УДК 341:004.056

ПРАКТИЧНІ АСПЕКТИ ФОРМУВАННЯ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Курмаєв П.Ю., Байрамов Е.А.

Анотація. Стаття присвячена практичним аспектам формування системи інформаційної безпеки. Для досягнення поставленої мети використовувалися методи: структурно-функціональний, історичний, експертних оцінок, логічного узагальнення. У статті вказується, що в сучасних умовах інформація стає невід'ємною частиною цивілізаційного розвитку. Визначено, що метою забезпечення інформаційної безпеки в Україні є створення розгалуженого та захищеного інформаційного простору, захист національних інтересів України.
Ключові слова: інформаційна безпека, державне регулювання, інформаційний простір.

Аннотация. Статья посвящена практическим аспектам формирования системы информационной безопасности. Для достижения поставленной цели использовались методы: структурно-функциональный, исторический, экспертных оценок, логического обобщения. В статье указывается, что в современных условиях информация становится неотъемлемой характеристикой цивилизационного развития. Определено, что целью обеспечения информационной безопасности в Украине является создание защищенного информационного пространства, защита национальных интересов Украины.
Ключевые слова: информационная безопасность, государственное регулирование, информационное пространство.

Постановка проблеми. Трансформація економічних відносин, що відбувається під впливом новітніх інформаційних технологій, зумовила широке використання знань та ідей, які людство накопичувало протягом століть, тому інформація стає невід'ємною частиною цивілізаційного розвитку [1]. Важливого значення, у даному контексті, набуває процес формування інформаційних ресурсів, який висвітлено у [2].

З метою найбільш повного використання переваг інформаційного суспільства відповідні технології повинні спрямовуватися на досягнення взаємодоповнюючих цілей: забезпечення економічного зростання регіонів, підвищення, на цій основі, добробуту населення, реалізації стабільного транспарентного і відповідального регулюючого впливу.

Аналіз останніх досліджень і публікацій з проблеми. Проблематиці забезпечення інформаційної безпеки присвячено наукові праці вчених: З. Варналія, В. Гавловського, О. Морозова, О. Сосніна та інших.

Разом з тим окремі практичні аспекти формування системи інформаційної безпеки потребують додаткового вивчення. Це й зумовлює проведення наукових розвідок у даному напрямі.

Формулювання цілей дослідження. Метою даної статті є дослідження практичних аспектів формування системи інформаційної безпеки.

Виклад основних результатів та їх обґрунтування. Інтереси держави в інформаційній сфері полягають у створенні умов для гармонійного розвитку інформаційної інфраструктури як регіону, так і країни в цілому, реалізації конституційних прав і свобод громадян, зміцненні конституційного ладу, суверенітету і територіальної цілісності, забезпечення економічної, політичної й соціальної стабільності, безумовного виконання законів і підтримки правопорядку, розвитку міжнародного співробітництва на основі партнерства [3].

У розвинутих країнах світу органи державної та регіональної влади є активними учасниками процесу розвитку інформаційно-комунікаційних технологій, створюючи для цього спеціальні умови, що включають упорядкування інформації, засобів телекомунікацій.

Організація управління інформаційними ресурсами передбачає створення норм і механізмів, що забезпечують [3]:

– координацію діяльності щодо формування регіональних інформаційних ресурсів;

– визначення повноважень і відповідальності щодо формування інформаційних ресурсів органів державного та регіонального управління;

– визначення порядку фінансування і фінансової звітності зі створення і ведення інформаційних ресурсів;

– організацію реєстрації й обліку інформаційних ресурсів;

– контроль використання інформаційних ресурсів;

– контроль захисту і збереження інформаційних ресурсів.

Ми пропонуємо інформаційну безпеку розглядати як стан функціонування інформаційної системи, що забезпечує відповідний рівень її захищеності від випадкових або навмисних дій, які можуть впливати на процеси формування, зберігання та використання інформаційних ресурсів.

Метою забезпечення 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 на отримання, поширення та використання інформації. Проблема інформаційної безпеки не може бути вирішена без впровадження нових ідей, знань та реалізації відповідної політики у сфері інформатизації. Ігнорування проблем інформаційної безпеки може негативно вплинути на прийняття найважливіших політичних, економічних, соціальних, військових рішень тощо [4].

Аналіз стану інформаційної безпеки України показує, що до основних проблем забезпечення інформаційної безпеки належать ті з них, що мають загальносистемний характер, пов'язані з відсутністю наукового обґрунтування і практичної апробації політики і методології організації державної системи інформаційної безпеки. За своїм характером це, переважно, правові, науково-технічні, економічні, організаційні, кадрові проблеми тощо.

Ситуація, що склалася в інформаційній сфері України, вимагає вирішення таких комплексних проблем, як [5, с.127]:

– розвиток науково-практичних основ інформаційної безпеки, а саме, визначення основних положень стратегії держави в сфері створення та забезпечення умов формування і використання інформаційних ресурсів,

– підтримка високих темпів їх формування і заданих критеріїв якості;

– створення законодавчої і нормативно-правової бази забезпечення інформаційної безпеки;

– розроблення механізмів реалізації прав громадян на інформацію загального користування;

– визначення основних положень стратегії держави у сфері використання засобів масової інформації у процесі формування суспільної свідомості, розробка методів і форм інформаційної політики держави.

Можна виділити декілька основних джерел загроз безпеці регіонального інформаційного простору:

За своєю загальною спрямованістю загрози інформаційній безпеці України можна поділити на такі види:

1. Загрози конституційним правам і свободам людини і громадянина у сфері духовного життя й інформаційної діяльності, індивідуальній, груповій і суспільній свідомості, духовному відродженню України.

2. Загрози інформаційному забезпеченню процесу регулювання економічного розвитку на регіональному рівні.

Загрозами конституційним правам і свободам людини і громадянина у сфері духовного життя й інформаційної діяльності, індивідуальній, груповій і суспільній свідомості, духовному відродженню України можуть бути [6]:

– прийняття органами державної влади нормативних правових актів, що обмежують конституційні права громадян у сфері духовного життя й інформаційної діяльності;

– створення монополій на формування, отримання й поширення інформації в Україні, в тому числі з використанням телекомунікаційних систем;

– нераціональне, надмірне обмеження доступу до суспільно необхідної інформації;

– протиправне застосування спеціальних засобів впливу на індивідуальну, групову і суспільну свідомість;

– невиконання органами державної влади, органами місцевого самоврядування, організаціями і громадянами вимог українського законодавства, що регулює відносини в інформаційній сфері;

– неправомірне обмеження доступу грома-

дян до відкритих інформаційних ресурсів органів державної влади України, органів місцевого самоврядування, відкритих архівних матеріалів, іншої відкритої соціально значущої інформації;

– порушення конституційних прав людини і громадянина у сфері засобів масової інформації;

– маніпулювання інформацією (дезінформація, приховування або перекручування інформації).

Інтереси особи в інформаційній сфері полягають, насамперед, у реальному забезпеченні конституційних прав і свобод людини і громадянина на доступ до відкритої інформації, на використання інформації для здійснення не забороненої законом діяльності, а також у захисті інформації, що забезпечує особисту безпеку, духовний і інтелектуальний розвиток [3].

Складність процедур, реалізованих у сучасних технологіях доступу до інформаційних ресурсів, збільшує залежність людини від створювачів інформаційних технологій, які визначають алгоритми пошуку інформації і надання їй вигляду, зручного для сприйняття. Власне кажучи, саме вони багато в чому формують інформаційне коло життя, визначають умови, в яких живе і вирішує свої життєві проблеми пересічний громадянин держави. За таких обставин винятково важливим завданням держави є забезпечення безпеки взаємодії людини з інформаційною інфраструктурою [3].

Саме несанкціоноване використання персональних даних, що накопичуються різними структурами, зокрема органами державної влади, є небезпечним джерелом загроз інтересам особистості. Розширення можливостей прихованого збирання інформації, що становить особисту і сімейну таємницю, відомостей про приватне життя, знижує правовий статус людини і громадянина. На жаль, сучасні технології не вирішують усіх труднощів реалізації механізмів охорони цих зведень.

Інтереси суспільства в інформаційній сфері на регіональному рівні полягають у досягненні й підтримці суспільної злагоди, підвищенні творчої активності населення.

Потенційно серйозні загрози інтересам суспільства в інформаційній сфері пов'язані, зокрема, з ускладненням і недостатнім професіоналізмом експлуатації та захисту інформаційних систем і мереж зв'язку, які обслуговують критично важливі об'єкти інфраструктури забезпечення життєдіяльності регіону, а саме: інформаційні системи енергетичної, транспортної, трубопровідної й деяких інших. Ці загрози можуть виявлятися як навмисні, так і ненавмисні помилки, збої та відмови техніки і програмного забезпечення, а також внаслідок шкідливого впливу на ці інфраструктури з боку злочинних структур і кримінальних елементів. Масштаб можливих наслідків некоректної роботи технічного і програмного забезпечення інформаційних систем, певною мірою, можна уявити за витратами на вирішення „Проблеми-2000", коли, за деякими оцінками, світове співтовариство витратило близько 500 млрд доларів США [3].

Загрозами інформаційному забезпеченню процесу регулювання економічного розвитку на регіональному рівні можуть бути:

– монополізація інформаційного ринку України, його окремих секторів закордонними інформаційними структурами;

– низька ефективність інформаційного забезпечення державної політики України внаслідок дефіциту кваліфікованих кадрів, відсутність системи формування і реалізації державної інформаційної політики.

З урахуванням майбутнього розвитку інформатизації, проникнення інформаційних технологій у найважливіші сфери життя суспільства необхідно передбачити перехід від принципу забезпечення безпеки інформації до принципу інформаційної безпеки.

Для запобігання та ліквідації загроз інформаційній безпеці використовують правові, програмно-технічні і організаційно-економічні методи.

В Україні правовий режим державної таємниці (ДТ) визначено Законом України „Про державну таємницю", іншими нормативно-правовими актами, а також укладеними Україною міжнародними договорами та угодами про взаємну охорону державних таємниць, які регулюють відносини, пов'язані з віднесенням інформації до державної таємниці, її засекречуванням, охороною та контролем з боку держави за станом цієї роботи. Їх дія не поширюється на відносини, пов'язані з

охороною іншої, передбаченої відповідним законом, таємниці (службової, військової, банківської, комерційної тощо), якщо остання водночас не є ДТ. Інформація розглядається як ДТ з часу її внесення до Переліку відомостей, що становлять ДТ України [3].

У розвинутих країнах Західної Європи і США інформаційне законодавство формується і вдосконалюється в умовах сталого функціонування структур громадянського суспільства і правових інститутів.

Удосконалення механізму використання правових методів передбачає розробку комплексу нормативно-правових актів і положень, які регламентують інформаційні відносини в суспільстві, керівні і нормативно-методичні документи щодо забезпечення інформаційної безпеки.

Програмно-технічні методи – це сукупність наступних засобів: запобігання витоку інформації, виключення можливості несанкціонованого доступу до інформації, запобігання впливам, які призводять до знищення, руйнування, спотворення інформації, або відмовам у функціонуванні засобів інформатизації, виявлення закладних пристроїв, виключення перехоплення інформації технічними засобами, використання криптографічних засобів захисту інформації при передачі по каналах зв'язку.

З метою створення системи інформаційної безпеки і безпечного використання інформаційних технологій розроблено ряд міжнародних стандартів, методик та інших документів, що регламентують ці питання [7; 364].

Так, найбільш відомий стандарт BS 7799 [8] визначає загальну організацію, класифікацію даних, системи доступу, напрями планування, відповідальність співробітників, використання оцінки ризику в контексті інформаційної безпеки. В процесі впровадження стандарту створюється відповідна система менеджменту, мета якої – скорочення матеріальних втрат, пов'язаних із порушенням інформаційної безпеки.

Заходи із забезпечення безпеки інформаційної системи повинні носити комплексний характер і ґрунтуватися на перевірених практикою прийомах і методах.

На рис. 1 наведено структурно-функціональний склад системи захисту інформації від загроз несанкціонованого доступу. Так, система захисту інформації від несанкціонованого доступу містить чотири типових (базових) підсистеми з наступними основними функціями захисту:

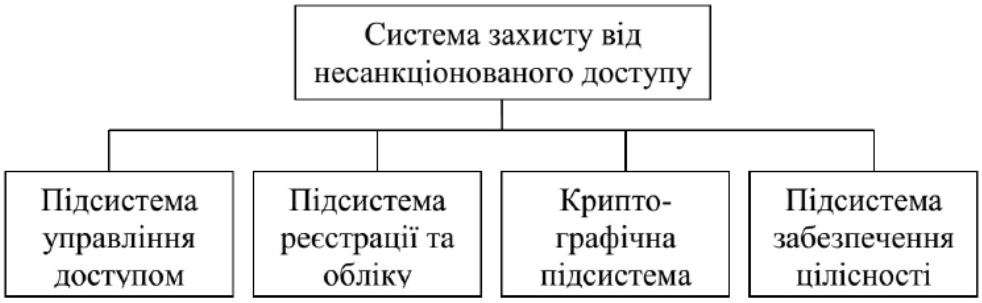

Рис.1. Структура системи захисту від несанкціонованого доступу

Джерело: складено на основі [9, с.53]

1. Підсистема управління доступом (ідентифікація, перевірка справжності, контроль доступу, управління потоками інформації);

2. Підсистема реєстрації та обліку (реєстрація та облік; облік носіїв інформації; сигналізація щодо спроб порушення захисту);

3. Криптографічна підсистема (шифрування конфіденційної інформації; шифрування інформації, що належить різним суб'єктам доступу або групам доступу з різними ключами);

4. Підсистема забезпечення цілісності (забезпечення цілісності програмних засобів та інформації, що оброблюється; фізична охорона засобів обчислювальної техніки та носіїв інформації; наявність адміністратора безпеки інформації; періодичне тестування системи захисту інформації від несанкціонованого доступу; засоби відновлення системи захисту інформації; використання сертифікованих засобів захисту).

Організаційно-економічні методи передбачають формування і забезпечення функціонування систем захисту секретної і конфіденційної інформації, сертифікацію цих

систем згідно вимог інформаційної безпеки, ліцензування діяльності в сфері інформаційної безпеки, стандартизацію способів і засобів захисту інформації, контроль за діями персоналу в захищених інформаційних системах [10, с.19-21].

Висновки та перспективи подальших досліджень. Формування системи інформаційної безпеки потребує розробки і реалізації системи заходів, метою яких є попередження, виявлення та припинення правопорушень у інформаційній сфері.

Зазначені у статті заходи необхідно розглядати як важливий елемент організаційно-економічного механізму забезпечення економічної безпеки України.

Список використаної літератури

1. Курмаєв П.Ю. Організаційно-економічний механізм регулювання розвитку регіонів / П.Ю. Курмаєв. – Умань: ПП Жовтий, 2010. – 332 с.

2. Курмаев П.Ю. Направления формирования модели электронного управления социально-экономическим развитием / П.Ю. Курмаев // Сборник научных трудов SWorld. – Выпуск 3. Том 38. – Иваново: МАРКОВА АД, 2013. – С. 3-5

3. Соснін О.В. Забезпечення інформаційної безпеки держави: теоретичний дискурс /О.В. Соснін// Стратегічна панорама. – 2004. – № 2. – С. 149-154

4. Інформаційна безпека України: сутність та проблеми [Електронний ресурс]. – Режим доступу: http://old.niss.gov.ua/book/panorama/kr_stil.htm

5. Скляренко О.А. Сучасні проблеми інформаційної безпеки України в умовах внутрішніх трансформацій / О.А.Скляренко //Актуальні проблеми міжнародних відносин. – 2006. – №64. – С.127

6. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності [Електронний ресурс] /О.Л. Морозов //Віче. – 2009. – Спецвипуск. – Режим доступу до журн.: http://www.viche.info/journal/598/

7. Бармен С. Разработка правил информационной безопасности / С. Бармен: Пер. с англ. − М.: Издательский дом «Вильямс», 2002. − 208 с.

8. British Standard. Code of practice for information security management British Standards Institution, BS 7799:1995

9. Шорошев В.В. Нова архітектура системи захисту інформації в комп'ютерних системах від несанкціонованого доступу / В.В. Шорошев // Інформаційна безпека. – 2009. – №2 (2). – С.53

10. Гавловський В. Удосконалення інформаційного законодавства як засіб оптимізації протидії комп'ютерної злочинності / В.Гавловський, М. Гуцалюк, В. Цимбалюк // Науковий вісник НАВСУ. – 2001. – №3. – С. 19-21