УДК 658.012.4(07)

Т. П. МАКАРОВСЬКА
Міжрегіональна Академія управління персоналом, м. Київ

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ ЯК ПЕРЕДУМОВА ЇЇ ВСТУПУ ДО СОТ

Наукові праці МАУП, 2006, вип. 2(14), с. 45–47

Розглянуті напрями державної політики щодо гарантування інформаційної безпеки України. Наведені основні джерела загроз інформаційній безпеці держави. Перелічені засоби впливу загроз на інформаційну безпеку за напрямами: інформаційні, програмно-математичні, фізичні, радіоелектронні. Зазначені першочергові заходи щодо забезпечення інформаційної безпеки України.

В умовах глобалізації трансферту інформаційних технологій, коли понад 70 % світового сукупного національного продукту так чи інакше залежить від інформації, що зберігається в інформаційних системах, економічна безпека кожної держави визначається передусім її інформаційною безпекою.

Глобалізація комп'ютерних мереж створила для бізнес-діяльності не тільки відомі зручності та переваги, а й певні проблеми. Ідеться як про прямі крадіжки, втрати даних персональних комп'ютерів фірм, несанкціоноване зовнішнє підключення до комп'ютерної мережі компаній, так і про використання доступу до інформаційних систем самими співробітниками, здійснення ними, наприклад, трансфертних операцій для переказу грошей на приватні банківські рахунки, цільові програми "вірусних нападів". Загалом через інформаційну вразливість втрати західних компаній щорічно сягають сотень мільярдів доларів [4]. Настав час перейматися подібними проблемами і в Україні.

На сучасному етапі в Україні немає реальних гарантій її інформаційної безпеки, відсутній комплекс нормативно-правових актів щодо захисту інформаційних ресурсів та інформаційної інфраструктури. Процес інформатизації просувається стихійно та некеровано, з переважним ухилом у бік використання засобів інформатизації іноземного виробництва.

Безсистемність процесів формування інформаційної інфраструктури України зумовлює складність розв'язання проблеми інформаційної безпеки, захисту інформаційних ресурсів на рівні як держави, так і окремої організації, підприємства, фірми. Специфіка цих проблем полягає в тому, що об'єктивно достатній рівень захищеності інформаційної інфраструктури та інформаційних ресурсів може бути досягнутий тільки шляхом чіткого визначення об'єктів інформаційної безпеки України, забезпечення надійного функціонування державних і суспільних інститутів для реалізації практичних заходів щодо захисту інформації [1].

Таким чином, за умови входження України до СОТ актуальність питання організації її інформаційної безпеки, приведення методів запобігання та ліквідації загроз до міжнародних стандартів не викликає сумнівів.

Інформаційна безпека відіграє суттєву роль у забезпеченні життєво важливих інтересів будь-якої країни. Основним завданням у забезпеченні інформаційної безпеки в Україні є створення розгалуженого та захищеного інформаційного простору, захист національних інтересів України в умовах формування світових інформаційних мереж, захист економічного потенціалу держави від незаконного використання інформаційних ресурсів, реалізація прав громадян, установ і самої держави на отримання, поширення та використання інформації.

З цією метою урядом України була розроблена Концепція національної інформаційної політики, дев'ятий розділ якої присвячений саме проблемам

© Т. П. Макаровська, 2006

інформаційної безпеки [2]. Згідно з цією Концепцією, державна політика забезпечення інформаційної безпеки України полягає в наступному:

- у забезпеченні конституційних прав людини на доступ до інформації, використанні інформації в інтересах здійснення не забороненої чинним законодавством діяльності, фізичного, інтелектуального й духовного розвитку, а також у захисті інформації, що стосується особистої безпеки громадянина;
- у створенні умов для гармонійного розвитку інформаційної структури, для реалізації конституційних прав і свобод людини й громадянина у сфері отримання інформації та використання її з метою забезпечення непорушності конституційного ладу, суверенітету й територіальної цілісності України, політичної, економічної та соціальної стабільності, безумовного забезпечення законності й правопорядку, розвитку та взаємовигідного міжнародного співробітництва.

Державна політика ґрунтується на таких засадах забезпечення інформаційної безпеки:

- дотримання конституційних прав і свобод людини й громадянина у сфері отримання інформації і користування нею, забезпечення духовного відродження України, зберігання і зміцнення моральних цінностей суспільства, традицій патріотизму й гуманізму, культурного й наукового потенціалу;
- здійснення інформаційного забезпечення державної політики України, пов'язане з доведенням до української та міжнародної громадськості достовірної інформації про державну політику України, її офіційну позицію стосовно соціально значущих подій українського та міжнародного життя, забезпечення доступу громадян до відкритих інформаційних ресурсів;
- розвиток сучасних інформаційних технологій, вітчизняної індустрії інформації, у тому числі індустрії засобів інформатизації, телекомунікації і зв'язку, забезпечення потреби внутрішнього ринку її продукцією і вихід цієї продукції на світовий ринок, а також забезпечення накопичення, зберігання та ефективного використання вітчизняних ресурсів;
- захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки інформаційних і телекомунікаційних систем як наявних, так і тих, що створюються на території України.

До джерел загроз інформаційній безпеці нашої держави належать такі:

- недружня політика іноземних держав у галузі глобального інформаційного моніторингу;
- цілеспрямована підривна діяльність іноземних спецслужб, політичних та економічних структур;
- злочинна діяльність міжнародних угруповань, формувань та окремих осіб;
- неправомірна чи протиправна діяльність посадових осіб державних органів, структур, формувань, спрямована проти інтересів України;
- некерований характер процесу створення інформаційної інфраструктури України;
- недосконалість технічних та програмних засобів й недостатня кваліфікація персоналу інформаційних служб і систем;
- недосконалість, неповнота і неузгодженість із відповідними міжнародними правовими актами чинного законодавства України в інформаційній сфері;
- недостатній розвиток лексикографічної бази української мови і національного лінгвістичного забезпечення інформаційних систем;
- низькі темпи науково-технічного і культурного розвитку суспільства внаслідок економічної кризи або неадекватної внутрішньої політики держави в інформаційній сфері;
- низька правова, організаційна та програмно-технічна забезпеченість у галузі інформаційної безпеки.

Засоби впливу загроз на інформаційну безпеку поділяються на інформаційні, програмно-математичні, фізичні, радіоелектронні, організаційно-правові [4].

До *інформаційних засобів* належать:

- порушення адреси і своєчасності інформаційного обміну, протизаконні збір і використання інформації;
- несанкціонований доступ до інформаційних ресурсів;
- маніпулювання інформацією (дезінформація, приховування та викривлення інформації);
- незаконне копіювання інформації в інформаційних системах;
- використання засобів масової інформації з позицій, які суперечать інтересам громадян, організацій чи держави;

- викрадення інформації з бібліотек, архівів, банків і баз даних;
- порушення технології обробки інформації.

До *програмно-математичних засобів* належать:

- запуск програм-вірусів;
- установка програмних і апаратних ретранслюючих пристроїв;
- знищення або модифікація даних в інформаційних системах.

До *фізичних засобів* належать:

- знищення або руйнування засобів обробки інформації та зв'язку;
- знищення, руйнування чи викрадання оригінальних носіїв інформації;
- викрадання програмних чи апаратних ключів і засобів криптографічного захисту інформації;
- постачання "інфікованих" компонентів інформаційних систем.

До *радіоелектронних засобів* належать:

- перехоплення інформації в технічних каналах її витоку;
- вбудова електронних пристроїв перехоплення інформації в технічні засоби та приміщення;
- перехоплення, дешифрування та подання хибної інформації в мережах передавання даних і мережах зв'язку;
- негативний вплив на парольно-ключові системи;
- радіоелектронне придушення мереж зв'язку і систем керування.

Наслідки інформаційних злочинів в економічній сфері на рівні окремих організацій, підприємств, фірм можуть призвести до економічних втрат через знецінення і втрати товарної частини інформаційного ресурсу — промислових та інформаційних технологій.

Вплив інформаційних загроз на структури державної влади, що відповідальні за підготовку та прийняття рішень, реалізація яких безпосередньо впливає на безпеку держави, може сприяти виникненню надзвичайних ситуацій у державі та суспільстві, завдати значні збитки через порушення функціонування систем зв'язку, контролю і керування або виток таємної інформації.

Загальнонаціональний рівень важливості проблеми інформаційної безпеки країни, її комплексний характер вимагають розробки і реалізації відповідної національної довгострокової програми.

Наведемо необхідні першочергові заходи щодо забезпечення інформаційної безпеки України [3]:

- визначення складу, послідовності і порядку розробки законодавчих і нормативно-правових актів з питань інформаційної безпеки, а також механізмів їх введення в дію (правове забезпечення);
- розробка державної цільової науково-технічної програми забезпечення інформаційної безпеки, створення інформаційної бази, спрямованої на реалізацію концепції інформаційної безпеки України (науково-технічне забезпечення);
- розробка і створення цілісної організаційної структури системи інформаційної безпеки України;
- створення вітчизняної системи сертифікації технічних і програмних засобів інформатизації на відповідність вимогам міжнародної інформаційної безпеки (організаційне забезпечення);
- забезпечення реальних потреб системи інформаційної безпеки у кваліфікованих кадрах, матеріально-технічних та фінансових ресурсах (ресурсне забезпечення).

Література

1. *Маліцький Б., Попович О.* Про невідкладні заходи щодо посилення ролі науки та технологій в економічному і соціальному розвитку України // Економіст. — 2005. — № 4. — С. 31–35.
2. http://www.gov.ua (веб-сторінка Кабінету Міністрів України).
3. http://www.ueplac.kiev.ua/ukr/index.shtml (веб-сторінка UEPLAC — Українсько-європейського центру з питань законодавства).
4. http://www/soskin.info (Наук. журн. "Економічний часопис").

Directions of public policy are considered in relation to the informative safe conducts of Ukraine. The basic sources of threats to informative safety of the state are indicated. Facilities of influencing of threats are transferred on informative safety after directions: informative, programmatic-mathematical, physical, radios electronic. Primary measures are marked in relation to providing of informative safety of Ukraine.

Надійшла 12 травня 2006 р.