

1 Загальні питання інформаційної безпеки. Правове забезпечення захисту інформації. Міжнародне співробітництво у сфері захисту інформації

УДК 002.6 : 681.06 : 638.253.231

ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УКРАЇНІ, ШЛЯХИ ЇХ ВИРІШЕННЯ

Михайло Згуровський

Національний технічний університет України "КПІ"

Анотація: Стаття присвячена питанням визначення положення інформаційної безпеки серед елементів національної безпеки, дослідженню загроз інформаційній безпеці, а також ролі інформаційних технологій, захисту інформації та систем підготовки, перепідготовки та підвищенню кваліфікації спеціалістів з інформаційної безпеки.

Summary: The article is devoted to the questions of the definition information security's position among the elements of the national security, investigation of the threat, which menace to the information security, and the role of the information protection, the system of training, retraining and raising the gualification of the specialists the information security, the role of the information technologis in the gnaranteeng the information security.

Ключові слова: інформаційна безпека, інформаційні технології, підготовка, перепідготовка спеціалістів з інформаційної безпеки

I Інформаційна безпека - компонент національної безпеки України

Під інформаційною безпекою розуміється такий стан інформаційного середовища, при якому гарантується розвиток цього середовища і його використання в інтересах особи, суспільства і держави, а також захищеність від будь-яких загроз.

Інформаційна безпека в загальній системі національної безпеки України посідає особливе місце. З урахуванням темпів інформатизації та розвитку інформаційних технологій, широкого втілення таких технологій у виробництво, оборону, правозахист, науку, освіту тощо, інформаційна діяльність стає обов'язковим і, часто-густо, вирішальним елементом усіх сфер діяльності суспільства, тому інформаційна безпека є елементом всіх складових національної безпеки країни. В цих умовах проблема інформаційної безпеки все більше набуває самостійного суспільного значення. У той же час система зовнішніх і внутрішніх загроз інформаційній безпеці носить комплексний характер і здійснення цих загроз має на меті нанесення збитків у політичній, економічній, соціальній, військовій, екологічній, науково-технічній сферах тощо.

II Загрози національній безпеці України в інформаційній сфері

Як відомо, Концепцією національної безпеки України, схваленою Постановою Верховної Ради України від 16 січня 1997 року ¹ 3/97-ВР, до загроз інформаційній безпеці віднесено:

- невиваженість державної політики та відсутність необхідної інфраструктури в інформаційній сфері;
- повільність входження України у світовий інформаційний простір, брак у міжнародного співтовариства об'єктивного уявлення про Україну;
- інформаційна експансія з боку інших держав;
- витік, модифікація та блокування інформації, яка становить державну та іншу передбачену законом таємницю, а також конфіденційної інформації, що є власністю держави;
- запровадження цензури.

На розгляді деяких з наведених вище положень доцільно зупинитися більш детально. Зокрема, невиваженість державної політики та відсутність необхідної інфраструктури в інформаційній сфері інколи призводить до недостатньо обгрунтованих кроків у плануванні та реалізації заходів по інформатизації, створенню та експлуатації автоматизованих інформаційних систем. Суттєві зміни, що відбулися в політичному та економічному житті країни після набуття суверенітету, потребують перегляду ролі та функцій держави в інформаційній сфері - практика перекриття кордонів та жорсткої цензури пішла в минуле, і держава, декларуючи

орієнтацію на ринкові відносини та свідомо не використовуючи важелів адміністративного впливу на процеси формування інформаційного простору, виявилася не готовою до конкуренції з безліччю вітчизняних та закордонних суб'єктів інформаційної діяльності. Нерозвиненість інфраструктури інформаційної діяльності примушує Україну створювати та реалізовувати національні концепції і програми з інформатизації, орієнтуючись на здобутки розвинутих країн. Широке використання відносно дешевих та якісних засобів обчислювальної техніки іноземного виробництва позбавляє країну можливості розвивати відповідні національні галузі науки та виробництва, що зрештою може призвести до стратегічної залежності базових сфер суспільної діяльності від неконтрольованих державою закордонних технологій.

Слабкість інфраструктури інформаційної діяльності найяскравіше проявляється в недостатній інформаційній забезпеченості процесів державного управління та координації. Практично не використовуються можливості з створення міжвідомчих довідково-інформаційних систем, повільно просуваються роботи із створення національних автоматизованих реєстрів, державної паспортної системи тощо. Технології обробки інформації, що використовуються в існуючих автоматизованих системах, за своїми характеристиками та рівнем технічного забезпечення не відповідають потребам сьогодення. В умовах економічної кризи наукову діяльність у сфері інформатизації практично призупинено, науковий та інженерно-технічний потенціал країни розмоктується по інших сферах діяльності та за кордон.

Однією з основних проблем інформатизації, що потребують невідкладного вирішення, є формування платоспроможного попиту на інформаційну продукцію світового рівня якості. Забезпечити в нашій країні цивілізований масовий збут продуктів інтелектуальної діяльності практично неможливо, що спонукає виробників, зокрема, програмного забезпечення шукати епізодичні «халтури» під конкретне замовлення. Така діяльність носить хаотичний характер, а вироблена продукція не є високотехнологічною. Викликає занепокоєння все більш широка орієнтація вітчизняних виробників програмних продуктів на закордонного замовника, який може забезпечити збут інтелектуального продукту у розвинених країнах і, відповідно, має можливість на належному рівні оплатити працю спеціаліста. Будь-який програміст в Україні, який має відповідну кваліфікацію та володіє англійською мовою, може виконувати замовлення із створення програмних продуктів, навіть не змінюючи місце проживання. Негативну роль у ситуації, що склалася, відіграє відсутність в Україні дієвої системи правового захисту авторських прав на продукти інформаційної діяльності.

Одним із шляхів вирішення проблеми використання інтелектуального потенціалу вітчизняних спеціалістів може бути створення та розвиток системи цивілізованого співробітництва українських наукових та учбових закладів з знаними закордонними виробниками програмних продуктів. По-перше, це дасть змогу нашим спеціалістам ознайомитися з передовими технологіями створення та маркетингу програмних продуктів, а по-друге, забезпечить можливість державного координування процесу формування інформаційних ресурсів країни в сфері інформатизації.

Важливе значення у формуванні інформаційних ресурсів у наш час відіграє створення систем електронного обігу та зберігання документів. Розробка таких систем потребує чіткого та вичерпного визначення поняття «електронний документ», регламентації порядку формування, збереження, знищення таких документів, створення дієвої системи захисту інформаційних ресурсів, що наведені в електронному вигляді. На сьогодні Україна не має таких систем. Головною причиною такого стану є брак інформаційних ресурсів в електронному вигляді, створених згідно з міжнародними стандартами, та нерозвиненість інфраструктури їх обробки.

Якісно нове значення в системі електронного документообігу набуває проблема захисту інформаційних ресурсів. Традиційне відношення до документу як до фізичного носія інформації (аркуш паперу, фотографія, кінострічка тощо) потребує коректування на рівні свідомості - технологія створення та обробки електронних документів створюється саме для спрощення процесів відтворення, передачі та розповсюдження інформації, що входить у конфлікт з концепцією збереження основних рис інформації - її цілості, доступності та конфіденційності. Сфера діяльності із захисту інформації, що наведена в електронному вигляді, є новою як з точки зору її об'єкту, так і з огляду на технологічний аспект здійснення такої діяльності, що викликає необхідність створення, зокрема, постійно діючої системи безперервного навчання спеціалістів відповідного профілю та підвищення їх кваліфікації.

III Роль сучасних інформаційних технологій у формуванні інформаційних ресурсів

Характерною рисою нинішнього етапу науково-технічного прогресу є масове використання обчислювальної техніки в усіх сферах суспільного життя. Це у повній мірі відноситься і до сфери інформатизації. У повсякденну практику широко увійшло поняття інформаційного ресурсу. Якщо раніше це поняття використовувалося для визначення суто інформації, що була накопичена у бібліотеках та архівах, то зараз під інформаційними ресурсами мають на увазі перш за все впорядковані інформаційні масиви в електронному вигляді. Їх накопичення у вигляді баз даних сприяло створенню якісно нової форми збереження інформації, головною особливістю якої є можливість поточного відновлення відповідності реальним подіям. Актуальною стає

проблема своєчасного одержання оновленої інформації, обробки комплексних інформаційних масивів в розподілених системах. Все більшого значення набуває необхідність збереження цілісності та доступності відкритої інформації, а також забезпечення конфіденційності інформації з обмеженим доступом в автоматизованих системах.

Разом з безсумнівним позитивним ефектом інформатизації базових сфер суспільного життя слід відзначити також і небезпеку вразливості цих сфер від інформаційних технологій, що викликає необхідність дуже ретельного вибору таких технологій з урахуванням об'єкту інформаційної діяльності, важливості цього об'єкту для суспільства, значущості наслідків порушення інформаційної технології.

IV Огляд ринку інформаційних технологій України

Ринок інформаційних технологій в Україні відтворює загальні тенденції на світовому ринку інформаційних технологій, хоча і робить це з деяким запізненням. На комп'ютерному ринку України сьогодні діють декілька великих вітчизняних фірм-виробників комп'ютерної техніки (Квазар-Мікро, МДМ-сервіс, Меркс та ін). Найновіша продукція «brand-name» світових лідерів у галузі комп'ютерної техніки на час анонсування в рекламних виданнях поступає в торгівельну мережу вітчизняних дилерів. Свої представництва в Україні мають майже усі крупні фірми-лідери світової комп'ютерної індустрії, які розглядають нашу країну як перспективний ринок сбуту продукції і бачать тут реальну можливість ведення цивілізованого бізнесу.

Що ж до програмного забезпечення широкого використання, то переважна більшість копій цього забезпечення є піратською, причому на так званому «сірому» (ближче до «чорного») ринку присутні найновіші версії програмних продуктів. Користувачі завідомо йдуть на невизначеність з якістю та функціональними властивостями цих продуктів, маючи на увазі перш за все їх низьку вартість. Такий підхід можна зрозуміти у випадку неможливого користувача персонального комп'ютера; для керівника великого підприємства або органу державної влади він недопустимий. Але чи багато керівників розуміють, що програмне забезпечення гарантованої якості не менш важливе, ніж найновіший комп'ютер?

Дуже важливою вважаю проблему повної залежності українських користувачів, зокрема, і у державних структурах, від інформаційних технологій та комплектуючих іноземного виробництва. Розвинуті країни використовують у важливих системах державного призначення компоненти та технології переважно вітчизняних розробки та виробництва, у іншому разі завжди буде існувати можливість використання країною-розробником інформаційних технологій фактору технологічної залежності. Система формування та використання інформаційних ресурсів України повністю базується на закордонних технічних та програмних засобах, що ставить її в стратегічну залежність від невідконтрольного виробника таких засобів.

Окремо треба торкнутись питання сертифікації засобів інформаційної діяльності. У той час, коли всі моделі комп'ютерів відомих фірм-виробників перед виходом на ринок проходять сертифікацію на відповідність міжнародному стандарту ISO-9000, а технологія їх виробництва раз на рік проходить сертифікацію на відповідність вимогам ISO-9001 та ISO-9002, жоден з українських виробників комп'ютерної техніки ще не отримав сертифіката ISO-9000, не кажучи вже про сертифікацію виробництва і системи якості на виробництві.

Українські виробники комп'ютерів, в значній більшості, мають сертифікати відповідності УкрСЕПРО тільки на комп'ютери, оскільки це є однією із вимог законодавства для ведення виробничої та комерційної діяльності. Виробництво ж цих комп'ютерів не сертифіковане, тому споживач не може бути впевненим, що комп'ютери збираються в постійних, однакових, відповідаючих вимогам стандартів технологічних умовах.

V Захист інформації як основна складова інформаційної безпеки

Розвиток телекомунікаційних систем та їх використання для забезпечення мережевих інформаційних технологій призвів до появи принципово нових явищ і закономірностей в інформаційній сфері. Можливість дистанційного доступу до практично невичерпних ресурсів глобальних комп'ютерних мереж, вражаюче зростання швидкості та обсягів обробки інформації, втілення телекомунікацій в забезпечення особистих потреб людини формують нові суспільні відносини. Наявність інформаційних ресурсів і широких можливостей їх використання, а також обмеженість трудових, сировинних та енергетичних ресурсів приводять у розвинутих країнах до того, що інформація стає стратегічним ресурсом. У цих обставинах систему захисту інформації можна вважати базовою підсистемою забезпечення інформаційної безпеки суспільства, без якої неможливе здійснення жодного виду інформаційної діяльності. Таким чином, не вирішивши проблеми захисту інформації на рівні, адекватному економічно розвинутим країнам, Україна не зможе увійти до мирової спільноти на правах рівноправного партнера.

Одним з факторів забезпечення надійного функціонування і розвитку захищених інформаційних систем є вирішення проблеми створення та розвитку системи підготовки спеціалістів в галузі інформаційної безпеки.

VI Створення системи підготовки, перепідготовки та підвищення кваліфікації спеціалістів з інформаційної безпеки

Для створення та підтримки Національної системи інформаційної безпеки на рівні, адекватному сучасним загрозам в інформаційній сфері, необхідно забезпечити цю систему професійними, висококласними спеціалістами, підготовленими з урахуванням сучасних досягнень науки, техніки та виробництва, які б могли працювати у всіх сферах народного господарства. Цій меті повинна служити Державна система підготовки, перепідготовки та підвищення кваліфікації спеціалістів з безпеки інформації. Концептуальний підхід до підготовки спеціалістів з інформаційної безпеки, як загальна тактика і стратегія, є методологічною основою для побудови такої системи.

Система підготовки, перепідготовки та підвищення кваліфікації спеціалістів з інформаційної безпеки має бути гнучкою та універсальною, здатною своєчасно реагувати на реальні потреби у таких спеціалістах, відповідати сучасному науково-технічному рівню і бути випереджаючою. Така система має бути орієнтована на підготовку спеціалістів з інформаційної безпеки для забезпечення системи державної влади, науково-технічного і промислового сектору економіки різних видів власності (з метою забезпечення надійності систем управління виробництвом, технологіями, енергетичними комплексами), систем управління усіма видами транспорту і вантажопотоками (з метою забезпечення надійності та безпеки), державних і недержавних фінансово-банківських та комерційних структур, військових частин усіх видів формувань.

Система має, також, забезпечувати перепідготовку та підвищення кваліфікації спеціалістів, що працюють у галузі інформаційної безпеки, але не мають відповідної спеціальної підготовки, а також підготовку висококваліфікованих науково-педагогічних кадрів через магістратуру, аспірантуру та докторантуру.

Розвиток учбових спеціальностей в галузі захисту інформації в Україні можливий при серйозному розвитку спеціальних наукових напрямків в таких галузях знань, які б надали поштовх у подальшому вирішенні проблем розпізнавання образів, завадозахищеності інформації, системному аналізі, розділах дослідження операцій, ефективної обробки інформації тощо.

Крім перелічених основних завдань, система має забезпечувати відповідну орієнтацію з проблем інформаційної безпеки керівної ланки центральних і місцевих органів державної влади, керівників підприємств, організацій, установ, державних і недержавних структур. Широке коло задач, що вирішуються, їх обсяг, необхідність фундаментальних знань спільно зі спеціальними потребують використання досвіду та практики навчальних закладів.

Державна система підготовки, перепідготовки та підвищення кваліфікації спеціалістів з безпеки інформації повинна охоплювати навчальні заклади Міністерства освіти України, інших органів державної влади.

Для координації роботи навчальних закладів різного підпорядкування з питань підготовки кадрів з інформаційної безпеки доречно створити дорадчо-керівний орган.

Підготовка спеціалістів з інформаційної безпеки повинна здійснюватись як за державним замовленням для державних структур, так і на контрактній основі для зацікавлених підприємств, організацій, установ недержавного сектору економіки.

Формування державної системи підготовки кадрів спеціалістів з інформаційної безпеки доцільно проводити в кілька етапів.

На першому етапі система підготовки спеціалістів з інформаційної безпеки повинна орієнтуватись на держзамовлення для комплектування системи захисту інформації з обмеженим доступом. Це не виключає одночасну підготовку на контрактній основі відповідних спеціалістів з захисту конфіденційної інформації в структурах недержавного сектору економіки.

На наступному етапі, при створенні відповідного навчально-методичного забезпечення і набуття досвіду підготовки спеціалістів, система підготовки буде поповнюватись відповідними навчальними структурами (вищими навчальними закладами, факультетами, кафедрами), призначеними для забезпечення підготовки спеціалістів з інформаційної безпеки, орієнтованих на підвищення надійності автоматизованих систем управління виробництвом, технологіями, енергетичними комплексами, транспортом.

Для вирішення цих задач в системі підготовки спеціалістів з інформаційної безпеки доцільно мати головний вищий навчальний заклад, а також базові кафедри з підготовки спеціалістів з інформаційної безпеки різних напрямків.

Головний навчальний заклад має працювати у тісній взаємодії з Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України і виконувати керівні та координуючі функції з питань навчально-методичного забезпечення навчальних процесів.

На базові кафедри покладається завдання навчально-методичного забезпечення процесу підготовки спеціалістів відповідних напрямків, координації робіт кафедр інших навчальних закладів, підготовки науково-педагогічних кадрів через магістратуру, аспірантуру, докторантуру, а також проведення науково-дослідних робіт з проблем інформаційної безпеки.

Враховуючи, що традиційна система підготовки спеціалістів може забезпечити замовника спеціалістами тільки через 4-6 років, для задоволення поточних потреб галузі з інформаційної безпеки доцільно створити в системі підготовки кадрів при базовому навчальному закладі підрозділ, який міг би надати прискорену підготовку (перепідготовку) особам з вищою освітою з суміжних або інших спеціальностей. Це може бути друга освіта, яку можна отримати на відповідних кафедрах та факультетах або в системі підвищення кваліфікації для керівної ланки установ, організацій, підприємств.

Система підготовки спеціалістів з інформаційної безпеки на першому етапі має забезпечити:

освітньо-професійну підготовку спеціалістів з інформаційної безпеки для кадрового забезпечення системи захисту інформації обмеженого доступу;

прискорену професійну підготовку для кадрового забезпечення системи інформаційної безпеки особам, що мають вищу освіту з суміжних спеціальностей, а також особам, що мають практичний досвід роботи з захисту інформації;

підготовку ознайомлювального характеру з проблем інформаційної безпеки керівної ланки центральних і місцевих органів державної влади, підприємств, організацій, установ.

При організації системи підготовки спеціалістів з інформаційної безпеки важливим є питання диференційованої підготовки з відповідних спеціальностей та спеціалізацій.

Підготовка спеціалістів з інформаційної безпеки на наступних етапах має орієнтуватись на захист інформації для усіх галузей, а також для усіх учбових напрямів і спеціальностей. Треба також передбачити спецкурс з інформаційної безпеки. В першу чергу спецкурс треба включити до навчальних планів спеціальностей з комп'ютерних інформаційних технологій, на факультетах кібернетики, інформатики, обчислювальної техніки, прикладної математики. Для більш ґрунтовного рішення проблеми підготовки спеціалістів для галузевих систем інформаційної безпеки, орієнтованих на забезпечення надійності комп'ютерних систем управління виробництвом, технологіями, енергетичними комплексами, транспортом тощо, є необхідним виконання відповідних наукових досліджень для з'ясування впливу захищеності інформації у сфері управління на функціональну надійність перелічених об'єктів управління, як діючих, так і перспективних. Можливим є також варіант підготовки спеціалістів з інформаційної безпеки за програмами післядипломної цільової підготовки за індивідуальними контрактами. У цій площині треба розглядати питання доцільності підготовки за спеціалізаціями з інформаційної безпеки спеціалістів радіотехнічного, хімічного та інших профілей з урахуванням проблем захисту інформації, яка обумовлена технічними демаскуючими ознаками. Як варіант, цю задачу можна покласти на курси перепідготовки та підвищення кваліфікації спеціалістів з інформаційної безпеки. Потребує самостійного вирішення питання підготовки спеціалістів з інформаційної безпеки проектно-будівельних спеціальностей.

Для підготовки спеціалістів усіх інших спеціальностей, що у своїй професійній діяльності використовують інформаційні технології, треба ввести в навчальні плани спеціальну дисципліну загальнотехнічного характеру з проблем інформаційної безпеки.

Підготовка та професійний рівень спеціалістів з інформаційної безпеки має відповідати таким вимогам: високий загальноосвітній рівень, широкий спектр технічних знань, навички системного підходу до вирішення завдань, вміння приймати нестандартні, але вірні рішення, знання правових питань, знання основ організації та управління, спеціальні знання в галузі інформаційної безпеки.

Спеціаліст з інформаційної безпеки повинен розробляти та забезпечувати організаційні, інженерно-технічні, дослідницькі, експлуатаційні, правові, екологічні заходи, гарантуючи права власника на інформацію.

Виходячи із різноманітності задач, що вирішуються, доцільно визначити групи спеціалістів та конкретизувати перелік існуючих спеціальностей, що необхідні для вирішення задач на новому етапі розвитку системи захисту інформації.

Загалом, передбачається подальша виважена робота для удосконалення системи підготовки спеціалістів з інформаційної безпеки для забезпечення захисту особи, суспільства, держави.

Більш того, вже зроблені перші кроки на цьому шляху. В ряді провідних вузів України, зокрема у Львові, Тернополі, Харкові, Миколаєві, Києві впроваджено навчання за спеціальностями та спеціалізаціями в галузі інформаційної безпеки. При фізико-технічному інституті НТУУ «КПІ» відкрито базову кафедру з інформаційної безпеки і започатковано навчання студентів за цим напрямом, шостий рік діють спеціальні курси з післядипломної освіти в галузі захисту інформації з обмеженим доступом, що восени 1999 року отримали статус навчально-методичного центру.