Таким чином, за рахунок прийняття зазначеного нормативно-правового акту відбудеться, на нашу думку, не лише деталізація механізмів державного регулювання відносин в сфері забезпечення інноваційної безпеки, але і формуватимуться певні засади державної економічної політики в науково-технічній та інноваційних сферах.

ЛІТЕРАТУРА

1. Інноваційна стратегія українських реформ / А. С. Гальчинський, В. М. Геєць, А. К. Кінах, В. П. Семиноженко. – К. : Знання України, 2002. – 336 с.
2. Про стратегію національної безпеки України [Електронний ресурс] : Указ Президента України від 12.02.2007 №105/2007 – Режим доступу: http://zakon4.rada.gov.ua/laws/show/105/2007.
3. Господарський кодекс України [Електронний ресурс] : Закон України від 16.01.2003 №436-IV. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/436–15.
4. Про основи національної безпеки України [Електронний ресурс] : Закон України від 19.06.2003 №964-IV. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/964–15.

Білоусов Євген Миколайович – к. ю. н., доцент кафедри міжнародного права Національного юридичного університету ім. Ярослава Мудрого, завідувач відділу загальних проблем формування та реалізації інноваційної політики НДІ правового забезпечення інноваційного розвитку НАПрН України

К. В. Єфремова

ТЕХНОЛОГІЧНА БЕЗПЕКА ВІРТУАЛЬНОЇ ІНФРАСТРУКТУРИ

Доповідь висвітлює основні аспекти технологічної безпеки віртуальної інфраструктури, необхідність створення головних засад та принципів для подальшого розвитку системи технологічної безпеки.

Ключові слова: *технологічна безпека, віртуальна інфраструктура, державна політика.*

Технологічна безпека України полягає у впровадженні новітніх технологій, досягненні технічного прогресу, збереженні такого рівня вітчизняного науково-технічного й виробничого потенціалу, який у разі погіршення внутрішніх і зовнішніх умов забезпечив би виживання на-

ціональної економіки за рахунок використання власних інтелектуальних і технологічних ресурсів, збереження державної незалежності.

Проблема нормативно-правового регулювання інформаційного простору в Україні не раз ставала предметом дискусій як науковців, законотворців, політиків, так і споживачів інформації.

Наказ Міністерства економіки України «Про затвердження Методики розрахунку рівня економічної безпеки України» № 60 від 02.03.2007 р., який втратив чиннбість згідно з наказом Міністерства економічного розвитку і торгівлі України від 29 жовтня 2013 року № 1277, визначав, що складовими економічної безпеки є: макроекономічна, фінансова, зовнішньоекономічна, інвестиційна, науково-технологічна, енергетична, виробнича, демографічна, соціальна, продовольча безпека. Науково-технологічна безпека – це такий стан науково-технологічного та виробничого потенціалу держави, який дає змогу забезпечити належне функціонування національної економіки, достатнє для досягнення та підтримки конкурентоздатності вітчизняної продукції, а також гарантування державної незалежності за рахунок власних інтелектуальних і технологічних ресурсів. Зараз же відповідно до наказу Міністерства економічного розвитку і торгівлі України «Про затвердження Методики розрахунку рівня економічної безпеки України» № 1277 складовими економічної безпеки виділяють такі: виробнича, демографічна, енергетична, зовнішньоекономічна, інвестиційно-інноваційна, макроекономічна, продовольча, соціальна, фінансова безпеки.

Нині особливо актуальною стала необхідність формування і реалізації державної технологічної політики як довгострокового стратегічного курсу держави, спрямованого на ефективне використання науково-технічного потенціалу і перетворення України в технологічно орієнтовану державу з високим рівнем розвитку національних галузей. У зв'язку з цим надзвичайно важливе значення має реалізація Національної програми України «Критичні технології», головними цілями якої є розвиток і своєчасне впровадження особливо пріоритетних з точки зору національної безпеки та економічного зростання технологій, які дадуть можливість вирішити першочергові критично важливі для держави проблеми, що безпосередньо впливають на обороноздатність, енергетичну незалежність, інформаційну безпеку держави в цілому, конкурентоспроможність, рівень життя народу.

Протягом останнього десятиріччя спостерігається зростання інформатизації, медіатизації та комп'ютеризації суспільства, що стало однією

із закономірностей сучасного соціального прогресу, розширюючи зв'язки держави з громадянським суспільством як у напрямі доведення рішень органів державної влади та місцевого самоврядування, висвітлення інформації про їх діяльність, так і отримання зворотної інформації про реакцію на них суспільства. Інформаційна політика держави виступає вагомим чинником реформування суспільства.

До об'єктів цієї сфери відносять, зокрема, «інформаційні системи і інформаційні технології, засоби їх забезпечення», де під інформаційною системою розуміють організаційно впорядковану сукупність документів (масивів документів) і інформаційних технологій, в тому числі з використанням засобів обчислювальної техніки і зв'язку, які реалізують інформаційні процеси [1].

Дуже часто, при вирішенні питань інформаційної безпеки, інформаційні системи, що виступають об'єктом захисту, розглядають виключно крізь призму інформаційно-обчислювальної техніки, визначаючи, наприклад, інформаційно-телекомунікаційну систему як «організаційно-технічну сукупність, що складається з автоматизованої системи та мережі передачі даних». Аналогічним шляхом пішли і автори Закону України «Про телекомунікації» визначивши інформаційну систему як сукупність телекомунікаційних мереж та засобів для накопичення, обробки, зберігання та передавання даних (ст. 1) [2].

Але звуження технологічного аспекту інформаційної безпеки виключно до інформаційних систем, як сукупності фізичних об'єктів, на нашу думку є невиправданим. Інформаційна безпека є комплексною категорією, що обумовлюється багатьма факторами. Інформаційні системи працюють не самі по собі. Будь-яка інформаційна система, особливо автоматизована, поділяється на функціональну частину та частину забезпечення, кожна з яких поділяється на складові елементи мінімально можливої розмірності. Функціональна частина інформаційної системи спрямована на виконання функцій і завдань, що підлягають реалізації за допомогою цієї системи. Частина забезпечення представляє собою «наповнення» функціональної частини, за допомогою якого фактично реалізуються функції і завдання системи. Узагальнюючи такий підхід ми можемо говорити, що інформаційна система функціонує за тими ж самими правилами і законами, що і будь-який інший вид систематизованої діяльності з розподілом ролей і функцій. Створення будь-якої системи обробки чи передачі інформації, починаючи від поштової служби і закінчуючи комп'ютерними ме-

режами, включає величезну кількість етапів та елементів. До цього переліку входить: створення фізичних об'єктів, на яких ця система розміщується, створення технічного і програмного забезпечення, підготовка кадрів, забезпечення фінансовими та енергетичними ресурсами тощо. І загрози інформаційній безпеці можуть виникати на будь-якому етапі створення та експлуатації інформаційної системи. Це означає, що існує певна сукупність об'єктів, суб'єктів та відносин між ними, що забезпечує здійснення інформаційних процесів у державі в цілому. Тому важливим для вивчення технологічного аспекту інформаційної безпеки є створення чіткого визначення і окреслення меж відповідної сфери. Останнім часом інформаційні технології дуже широко використовуються в політичній, економічній, соціальній та інших сферах суспільного життя, за їх допомогою активізується участь різних груп і верств населення в управлінні країною, її регіонами та громадою. В той же час поширення інформатизації суспільства зумовило зростання реальних та потенційних загроз національним інтересам в інформаційній сфері та визначило коло питань щодо необхідності забезпечення інформаційної безпеки. Як зазначено у проекті доктрини інформаційної безпеки України, «інформаційна безпека є невід'ємною складовою кожної зі сфер національної безпеки. Водночас інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності національних інтересів в інформаційній сфері від зовнішніх та внутрішніх загроз і являє собою сукупність інформаційно-психологічної (психофізичної) та інформаційно-технологічної безпеки держави.

Останнім часом набирає обертів віртуалізація інфраструктури. У даному випадку, будемо розуміти під цим терміном створення IT-інфраструктури, незалежної від апаратної частини. Наприклад, коли потрібний нам сервіс знаходиться на гостьовій віртуальній машині і нам не важливо, на якому фізичному сервері він розташовується. Складні операції IT характерні не тільки для великих організацій. Підприємства малого та середнього бізнесу також стикаються зі значною неоднорідністю IT-операцій. При цьому вони мають у своєму розпорядженні набагато меншим числом співробітників. Незважаючи на те, що близько 80% всіх організацій мають фізичні сервери, 34% всіх організацій одночасно керують фізичними та віртуальними серверами, а також операціями в хмарних середовищах, – так звана «потрійна послуга» в комп'ютерних середовищах.

За короткий час віртуалізація справила величезний вплив на сферу IT та мережеві технології, вона вже посприяла величезної економії витрат і окупності вкладень для дата-центрів, підприємств і «Хмари». Що здається менш значним і сильно відстає від реальності – це розуміння віртуалізації і віртуалізованих середовищ з точки зору безпеки. Деякі люди вважають, що віртуалізація є більш безпечною, ніж традиційні середовища, так як вони чули про ізоляція між віртуальними машинами (ВМ) і тому що вони раніше не чули про будь-яких успішних атак на гіпервізори. Інші вважають, що нові віртуальні середовища потребують безпеки так само, як традиційні фізичні середовища, тому застосовують той же багаторічний підхід до безпеки. Найбільш важливим фактором є те, що нова середовище більш складна. Віртуальні підходи, додані до вже існуючих мереж, створюють нову мережу, яка вимагає іншого підходу до безпеки. Крім звичайних заходів слід застосовувати і спеціальні заходи безпеки для віртуалізації. В цьому документі ми розглянемо відмінності, проблеми, труднощі, ризики, викликані застосуванням віртуалізації, а також надамо слушні рекомендації та практичні поради, щоб переконатися, що після застосування віртуалізації мережа залишиться такою ж захищеною.

Інформаційний суверенітет виступає володінням і розпорядженням національними інформаційними ресурсами, які включають усю належну державі інформаційну інфраструктуру, інформацію – незалежно від змісту, форми, часу і місця її створення, і забезпечується виключним правом держави на формування і здійснення національної інформаційної політики, власності на інформаційні ресурси, сформовані за державний кошт, створенням національних систем інформації, встановленням режиму доступу інших держав до інформаційних ресурсів України [3].

Протягом 2012–2013 рр. у Верховній Раді України було зареєстровано проекти законів України, якими визначаються правові та організаційні засади забезпечення кібернетичної безпеки України, основоположні принципи державної політики та національної системи у сфері кібернетичної безпеки, а також повноваження суб'єктів її забезпечення: «Про внесення змін до Закону України «Про основи національної безпеки України щодо кібернетичної безпеки», «Про кібернетичну безпеку України», «Про внесення змін до деяких законів України щодо забезпечення кібернетичної безпеки України» [4].

Якщо у віртуальному середовищі обробляються дані обмеженого доступу (конфіденційна інформація, персональні дані, банківська інформація,

державна таємниця, комерційна таємниця тощо), захищеність віртуальної інформаційної системи має відповідати вимогам законодавства.

Методичні рекомендації та матеріали регуляторів щодо забезпечення безпеки персональних даних не розрізняють вимоги між фізичним та віртуальним середовищем обробки даних. Віртуальна інфраструктура підвищує ступінь інтеграції обчислювальних засобів в інформаційній системі, зменшуючи кількість фізичного обладнання, але зовсім не зменшує, а збільшує кількість об'єктів і суб'єктів інформаційного обміну і ускладнює структуру їх взаємодії. Тому підвищувати захищеність віртуальної інфраструктури потрібно комплексно шляхом комбінації мережевих і локальних засобів захисту поряд з інтеграцією широкого набору захисних механізмів, що застосовуються одночасно.

На сьогодні вкрай необхідно створити головні засади та принципи, на основі яких можливо здійснювати подальший розвиток системи технологічної безпеки віртуальної інфраструктури. У світі існує досить багато країн з більш високим рівнем інформатизації та віртуалізації, які раніше зіткнулися з тими проблемами, які постають перед Україною сьогодні. Таким чином, пропоную використати їх досвід для добору тих правових засобів, які саме необхідні для правого регулювання у цій сфері нашої країни.

ЛІТЕРАТУРА

1. Кормич Б. А. Деякі проблеми інформаційної безпеки в Україні / Б. А. Кормич // Держава і право : зб. наук. пр. Юрид. і політ. науки. – К. : Ін-т держави і права ім. В. М. Корецького НАН України, 2001. – Вип. 14. – С. 180–185.
2. Про телекомунікації : Закон України від 18 листоп. 2003 р. №1280-IV // Відом. Верхов. Ради України. – 2004. – №12. – Ст. 155.
3. Набруско В. Чи стане Україна господарем у власному інформаційному просторі? [Електронний ресурс] / Віктор Набруско // Дзеркало тижня. – 2008. – №34 (713). – Режим доступу: http://gazeta.dt.ua/SOCIETY/viktor_nabrusko__chi_stane_ukrayina_gospodarem_u_vlasnomu_informatsiynomu_prostori.html. – Назва з екрана.
4. Долженко К. І. Нормативно-правове регулювання інформаційної безпеки регіону / К. І. Долженко // Право і безпека. – 2014. – №3 (54) – С. 43–48.

Єфремова Катерина Вікторівна – к. ю. н., в. о. вченого секретаря НДІ правового забезпечення інноваційного розвитку НАПрН України