будь-якої теорії у методологічному аспекті передбачає визначення методів пізнання предметної галузі та науково обґрунтованого впливу (організовування, управління тощо) на предметну галузь.

Аналіз науково-практичних джерел та іншого емпіричного матеріалу дав змогу сформулювати предметний метод ("метод застосування методів", метод — принцип) — комплексне застосування управлінських, правових та інженерно-технічнотехнологічних методів захисту інформації в автоматизованих комп'ютерних системах.

На основі зазначених положень можна зробити висновок про наявність потреби формування проблематики окремих аспектів (інститутів) загальної теорії і практики інформаційної безпеки щодо захисту інформації в автоматизованих комп'ютерних системах. У зв'язку з цим є можливість виокремлення двох частин теорії: загальної (фундаментальних, загальних положень) та особливої частин (відносин щодо окремих напрямків функцій на основі загальних положень).

8.2.3. Інститути тектології інформаційної безпеки

На загальнотеоретичному рівні визначимося в таких ключових, особливих проблемах інформаційної безпеки щодо організаційного аспекту захисту інформації в автоматизованих системах:

Першу групу утворюють такі проблемні інститути:

1) проблеми організації доступу до інформації;

2) проблеми організації забезпечення цілісності інформації щодо загроз її порушення;

3) проблеми організації комплексного контролю за інформаційними ресурсами у відповідному середовищі функціонування їх відповідно до матеріальних носіїв інформації (людських (соціальних), людино-машинних (людино-технічних, соціотехнічних) та технологічних);

4) проблеми організації сумісності систем захисту інформації в автоматизованих (комп'ютерних) системах з іншими системами безпеки відповідної організаційної структури;

5) проблеми організації виявлення можливих каналів несанкціонованого витоку інформації (фізичних, соціотехнічних, соціальних);

6) проблеми організації блокування (протидії) несанкціонованого витоку інформації;

7) проблеми організації виявлення, кваліфікації, документування порушення інформаційної безпеки (як стану у визначеному просторі, часі і колі осіб);

8) формулювання відповідальності та правове визначення санкцій та організація притягнення винних до відповідальності (дисциплінарної, цивільної, адміністративної, кримінальної).

8.2.4. Інформаційна безпека як функція

На базі аналізу накопиченого емпіричного матеріалу пропонується узагальнити на рівні теоретичних засад (основ) організацію захисту інформації в автоматизованих (комп'ютерних) системах як функції. Задля цього організацію захисту інформації в автоматизованих системах умовно поділяють на три види функцій. За основу поділу визначено такий критерій, як середовище, в якому перебуває інформація: а) соціальне (окрема людина, спільноти людей, держава); б) інженерно-технікологічне (машинне, апаратно-програмне, автоматичне); в) соціотехнічне (людино-машинне).

Кожен названий рівень щодо середовища об'єктивно доповнює і взаємозумовлює інші функції, в основі утворюючи триєдину гіперсистему: організація інформаційної безпеки. У цій гіперсистемі визначними є такі напрямки (підрівні), що визначаються на основі інтегративного підходу протилежностей (антиподів) — воздії і протидії.

1. Організація протидії небажаній для суб'єкта воздії за допомогою технічних засобів захисту, тобто засоби захисту мають бути адекватними засобам добування (наприклад, протидія розвідці (котррозвідка) відповідними технічними засобами захисту: створення системи просторового зашумлення для приховування інформації у відповідному середовищі (акустичному (звуковому), аудіо (відео), електромагнітному) чи екранування технічних засобів у приміщенні).
2. Організація протидії негативному впливу на учасників інформаційних відносин (наприклад, конкурентів на персонал організації з метою отримання інформації (протидія підкупові персоналу, впровадження представника конкурента в організацію для отримання інформації з обмеженим доступом тощо). Щодо цього та деяких інших факторів можна застосувати принцип, визначений у народній мудрості: "Клин клином вибивають".
3. У разі порушення функціонування інформаційної системи — визначення майнових втрат та мінімізація їх (наприклад, у разі виявлення несанкціонованого доступу до інформації визначення матеріальних і моральних втрат, за необхідності — взаємодія з державними правоохоронними та судовими органами щодо притягнення винних до відповідальності відповідно до законодавства).

На названі напрямки організації інформаційної безпеки відповідного об'єкта захисту впливають такі визначальні фактори:

а) фактор рівня досягнень науково-технічного прогресу (переважно в галузі розвитку, удосконалення технічних засобів);

б) технологічний фактор (в окремих джерелах його ще називають алгоритмічним фактором, коли техніка може бути одна, а технології її застосування різні, цей фактор ще є визначальним для формування методик: як отримання інформації, так і захисту її);

в) соціальний (людський) фактор.

8.3. Агреговані моделі тектології інформаційної безпеки

Загальний аналіз проблем організовування захисту інформації в автоматизованих комп'ютерних системах дає можливість визначити три агреговані організаційні моделі заходів:

1) організація запобіжних заходів;

2) організація блокування (протидії) реальним загрозам, що реалізуються;
3) організація подолання наслідків загроз, які не вдалося блокувати або запобігти їм.
Важливий елемент організації інформаційної безпеки — захисту інформації — поділ заходів на групи щодо протидії. У теорії і практиці майже однозначно виокремлюють три такі групи: активні засоби захисту (наприклад, розвідка, дезінформація, зашумлення тощо); пасивні засоби захисту (наприклад, встановлення екранів несанкціонованому витоку інформації тощо); комплексні засоби захисту (органічне поєднання названих груп).
Ми не будемо докладно їх пояснювати. Звернемо увагу на організаційні заходи при блокуванні (протидії) несанкціонованого доступу до автоматизованої інформаційної системи та подоланні наслідків загроз, які не вдалося блокувати або запобігти їм. Зазначимо, що ці заходи можуть бути спрямовані: на документування методів несанкціонованих дій щодо доступу до автоматизованої системи для наступного дослідження їх; збереження слідів правопорушення; взаємодію (у разі необхідності) з державними правоохоронними органами щодо виявлення та розкриття правопорушення (в тому числі за готування до злочину і за замах на злочин); сприяння притягненню винних до відповідної відповідальності (кримінальної, адміністративної, цивільно-правової, дисциплінарної).
Всі заходи організації інформаційної безпеки, у тому числі в умовах застосування автоматизованих комп'ютерних систем, базуються на знаннях і використанні певних фізичних явищ, що характеризують відповідні форми подання (виразу) інформації. Ці фізичні явища, зокрема ті, що може використати зловмисник, добре відомі.
Завдання організовування інформаційної безпеки щодо захисту інформації в автоматизованих системах визначаються за напрямком, протилежним до загроз безпеки. При реалізації заходів захисту інформації важливим аспектом є визначення і перевірка стану безпеки. У теорії і практиці це набуває втілення в категорії "метрологія". За допомогою метрологічної діяльності з'ясовують рівень розробки і наявність відповідних засобів, норм і методик, які дають можливість оцінити якість функціонування системи захисту інформації, тобто визначити, чи задовольняє чинним нормам система захисту на певний момент часу.
Формалізація норм і методів метрології стану безпеки об'єкта набуває втілення у відповідних нормативних актах. Застосовуючи визначені в них нормативи слід враховувати природну властивість таких нормативів з часом втрачати актуальність. Це пов'язано з тим, що в міру розвитку науково-технічного прогресу можуть змінюватися норми і методи контролю захищеності інформації у відповідному середовищі її існування. Практика свідчить, що, як правило, норми і методи контролю мають тенденцію до удосконалення. Попередні нормативи виступають як орієнтири, точки опори для формування нових нормативів. Сама назва "норматив" свідчить про те, що є фундаментальні межі можливостей існуючих фізичних приладів метрології на певному етапі пізнання людством законів природи.
У ході організації (в тому числі створення алгоритмів (методик) захисту інформації технічними засобами) завдання суб'єктів полягає не тільки в удосконаленні існуючих засобів технічного захисту інформації, а й урахуванні можливих новацій. При цьому переважно має реалізовуватися принцип агрегації новацій до наявної системи захисту. Найкраще, коли можна інтегрувати через новації засоби захисту і вилучити із системи захисту застаріле обладнання. Але водночас не слід забувати, що старі засоби захисту,

які можуть функціонувати автономно в системі захисту, не повинні "зніматися з озброєння" бездумно.

Організовуючи захист інформації в автоматизованих системах, слід враховувати, що хоч в основі автоматизованої системи є технічний пристрій, який обробляє інформацію, але при його використанні так чи інакше присутній людський фактор. При цьому людина виступає в ролі або безпосередньо (як користувач автоматизованої системи), або опосередковано (як розробник системи).

З цього випливає, що на надійність системи захисту інформації в автоматизованих комп'ютерних системах впливають дві групи взаємопов'язаних факторів: людські (соціальні) та інженерно-технологічні.

В аспекті теорії систем організація захисту інформації в автоматизованих системах передбачає обумовлене виокремлення внутрішньо- і зовнішньо-системних ознак, які утворюють діалектичну гіперсистему організації рубежів безпеки.

8.4. Методологічні положення інформаційної безпеки

Названі елементи основ теорії організації захисту інформації зумовлюють необхідність формування і розвитку окремих теорій інформаційної безпеки (зокрема її складової — теорії організації захисту інформації в автоматизованих системах) у таких аспектах: організаційному, інженерно-технологічному та пов'язаному з ними правовому. Як відомо, інженерно-технологічний аспект поєднує взаємопов'язані технічний (апаратний) та алгоритмічний (програмний) аспекти (саме тому ми вжили раніше категорію "інженерно-технікотехнологічний").

Будь-яка загальна теорія вважається науковою, якщо вона має чітко визначені методи пізнання предметної галузі, закономірностей природи (фізики) і суспільства. Таким чином, щоб претендувати на статус науковості, загальна теорія організації інформаційної безпеки повинна мати визначену множину методів пізнання її предмета й об'єкта.

Враховуючи міжгалузевий характер теорії організації інформаційної безпеки, в ній поєднуються методи пізнання традиційних фундаментальних наук: соціології та фізики. Це зумовлено безпосереднім предметом теорії: людино-машинними (соціотехнічними) системами, якими є автоматизовані комп'ютерні інформаційні системи.

Звичайно сферою дослідження теорії є практика захисту інформації в автоматизованих (комп'ютерних) системах: її закономірності, принципи, різного рівня проблеми і завдання вирішення їх. Нині проблема і завдання формалізують переважно за допомогою методів евристики: формально-евристичного та інтуїтивно-евристичного. Домінуюче становище серед цих методів мають методи експертних оцінок та оцінки критичної маси інформації, за допомогою яких, зокрема, оцінюють функціонування систем захисту інформації.

Проте ці методи мають і недоліки: наявність людського фактора — суб'єктивізм експерта та потенційне обмеження інформації у формі знань, якими володіє експерт.

Подоланню цих недоліків допомагає когнітологія — наука про знання. Відповідно до положень цієї науки в загальній теорії захисту інформації визначаються як аксіоми когнітологічні положення про рівень і відносність ентропії (невизначеності) системи пізнання (людини, спільноти та ін.) і її вплив на формування теоретичних положень, відносну істинність їх (у часі та колі осіб). Відносність істини визначається кількісними і якісними характеристиками множини знань, якими володіє певний суб'єкт відносин, навичками застосування їх, інтелектуальним потенціалом та швидкістю розумових реакцій на відповідні ситуації. Відносність захисту інформації визначається відносністю знань суб'єкта захисту і відносністю загроз захисту, зокрема знань зловмисника.

У контексті визначення об'єктивності експертної оцінки організації захисту інформації, подолання суб'єктивізму, наприклад при визначенні стану інформаційної безпеки об'єкта, застосовують метод залучення кількох експертів. Але, як справедливо зазначають деякі дослідники, при цьому виникає питання, хто може вважатися висококваліфікованим експертом (кваліфікаційні ознаки експерта) і скільки таких експертів потрібно для істинності висновків, подолання суб'єктивізму (Организация и современные методы защиты информации / Под общ. ред. С.А. Диева, А.Г. Шаваева. — М.: Банковский Деловой Центр, 1998. — С. 36).

8.5. Людський фактор в організації інформаційної безпеки

Наявність людського фактора має провідне значення в теорії організації захисту інформації. Через цей елемент теорія організації захисту інформації як система знань має предметний гіперзв'язок з фундаментальними гуманітарними науками — соціологією, соціальною психологією, соціальною інженерією.

За природою організації захист інформації має комплексний характер, тобто між окремими її складовими є певний зв'язок. У рамках теорії організації захисту інформації чітко визначився постулат, що організація захисту інформації повинна враховувати не тільки складність технічної і технологічної компонент системи, а й людський фактор. Тобто, формуючи конкретну систему технічного захисту, слід враховувати якісні індивідуально- і соціально-психологічні, моральні, етичні та інші особисті характеристики людей, задіяних у системі захисту інформації.

У такому аспекті визначається також напрямок теорії щодо оцінки, характеристики зловмисників, які посягають на безпеку інформаційної системи. У цьому аспекті теорія захисту інформації має зв'язок з кримінологією, її складовими вченнями: віктимологією та теорією формування соціально-психологічного портрету зловмисника.

8.6. Правовий аспект інформаційної безпеки

8.6.1. Основні питання правової культури щодо інформаційної безпеки
8.6.2. Стан правового регулювання охорони та захисту інформації

8.6.1. Основні питання правової культури щодо інформаційної безпеки

Правовий напрямок теорії охорони та захисту інформації визначається необхідністю формування правил поведінки, відносин у так званому віртуальному або кібер-просторі. У цьому аспекті теорія захисту інформації пов'язана з інформаційним правом та правовою інформатикою. Щодо формування методик виявлення та розкриття злочинів,

які вчиняються за допомогою сучасних інформаційних технологій, теорія захисту інформації формує понятійний апарат такої інституції криміналістики, як криміналістична інформатика.

При формуванні системи захисту інформації виникає необхідність застосування методів інтеграції та агрегації складових системи як її підсистем, що можливо при адаптації до предметної галузі теорії алгоритмізації, моделювання, теорії систем тощо.

Когнітивно-юридичний аналіз нормативно-правових актів у сфері суспільних інформаційних відносин, з позицій накопичених наукових знань сьогодення, свідчить про те, що в суспільстві вже сформувалося усвідомлення необхідності формування інституції суспільних відносин інформаційної безпеки: захисту інформації. Але рівень ентропії, наявний на момент прийняття нормативно-правових актів у цій сфері суспільних відносин, об'єктивно не дозволив сформувати їхній зміст у обсязі, необхідному для практики. До того ж практика розвивалася, апробовуючи юридичні норми як соціотехнічні стандарти (алгоритми) однозначно розуміння їхнього змісту широким загалом суб'єктів суспільних відносин.

Сьогодні створено передумови для формування умовно автономної теорії, в рамках якої має сформуватися специфічний понятійний апарат (термінологія, категорії), змістовний аспект якого є проблематикою теорії для задоволення потреб практики: наирацювання стандартів категорій для розуміння широким загалом сутності нових соціальних явищ, у тому числі передачі інформації у формі знань у межах відповідної навчальної дисципліни.

Сучасний рівень суспільної ентропії — теоретичної розробленості проблематики — дає можливість визначити об'єктивність потреб формування у вітчизняній науці системи знань, ідей, доктрин, концепцій щодо інформаційної безпеки, формулювання (формалізації) її у змістовному, сут-нісному, понятійному аспектах тощо. При цьому як мету визначено формування ядра самої загальної теорії на елементарному рівні. Такі положення покликані формувати синтетичний науковий напрямок на межі багатьох наук, в яких проблематика інформаційної безпеки, захисту інформації визначена фрагментарно, ситуаційно, розпорошена серед багатоманітної галузевої проблематики. Передбачається, що з часом сформується розвинута теорія організації інформаційної безпеки, захисту інформації в автоматизованих (комп'ютерних) системах у таких науках, як правова інформатика та інформаційне право.

Базуючись на методології гіперсистем права та теорії критичної маси норм правовідносин, можна прогнозувати, що в майбутньому інформаційна безпека, у міру розвитку інформаційного суспільства, виокремиться з інформаційного права в окрему субінституцію подібно до права інтелектуальної власності, його провідних складових — авторського права та права промислової власності.

8.6.2. Стан правового регулювання охорони та захисту інформації

У контексті проблематики слід звернути увагу на стан правового регулювання питань захисту інформації, зумовлюваний в Україні такими чинниками:

- нормативною невизначеністю понять та категорій, зокрема на рівні юридичних актів (документів);
- недосконалістю правового регулювання в інформаційній сфері, зокрема у сфері захисту таємниць (крім державної), конфіденційної інформації та відкритої інформації, важливої для особи, суспільства та держави;
- недостатністю нормативно-правових актів і нормативних документів з питань проведення досліджень, розроблення та виробництва засобів забезпечення захисту;
- незавершеністю створення системи сертифікації засобів забезпечення технічного захисту інформації (ТЗІ);
- недосконалістю системи атестації на відповідність вимогам ТЗІ об'єктів, робота яких пов'язана з інформацією, що підлягає технічному захисту;
- недостатньою узгодженістю чинних в Україні нормативно-правових актів та нормативних документів з питань ТЗІ з відповідними міжнародними договорами України.

З аналізу нормативно-правової бази захисту інформації в автоматизованих системах впливає, що в сучасних умовах важливе значення щодо захисту інформаційних відносин надається створенню системи технічного захисту інформації. У публічному праві України під системою ТЗІ розуміють сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правову та матеріально-технічну базу.

З позиції когнітивного (пізнавального) підходу таке визначення має, на нашу думку, певні недоліки.

У нашому розумінні редакцію визначення категорії "система технічного захисту інформації" слід подати, таким чином у двох аспектах.

Система організації технічного захисту інформації — це множина комплексних заходів, що здійснюються визначеними в нормативних актах, на основі наявної матеріально-технічної бази, відповідними суб'єктами, об'єднаних цілями та завданнями захисту інформації інженерно-технічними засобами.

Система ТЗІ — це множина інженерно-технічних засобів, що визначають заходи на основі наявної матеріально-технічної бази у суб'єктів, об'єднаних цілями та завданнями захисту інформації у порядку, визначеному у відповідних нормативно-правових документах (законах та підзаконних актах).

З аналізу чинного законодавства та підзаконних нормативних актів можна зробити узагальнення, що в Україні є національна система правового регулювання захисту інформації в автоматизованих системах. Правову основу забезпечення захисту інформації в Україні як інституції права становлять Конституція України, Концепція (основи державної політики) національної безпеки України, закони України "Про інформацію", "Про захист інформації в автоматизованих системах", "Про державну таємницю", "Про науково-технічну інформацію", інші нормативно-правові акти, в тому числі міжнародні договори України (які відповідним чином ратифіковані Україною), що стосуються сфери інформаційних відносин.

Критичний підхід щодо аналізу Концепції технічного захисту інформації, як нормативно-правового акта (документа) свідчить про невідповідність його назви

(форми) та змісту. По суті, цей документ становить собою не систему, а звичайну сукупність норм. У ньому йдеться не стільки про організацію інженерно-технічного захисту (організаційно-технічні заходи), скільки про організаційно-управлінські та організаційно-правові заходи.

Виходячи із зазначеного, можна зробити висновок, що проблематика захисту інформації в автоматизованих системах у науці й практиці України перебуває на стадії становлення і потребує ґрунтовного наукового забезпечення, зокрема систематизації, в тому числі на рівні організаційно-правового аспекту.

У зв'язку з цим є потреба формування комплексної наукової дисципліни теорії організації (тектології) інформаційної безпеки, а в її складі — субінституту захисту інформації в автоматизованих системах.