Петренко Т.А.
Викладач кафедри фінансів, управління
персоналом та економіки праці

ІНФОРМАЦІЙНА БЕЗПЕКА В СУЧАСНИХ УМОВАХ

Інформаційні системи все більше ускладнюються, взаємозалежність між різноманітними компонентами вже не завжди очевидна, та інформаційна безпека набуває таким чином все більш глобального характеру, виходячи у більшості випадків на перший план.

XXI ст. перед суспільством з погляду безпеки поставило цілу низку нових проблем. Процеси глобалізації дуже гостро дали про себе знати й, окрім позитивних елементів, були й серйозні негативні явища, до яких світова спільнота виявилася не готовою. Виклики, пов'язані з глобалізацією, завдали колосальних збитків майже всім країнам.

Явища глобалізаційного характеру у інформаційній та телекомунікаційній сферах дуже гостро поставили питання про охорону національної самоідентичності, оскільки в цьому аспекті є величезна загроза.

Слід відмітити, що в силу суб'єктивних факторів категорія "інформаційна безпека" сьогодні розглядається в Україні і за кордоном переважно у організаційно-управлінському та інженерно-технологічному аспектах, що, на мою думку, не зовсім правильно і в майбутньому може призвести до неправильного формування державної політики.

Виходячи з правового аналізу інформаційного законодавства України, інформаційна безпека виступає одним із багатьох його провідних багатоаспектних чинників (об'єктом правовідносин). Таким чином, можна подати зміст інформаційної безпеки у контексті окремих організаційно-правових аспектів наступним чином. Інформаційна безпека - це суспільні правовідносини щодо процесу організації створення, підтримки, охорони та захисту необхідних для особи (людини чи юридичної особи, установи, підприємства, організації), суспільства і держави безпечних умов їх життєдіяльності; суспільні

правовідносини пов’язані із організацією технологій створення, розповсюдження, зберігання та використанням інформації (відомостей, даних, знань) для забезпечення функціонування і розвитку інформаційних ресурсів людини, суспільства, держави.

Тривалий час методи захисту інформації розробляли лише державні органи, а їх впровадження розглядалось як виключне право тієї чи іншої держави. Однак в останні роки з розвитком комерційної та підприємницької діяльності збільшилась кількість спроб несанкціонованого доступу до конфіденційної інформації, а проблеми її захисту стали у центрі уваги багатьох учених та фахівців різних країн.

Захист інформаційного суверенітету тісно пов’язаний із поняттям інформаційної безпеки, що може бути розглянута, з одного боку, як захищеність внутрішньої інформації як такої, що припускає захищеність якості інформації, її надійність, захищеність різних галузей інформації (державної, банківської, комерційної таємниці) від розголошення; захищеність інформаційних ресурсів. З іншого боку, інформаційна безпека означає контроль над інформаційними потоками, обмеження використання провокаційної, ворожої суспільної інформації, включаючи контроль над рекламою; захист національного інформаційного простору від зовнішньої інформаційної експансії.

Ще одним важливим аспектом інформаційної безпеки є захист комп’ютерної інформації від розкрадань. Державна політика забезпечення інформаційної безпеки, будучи складовою частиною політики національної безпеки, припускає системну превентивну діяльність органів влади щодо забезпечення гарантій інформаційної безпеки особистості, соціальних груп і суспільства в цілому.

Існує багато різних засобів несанкціонованого доступу до інформації. Але слід одразу ж відмітити, що ніякий окремо взятий засіб захисту не в змозі гарантувати адекватну безпеку. Надійний захист можливий лише за умови створення механізму комплексного забезпечення безпеки. Можна виділити три основні складові такого комплексу:

- нормативно-правові;
- технічні;

– організаційні засоби.

Нормативно-правові засоби захисту визначаються законодавчими актами держави, які регламентують правила використання, обробки та передачі інформації обмеженого доступу та встановлюють ступінь відповідальності за порушення цих правил. У ст. 34 Конституції України розглядається право громадян України на інформацію, забезпечення інформаційних процесів. Ця та деякі інші статті Конституції мають стати основою розвитку інформаційного законодавства. Невідповідність чинного законодавства України сучасним вимогам інформаційного розвитку є однією з основних проблем щодо захисту інформації, яка за наявності в державі потужного науково-технічного потенціалу може призвести до особливо тяжких наслідків.

Вся сукупність технічних засобів поділяється на фізичні та апаратно-програмні та включає в себе електричні, механічні, електромеханічні та електронні пристрої. Фізичні засоби реалізуються у вигляді автономних пристроїв та систем, що виконують функції загального захисту об’єктів, на яких обробляється інформація. Апаратні технічні засоби розміщують безпосередньо в обчислювальній техніці, в телекомунікаційній апаратурі чи в пристроях, що зв’язані з подібною апаратурою за допомогою стандартного інтерфейсу. Програмні засоби є програмним забезпеченням, що виконує функції захисту інформації.

Організаційні засоби захисту поділяються на організаційно-технічні та організаційно-правові, які використовуються в процесі створення та функціонування будь-якої структури. Інакше кажучи, тільки на основі нормативно-правової бази та за наявності апаратно-програмних засобів можливе ефективне керування в умовах широкого впровадження нових інформаційних технологій. Практика сьогодення свідчить про недооцінювання цих питань керівниками різних організацій.

Таким чином, інформаційна безпека не зводиться до комп’ютерної безпеки, як, утім, і поняття інформатизації не зводиться до поняття комп’ютеризації (інформатизація включає соціально-економічне, організаційно-правове, політичне забезпечення і т.д.). Комп’ютерна безпека стосується лише охорони устаткування

і інформації в ЕОМ від саботажу, порушення правил технічної експлуатації, присвоєння майна, стихійних лих, нанесення навмисного чи випадкового збитку і т.д. Інформаційна безпека, включаючи в себе комп'ютерну безпеку в якості необхідної складової, поширюється на всі соціальні процеси, у яких функціонує інформація і використовується інформатика.

Серед негативних наслідків інформатизації, викликаних порушенням інформаційної безпеки, – комп’ютерний тероризм і комп’ютерне хуліганство. “Телефонний фанатик”, “хакер”, “крекер” – вираження сьогоднішнього лексикона. Якщо хакери проникають у пам’ять комп’ютеризованих систем для задоволення особистих амбіцій, то крекери ще і “викачують” інформаційні банки. Подібні “фахівці” катастрофічно небезпечні для комп’ютерних систем, керуючих бойовими ракетами, космічною і ядерною зброєю. До яких наслідків може привести їхнє “професійне” втручання, догадатися неважко. Це може стати трагедією не тільки для однієї країни, але і для всього людства.

Далеко не небезпечний вплив комп’ютерів, особливо персональних, на здоров’я людини, його психіку. По-перше, у більшості використовуваних в утворенні і побуті ЕОМ перевищена норма випромінювань від монітора. Дисплей сильніше телевізора впливає на зір, викликає розумові перевантаження і швидке стомлення нервової системи, сприяє виникненню психічних захворювань. Сьогодні ніхто не може сказати, який вплив комп’ютера на біосферу, його вплив на живі організми. По-друге, поширення ПЕОМ і інших подібних досягнень електроніки буде сприяти посиленню в людях психології індивідуалізму, підриву колективістських початків. Це побоювання не позбавлене основ: комп’ютерна та інша інформаційна техніка індивідуального користування і справді обмежує спілкування людей (партнером людини в роботі, навчанні, грі, на відпочинку всі частіше буде ЕОМ), може повести людини від реальності у світ мрій, створити штучний замінник дійсності і тим самим підсилити соціальну ізоляцію.

“Комп’ютерні” небезпеки прогнозувалися ще на зорі розвитку кібернетичного знання. Але то були утопічні застереження. Сьогодні у зв’язку з появою “дружньої” та інтелектуальної, що не має своїх корисливих інтересів ЕОМ, вона несе реальну погрозу ізоляції людини від інших людей, що може

привести навіть до розпаду родини. У техноцентрованих людей відбувається навіть зміна поглядів на любов і сексуальне життя. Сексуальність у таких випадках не стільки придушується, скільки контролюється і розглядається як полегшення напруги, але не як позитивний стимул.

По-третє, при використанні комп'ютера виникає явище, називається технострес. Це зовсім нова, сучасна хвороба адаптації, викликана нездатністю здоровим образом реагувати на неординарну інформаційно-комп'ютерну технологію. Виділяються кілька процесів, пов'язаних з адаптацією і розвитком нових інформаційних технологій. По-перше, це розумове перевантаження та утома, ступінь якої зростає все більше і більше. Крім того, комп'ютери призводять до централізації, а остання збільшує помилки, що можуть викликати серйозні наслідки і для виправлення яких часто немає часу. По-друге, це постійний контроль, спостереження за роботою та її якістю з боку ЕОМ. Тісна залежність праці робітника від машини, його предзаданість програмою викликають неприйняття, протест, почуття інформаційної незахищеності.

Ще один парадокс інформатизації, медіатизації і комп'ютеризації полягає в тім, що вміння використовувати інформаційні технології стимулює розвиток інтелектуальних здібностей в одному відношенні, але в той же час може негативно позначитися на них в іншому. Подібних прикладів в історії техніки чимало. Сучасні транспортні засоби полегшили людині переміщення в просторі. Але одночасно з'явилося і таке явище, як гіподинамія. За аналогією можна говорити і про свій рід "інтелектуальної гіподинамії", тобто утрудненнях і здійсненні рутинних операцій, наприклад елементарного зчитування.

Україна, з огляду на її геополітичне положення, цілком може використовуватися як своєрідний полігон боротьби національних інтересів ведучих країн світу. Крім того, на чисто політичні моменти органічно накладаються і загальносвітові тенденції діалогу країн "першого" і "третього" світу. Ні для кого не секрет, що існуючі могутні політичні сили, що намагаються забезпечити соціально-економічну стабільність у розвинутих країнах за рахунок закріплення їхнього пануючого положення у світі, нарощування розриву з непривілейованою більшістю. При цьому, якщо раніш, у колоніальну епоху,

основний розрахунок будувався на могутності збройних сил, то в наш час розвинуті країни орієнтовані на економічне панування, експлуатацію ресурсів інших народів і використовують в основному невоєнні засоби: формування в цих країнах маріонеткових компрадорських еліт, морально-духовне поневолення через тиражовані ЗМІ зразки псевдокультури.

Література

1. Маракова І., Рибак А., Тесленко П. Проблеми комплексного забезпечення безпеки інформації в Україні // Вісник УАДУ. – 2001 р.– № 3. – С. 343-346.

2. Митилино С. Безопасность и человеческий фактор // Компьютерное обозрение. – № 27. – 11 июля 2001 г.– С. 42-43, 47.

3. Несвіт Г.П. Інформаційна політика держави як фактор реформування суспільства: Автореф. дис. на здобуття наук. ступ. канд. політ. наук; Одес. нац. юрид. Акад. – О., 2001. – 16 с.

4. Конституція України: Прийнята на п’ятій сесії Верховної Ради України 28 червня 1996 р. – К.: Парламент, вид-во, 1999. – 95 с.

6. Информационная безопасность в условиях информатизации общества.– http://www.ase.moldnet.md/~osa/Publication/pubru06.html

7. Роговец В.И. Информационные войны в современном мире: причины, механизмы, последствия. // Персонал.– 2000.– № 5 (59).– С. 35-38.