УДК 681.3

ОКРЕМІ ПИТАННЯ ЩОДО ВИЗНАЧЕННЯ КАТЕГОРІЇ “ІНФОРМАЦІЙНА БЕЗПЕКА” У НОРМАТИВНО-ПРАВОВОМУ АСПЕКТІ

Віталій Цимбалюк
Національна академія внутрішніх справ України

Анотація: **Розглянуто нормативно-правовий аспект інформаційної безпеки.**
Summary: **The normative legal aspect of information safety is considered.**
Ключові слова: **Інформаційна безпека, інформаційний простір, інформаційний ресурс.**

I Вступ

Як свідчать дослідження, безпека інформаційних систем не зводиться до звалювання в одну кучу (сукупність) засобів, способів і методів захисту. Враховуючи суспільну значимість категорія “інформаційна безпека” в нормативно-правовому аспекті має конституційний статус. В системі юридичних норм України вона знайшла відображення у статті 17 Конституції України. Відповідно до положень зазначеної статті визначення інформаційної безпеки можна подати як функцію:

інформаційна безпека України – ***це одна з найважливіших функцій держави, справа всього Українського народу щодо захисту суверенітету України.***

II Основна частина

Сутність інформаційної безпеки України за змістом у контексті інформаційної діяльності було визначено на законодавчому рівні у Концепції (основах державної політики) національної безпеки України, схваленій Постановою Верховної Ради України 16. 01. 1997 року “3/97-ВР (Відомості Верховної Ради, 1997, № 10. С. 85)”.

Відповідно до цього нормативного акту, інформаційна безпека України включає: вжиття комплексних заходів щодо захисту свого інформаційного простору та входження України в світовий інформаційний простір; виявлення та усунення причин інформаційної дискримінації України; усунення негативних чинників порушення інформаційного простору, інформаційної експансії з боку інших держав; розробку і впровадження необхідних засобів та режимів отримання, зберігання, поширення і використання суспільно значущої інформації, створення розвиненої інфраструктури в інформаційній сфері.

Інформаційна безпека - невід'ємна частина політичної, економічної, оборонної та інших складових національної безпеки.

З метою зменшення ентропії щодо сутності та змісту законодавець визначає орієнтовний перелік об’єктів інформаційної безпеки. Об'єктами інформаційної безпеки є інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни.

Інформаційна безпека щодо інформатизації знайшла юридичний вираз на законодавчому рівні в Концепції Національної програми інформатизації (Затверджена Законом України від 4 лютого 1998 року № 75/98-ВР). Відповідно до цього нормативно-правового акту **інформаційна безпека** – ***це комплекс нормативних документів з усіх аспектів використання засобів обчислювальної техніки для оброблення та зберігання інформації обмеженого доступу; комплекс державних стандартів із документування, супроводження, використання, сертифікаційних випробувань програмних засобів захисту інформації; банк засобів діагностики, локалізації і профілактики комп’ютерних вірусів, нові технології захисту інформації з використанням спектральних методів, високонадійні криптографічні методи захисту інформації тощо***.

Відповідно до Розділу IV Концепції національної програми інформатизації створення умов для інтеграції України у світовий інформаційний простір має здійснюватися згідно з сучасними тенденціями інформаційної геополітики, забезпечення обороноздатності та державної безпеки.

В науковій літературі сутність категорії “інформаційна безпека” розкривається неоднозначно, подібно до сутності категорії “безпека”. Для прикладу наведемо декілька з них.

На думку В. Я. Рубана інформаційна безпека людини, суспільства, держави – це стан їхньої інформаційної озброєності (мається на увазі духовної, інтелектуальної, морально-етичної, політичної), за якого ніякі інформаційні впливи на них неспроможні викликати деструктивні думки і дії, що призводять до негативних відхилень на шляху стійкого прогресивного розвитку названих суб’єктів (Рубан В. Я.

Інформаційна безпека України: сутність та проблеми. //Стратегічна панорама. 1998. №3 – 4. С. 170).

Інформаційна безпека розглядається також як єдність концептуальних, теоретичних і технічних основ забезпечення на інформаційному рівні безпеки всіх сфер державної і суспільної діяльності (політичної, економічної, соціальної, військової, економічної, духовної та ін.), а також сфер формування, циркулювання, накопичення і використання інформації (інформаційний простір, інформаційні ресурси, інформаційно-аналітичне забезпечення органів державного управління в усіх різновидах діяльності тощо; див. Рубан В. Я. Інформаційна безпека України: сутність та проблеми. //Стратегічна панорама. 1998. №3 – 4. С. 172)

В організаційно управлінському аспекті (статичному, статистичному та щодо інтересу суб'єктів суспільних відносин) категорія "інформаційна безпека" розглядається окремими авторами, як стан захищеності життєво важливих інтересів особи, суспільства і держави, при якому зводиться до мінімуму завдання збитку через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації (Рубан В. Я. Інформаційна безпека України: сутність та проблеми. //Стратегічна панорама. 1998. №3 – 4. С. 174).

Автори книги "Організація і сучасні методи захисту інформації" (під заг. ред. Дієва С. А. та Шаваєва А. Г. – М. 1998. – С. 52) пропонують наступне визначення категорії "інформаційна безпека":

"Інформаційна безпека" … – стан захищеності інформаційного середовища суспільства, що забезпечує її формування і розвиток в інтересах громадян, організацій і держави.

Дане визначення подається у змісті державної політики в галузі безпеки, як категорії державного управління щодо загальносуспільного, національного інтересу.

Також в літературних джерелах вживається така категорія, як "б**езпека інформаційної системи" –** заходи, які охороняють інформаційну систему від несанкціонованого доступу, випадкового чи зловмисного втручання в нормальні дії або намагання зруйнувати її компоненти (Лекарев С. В., Порк В. А. Бизнес и безопасность. /Толковый терминологический словарь. Под науч. ред. проф. Гурова А. И., проф. Тетерина В. С./. – М.: "ЦКСИиМ", "Ягуар". 1995. С. 52).

З точки зору когнітивного підходу різні автори, переважно на основі базового освітнього світогляду, подають по різному її визначення, спираючись на ті чи інші критерії.

На погляд ряду авторів, провідними елементами системи інформаційної безпеки, у тому числі щодо підтримки режиму, охорони та захисту інформації в автоматизованих (комп'ютерних) інформаційних системах, виступають наступні найважливіші чинники:

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

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

Провідний предмет суспільних правовідносин – інформація (відомості, дані), в тому числі в автоматизованих (комп'ютерних) системах, електронних телекомунікаціях, в Інтернет.

Провідна системна мета правовідносин (процесів) – підтримка режиму функціонування, охорона і захист суспільних інформаційних відносин від негативних впливів соціальних (соціогенних, антропогенних, у їх складі криміногенних), техногенних та природних (стихійних) впливів (загроз).

Визначним у проблематиці теорії організації інформаційної безпеки є з'ясування її напрямків на засадах комплексного підходу щодо методів підтримки режиму, охорони та захисту інформаційної безпеки. Умовно можна визначити наступні напрямки організації підтримки, охорони та захисту: правові, управлінські, інженерно – технологічні. У складі останніх щодо комп'ютерних систем, як автономні визначаються програмно-математичні (комп'ютерні програмні продукти захисту) та апаратні. В окремих джерелах вони об'єднуються в категорії "апаратно-програмні".

На основі зазначених положень можна зробити висновок про існування потреби формування проблематики окремих аспектів (інститутів) у складі комплексної наукової дисципліни - загальної теорії і практики інформаційної безпеки щодо підтримки, охорони та захисту інформації. У зв'язку з цим існує можливість виділення двох частин теорії: загальної частини (фундаментальних, загальних положень) та особливої частини (відносин щодо окремих напрямків функцій на основі загальних положень).

На загально-теоретичному рівні визначимося в наступних ключових, особливих проблемах інформаційної безпеки щодо організаційного аспекту підтримки, охорони та захисту інформації в автоматизованих (комп'ютерних) інформаційних системах.

Їх складають наступні проблемні інститути:

1) проблеми організації доступу до інформації (сигналів, даних, відомостей, документів, матеріалів);

2) проблеми організації забезпечення цілісності інформації (даних) щодо загроз, які можуть спричинити порушення життєдіяльності об'єкта;

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

4) проблеми організації сумісності систем підтримки, охорони та захисту інформації (даних) 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 (даних, відомостей);

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

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

На базі аналізу накопиченого емпіричного матеріалу пропонується здійснити узагальнення на рівні теоретичних засад (основ) організації підтримки, охорони та захисту інформації в автоматизованих (комп'ютерних) системах як функції. Задля цього організація безпеки умовно розділяється на три рівня. За основу поділу визначено такий критерій, як середовище, в якому знаходиться інформація: а) соціальне середовище (окрема людина, спільноти людей, держава); б) інженерно-технічнологічне (машинне, апаратно-програмне, автоматичне, телекомунікаційне) середовище; в) соціотехнічне (людино - машинне) середовище.

Кожен зазначений рівень щодо середовища об'єктивно доповнює і взаємообумовлює інші рівні, в основі утворюючи триєдину гіперсистему – організація інформаційної безпеки. В цій гіперсистемі визначними є наступні напрямки (підрівні) протидії загрозам інформаційній безпеці, які визначаються на основі інтегративного підходу протилежностей (антиподів) – воздії і протидії:

1. **Організація підтримання режиму, охорони та захисту небажаній для суб'єкта воздії за допомогою технічних засобів**. Тобто засоби протидії мають бути адекватними засобам і технологіям дії (наприклад, розвідки: протидія технічній розвідці відповідними технічними засобами протидії: створення системи просторового зашумлення для приховання 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 підкупу персоналу, впровадження представника конкурента в організацію для отримання інформації з обмеженим доступом тощо). Щодо цього фактору та деяких інших можна застосувати принцип, визначений у народній мудрості: "клин клином вибивають".

3. **В разі порушення функціонування інформаційної системи – визначення майнових втрат та їх мінімізація** (наприклад, в разі виявлення несанкціонованого доступу до інформації – визначення матеріальних і моральних втрат, при необхідності – взаємодія з державними правоохоронними та судовими органами щодо притягнення винних до відповідальності згідно з законодавством).

На зазначені напрямки підтримки інформаційної безпеки відповідного об'єкта захисту впливають наступні визначні фактори: а) фактор рівня досягнень науково-технічного прогресу (переважно в галузі розвитку, удосконалення технічних засобів); б) технологічний фактор (в окремих джерелах його ще називають алгоритмічний фактор, коли техніка може бути одна, а технології її застосування різні, цей фактор ще є визначним для формування методик як отримання інформації, так і захисту її); в) соціальний (людський) фактор.

Важливим елементом організації інформаційної безпеки є поділ заходів на групи щодо протидії. В теорії і практиці майже однозначно виділяють три такі групи: активні засоби захисту (наприклад, розвідка, дезінформація, зашумлення тощо); пасивні засоби захисту (наприклад, створення перешкод несанкціонованому витоку інформації тощо); комплекс засобів захисту (органічне поєднання попередньо вказаних груп).

Виходячи з зазначеного поняття в умовах інформатизації України можна визначити наступну класифікацію загроз інформаційній безпеці людини, суспільству, державі.

За сутністю походження, з точки зору системно-інтегративного підходу їх можна умовно поділити на три види:

Природні загрози (стихійні лиха): землетруси, повені, смерчі, стихійні пожежі, зливи тощо.

Техногенні загрози: аварії, катастрофи тощо, породжені технічними (штучними) та технологічними системами.

Соціальні (антропогенні) загрози (можна поділити за кількісною ознакою їх учасників)**.**

Класифікацію соціогенних загроз можна здійснити також за кримінально-правовими та кримінолого-

криміналістичними ознаками способу вчинення правопорушення.

Аналіз наукової думки різних авторів та емпіричного матеріалу дозволяє визначити наступні принципові положення сутності та змісту категорії "інформаційна безпека":

- вид інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов їх життєдіяльності;
- суспільні процеси, пов'язані зі створенням безпечних (життєво важливих, нормальних) умов поширення (розповсюдження), обробки, зберігання та використання інформації;
- стан правовідносин, пов'язаний з нормальним (безпечним) створенням, розповсюдженням, обробкою, зберіганням та використанням інформації у певному просторі, часі та колі осіб;
- складовий чинник організаційно-правового режиму безпеки людини, соціальних утворень, суспільства, держави і міжнародної безпеки.

Інформаційна безпека, як наукове явище, сьогодні формується на рівні міжгалузевого комплексного інституту (комплексної наукової дисципліни), який утворився на межі поєднання технічних і гуманітарних наук: правової інформатики, інформаційного права та тектології (теорії організації соціальних систем).

За природою свого походження інформаційна безпека як діяльність (процес) і як наукова дисципліна має триєдиний зміст: організаційний, інженерно-технічний (в тому числі програмно-математичний) та правовий.

У перспективі сутність інформаційної безпеки, в тому числі щодо підтримки, охорони та захисту інформації в соціотехнічних системах, буде доповнюватися спеціальними знаннями з інших галузей, підгалузей, інституцій технічних та суспільних наук.

Наукова розробка положень теорії інформаційної безпеки покликана створити фундаментальну базу для загальної теорії безпеки особи, суспільства, держави, світового співтовариства, стати основою формування державної інформаційної політики та міжнародної безпеки глобальної інформаційної цивілізації.

На завершення, на основі проведеного системно-структурного правового аналізу можна зробити узагальнене визначення категорії "інформаційна безпека" як соціального явища та правового чинника суспільних інформаційних відносин.

Інформаційна безпека – ***це суспільні відносини щодо створення і підтримання в належному стані нормального режиму функціонування відповідної інформаційної системи; комплекс організаційних, правових та інженерно-технологічних заходів щодо охорони, захисту, запобігання і подолання природних, техногенних і соціогенних (антропогенних) загроз, реалізація яких може порушити чи припинити життєдіяльність конкретної системи***.

III Висновки

Поняття та сутність інформаційної безпеки в умовах інформатизації України як соціального явища пропонується визначити наступним чином.

Інформаційна безпека в умовах інформатизації України (формування інформаційного суспільства) – ***це суспільні відносини щодо створення і підтримання в належному стані режиму нормального функціонування відповідної автоматизованої (комп'ютеризованої) інформаційної системи, систем телекомунікації; комплекс організаційних, правових та інженерно-технологічних (технічних та програмно-математичних) заходів щодо охорони, захисту, запобігання і подолання природних, техногенних і соціогенних загроз, реалізація яких може порушити чи припинити життєдіяльність конкретної соціо-технічної інформаційної системи.***

Більш детально окремі проблеми щодо інформаційної безпеки в авторському розумінні подаються в публікаціях, наведених у списку літератури.

Література: ***1.*** *Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. та ін. Комп'ютерна злочинність. Навчальний посібник. – Київ: "Атіка", 2002. – 240 с.* ***2.*** *Виявлення та розслідування злочинів, що вчиняються з використанням комп'ютерних технологій. Наукове видання. /Камлик М .І., Романюк Б. В., Гавловський В. Д., Хахановський В. Г., Цимбалюк В. С. /Заг.ред. Я. Ю. Кондратьєва – К. НАВСУ. 2000. – 64 с.* ***3.*** *Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій. Монографія /За заг. ред. д. ю. н. Калюжного Р. А. – Запоріжжя: "Просвіта". 2001. – 252 с.* ***4.*** *Інформаційне право та інформаційна безпека /Сучасний стан, поняття та визначення змістовної частини, інкорпорація нормативних актів з правових питань у сфері інформації та її захисту. Наукове видання. /Гавловський В. Д., Коваленко О. І., Гіжевський В. К. Цимбалюк В. С. та ін. /Заг. ред. Р. Калюжного та В. Філонова – Київ – Донецьк: Донецький інститут внутрішніх справ МВС України. Інститут економіки та права "КРОК", 2001. –230 с.* ***5.*** *Цимбалюк В. С., Іванова Т. С. Захист електронних засобів від несанкціонованого доступу. Навчально-методичний посібник. Ірпінь. УФЕІ. 1998.*