УДК 002.6:342.7:347.777:343.50:35.078

ІНФОРМАЦІЙНА БЕЗПЕКА: ЗАХИСТ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ (ОРГАНІЗАЦІЙНО-ПРАВОВИЙ АСПЕКТ)

Владислав Гавловський

Анотація: **В статті розглядаються питання теорії інформаційного права, правової інформатики, інформаційної безпеки та захисту інформації в автоматизованих системах (організаційно-правовий аспект).**
Summary: **In the article the questions of the theory of the information right, legal computer science, information safety and protection of the information in the automized systems (organization-legal aspect) are considered.**
Ключові слова: **право, захист інформації в автоматизованих системах.**

Як і будь-яке соціальне явище інформатизація має не тільки позитивну для суспільства сторону, але і зворотну, негативну: використання комп`ютерних технологій в протиправних, антисоціальних, злочинних цілях. Дослідження свідчать, що комп`ютерна злочинність у світі має тенденцію до зростання. Особливу небезпеку в складі комп`ютерних правопорушень мають злочини, що вчиняються організованими угрупуваннями. Проникнення організованих злочинних формувань у кіберпростір - комп`ютерний інформаційний простір, породило зміну засобів і способів вчинення деяких традиційних злочинів (крадіжки, шахрайства, тероризм, шпигунство, вимагательство, політичний шантаж, недобросовісна конкуренція тощо). Поряд з цим виникли і нові антисоціальні діяння: порушення права інтелектуальної власності на комп`ютерні програми та топографії інтегральних мікросхем ("комп`ютерне піратство"), комп`ютерне хуліганство, розповсюдження програмних і технічних засобів, здатних спричинити перекручення чи знищення інформації тощо.

У зв`язку з цим виникла потреба у формуванні нового світогляду, як у юридичної так і у іншої громадськості: інформаційного світогляду, інформаційної правосвідомості, інформаційної правової культури. Це має відношення і до загалу працівників правоохоронних органів України.

Одним із завдань формування інформаційної правосвідомості є відпрацювання на теоретичному рівні понятійного апарату, нових для юриспруденції категорій, а звідси - формування практичних дієвих, ефективних засобів та заходів протидії правопорушенням, що вчиняються з використанням комп`ютерних технологій, в тому числі комп`ютерній злочинності, особливо такої, що має ознаки організованої.

Як тенденцію визначимо, що сучасне життя, в епоху глобальної інформаційної цивілізації висуває потребу виникнення нових наукових міжгалузевих комплексних інституцій, які сьогодні набули умовної назви - інформаційне право та правова інформатика. Ці міжгалузеві комплексні наукові дисципліни активно розвиваються, формуючи відповідно свій, новий термінологічний, понятійний апарат шляхом інтеграції правознавства та інформатики.

Однією з важливих категорій правової інформатики та інформаційного права є категорія "інформаційна безпека". Важливість з`ясування сутності цієї категорії випливає з того, що вона зазначена в Конституції України (стаття 17): "захист суверенітету і територіальної цілісності України, забезпечення її … **інформаційної безпеки** є найважливішими функціями держави, справою всього Українського народу".

Легітимізована сутність категорії "інформаційна безпека" подається законодавцем у Концепції Національної програми інформатизації (Затверджена Законом України від 4 лютого 1998 року N 75/98-ВР): "**інформаційна безпека"** - невід'ємна частина політичної, економічної, оборонної та інших складових національної 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".

Зміст категорії "інформаційна безпека" знаходить розвиток у комплексі нормативно-правових документів щодо використання засобів обчислювальної (комп`ютерної) техніки для оброблення та зберігання інформації обмеженого доступу; державних стандартів із документування, супроводження, використання, сертифікаційних випробувань комп`ютерних програмних засобів захисту інформації; банк засобів діагностики, локалізації та профілактики комп`ютерних вірусів, нові технології захисту інформації з використанням спектральних методів, високонадійні криптографічні методи захисту інформації тощо.

Аналіз чинного інформаційного законодавства свідчить, що український законодавець в значній мірі пов`язує сутність категорії "інформаційна безпека" з категорією "захист інформації в автоматизованих системах". Ця категорія також має визначення на законодавчому рівні, як системоутворюючий чинник (об`єкт) правовідносин - правового регулювання суспільних інформаційних відносин, пов`язаних з використанням автоматизованих

(комп`ютерних) систем (АС). В нашій країні системоутворюючим цієї галузі суспільних відносин виступає Закон України "Про захист інформації в автоматизованих системах" (від 5 липня 1994 року).

Слід зазначити, що поряд з цим Законом сьогодні в України існує значний масив нормативних актів, які регулюють суспільні інформаційні відносини в умовах інформатизації. Це дає підстави для умовного виділення таких відносини як об`єкт (предмет) наукового дослідження, в межах міжгалузевого комплексного інституту права - інформаційного права. Серед інших, в ньому визначаються такі складові: інформаційна безпека та захист інформації в автоматизованих системах. Про комплексність правового захисту інформації в АС свідчить те, що кримінально-правовий аспект його сьогодні базується на положеннях ст. 198-1 Кримінального кодексу України (КК) (Порушення роботи автоматизованих систем). Дана стаття розміщена у Главі IX серед злочинів проти порядку управління.

Як свідчать дослідження, незважаючи на наявність правової бази, в нашій країні боротьба з правопорушеннями, що вчиняються з використанням комп`ютерних технологій, зокрема з комп`ютерною злочинністю, особливо з організованими її проявами не набула адекватного, щодо потреб часу, рівня. Це в першу чергу зумовлено наступними чинниками: невідповідним рівнем підготовки висококваліфікованих кадрів, здатних вести активну ефективну боротьбу з комп`ютерними злочинами; та низьким розвитком фундаментальних досліджень на національній емпіричній базі.

На нашу думку проблематика інформаційної безпеки в Україні потребує глибокого наукового дослідження на міжгалузевому рівні з метою напрацювання науково обгрунтованих методик виявлення та розкриття правопорушень, що вчиняються за допомогою сучасних інформаційних технологій, особливо комп`ютерних злочинів. Адже підготовка висококваліфікованих кадрів передбачає попередню підготовку навчальної та наукової літератури, розробки програми навчальної дисципліни і введення її в навчальні плани учбових закладів. Орієнтовно назва такої навчальної дисципліни пропонується наступна - "Захист інформації в автоматизованих (комп'ютерних) системах". Легальною підставою такої назви є відповідно зазначений вище Закон України.

Для з`ясування сутності категорії "захист інформації в автоматизованих системах", як правового явища (як інституції права) слід визначити його місце в системі права та правознавства. Визначимо місце захисту інформації як інституції права за допомогою положень теорії систем, її складової - теорії гіперсистем.

З точки зору теорії критичної маси норм права та теорії соціальних систем, на межі галузей права виник синтетичний міжгалузевий комплексний гіперінститут права - інформаційне право. Системоутворюючим цього інституту права в нашій країні виступає Закон України від 2 жовтня 1992 року "Про інформацію".

Однією із складових інформаційного права, як гіперінституту права є субінститут (підсистема, система другого порядку) права - захист інформації в автоматизованих (комп'ютерних) системах.

Характерним для інформаційного законодавства є те, що в ньому зазначаються опосередньо методи правового регулювання через посилання на провідні галузі національного права: цивільне, адміністративне, кримінальне. На цих підставах можна зробити висновок, що захист інформації в автоматизованих системах, як інституція права має комплексний міжгалузевий характер.

Наступна проблема, яка пропонується до розгляду, це визначення категорії "захист інформації". У законодавстві подається наступне її визначення:

Захист інформації - ***сукупність організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованій системі та осіб, які користуються інформацією*** (частина 4 статті 1 Закону України "Про захист інформації в автоматизованих системах").

Існує думка, що визначення зазначеного поняття, подане законодавцем не досить вдале. Проаналізуємо його зміст виходячи із сучасних (поки що нетрадиційних для правознавства) новітніх методологічних підходів: теорії соціальних систем, когнітивного (пізнавального) суспільствознавства (когнітології). Методологічною базою є також теорія інформації, яка, поряд з теорією права, є базовою для ***правової інформатики - науки про застосування положень, методів, термінології інформатики щодо дослідження і з`ясування закономірностей і тенденцій суспільних інформаційних правовідносин, та інших правових системах, їх інформаційного забезпечення на базі сучасних електронно-обчислювальних (комп'ютерних) технологій.***

Перш за все звернемо увагу на вживання категорії "сукупність" для розкриття змісту категорії "система". Під кутом зору когнітології та теорії систем, категорія "сукупність" - нейтральна категорія, вона має відношення і щодо неупорядкованої множини елементів - "кучі" ("купи"), що притаманно більше такій категорії, як "хаос". Існує думка, що доцільнішим було б вживати у визначенні категорії "система" категорію "множина", а не - "сукупність".

Система, як когнітивна категорія передбачає чітке визначення комплексу складових явища: його елементів, їх структури взаємозв'язків між собою та врахування можливих зв`язків із зовнішнім середовищем (системою більшого порядку). Тобто у статичному змісті ***система - це умовно виділена множина відповідним чином визначених чи упорядкованих з конкретною метою складових (елементів, компонентів), які в єдності утворюють нову якість не притаманну окремим елементам, що утворюють визначену єдність***.

Під кутом зору теорії організації (тектології), як складової теорії управління соціальними системами, організація, як вид соціальної діяльності містить у собі не тільки заходи визначення та упорядкування технічної

(інженерної, апаратної) структури якоїсь технічної (штучної, синтетичної, створеної руками людей) системи (машини, її агрегатів, деталей). Організація соціальної системи передбачає наявність управлінських заходів: визначення мети (цілі, підцілей), завдань, напрямів їх досягнення; формулювання методології, управлінської ідеології, принципів, методів, засобів, заходів, функцій, структур, операцій тощо. Багато з цих складових організації можуть бути і не правовими (тобто не визначеними у юридичних нормах, нормативно-правових актах), і не технічними. В тектології їх визначають як організаційно-управлінські. До них, зокрема, входять такі складові, як: аналіз і синтез; формулювання гіпотез, версій управлінських рішень; планування, підготовка і прийняття управлінських рішень; контроль, координація тощо. При цьому зазначені складові організації (організовування) може знаходити вираз (позначення) в таких правових формах як: техніко-юридичні чи юридико-технічні норми.

В теорії управління соціальними системами, для зручності усвідомлення та з`ясування сутності явища поділяють організаційні заходи на види: організаційно-технічні, організаційно-управлінські (адміністративні) та організаційно-правові. Останні знаходять вираз в нормах права.

З точки зору праксеології (науки про розумну, оптимальну, доцільну діяльність), як засоби соціального управління (керування), правила діяльності (дій чи бездій - утримання від небажаних дій) виражені в юридичних актах, нормах права виконують функцію типових моделей, алгоритмів функцій суб'єктів управлінських відносин. Зазначені положення мають відношення і до сфери захисту інформації (як до соціальної діяльності та як до сфери правовідносин). Тобто, з точки зору когнітології, кожне визначення (поняття, категорія) повинно викликати відповідну однозначну рефлексію щодо свідомої поведінки суб`єкта правовідносин (а не викликати ентропію). Це, в першу чергу, має відношення в оцінці суб'єктом правомірності свого діяння (дії чи бездії) та, відповідно, поведінки іншого суб`єкта правовідносин (чи інших суб`єктів). В теорії права це називається чітке визначення прав і обов`язків, зобов`язань осіб (фізичних та юридичних) у відносинах між собою. З точки зору теорії гри, це означає, що кожен з учасників суспільних відносин повинен чітко знати свою роль в суспільстві, роль інших, правила гри (суспільних відносин) і дотримуватися їх.

Виходячи з зазначених теоретичних положень подамо узагальнене наше бачення провідної категорії правовідносин, що розглядаються:

Захист інформації в автоматизованих (комп`ютерних) системах - це *комплексна підсистема організаційно-управлінських, організаційно-технічних та організаційно-правових заходів, засобів, методів, які здійснюються відповідними суб'єктами інформаційних відносин для запобігання заподіянню шкоди інтересам власника інформації чи автоматизованої системи та правомірних користувачів інформацією, яка обробляється, передається і/або зберігається на комп`ютерних носіях (в електронно-цифровому виразі); в разі виникнення делікту (правопорушення) вжиття правового впливу для відновлення реституції попереднього стану, покарання винного і відшкодування завданої матеріальної і моральної шкоди у відповідності з законодавством.*

Як висновок зазначимо, що зміст категорії "інформаційна безпека" сьогодні все більше і більше пов`язується з безпечним функціонуванням автоматизованих (комп`ютерних) систем у всіх галузях суспільної діяльності. Як говорить народна мудрість - "Визначившись в поняттях, люди вирішать половину своїх проблем".

Щодо понятійного апарату такої наукової дисципліни, як захист інформації, то це завдання сьогодні повинно вирішуватися на межі наук в межах правової інформатики та інформаційного права.

Не є таємницею, що антисоціальні прояви щодо порушення роботи АС можуть привести до значних порушень функціонування суспільства. Зокрема організовані злочинні формування, як свідчать дослідження практики, добре це розуміють і намагаються використати досягнення науково-технічного прогресу на свою користь. У зв`язку з цим існує нагальна потреба визначення та визнання також на науковому рівні організованої комп`ютерної злочинності як соціального явища і відпрацювання практичних, обгрунтованих заходів боротьби з нею.

Окремі аспекти проблематики висвітлені в публікаціях підготовлених автором особисто та у співавторстві:

Гавловський В.Д., Цимбалюк В.С. Щодо проблем боротьби із злочинами, що вчиняються з використанням комп'ютерних технологій //Боротьба з контробандою: проблеми та шляхи їх вирішення. -К. НДІ «Проблем людини».1998. С.148-154.

Гавловський В.Д., Цимбалюк В.С. Інформаційне право України. Навчально-методичний комплекс. -К. 1999.

Цимбалюк В.С., Гавловський В.Д., Корочанський О.Е. Проблеми юридичної деліктології в інформаційних відносинах \\Бизнес и безопасность. 1998. № 6 . С.19-21.

Гавловський В.Д. Інформаційне законодавство України: від інкорпорації до кодифікації //Систематизація законодавства в Україні: проблеми теорії і практики. Матеріали міжнародної науково-практичної конференції. -К. Інститут законодавства Верховної Ради України. 1999.

Гавловський В.Д., Камлик М.І. Законодавчі та інші нормативно-правові акти, спрямовані на боротьбу з організованою злочинністю та корупцією (параграф 5.2. Розділу V. Прогноз і правова база протидії організованій злочинності в Україні) // Організована злочинність в Україні /за ред. Я.Ю. Кондратьєва. - К.: НАВСУ, 1999. С. 94-107.

Гавловський В.Д., Цимбалюк В.С. Організована злочинність та інформаційні технології (параграф 3.5. Розділу III. Основні напрями та тенденції організованої злочинності в Україні) // Організована злочинність в Україні /за ред. Я.Ю. Кондратьєва. - К.: НАВСУ, 1999. С.73-78.

Романюк Б.В. Камлик М.І., Гавловський В.Д., Хахановський В.Г. Цимбалюк В.С. Виявлення та розслідування злочинів, що вчиняються за допомогою комп`ютерних технологій. Посібник /За ред. Я.Ю. Кондратьєва. - К. НАВСУ. 2000. - 64с.

УДК 681. 3: 34

ПРОБЛЕМИ КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА ВТРУЧАННЯ В РОБОТУ АВТОМАТИЗОВАНИХ СИСТЕМ (ст. 198[1] КК)

Петро Андрушко
Київський Національний університет імені Тараса Шевченка

Анотація: **Стаття присвячена проблемам кримінальної відповідальності за злочин проти нормальної роботи автоматизованих систем, у відповідності із законодавством України**.
Summary: **This article is devoted to the problems of the criminol responsibilitu for the commiting crimes against the normal work of the automation systems, acording to the Ukrainian laws.**
Ключові слова: **Злочин, автоматизовані системи, інформація, втручання в роботу, перекручення, знищення.**

Втручання у роботу автоматизованих систем (АС) є однією із двох форм вчинення злочину, передбаченого ст. 198[1] КК. Інша форма вчинення цього злочину – це розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекручення або знищення інформації чи то носіїв інформації. Зазначимо, що само по собі виготовлення таких програмних і технічних засобів не є злочином, за винятком випадків, коли метою такого виготовлення є їх наступне розповсюдження. У цьому разі дії особи мають кваліфікуватися як готування до вчинення злочину у формі розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекручення або знищення інформації чи носіїв інформації. Названі програмні і технічні засоби і є предметом цього злочину.

Під розповсюдженням програмних і технічних засобів, призначених для незаконного проникнення в АС і здатних спричинити перекручення або знищення інформації чи носіїв інформації треба розуміти: 1) їх передачу будь-яким способом і на будь-яких підставах (продаж, дарування, обмін, надання можливості скопіювати тощо) з метою їх використання для несанкціонованого доступу до інформації особами, які згідно з правилами розмежування доступу до інформації, встановленими власником інформації чи уповноваженою ним особою, не мають права доступу до такої інформації; 2) їх "закладку" в АС на стадії її виготовлення, ремонту, реалізації, користування з метою використання в майбутньому для здійснення несанкціонованого доступу до інформації; 3) ознайомлення інших осіб із змістом програмних засобів чи технічними характеристиками або технологією виготовлення та використання програмних і технічних засобів для незаконного проникнення в АС.

Програмні засоби, призначені для незаконного проникнення в АС, — це спеціальні комп'ютерні програми (програмні блоки, програмне забезпечення), з допомогою яких можна здійснити несанкціонований доступ до інформації, яка зберігається чи обробляється в АС, і які здатні спотворити або знищити інформацію (її носії) шляхом спотворення процесу обробки інформації.

Технічні засоби, призначені для незаконного проникнення в АС — це різного роду прилади, обладнання, устаткування тощо, з допомогою яких можливе або безпосереднє підключення до АС чи каналів передачі даних, або які здатні шляхом формування сигналів, полів, середовищ створити умови для несанкціонованого доступу до інформації з метою ознайомлення з такою інформацією особами, які не мають права доступу до неї, або з метою впливу на процес обробки інформації в АС, порушення роботи АС, перекручення або знищення інформації чи її носіїв.