УДК 355.40

В.С. Наконечний

СТАН РОЗВИТКУ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В СВІТОВІЙ ПРАКТИЦІ ТА ЇЇ ВПЛИВ НА ЕКОНОМІЧНИЙ РОЗВИТОК УКРАЇНИ

В статті розглянуті питання розвитку інформаційних технологій та інформаційного суспільства, яке визначено одним з головних пріоритетів державної політики, що знайшло своє формальне відображення в європейській стратегії економічного розвитку «Європа 2020: стратегія розумного, сталого та всеохоплюючого зростання». Визначені джерела загроз національній безпеці України, показані головні причини цього процесу та надані пропозиції щодо вирішення проблеми захисту національних інтересів України.

Ключові слова: загроза, захист, інформація, кіберзлочинність, національна безпека.

Вступ

На сьогодні розвиток інформаційних технологій (ІТ), їх поширення в усі сфери життєдіяльності людини та суспільства стали нормою подальшої еволюції цивілізації. В розвинутих країнах світу продовжується перехід до інформаційної сервісно-технологічної економіки, де значна частина валового внутрішнього продукту (ВВП) забезпечується діяльністю з виробництва, обробки та поширення інформації і знань. Економістами та політиками усього світу усвідомлено, що розвиток ІТ створює засади сучасної економіки держави та добробуту її людей.

Основна частина

В провідних країнах світу, у тому числі країнах-членах ЄС, розвиток інформаційного суспільства визначено одним з головних пріоритетів державної політики, що знайшло своє формальне відображення в європейській стратегії економічного розвитку «Європа 2020: стратегія розумного, сталого та всеохоплюючого зростання»[1].

Україна, яка прагне стати асоційованим членом ЄС, повинна враховувати та максимально адаптувати діючі національні механізми в рамках міжнародної угоди «Порядок денний асоціації Україна – ЄС». В той же час, неузгодженість, суперечливість, некоординованість, необґрунтованість механізмів державного управління призводять не тільки до зниження їх ефективності та результативності, а й є джерелом загрози національній безпеці. Тому Законом України «Про основи національної безпеки України» [2]серед пріоритетних напрямів забезпечення інформаційної безпеки визначено: «вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері..».

В той же час, цей процес значною мірою залишається несистемним, занадто забюрократизованим та непрозорим. Одними з головних причин такого стану є недосконаліть діючих механізмів державного управління в цій сфері. Крім міжнародних та безпекових аспектів актуальність формування та реалізації ефективної державної політики в цій сфері обумовлена наступними факторами:

- зростаючим значенням інформації для будь-якої сфери життєдіяльності особи, суспільства та держави;
- прагненням України набуття статусу асоційованого члена ЄС;
- входженням нашої країни в світовий інформаційний простір;
- появою нових та зростанням рівня традиційних загроз в інформаційній сфері;
- загостренням комплексу проблем в інформаційній сфері;
- недосконалістю чинного законодавства;
- важливістю державного регулюючого впливу на інформаційну сферу та реалізації державної політики у сфері інформаційного суспільства.

Концепція державної політики у сфері інформатизації та розвитку інформаційного суспільства визначено законодавчими актами, в яких позначені головна мета, основні завдання, шляхи розв’язання проблем, завдання та функції органів влади, механізми

взаємодії їх між собою та суспільством. До числа таких законодавчих актів належать закони України:

«Про телекомунікації»;

«Про основні засади розбудови інформаційного суспільства в Україні на 2007-2015 роки»;

«Про інформацію»;

«Про Національну програму інформатизації»;

«Про доступ до публічної інформації;

«Про захист персональних даних»;

«Про захист інформації в інформаційно-телекомунікаційних системах»;

«Про електронний документ та електронний документообіг»;

«Про електронний цифровий підпис»;

«Про захист персональних даних» тощо.

Зокрема в Законі України «Про інформацію» серед основних принципів державної інформаційної політики зазначені[3]:

- гарантованість права на інформацію;
- відкритість, доступність інформації, свобода обміну інформацією;
- достовірність і повнота інформації;
- правомірність одержання, використання, поширення, зберігання та захисту інформації;
- захищеність особи від втручання в її особисте та сімейне життя.
- забезпечення доступу кожного до інформації;
- забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації;
- створення умов для формування в Україні інформаційного суспільства;
- забезпечення відкритості та прозорості діяльності суб'єктів владних повноважень;
- створення інформаційних систем і мереж інформації, розвиток електронного урядування;
- постійне оновлення, збагачення та зберігання національних інформаційних ресурсів;
- забезпечення інформаційної безпеки України;
- сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору.

З кожним роком рівень інтегрованості України до світових інформаційних процесів зростає. Проникнення інформаційних технологій в усі сфери життя українського суспільства досягає загальносвітових показників. Водночас, поряд із очевидними перевагами такого інтенсивного інноваційного розвитку,Україна, так само як і інші розвинуті країни світу, зазнає все зростаючого тиску на власний інформаційний суверенітет та інформаційну безпеку держави. Наша держава все частіше стикається із все більш масштабними проявами комп'ютерної злочинності, що загрожують сталому та безпечному функціонуванню національних інформаційно-телекомунікаційних систем(ІТКС). Технічні особливості та глобальність процесів інформатизації роблять питання забезпечення інформаційної безпеки (ІБ) в таких умовах дійсно не лише «найважливішою функцією держави», але й «справою всього українського народу», як це зазначається в ст. 17 Конституції України[4].

Національна безпека України, її економічне процвітання та соціальне благополуччя все більше залежать від інформаційних ресурсів, що забезпечуються інформаційно-телекомунікаційними технологіями.Водночас, зростання залежності від ІТ робить сучасне українське суспільство більш уразливим перед можливими негативними наслідками протиправного використання кіберпростору.

Кожного року зростає кількість кібернападів на всі елементи життєдіяльності нашої держави. За результатами спільного дослідження Центру відповідального підприємництва та торгівлі (CREATe.org) та фірми PwC (PricewaterhouseCoopers), фінансові наслідки крадіжки

комерційної таємниці складають від 1 до 3% ВВП країни.Потенційні збитки здаються ще більш жахливими, якщо прийняти до уваги ймовірність зламу систем кібербезпеки.

Виходячи з підготовленої міністерством фінансів України номінального показника ВВП за 2015 рік на рівні приблизно 1 400 000 млн. грн., (рис. 1) прогнозований розмір збитків від втрати інформації, що складає комерційну таємницю, може знаходитися в діапазоні від 14000 млн. грн., до 42000 млн. грн. на рік (рис. 2).

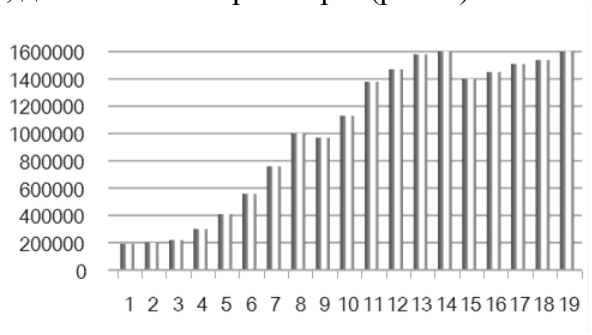

Рис.1. Номінальний показник ВВП за 2001-2019 рокимлн. грн.
(за оптимістичними прогнозами)

В цих умовах головним завданням держави є вжиття необхідних заходів, що дозволять принципово зменшити (а подекуди - унеможливити повністю) наслідки від кібератак.

Зазначене критично підвищує значення інформаційної безпеки держави, заходів з її планування та забезпечення.

Рис. 2. Прогнозований розмір збитків ВВП України у 2015 році
від втрати інформації, що складає комерційну таємницю

Відповідно до звітів аналітиків Gartner, витрати на ІБ у світі в цьому році зросли на 8,2%, а загальний обсяг глобального ринку кібербезпеки в 2015 році складе 106 млрд дол. У 2017 році обсяг цього ринку досягне 120 млрд дол., а до 2020 року ця цифра зросте до 170 млрд дол. (рис. 3).

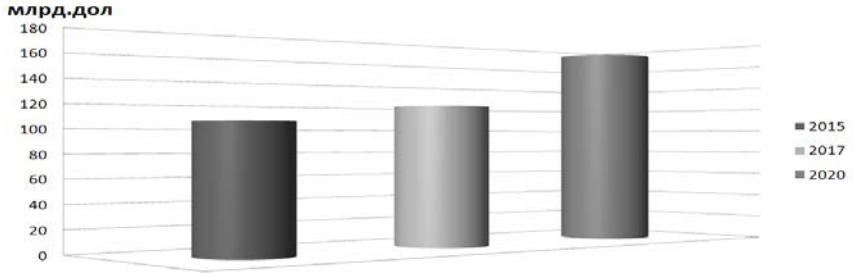

Рис. 3. Витрати на інформаційну безпеку в світі

Джерелами таких загроз і викликів можуть бутиміжнародні злочинні групи хакерів, окремі підготовлені у сфері ІТ злочинці, іноземні державні органи, терористичні угруповання, недержавні організації, політичні структури, неформальні об'єднання екстремістського спрямування, транснаціональні корпорації та фінансово-промислові групи.

Питаннями забезпечення інформаційної безпеки України опікуються понад 20 державних органів і центральних органів виконавчої влади основними з яких є:

1. Президент України.
2. Рада національної безпеки та оборони України.
3. Кабінет Міністрів України.
4. Служба безпеки України
5. Міністерство внутрішніх справ України
6. Державна служба спеціального зв'язку та захисту інформації
7. Міністерство оборони України
8. Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації
9. Науково-дослідні установи, поза урядові структури, оператори провайдери телекомунікацій і. т. ін.

Незважаючи на це, досі не налагоджено ефективної міжвідомчої взаємодії та не визначено єдиного спеціально уповноваженого органу, який займався б комплексним вирішенням усього спектру проблем у сфері ІБ.

Відсутність належної централізації управління та координації діяльності відповідних органів державної влади обумовлює неефективність системи формування та реалізації державної політики в цій сфері.

На сьогоднішній день сфера забезпечення ІБ регулюється понад 20 законами України, переважна більшість яких в умовах стрімкого розвитку новітніх технологій суперечать один одному та морально застарівають. На етапі розробки відповідних нормативно-правових актів виникають проблеми які пов'язані із розбіжністю підходів зацікавлених відомств не лише до розподілу функціональних обов'язків, але й принципових відмінностей у питаннях термінології, оцінки ризиків та групуванні загроз за ступенем важливості.

Дослідження відомого німецького оператора зв'язку Deutsche Telecom підтверджує високий рівень загроз у кібернетичному просторі України [5]. За його даними наша держава опинилася на четвертій позиції у світі серед країн-джерел кібернетичних атак, найбільш розповсюдженими серед яких були несанкціонований доступ до автоматизованих систем та DDoS атаки на державні інформаційні ресурси, що свідчить про збільшення кількості цілком свідомих атак на певні системи і як правило, приводить до дезорганізації в роботі та зменшенню економічної ефективності структур, що атакуються.

Викликає велике занепокоєння швидке поширення кількості шахрайств, які здійснюються за допомогою високих ІТ, що пов'язані із незаконними діями з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків і т. п.Тому з метою недопущення несанкціонованого доступу до такої інформації чи інформації з обмеженим доступом відповідно до Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [3] здійснюється система заходів, спрямованих на виконання його положень, у тому числі – створення в інформаційних системах комплексних систем захисту інформації (КСЗІ).

Водночас, незважаючи на значний досвід та зростаючі можливості державних структур у забезпечені безпеки інформації в інформаційно-телекомунікаційних системах, все ще спостерігаються і проблемні точки такого забезпечення.В ряді випадків строго формалізовані методи опису механізмів захисту при побудові КСЗІ є надмірними, вимагають значних бюджетних витрат, не відповідають рівню загроз та ризикам. Для систем з помірним рівнем ризиків повинні більш широко використовуватися міжнародні стандарти з побудови систем

управління ІБ, які орієнтовані на процесний підхід та запровадження системи більш гнучких заходів безпеки. Все ще перебуває на етапі становлення повноцінна система визнання сертифікатів відповідності засобів криптографічного та технічного захисту інформації вимогам визнаних міжнародних стандартів, виданих в інших країнах значно звужує можливість використання засобів захисту КСЗІ в ІТКС.

Порівнюючи ІТ галузь України, наприклад з країною Ізраїль, яка з країни експортерів помаранчів стала країною 70% ВВП якої є високі інформаційні технології, можна стверджувати,що зараз ця країна завдяки нашим колишнім співвітчизникам, які своїми справами в ІТ галузі переконали весь світ у тому, що вони можуть створювати великі міжнародні компанії та сплачувати стабільно високі податки, підвищуючи могутність і збільшуючи міжнародний статус Ізраїлю, перетворилася в країну, яка по суті стала стартапом нації. В країну яка довела, що можна використовувати інтелектуальні ресурси та створювати конкурентоспроможні високотехнологічні ІТ продукти. При цьому, як свідчить faktu.ictv.ua (рис. 4) на ІТ галузь в нашій країні виділяється лише приблизно 2% ВВП.

Рис. 4. Доля виділених ресурсів на ІТ галузь в Україні

Сучасні ІТ це не просто сектор економіки, сьогодні коли ми говоримо про нову,сучасну Україну, ми говоримо про молодь 25-30 років, яка зараз працює в цій галузі та конкурує на міжнародному рівні. Тому сьогодні до України відносяться як до експортера того, що люди створюють власною інтелектуальною працею, країни айтішників й це дуже важливо.

На сьогодні висококваліфіковані спеціалісти ІТ галузі є досить високооплачувані люди і коло ми говоримо про Український сектор ІТ треба казати, що ці фахівці завдяки своїй інтелектуальній праці є надією нашої нації.

Проте, на теперішній час, в зв'язку з ситуацією, що склалася на цьому ринку, а саме:

−відсутність підтримки галузі з боку держави;

−проблеми з захистом інтелектуальної власності;

−політична та економічна нестабільність;

−складне юридичне, податкове та бізнес оточення;

−висока складність старту та ведення бізнесу в Україні;

−велика кількість ризиків для бізнесу;

−часті та іноді незаконні перевірки, погрози, вилучення серверів і т. п.

ті люди, які хочуть працювати в цій галузі в Україні, заробляти та сплачувати податки державі мусять виїжджати не тільки до США, але і до Польщі, країн Балтії де їх праця вище цінується та більш захищена.Для того, щоб змінити імідж України, держава має бути в цьому зацікавлена.

З загальної думки експертів цієї галузі стає вочевидь, що завдяки айтішникам ми сьогодні тримаємося з точки зору інвестицій, тому, що,практично, єдині інвестиції, які зараз надходять до України – це інвестиції в сектор ІТ.

Україна має отримувати інвестиції саме в цю галузьтому, що без ІТ неможливо модернізувати жодну з інших галузей (хімічну, металургійну, транспортну і т. д.), неможливо побудувати сучасне інформаційне суспільство або електронний уряд. Це дуже великий та важливий спектр питань.Цей бізнес є індикатором інвестиційної привабливості нашої країни і його треба розвивати. І якщо інвестори припинять інвестиційну інжекцію в ІТ галузь нашої держави Україна без інвестування не зможе бути високорозвиненою країною. Відповідно це питання не тільки інформаційної безпеки але й інвестиційної безпеки нашої держави. І якщо цей процес не розвивати, ми можемо загубити не тільки висококваліфікованих спеціалістів, не тільки інвесторів але й можемо загубити Україну.

Висновки

З метою вирішення проблеми захисту національних інтересів України пропонується створення відповідного Центрального органу виконавчої влади в сфері телекомунікації та інфотматизації на чолі з державною, висококваліфікованою, порядною та досвідченою в цій галузі людиною – науковцем.

Основним завданням цієї державної структури мають бути:

- всебічний розвиток та захист галузі ІТ;
- заходи щодо її інвестиційної привабливості;
- вихід нашої держави в світові лідери в ІТ галузі;
- стимулювання впровадження новітніх ІТ і виробництва конкурентоспроможного національного інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів;
- забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури;
- розробка та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними стандартами держав – членів ЄС, у тому числі згідно з вимогами Конвенції про кіберзлочинність;
- створення національної системи кібербезпеки;
- і в кінці кінців, розбудова сучасної, заможної України.

Література

1. Україна 2020. Стратегія розвитку [Електронний ресурс]. – Режим доступу : http://reforms. in.ua/ 2020/strategy2020.pdf.

2. Закон України «Про основи національної безпеки України» // Відомості Верховної Ради України. – 2003. – № 39. – Ст. – 351. Із змінами, внесеними згідно із Законом № 3200-IV (3200-15) від 15.12.2005. ВВР. – 2006. – № 14. [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/show/964-15.

3. Закон України Про захист інформації в інформаційно-телекомунікаційних системах (Відомості Верховної Ради України (ВВР), 1994, N 31, ст.286) [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80/.

4. Конституція України (відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141) [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80.

5. [Електронний ресурс]. – Режим доступу :http://antivirus.ua/taxonomy/term/556.

Надійшла 09.11.2015 р. Рецензент: д.т.н., проф. ШевченкоВ.Л.