УДК 004.056.5 (045)

Т.М. ВОЙТЕШЕНКО, фахівець 1-ї категорії наукової лабораторії проблем інформаційного права Науково-дослідного центру правової інформатики Національної академії правових наук України

ПРАВОВІ АСПЕКТИ ОХОРОНИ ТА ЗАХИСТУ ІНФОРМАЦІЇ В КОМП`ЮТЕРНИХ СИСТЕМАХ

Анотація. *Щодо проблем визначення поняття “безпека інформації”, а також класифікації основних засобів її охорони і захисту в комп`ютерних системах в органах державної влади.*

Аннотация. *О проблемах определения понятия “безопасность информации”, а также классификации основных средств ее охраны и защиты в компьютерных системах в органах государственной власти.*

Summary. *On the problems of determination of the notion ‘safety of the information’, as well as classification of main methods of its security and protection of the computer systems at the public authorities.*

Ключові слова: безпека інформації, охорона і захист інформації.

На сучасному етапі розвитку глобального інформаційного суспільства гостро постає проблема інформаційної безпеки. Це викликано тим, що інформація є не тільки об’єктом співпраці, а й суперництва. У свою чергу інформаційна безпека стає важливим чинником підтримки життєво важливих інтересів будь-якої держави у всьому світі. Наразі слід звернути увагу на ті якісні зміни у процесах управління на всіх рівнях, обумовлені інтенсивним впровадженням сучасних інформаційних технологій, а також на паралельно зростаючу небезпеку можливості просочення та несанкціонованого доступу до інформації зі злочинною метою.

Ця проблема торкнулася і діяльності державних органів різних рівнів, у яких застосовуються засоби електронної обчислювальної техніки. Напрями застосування комп'ютерів цими органами постійно розширюються: формування правоохоронних обліків різної спрямованості, накопичення службової інформації, складання документів різного рівня доступу. Розвиток засобів, методів та форм автоматизації процесів обробки інформації, поширення застосування комп’ютерів роблять інформацію набагато вразливішою.

Отже, саме ці причини змушують правлячі кола країн все більше і більше приділяти уваги проблемам охорони та захисту інформації та пошуку шляхів її вирішення. Не відстає в цьому питанні й Україна. В нашій державі активно впроваджуються ряд важливих для суспільства інформаційно-телекомунікаційних систем, мереж зв’язку, передачі даних, систем прийняття рішень.

Актуальність обраної теми полягає також в наступному:

- постійно існують реальні загрози витоку, блокування або порушення цілісності інформації, що становить державні інформаційні ресурси;
- можливість руйнування та дезорганізації інформаційної інфраструктури держави прирівнюються за наслідками до застосування зброї масового знищення.

Метою роботи є висвітлення результатів дослідження правових аспектів охорони та захисту інформації в комп’ютерних системах в органах державної влади.

*Об`єктом* дослідження виступають суспільні відносини щодо охорони та захисту інформації в комп`ютерних системах в органах державної влади.

Предметом дослідження є окремі правові аспекти охорони та захисту інформації в

комп’ютерних системах в органах державної влади.

Методологія дослідження базується на системному підході, що дозволяє розглянути суспільні відносини як систему – множину взаємопов’язаних елементів, які в єдності утворюють нову якість, не притаманну її складовим охорони та захисту інформації в комп’ютерних системах.

Слід зазначити, що окремі результати дослідження апробовані на конференціях, круглих столах тощо та у складі ініціативної групи дослідників при розробці проекту Кодексу України про інформацію в Науково-дослідному центрі правової інформатики Національної академії правових наук України.

Розробкою даної проблематики займалися ряд науковців, серед яких Брижко В.М., Цимбалюк В.С., Голубєв В.О., Гавловський В.Д., Хорошко В.О., Лазарєв Г.П., Куранов О.І., Шміт М.Н. та інші.

Широке впровадження комп’ютерних інформаційних технологій у сферах державної діяльності, економіки, фінансів, банківської справи тощо зумовило підвищення вимог до безпеки інформації в комп’ютерних системах [8, с. 12]. У цьому контексті поняття “безпека інформації” розуміють у таких аспектах:

- технічному або технологічному: безпека змістовної частини (змісту) інформації – відсутність спонукання людини до негативних діянь, навмисно закладених механізмів негативного впливу на людську психіку або негативний вплив на інший блок інформації (наприклад, інформацію, що міститься в програмі для ЕОМ, іменованою комп’ютерним вірусом);
- правовому: захищеність інформації від зовнішніх впливів (спроб неправомірного копіювання, поширення, модифікації (зміни змісту) або знищення).

Але особливої гостроти це питання набуло в контексті появи нової гілки правопорушень, так званих комп'ютерних злочинів. Для законодавчого забезпечення вирішення цієї проблеми Верховною Радою України був прийнятий Закон України “Про захист інформації в інформаційно-телекомунікаційних системах” (далі – Закон) [3].

Дія Закону поширюється на будь-яку інформацію, що обробляється в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Згідно з цим Законом об’єктами суспільних відносин у системі є інформація, що обробляється в комп’ютерних системах, та програмне забезпечення, яке призначено для обробки цієї інформації. Цим Законом встановлюються об’єкти не стільки правового захисту, скільки охорони: інформація, що обробляється, та програмне забезпечення, яке призначено для обробки цієї інформації. Безпосередньо встановлені загальні вимоги не стільки щодо захисту, скільки стосовно охорони інформації (ст. 8) та декларативний обов'язок винних осіб понести дисциплінарну, адміністративну, кримінальну чи матеріальну відповідальність за порушення вимог закону (ст. 11).

На цьому ґрунті виникала проблема: розмежування комп`ютерних злочинів і проступків, за які може наступати адміністративна, дисциплінарна чи матеріальна відповідальність. Голубєв В.О. вважає, що встановлення кримінальної відповідальності буде доцільним лише у випадках заподіяння великої шкоди, тобто склади відповідних злочинів за конструкцією повинні бути матеріальними. При відсутності злочинних наслідків або при незначних розмірах заподіяної шкоди особа повинна нести адміністративну відповідальність. Стосовно останнього можуть бути склади правопорушень, передбачені Кодексом України про адміністративні правопорушення (далі – КУпАП), а саме:

- ст. 186-3 (порушення порядку подання або використання даних державних статистичних спостережень);

• ст. 195-5 (незаконне придбання або зберігання спеціальних технічних засобів для зняття інформації з каналів зв’язку, інших засобів негласного отримання інформації);

• ст. 212-2 (порушення законодавства про державну таємницю);

• ст. 212-3 (порушення права на інформацію);

• ст. 212-5 (порушення порядку обліку, зберігання і використання документів та інших носіїв інформації, які містять конфіденційну інформацію, що є власністю держави);

• ст. 212-6 (здійснення незаконного доступу до інформації в автоматизованих системах).

Дисциплінарна відповідальність наставатиме за скоєння подібних діянь (при відсутності злочинних наслідків) спеціальним суб’єктом – персоналом, що обслуговує автоматизовані системи, співробітниками відділів чи інших структурних одиниць, обсяг професійних обов’язків яких включає обробку інформації чи надання інформаційних послуг [8, с. 17].

Слід зазначити, що на сьогодні досліджувана проблема частково вирішена на рівні кримінального законодавства: у Кримінальному кодексі України (2001 року) передбачено розділ XVI “Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку”.

Не можна не звернути увагу на досить невдалу назву вищезгаданого Закону. Згідно із законами формальної логіки поняття “захист” передбачає наявність активних дій правопорушника, тобто посягань. У свою чергу поняття “охорона” переважно включає в себе загрозу посягань. З цього слідує, що питання, пов’язані з поняттям “захист” регулюються Кримінальним кодексом України або Кодексом України про адміністративні правопорушення. Тому доцільніше було б назвати даний Закон – Законом України “Про охорону інформації в інформаційно-телекомунікаційних системах”, а якщо врахувати, що він містить і цивільно-правові положення – то Законом України “Про інформацію в інформаційно-телекомунікаційних системах”.

Як показує практика, для боротьби з правопорушеннями у сфері комп’ютерної інформації необхідно адекватно вибирати заходи і засоби охорони та захисту інформації від просочування та несанкціонованого доступу до неї. Необхідно також законодавчої структурувати велику кількість законодавчих положень в цій сфері суспільних відносин.

Загалом, усі засоби охорони і захисту інформації в комп`ютерних системах, що наразі існують, спрямовані на:

• забезпечення захисту інформації від неправомірного доступу, знищення, модифікування, блокування, копіювання, надання, поширення, а також від інших неправомірних дій щодо такої інформації;

• дотримання організаційно-правового режиму обмеженого доступу до вірогідної інформації;

• реалізацію права на доступ до інформації з урахуванням правового режиму доступу.

Необхідно зауважити, що ефективність систем безпеки інформації залежить від:

по-перше, реалізації цілого ряду різних заходів, які мають базуватися на наступних принципах:

• нормативно-правова база інформаційних відносин у суспільстві чітко регламентує механізми забезпечення прав громадян вільно шукати, одержувати, виробляти й поширювати інформацію будь-яким законним способом;

• інтереси власників інформації гарантовано охороняються законом;

• засекречування (закриття) інформації є виключенням із загального правила на доступ до інформації;

• відповідальність за збереження інформації, її засекречування й розсекречування персоніфікується;

• розвиток сфери інформаційних послуг, що надаються населенню й фахівцям на основі сучасних комп'ютерних мереж, системи загальнодоступних баз і банків даних, що містять довідкову інформацію соціально-економічного, культурного й побутового призначення, право доступу до яких гарантується й регламентується законодавством,

по-друге, розробки засобів охорони і захисту, якими повинні займатися фахівці з відповідних галузей знань. Природно, що кожний з фахівців по-своєму вирішує завдання інформаційної безпеки й застосовує свої способи й методи для досягнення заданих цілей. При цьому кожний з них у своєму конкретному випадку знаходить свої найбільш ефективні рішення, але ці рішення повинні узгоджуватися відповідно до законодавства.

Охорона і захист інформації викликає необхідність системного підходу, тобто тут не можна обмежуватися окремими фрагментарними заходами. Системний підхід до охорони і захисту інформації вимагає, щоб засоби й дії, що застосовують для інформаційної безпеки, розглядалися як єдиний комплекс взаємозалежних, взаємодоповнюючих і взаємодіючих заходів. Один з основних принципів системного підходу до охорони і захисту інформації – принцип “розумної достатності”, суть якого зводиться до того, що стовідсоткової гарантії не існує ні за яких умов, тому прагнути варто не до теоретично максимально досяжного рівня безпеки, а до мінімально необхідного в даних конкретних умовах і при даному рівні ймовірно можливих загроз. При цьому існує потреба і визначення нових загроз, що зумовлює постійний моніторинг відносин в інформаційній сфері.

Для охорони і захисту інформації використовують переважно такі засоби:

• організаційно-технічні, засновані на створенні фізичних перешкод для зловмисника чи до особи, яка веде себе безпечно. До них відносять зберігання носіїв і пристроїв у сховищах, фільтри, екрани на апаратуру, ключ для блокування клавіатури, блокування екрана й клавіатури. Ці засоби дають захист тільки від “зовнішніх” зловмисників і не захищають інформацію від тих осіб, які володіють правом входу в приміщення [11, с. 40];

• організаційно-правові – засновані на застосуванні законодавчих актів, які регламентують правила обробки інформації обмеженого доступу, а також визначають кримінальну відповідальність за порушення норм законодавства;

• організаційно-управлінські – підбір, виховання, навчання кадрів, застосування примусу та заохочення, пропускний режим, обмеження доступу осіб у комп’ютерні приміщення тощо;

• організаційно-технологічні – до них можна віднести криптографію, шифрування, програмний контроль доступу, цифровий підпис.

Отже, на нашу думку, застосування даних заходів є необхідним елементом забезпечення охорони та захисту інформації в комп`ютерних системах в органах державної влади. Ці заходи, в свою чергу, мають здійснюватися за такими основними напрямами:

• чітке нормативне закріплення порядку проведення робіт і надання послуг заінтересованим особам у сфері інформаційної безпеки;

• підготовка і перепідготовка національних кадрів для роботи в сфері інформаційної безпеки: юристів, інженерів, менеджерів та інших;

• створення вітчизняної інфраструктури розробки, виробництва, впровадження та експлуатації засобів охорони і захисту інформації;

• прийняття нових державних стандартів, які адекватно регламентували б такі явища, як життєвий цикл інформаційних систем, ефективність системи охорони і захисту інформації, а також містили чіткий перелік критеріїв оцінки рівня безпеки інформації в інформаційно-телекомунікаційних системах.

На сьогодні для підтримки інформаційної безпеки держави вже здійснені перші кроки, що допоможуть частково реалізувати все вищенаведене. Серед цих кроків особ-

ливу увагу слід приділити таким організаційно-правовим заходам:

1. Удосконалення правової основи загальнодержавної системи інформаційної безпеки.
2. Встановлення дієвого державного контролю за такими напрямами: ввезення імпортних засобів електронно-обчислювальної техніки, моніторинг інформаційної безпеки в системах зв`язку у певному просторі, колі осіб і часі.
3. Вдосконалення системи сертифікації систем та засобів охорони і захисту інформації, програмних та апаратно-програмних засобів, що застосовуються тими, хто професійно надає послуги через Інтернет (оператори, провайдери).
4. Створення ефективної системи підготовки/перепідготовки професійних кадрів у галузі інформаційної безпеки (юристів, інженерів, менеджерів та інших).
5. Відтворення системи обов’язкових органів контролю за станом інформаційної безпеки на підприємствах та контроль за їх діяльністю з боку держави.
6. Розвиток системи державної допомоги для створення приватних підприємств і установ, які займалися б розробкою і створенням ефективних систем захисту інформації в комп`ютерних системах, та державної закупівлі таких систем у розробників.
7. Врегулювання відносин у галузі використання Інтернету, і в першу чергу стосовно безпеки державних інформаційних ресурсів.
8. Розвиток системи інформаційної безпеки, яка спроможна підтримувати належний рівень її захищеності в умовах постійного удосконалення можливостей технічних розвідок та засобів ведення інформаційних війн.

Висновки.

Як висновок, треба зазначити, що інститут охорони та захисту інформації в комп`ютерних системах з кожним роком набуває все більшої актуальності в кожній країні, і Україна не є виключенням. Тому, на мою думку, необхідним є створення і затвердження проекту Кодексу України про інформацію, який містив би розділ про національну інформаційну безпеку, що в свою чергу не лише закріплював б положення про охорону та захист інформації в комп’ютерних системах не тільки в органах державної влади, а й встановлював конкретні зобов’язання державних органів стосовно підтримки інформаційної безпеки держави в Інтернеті. У сфері адміністративного законодавства статтю 212-6 КУпАП доцільніше було б назвати “Здійснення незаконного доступу до інформації в інформаційно-телекомунікаційних системах” згідно з назвою Закону України – “Про захист інформації в інформаційно-телекомунікаційних системах”.

Кваліфікований підхід до побудови системи охорони і захисту інформації в інформаційно-телекомунікаційних системах має на увазі конкретну оцінку імовірних виявів загроз на конкретній комп`ютерній системі.

Кожному підприємству, установі, організації залежно від конкретних умов їх роботи потрібна своя система охорони і захисту інформації. Визначення такої системи можливе лише на аудиторських умовах спеціально залученими фахівцями і фірмами, що повинні мати ліцензію на здійснення вказаної діяльності. Розглянувши теоретичні положення щодо охорони і захисту інформації в комп`ютерних системах, потрібно зазначити, що комплексна інформаційна безпека в автоматизованих системах має в своїй основі застосування організаційно-технічних, організаційно-правових, організаційно-управлінських та організаційно-технологічних заходів.

Використана література

1. Конституція України, прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 року 28 червня 1996 року № 254к/96-ВР // Відомості Верховної Ради України. – 1996. – № 30.
2. Про інформацію : Закон України від 02.10.92 р. (із змінами та доповненнями). – Режим

доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2657-12

3. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.94 р. (із змінами та доповненнями). – Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=80%2F94-%E2%F0

4. Про рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні: Постанова Верховної Ради від 01.12.05 р. (із змінами та доповненнями). – Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=3175-15

5. Про Положення про порядок здійснення криптографічного захисту інформації в Україні : Указ Президента України від 22.05.98 р. (із змінами та доповненнями). – Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=505%2F98.

6. Про внесення змін до наказу Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України : Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України від 22.10.99 р. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=z0022-05

7. Цимбалюк В. С. Організація та координація боротьби з організованою транскордонною кіберзлочинністю // Право України. – 2003. – № 2. – С. 35-39.

8. Голубєв В.О. Правові аспекти захисту інформації в автоматизованих системах // Юрист. – 2007. – № 5. – С. 12-19.

9. Голубєв В. О. Проблеми боротьби зі злочинами у сфері використання комп’ютерних технологій : навч. посібник / В.О. Голубєв, В.Д. Гавловський, В.С. Цимбалюк ; за заг. ред. доктора юридичних наук, професора Р. А. Калюжного. – Запоріжжя : ГУ “ЗІДМУ”, 2002. – 292 с.

10. В.М. Брижко. е-боротьба в інформаційних війнах та інформаційне право : монографія / В.М. Брижко, М.Я. Швець, В.С. Цимбалюк. – К. : ТОВ “ПанТот”, 2007 р. – 234 с.

11. Лазарєв Г.П., Кльоцкін С.М., Хорошко В.О. Шляхи вирішення проблеми інформаційної безпеки в Україні // Вісник УАДУ. – 2000р. – № 4. – С.43-46.

12. Куранов А.И. Безопасность банковской информации // Системы безопасности. – 1995. – № 4. – С. 32-42.

13. Schmitt M.N. Preemptive Strategies in International Law // International Law. − 2002. − № 513. – P. 525-532.

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