УДК: 35.073.533

В.М. Пригода

РОЗБУДОВА СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ: СТАН ТА ПЕРСПЕКТИВИ

Стаття присвячена розкриттю стану та проблем впровадження системи інформаційної безпеки в Україні на тлі світового досвіду.

The article is devoted to the exposing of the state and the problems as for implantation of the informatic security system in Ukraine at the world experience background.

Ключові слова: інформаційна безпека, стан, перспективи, Україна, світовий досвід.

Становлення інформаційного суспільства в Україні зумовлене щораз вищим значенням інформаційної сфери, яка являє собою сукупність інфокомунікаційної інфраструктури, власне інформації, суб'єктів, що здійснюють збір, формування, поширення і використання інформації, системи регулювання суспільних відносин, які виникають при цьому, а також взаємовідносин держава — суспільство, держава — бізнес — споживач та держава — громадянин.

Основу світової інфокомунікаційної структури становить мережа Інтернет, яка впливає на розвиток економік країн, всієї інформаційної сфери і забезпечує доступ до інформаційних ресурсів та послуг. Розвиток інфокомунікаційної структури, мережі Інтернет і сервісів, що на них базуються, становлять предмет підвищеної уваги як світової спільноти в цілому, так і окремо взятих держав.

Формування інформаційного суспільства є однією з важливих умов економічного розвитку і духовного розквіту цивілізації і, врешті-решт, збереження стратегічної стабільності у світі. Рух України до спільноти інформаційного суспільства не відмінює наявності у нас своїх власних національних інтересів і необхідності забезпечення безпеки цих інтересів. Саме тому обговорення аспектів інформаційної безпеки сьогодні є актуальним.

За дослідженнями Boston Consulting Group (BCG) серед країн G20 найбільш інтернет-орієнтовану економіку має Велика Британія. Частка інтернет-бізнесу у ВВП країни в 2010 р. становила 8,3 %. Обсяг інтернет-економіки країни оцінювався в 121 млрд фунтів ($192 млрд). Прогнозоване зростання інтернет-бізнесу в найближчі чотири роки — на 11 % щорічно [6].

Для оцінки відносного стану України у світовій і європейській ієрархії розвитку інформаційного суспільства доцільно навести таку статистику.

За даними Міжнародного союзу електрозв'язку (МСЕ, ITU) у світі продовжується щорічне зростання кількості користувачів Інтернету на 9 %. У другому кварталі 2011 р. їх нараховувалося більше ніж 2 млрд. У Європі знаходиться більше ніж 476 млн користувачів. Україна за кількістю інтернет-користувачів займає в Європі 9-те місце [3].

У сфері електронної комерції в 2011 р. покупки через Інтернет здійснювали 52 % інтернет-користувачів України. За оцінками експертів у 2010 р. обсяг українського ринку інтернет-торгівлі перевищив $1,0 млрд [3].

Обсяг вітчизняного ринку IT (без телекомунікацій) у 2011 р. становив близько $3,3 млрд, що відповідає приблизно 2 % ВВП України. З них майже 88 % припадає на комп'ютери, комп'ютерну периферію та мережні пристрої, решта 12 %, приблизно порівну, — на програмне забезпечення і послуги, включаючи розробку програм. Така структура IT-витрат, на жаль, залишається незмінною вже багато років. Наприклад, у Польщі й Чехії ємність IT-ринку становить відповідно $8,5 млрд і $4,9 млрд (1,6 % і 2,2 % ВВП), а сукупна частка програмного забезпечення і послуг — 54 % і 58 % [9].

У сфері інформатизації працює 3119 юридичних осіб, з них близько 2 тис. компаній працюють у галузі розробки програмного забезпечення. Кількість IT-спеціалістів в Україні на кінець 2010 р. становила близько 215 тис. осіб. При цьому відзначено розвинений бізнес офшорного програмування, оборот якого становить не менше ніж $1,0 млрд і демонструє щорічне зростання у 30—40 % [3; 9].

З інформаційної мережі, призначеної для обміну інформацією засобами електронної пошти і для забезпечення доступу до віддалених файлових архівів, Інтернет перетворюється на ринок послуг зі значними інвестиціями, зростає також частка ВВП інформаційної сфери. В Інтернеті розвивається рекламний бізнес, онлайн-аукціони, ігровий бізнес, електронна комерція.

Наведені дані об'єктивно свідчать, що інформаційна сфера стає невід'ємною і основоположною частиною життя суспільства. Як системоутворювальний чинник, вона перетворюється на домінантне джерело створення та примноження національного багатства та стає об'єктом безпеки держави, визначає і, відповідно, впливає на стан політичної, економічної, оборонної й інших її складників. Комерціалізація та інтенсивна капіталізація інформаційних ресурсів призводять до необхідності формування та розвитку системи безпеки інформаційної сфери.

Саме стан і проблеми розвитку системи безпеки інформаційної сфери, яка все більше займає провідні позиції, ще і досі малодосліджені. Тому метою даної статті й стало розкриття стану й проблем розвитку такої системи в Україні на тлі світового досвіду з урахуванням конкретики країни.

Стрімке поширення інформаційних і комунікаційних технологій (ІКТ) у всіх сферах суспільної діяльності призвело до появи таких видів злочинів, як комп'ютерна злочинність і комп'ютерний тероризм: незаконне втручання в роботу електронно-обчислювальних машин, комп'ютерних та інфокомунікаційних систем і мереж, викрадання і присвоєння інформації з комп'ютерів, комп'ютерних мереж, а також із систем збору та зберігання інформації. Кібертероризм і кіберзлочинність уособлюють форми цілеспрямованої злочинної діяльності з використанням інфокомунікаційних технологій та вкрай негативно впливають на розвиток ринку інформаційних ресурсів.

Саме кіберзлочинність і кібертероризм стають світовою загрозою номер один. Виникли міжнародні спільноти хакерів, які мають на меті політичні або навколополітичні цілі, перешкоджають діяльності органів офіційної влади всіх рівнів в Інтернеті. Таким чином поширюється «чорний піар» територією країн СНД: відбувається маніпуляція свідомістю громадян, спотворення об'єктивної інформаційно-політичної реальності.

Регулярно повідомляють про випадки несанкціонованого доступу комп'ютерних злочинців до приватної і секретної державної інформації [11]. Найпоширеніші кіберзлочини — це несанкціонований доступ та пошкодження баз даних компаній і урядових організацій, виведення з ладу промислових об'єктів, викрадення інновацій або технологій, крадіжка грошей із рахунків юридичних та фізичних осіб. Успішна атака через Інтернет може викликати значні фінансові втрати для будь-якого суб'єкта економічної діяльності. За деякими оцінками через кіберзлочинність світова економіка щорічно втрачає $114 млрд. США оцінюють свої збитки за всі роки існування глобальної мережі в $400 млрд. Щорічні втрати тільки від крадіжки грошей із зарплатних рахунків працівників американських компаній оцінюють у $1 млрд [1].

Останнім часом відзначають зростання рівня кіберзлочинності в Росії, Бразилії, Китаї, Індії, Україні. На жаль, Україна увійшла до трійки лідерів за DDoS-атаками: за даними «Лабораторії Касперського» 12 % всіх атак припадає на нашу країну. За статисткою МВС України в Україні в 2010 р. сталося 190 злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку. За даними 3-го кварталу 2011 р. питома вага таких злочинів становила 0,03 % [3]. При цьому в Україні один із найнижчих у Європі рівнів підключення до Інтернету [1].

До збитків компаній можна віднести не тільки прямі втрати від дій хакерів, але й витрати на захист від кібератак. Якщо в 2006 р. видатки компаній США на інформаційну безпеку становили $61,5 млрд, то в 2011 р. оцінка витрат становила $130 млрд, тобто за п'ять років витрати на інформаційну безпеку подвоїлися [2]. На жаль, превентивні заходи не завжди достатньо ефективні і втрати продовжують збільшуватися.

Розгортається безкомпромісна боротьба зі злочинами у сфері інформаційних технологій. Наприклад, у Великій Британії, відповідно до «Закону про тероризм 2000 року», жорсткому покаранню підлягають дії, які можуть бути класифіковані як серйозне несанкціоноване втручання в роботу електронної системи. У КНР створено систему державних організацій з боротьби з небажаним інформаційним впливом в Інтернеті. Закони КНР жорстко контролюють спроби іноземних компаній взяти участь в інтернет-бізнесі на території Китаю, незалежно — у формі інвестицій або постачання апаратних засобів [11].

В Україні, як вважає голова СБУ, головними загрозами національній безпеці є посягання на територіальну цілісність, міжнародний тероризм, корупція і кіберзлочинність. Збиток, який завдає кіберзлочинність, вже значно перевищує розмір збитків від традиційних видів злочинів. Кількість протиправних посягань на інформаційні ресурси держави продовжує зростати. Державі необхідно захищатися ще й тому, що інформаційна безпека є одним із чинників соціальної безпеки. Вважається, що проблеми в цій сфері часто мають не техногенне походження, а їх розв'язання може полягати в тому, щоб обмежити доступ людей, які становлять потенційну загрозу. Нині забезпечення комп'ютерної безпеки ведеться переважно у площині технологічних рішень [12].

Існує два бачення поняття безпеки. Відповідно до першого її розглядають як поглиблення відкритості соціального простору. Друге передбачає утримання наявних форм комунікації в контрольованому стані зі створенням системи регулювання умов та порядку входження у глобальний інфокомунікаційний простір. В обох випадках проблему безпеки розв'язують завдяки політичній владі.

Цензура, як механізм інформаційної безпеки, була дієвою, але пережила себе, залишилася в минулому. Сьогодні безпека можлива лише за умов використання соціальних технологій, які відповідають вимогам цього єдиного простору. У майбутньому більш адекватними стануть спеціально орієнтовані програми освіти, соціальної підтримки, легітимації (суспільного визнання), культурні акції тощо. Насправді, необхідно навчитися створювати самодостатні локальні інформаційні середовища. При цьому однією з найпоширеніших проблем є розповсюдження шкідливого програмного забезпечення [15]. За даними «Лабораторії Касперського» кількість шкідливих програм для мобільних пристроїв за 2011 р. зросла більше ніж у 6 разів. Як і раніше, домінують примітивні SMS-трояни. Друге місце зайняли бекдори — шкідливі програми, які дозволяють віддалено контролювати заражений пристрій. На третьому місці — програми-шпигуни, які «крадуть» особисті дані користувача і/або дані про мобільний пристрій. Звертають на себе увагу витончені схеми атак на користувачів онлайн-банкінгу за допомогою мобільних троянців, зафіксовані в 2010 р. Мобільні троянці працюють спільно із шкідливим програмним забезпеченням на комп'ютері користувача. Це надає кіберзлочинцям можливість підтверджувати фінансові операції, що здійснюються із зламаних банківських акантів.

У вересні 2011 р. було зафіксовано перший випадок розповсюдження шкідливого програмного забезпеченням за допомогою QR-кодів (quick response — швидкий відгук), які замінили кіберзлочинцям звичайні надсилання через особливу зручність їх використання на мобільних пристроях. У мережі з'явилися сайти з QR-кодами для мобільних додатків, в які були зашифровані посилання на шкідливий файл. Після сканування зараженого коду на смартфон завантажувався троянець, який відправляв SMS-повідомлення на короткі платні номери. Можна вважати, що кіберзлочинці фактично автоматизували виробництво та розповсюдження шкідливого файлу програним забезпеченням [15].

Слід навести особливо значущий приклад хоча й незловмисного, але негативного впливу засобів ІКТ саме на діяльність бірж [2].

Як великі, так і дрібні учасники біржових торгів легально застосовують електронні торгівельні програми, так звані роботи, не усвідомлюючи при цьому повною мірою можливі наслідки. Проблема у швидкості їх реакції та впливу на динаміку процесів торгів. Саме надшвидка робота біржових комп'ютерних програм найчастіше провокує раптові стрибки показників ринків. Достатньо одній машині почати активно знижувати ціни на акції, як у процес залучаються інші, починається ланцюгова реакція.

За останні 6 років зареєстровано 18,5 тис. подібних збоїв. Найбільш значний із них у травні 2010 р. призвів до втрат ринку у $1 трлн. Тоді лише за 6 хвилин індекс Dow Jones впав на 1 тис. пунктів. Це стало найсильнішим миттєвим провалом фондового індикатора за всю його історію. Ціни на акції деяких компаній знизилися до нуля. Не встояли навіть гіганти ринку, наприклад, папери Procter & Gamble обвалилися на 60 %. Ланцюговий процес вдалося зупинити, а колосальні втрати — відновити.

Наведений приклад наочно ілюструє можливі загрози, які потрібно передбачати, щоб мати засоби для захисту та відповідної протидії.

Також наочною виглядає резонансна подія, яка сталася в Україні в січні 2012 р. Вона пов'язана із закриттям українського файлообмінного ресурсу EX.UA та вилученням серверів із контентом [12]. Приводом для відкриття судової справи стало звернення кількох офіційних представників світових розробників програмного забезпечення,

програмні продукти яких протизаконно розповсюджувалися через вказаний веб-сайт. Зазначені дії було проведено за постановою слідчого, яка вже 2 лютого 2012 р. була визнана незаконною, оскільки дії МВС України викликали обурення. Користувачі Інтернету влаштували спротив, розгорнувши DDoS-атаки на сайти державних органів, насамперед — МВС України. Під час виконання значної кількості запитів одночасно з великої кількості комп'ютерів така атака призвела до «відмови в обслуговуванні». Аналогічна ситуація може виникнути ненавмисно через великий наплив користувачів [13].

Таким чином сайти державних органів припинили роботу. Це навіть не були «хакерські» атаки, під якими нині розуміють замах на систему безпеки з метою захоплення контролю над віддаленою/локальною обчислювальною системою, або її дестабілізація, або «відмова в обслуговуванні». Юристи вважають, що спроба представити закриття ресурсу як боротьбу з піратством не може сприйматися серйозно. Правова позиція така: ресурс не повинен нести відповідальність за піратський контент, розміщений користувачами. Ресурс є лише інструментом і працює легально. Крім того, постанову проти EX.UA було винесено з порушенням законодавства, яке чітко визначає, що питання про використання домена повинні розв'язувати в судовому порядку [13].

Згідно з Конституцією України кожний має право вільно збирати, зберігати, використовувати й поширювати інформацію усно, письмово або іншим способом — на свій вибір. Згідно із Законом України «Про інформацію» одним із основних принципів інформаційних відносин є доступність інформації і свобода її обміном. Ресурс є засобом обміну інформацією, а блокування його роботи за даних обставин є істотним обмеженням права на обмін інформацією. Отже, масштаби дій слідства не відповідали поставленому завданню і можуть вважатися неправомірними.

Розглянута ситуація фокусує увагу як на проблемі стану захищеності держави від можливих проявів кіберзлочинності, так і на проблемах неготовності держави, тобто українського законодавства та правоохоронних органів, до боротьби з кіберзлочинністю.

Останнім часом з'являються публікації, присвячені проблемам психічного впливу інформації на людину та можливості адаптації людини до умов нового інформаційного середовища. Сучасна людина живе й діє в інформаційному світі, у якому різко зросли обсяги інформації. Для позначення цього явища застосовують термін «інформаційний вибух».

В антропологічному аспекті інформаційний вибух і стрімка комп'ютеризація вплинули на людську життєдіяльність. З одного боку, інформація розширила межі життєвого середовища людей, допомогла їм стати причетними до подій, що відбуваються у світі. Але, з другого боку, збагативши й розширивши сферу спілкування, інформаційний вибух призвів до розмиву меж особистого мікропростору, певною мірою зменшив можливості психологічного контакту. Більші обсяги інформації перевантажують нервову систему людини, її інтелектуальні можливості. Так виникає інформаційне перенапруження, що свідчить про невідповідність біологічних можливостей людини сучасним темпам зростання інформаційного навантаження. Допомогти людині в інформаційно перенасиченій обстановці може висока інформаційна культура, яку забезпечує послідовна інформаційна політика держави, що має забезпечувати інформаційну безпеку.

Як підсумок стану національної інформаційної безпеки слід навести такі висловлення [4]: «Попри те, що Україна, завдячуючи, перш за все, потужному на початках незалежності державницькому інтелектуальному потенціалу, що був залучений до ство-

рення основ держави, першою на пострадянському просторі створила всебічну нормативно-правову основу національної безпеки і оборони, нині наша країна не захищена ні економічно, ні політично, ні інформаційно, духовно, ні військовою потугою».

Питання національної інформаційної безпеки загалом поділяють на три сфери життєво важливих інтересів [7]:

— держави — недопущення інформаційної експансії з боку інших держав та структур, ефективна взаємодія органів державної влади та інститутів громадянського суспільства, побудова та розвиток інформаційного суспільства, забезпечення економічного та науково-технологічного розвитку України, інтеграція її у світовий інформаційний простір;

— суспільства — забезпечення суспільно-політичної стабільності, формування і розвиток демократичних інститутів громадянського суспільства;

— особи — недопущення несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних та захищеність від негативного інформаційно-психологічного впливу.

Одним із джерел загроз в інформаційній сфері є поступальний розвиток та ускладнення інфокомунікаційної складової частини критично важливих об'єктів інфраструктури. Найнебезпечнішими загрозами інтересам держави в інформаційній сфері є застосування «інформаційної зброї» і розгортання «інформаційних воєн». «Інформаційна зброя» надає можливість силового впливу на інформаційну сферу конфронтуючої сторони з метою досягнення певних політичних і військових цілей. Такі загрози можуть включати одержання доступу до відомостей, що становлять державну таємницю, а також до іншої конфіденційної інформації, що може завдати шкоди інтересам держави.

Загрози інтересам суспільства полягають у порушенні функціонування складників інформаційної інфраструктури або у несанкціонованому доступі до інформації, яка охороняється законом, з боку злочинних, зокрема терористичних організацій. Об'єктами таких дій можуть бути органи державної влади, силові та правоохоронні відомства, суб'єкти економічної діяльності, фінансові установи, об'єкти інфраструктури. Кіберзлочинність проявляється у здійсненні шахрайських операцій із використанням інфокомунікаційних систем, «відмиванні» фінансових коштів, отриманих протиправним шляхом, одержанні неправомірного доступу до фінансової, банківської та іншої інформації в корисливих цілях. Метою кіберзлочинності може бути примушення до прийняття необхідних терористам рішень.

Загрозою соціальним інтересам людини є використання на шкоду її інтересам персональних даних, які збирають, наприклад, органи державної влади, а також прихований збір інформації, яка становить її особисту таємницю, відомостей про її приватне життя. Найнебезпечнішою загрозою є розширення можливості маніпулювання свідомістю людини за рахунок формування індивідуального віртуального інформаційного простору, а також використання технологій впливу на її психічну діяльність. Саме тому важливо забезпечити безпеку спілкування людини з інформаційною інфраструктурою.

Це обумовлює наявність життєво важливих, національних інтересів в інформаційній сфері як збалансованої сукупності соціальних інтересів людини, інтересів суспільства й держави. Захищеність цих інтересів характеризує інформаційну безпеку, забезпе-

чення якої передбачає реалізацію комплексу правових, організаційних, технологічних і кадрових заходів.

На етапі розбудови в нашій країні інформаційного суспільства потрібен глобальний комплексний підхід до розв'язання проблеми інфраструктурного забезпечення інформатизації, основними складниками якого мають бути завдання створення відповідної законодавчої бази і побудованої відповідно до неї системи забезпечення інформаційної безпеки.

Нині в Україні не вистачає сучасних системних нормативних документів, які мають визначати загрози і формувати власне єдину державну політику з інформаційної безпеки у національному інформаційному просторі.

У Стратегії національної безпеки 2007 р. зазначено, що Україна має розробляти та впроваджувати національні стандарти і технічні регламенти застосування ІКТ, гармонізовані з європейськими стандартами, зокрема з вимогами Конвенції про кіберзлочинність. Проте зазначена конвенція більше орієнтована на протидію шахрайству, порушенню авторських прав тощо, які здійснюються з використанням ІКТ. Нова редакція Стратегії національної безпеки вже враховує кібербезпекову проблематику в осучасненому розширеному обсязі [3].

Основоположним документом у сфері національної інформаційної безпеки є Доктрина інформаційної безпеки України, затверджена Указом Президента України від 08.07.2009 [7]. У документі зазначено, що інформаційний простір стає головною ареною боротьби національних інтересів держав. Інформаційна складова частина є одним із найважливіших елементів забезпечення національної безпеки. Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою впливають і визначають рівень і темпи соціально-економічного, науково-технічного і культурного розвитку. Розвиток України в сучасних умовах можливий тільки за умови забезпечення належного рівня її інформаційної безпеки.

Серед основних засад інформаційної безпеки країни документ визначає, зокрема, такі, як: гармонізація особистих, суспільних і державних інтересів; запобігання правопорушенням в інформаційній сфері; гармонізація українського законодавства в інформаційній сфері з міжнародним.

До напрямків реальних і потенційних загроз інформаційній безпеці України належать такі: внутрішньополітичний, економічний, соціально-гуманітарний, науково-технологічний, екологічний.

Як загрози розглядають: поширення цілеспрямовано викривленої інформації через ЗМІ або мережу Інтернет з метою негативного інформаційного впливу; недостатню розвиненість інститутів громадянського суспільства, відставання України за рівнем інформатизації соціальної та гуманітарної сфер.

Зусилля держави, громадянського суспільства і людини мають бути зосереджені на спільній діяльності за такими головними напрямами, як: технологічний розвиток національних ІКТ, інноваційне оновлення національних інформаційних ресурсів, технологій їх створення, обробки та поширення; протидія проявам кіберзлочинності, комп'ютерного тероризму з метою захисту національних інфокомунікаційних систем, мереж, інформації та інформаційних ресурсів, зокрема захисту від кібернетичних атак; інформаційно-психологічний, зокрема стосовно забезпечення конституційних прав і сво-

бод людини, утвердження і захисту загальнолюдських та національних моральних цінностей [7].

Для створення довершеної системи національної інформаційної безпеки держава повинна забезпечувати:

— розвиток міжнародного співробітництва у сфері захисту інформації в інфокомунікаційних системах, інтеграцію в міжнародні інфокомунікаційні системи та організації за умови збереження інформаційного суверенітету;

— удосконалення національного законодавства, його гармонізацію з міжнародними документами; координацію діяльності органів державної влади у сфері інформаційної безпеки;

— захист інформаційних ресурсів на державному рівні, розробку методів і засобів захисту інформації від несанкціонованого доступу;

— контроль за додержанням вимог інформаційної безпеки в системах збирання, обробки, зберігання і передачі статистичної, фінансової, біржової, податкової та митної інформації;

— удосконалення системи статистичної звітності з метою підвищення об'єктивності і відповідності міжнародним вимогам;

— формування і розвиток в Україні інформаційного суспільства, розширення можливостей безпечного доступу громадян до світового інформаційного простору;

— взаємодію органів державної влади з громадськими організаціями та громадянами, створення системи громадського контролю за діяльністю органів державної влади і місцевого самоврядування.

Наступним документом, який визначав би державну інформаційну політику, питання інформаційної безпеки, мав стати Проект закону України «Про Основні засади державної інформаційної політики» від 13.10.2010 (остання редакція від 23.06.2011) [14.1]. На жаль, проект закону був відхилений Постановою Верховної Ради України від 05.07.2011 [14.2].

У зазначеній редакції розглядалася низка актуальних на сьогодні проблем, які виникли на шляху розвитку та захисту національної інформаційної сфери:

— відсутність довгострокової державної стратегії щодо її розвитку;

— недооцінка значення інфокомунікаційного аспекту в процесі демократизації суспільства, розбудови держави, її європейської інтеграції;

— недосконалість законодавства про інформацію;

— намагання суб'єктів інформаційних відносин маніпулювати громадською думкою шляхом поширення недостовірної, неповної та упередженої інформації у ЗМІ;

— наявність інформаційної продукції, що не відповідає вимогам законодавства, негативно впливає на систему суспільних цінностей, фізичний, психічний, інтелектуальний та моральний розвиток людини, призводить до деградації суспільства;

— неефективність дій органів державної влади, спрямованих на захист стратегічних національних інтересів на міжнародному рівні, зокрема стосовно контролю і регулювання інформаційних потоків з-поза меж держави [3].

Таким чином, розв'язання проблем в інформаційній сфері потребує удосконалення державної інформаційної політики, розвитку міжнародного співробітництва і гарантування інформаційного суверенітету України.

Важливими напрямками реалізації державної інформаційної політики є створення умов для формування її сучасної моделі, підвищення ефективності використання інформаційних ресурсів і управління елементами інфокомунікаційної інфраструктури, забезпечення розвитку та захисту вітчизняної інформаційної сфери. Базовими принципами державної інформаційної політики мають бути: верховенство права, пріоритет прав і свобод людини; дотримання балансу інтересів особи, суспільства і держави; захист національних інтересів у сфері інформаційної безпеки; сприяння розвитку та захисту національних інформаційних ресурсів; забезпечення системності та координації дій органів державного управління і регулювання в інформаційній сфері; забезпечення охорони і захисту інформації, зокрема інформації з обмеженим доступом; недопущення зловживання свободою діяльності ЗМІ на шкоду правам і свободам людини.

До пріоритетних завдань державної інформаційної політики входять: забезпечення розвитку вітчизняної інформаційної сфери з метою консолідації української нації, зміцнення цілісності України на основі суспільних цінностей, завдань, ідей; забезпечення розвитку громадянського суспільства, його демократичних інституцій; формування демократично орієнтованої громадської свідомості, сприяння розвитку духовності, культурних, освітньо-виховних і моральних засад, підвищення інтелектуального потенціалу, збереження національної та культурної самобутності; захист від інформаційної продукції, що негативно впливає на фізичний, психічний, інтелектуальний та моральний розвиток людини; забезпечення інформаційного суверенітету України.

До основних напрямків реалізації державної інформаційної політики щодо захисту інформаційних ресурсів слід віднести: узгодження законодавства про інформацію із сучасними вимогами, адаптацію його до законодавства ЄС; запровадження дійового державного, парламентського та громадського контролю за дотриманням вимог законодавства про інформацію та встановлення відповідальності за їх порушення; забезпечення прозорості і публічності діяльності органів державної влади та органів місцевого самоврядування; захист вітчизняного інформаційного ринку; забезпечення захисту прав споживачів шляхом сертифікації інформаційного обладнання і послуг, контролю їх якості; забезпечення дотримання норм суспільної моралі, обмеження поширення інформаційної продукції, яка може завдати шкоди людині і суспільству, в інтересах національної, громадської та економічної безпеки, для захисту прав і свобод людини; консолідацію дій органів державної влади та суспільства, спрямованих на запобігання поширенню інформаційної продукції, що негативно впливає на фізичний, психічний, інтелектуальний та моральний розвиток дітей; забезпечення дійового захисту інформаційного суверенітету України, зокрема, вітчизняного сегмента Інтернету [14].

Реалізація державної інформаційної політики має здійснюватися шляхом внесення змін до законодавства щодо: визначення механізму реалізації права кожного на доступ до інформації, яка знаходиться у володінні суб'єктів владних повноважень; посилення відповідальності за порушення законодавства про інформацію та у сфері захисту суспільної моралі; регулювання відносин, пов'язаних із обігом інформаційної продукції, що негативно впливає на фізичний, психічний, інтелектуальний та моральний розвиток людини.

В Україні у забезпеченні інформаційної безпеки держави беруть участь Державна служба спеціального зв'язку та захисту інформації, а також відповідні підрозділи Служби безпеки України, Міністерства внутрішніх справ та Міністерства оборони України. Але при цьому відсутній єдиний національний координаційний центр, який би спрямовував у єдине русло діяльність зазначених відомств з метою створення ефективної системи захисту вітчизняного інформаційного простору. Ситуація ускладнюється відсутністю і невизначеністю на сьогодні нормативного поля, що породжує проблему чіткого розмежування обов'язків і повноважень зазначених державних інституцій.

Отже, в умовах зростання ролі інформації та інформаційних послуг у житті суспільства знищення або перекручування інформації в одній із взаємопов'язаних інформаційних систем може викликати ланцюгову реакцію поширення такої неадекватної інформації і призвести до катастрофічних наслідків. Гарантована безпека, надійність і можливість швидкого відновлення інформаційних систем стають основними вимогами безпеки суспільства в цілому. При цьому стає неприпустимою ситуація, за якої у взаємопов'язаних інформаційних системах і електронних ресурсах можуть існувати ланки з високим ступенем ризику бути виведеними з ладу на тривалий час або бути остаточно втраченими внаслідок непередбачених стихійних обставин, терористичного акту, комп'ютерного злочину або дій обслуговувального персоналу.

1. [Электронный ресурс]. — Режим доступа: http://korrespondent.net/business/web/1326089-kiberprestupnost-obhoditsya-mirovoj-ekonomike-v-114-mlrd-v-god. — 05.03.2012; 2. *Наймушин И.* Страна чудес: кто правит бал на рынках? Заглянуть в кроличью нору [Электронный ресурс] / И. Наймушин. — Режим доступа: http://investfunds.ua/news/strana-chudes-kto-pravit-bal-na-rynkah-vestiru-94053. — 05.03.2012; 3. Доповідь про стан інформатизації та розвиток інформаційного суспільства в Україні за 2011 рік / Кабінет Міністрів України. — К., 2011 [Електронний ресурс]. — Режим доступу: http://dki.org.ua/node/119; 4. *Процик П.* Обеззброєна країна [Електронний ресурс] / П. Процик. — Режим доступу: http://maidan.org.ua/2012/02/obezzbrojena-krajina.— 03.02.2012; 5. Розпорядження Кабінету Міністрів України від 01.11.2010 № 2071-р «Про затвердження переліку урядових комітетів та їх посадового складу» [Електронний ресурс]. — Режим доступу: http://zakon2.rada.gov.ua/laws/show/2071-2010-%d1%80; 6. [Электронный ресурс]. — Режим доступа: http://www.ukrrudprom.ua/news/dolya_internetekonomiki_v_vvp_britanii_sostavlyaet_8.html. — 20.03.2012; 7. Доктрина інформаційної безпеки України. Затверджено указом Президента України від 8 липня 2009 року [Електронний ресурс]. — Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=514%2f2009; 8. *Поздняков В.* Сделайте с умом [Электронный ресурс] / В. Поздняков. — Режим доступа: http://blogs.korrespondent.net/business_blogs/blog/vpozdnyakov/a60995. — 23.03.2012; 9. СБУ: головні проблеми для України — тероризм і кіберзлочинність [Електронний ресурс]. — Режим доступу: http://www.pravda.com.ua/news/2012/03/23/6961285/.— 23.03.2012; 10. У Росії вже подумують про атаки у кіберпросторі [Електронний ресурс]. — Режим доступу: http://www.pravda.com.ua/news/2012/03/22/6961200. — 22.03.2012; 11. МВД изъяло 200 серверов сервиса хранения информации ex.ua. [Электронный ресурс] // РБК-Украина. — Режим доступу: http://www.rbc.ua/rus/newsline /show/mvd-izyalo-200-serverov-servisa-hraneniya-informatsii-ex-ua-31012012171300. — 31.01.2012; 12. *Сизов Д.* Скандал с EX.UA обнажил целый пласт украинских web-проблем [Электронный ресурс] / Д. Сизов. — Режим доступа: http://internet-ua.com/skandal-s-EX-UA-obnajil-celii-plast-ukrainskih-webproblem. — 02.03.2012; 13. Кількість мобільних загроз зросла в шість раз. Кіберзлочинці обирають Android. [Електронний ресурс]. //Економічна правда.— Режим доступу: http://www.epravda.com.ua/news/2012/03/5/317795/

— 05.03.2012; 14. 1. Закон України (проект) «Про Основні засади державної інформаційної політики» (ред. від 23.06.2011) [Електронний ресурс]. — Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/ ed_2011_07_05/JF5LF00I.html; 2. Відхилений Постановою ВР України від 05.07.2011 № 3590-VI, чинною з 05.07.2011: [Електронний ресурс]. — Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/ link1/ed_2011_07_05/ T113590.html; 15. Щербина В.Н. Сетевые сообщества в ракурсе социологического анализа [Електронний ресурс] / В.Н.Щербина. — Режим доступу: http://lib.socio.msu.ru/l/library?e=d-000-00---001ucheb--00-0-0-0prompt-10---4------0-0l--1-ru-50---20-help---00031-001-1-0windowsZz-1251-10&a=d&c=01ucheb&cl=CL1&d=HASH74dcd f8c4002593e2d3a18.6.— 2012.