***Ольга Галько**, аспірант*
Тернопільський національний економічний університет
м. Тернопіль, Україна

СКЛАДОВІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Початок нового тисячоліття характеризується глобалізацією світових економічних і політичних процесів, невід'ємною складовою яких є інтенсивне використання досягнень сучасних інформаційних технологій. Після вибору Україною шляху до інтеграції в Європу, яка сьогодні активно розбудовує інформаційне суспільство, гостро постала проблема ефективного забезпечення інформаційної безпеки молодої держави.

У сучасному світі інформація є найціннішим глобальним ресурсом. Економічний потенціал суспільства переважно визначається обсягом інформаційних ресурсів та рівнем розвитку інформаційної інфраструктури. Інформація постійно ускладнюється, змінюється якісно, зростає кількість її джерел і споживачів. Водночас зростає уразливість сучасного інформаційного суспільства від недостовірної (а іноді й шкідливої) інформації, її несвоєчасного надходження, промислового шпигунства, комп'ютерної злочинності і т. ін. Тому Конституція України забезпечення інформаційної безпеки відносить до найважливіших функцій держави [1].

Сучасні масштаби і темпи впровадження засобів автоматизації керування з особливою гостротою ставить задачу проведення комплексних досліджень, зв'язаних із усебічним вивченням і узагальненням виникаючих при цьому проблем як практичного, так і теоретичного характеру.

Проблеми у сфері інформаційних відносин, формування інформаційних ресурсів і користування ними загострюються внаслідок політичного й економічного протиборства держав. Це стає актуальним у зоні забезпечення національної безпеки України. У ній чітко виділяється специфіка забезпечення інформаційної безпеки. Вона знайшла відображення в законах України «Про основи національної безпеки України» [2], «Про концепцію національної програми інформатизації» [3], «Про національну програму інформатизації» [4], а також у Стратегії національної безпеки України, яка затверджена указом Президента [5].

У Законі «Про основи національної безпеки України» вперше дано офіційну оцінку значущості й системної сутності інформаційної безпеки як невід'ємної складової національної безпеки України [2].

Як свідчать наукові дослідження, система забезпечення інформаційної безпеки України не виконує окремих важливих функцій. Зокрема, неефективними є управління її діяльністю, організаційні зміни, що здійснюються в рамках адміністративної реформи, мають несистемний характер, проводяться без попереднього функціонального дослідження органів дер-

жавної влади. Негативні тенденції розвитку національного інформаційного простору, кризовий стан економіки України та інші чинники зумовлюють ескалацію загроз, що може призвести (і призводить) до значних втрат політичного, економічного, воєнного та іншого характеру, завдання шкоди юридичним особам та громадянам України [6].

Вагомим кроком на шляху до координації діяльності державних органів став Указ Президента України "Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України" від 22 січня 2002 р. № 63/2002, згідно з яким було створено відповідну Міжвідомчу комісію на чолі з Секретарем Ради національної безпеки і оборони України [7].

Одну з найнебезпечніших загроз національній безпеці України в інформаційній сфері становить так звана "комп'ютерна злочинність" [8]. Як показують дослідження Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю, рівень загрози буде зростати пропорційно розширенню використання нових інформаційних технологій в управлінні, бізнесі, торгівлі. Загрози можуть бути як зовнішніми, так і внутрішніми. Слід зазначити, що у зв'язку із поширенням використання в Україні глобальної комп'ютерної мережі Інтернет та з приєднанням до міжнародних систем телекомунікацій нових країн, підвищенням інтелектуального рівня зловмисників зовнішня загроза постійно зростатиме. Через глобальну комп'ютерну мережу Інтернет, що не має державних кордонів, хакери мають несанкціонований доступ до комп'ютерної інформації, а для проведення безподаткових фінансових операцій, "відмивання брудних" коштів через електронні банківські системи глобальна мережа створює принципово нові умови, які у повному обсязі використовують кримінальні структури.

Із зростанням науково-технічного прогресу буде зростати і важливість питання інформаційної безпеки громадянина, суспільства, держави. Враховуючи той факт, що під впливом інформаційних атак може цілеспрямовано змінюватися кругозір та мораль як окремих осіб, так і суспільства в цілому, нав'язуються чужі інтереси, мотиви, спосіб життя, на перший план випливає аналіз сутності та форм проявів сучасних методів скритого агресивного впливу, вияву дій, що мають цілеспрямований агресивний характер і які протирічать інтересам національної безпеки, вироблення механізмів протидії їм у всіх напрямах [9, с. 35-38].

Отже, інформаційна безпека суспільства, держави характеризується ступенем їх захищеності, та, як наслідок, стійкістю головних сфер життєдіяльності у відношенні до небезпечних інформаційних впливів. Інформаційна безпека визначається здатністю нейтралізувати такі впливи. Загальноприйнятим є таке визначення інформаційної безпеки, як стан захищено-

сті життєво важливих інтересів громадян, суспільства та держави в інформаційній сфері.

Розрізняють внутрішні та зовнішні джерела інформаційної безпеки. Під внутрішніми джерелами розуміють відсутність історичного, політичного та соціального досвіду життя у правовій державі, що стосується процесу практичної реалізації конституційних прав та свобод громадян, у тому числі в інформаційній сфері. Е. Макаренко та В. Кирик вважають внутрішнім джерелом інформаційної безпеки посилення організованої злочинності та збільшення кількості комп'ютерних злочинів, зниження рівня освіченості громадян, що суттєво ускладнює підготовку трудових ресурсів для використання новітніх технологій, в тому числі інформаційних [10, с. 211].

Недостатня координація діяльності вищого державного керівництва, органів влади та військових формувань в реалізації єдиної державної політики забезпечення національної безпеки теж можна вважати таким джерелом. До цього слід додати і відставання України від розвинутих країн за рівнем інформатизації органів державної влади, юридично-фінансової сфери, промисловості та побуту громадян.

До зовнішніх джерел належать діяльність іноземних політичних, військових, економічних та розвідувальних структур в інформаційній та економічній сферах; політика домінування деяких країн в інформаційній сфері; діяльність міжнародних терористичних груп; розробка концепцій інформаційних війн будь-якими структурами; культурна експансія у відношенні до конкретної країни.

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. Розгляд інформаційної безпеки з позицій системного підходу дозволяє побачити відмінність наукового розуміння цієї проблеми від повсякденного. В повсякденному житті інформаційна безпека розуміється лише як необхідність боротьби з відтоком закритої (таємної) інформації, а також з розповсюдженням хибної та ворожої інформацій. Осмислення нових інформаційних безпек у суспільстві ще тільки починається [10, с. 212].

Особливо складна сьогодні проблема завчасного створення засобів, необхідних для інформаційного протиборства, або, якщо користуватися американською термінологією, – "інформаційної війни" [11, с.7].

Таким чином, інформаційна безпека – принципово нове явище в житті суспільства і держави. Відсутність інформаційного захисту веде до втрати політичної незалежності, тобто до фактичного програшу війни невійськовими засобами, а саме – національні інтереси однієї держави перепідпоря-

дковуються інтересам іншої держави, у якій більш високий інформаційний потенціал.

Характер будь-яких масштабних збройних конфліктів і війн, в які може бути втягнена Україна, багато в чому буде визначатися домінуючими тенденціями в розвитку засобів збройної боротьби. Головну роль набуває проблема завоювання інформаційної переваги в управлінні військами (силами) і зброєю. Вже в мирний час готується і ведеться перманентна інформаційна боротьба навіть між союзниками з різних військово-політичних блоків. У воєнний же час вона може прийняти характер широкомасштабних спеціальних операцій. Від результатів боротьби в інформаційній сфері залежить панування в повітрі і перевага в засобах вогневої поразки.

Аналіз досліджень по військовій тематиці дозволяє зробити висновок, що у військовій справі настає новий етап розвитку: ефективність сучасних засобів поразки все більше визначається не стільки вогневою міццю, скільки ступенем інформаційного забезпечення. Інформатизація військових структур стала пріоритетним завданням військово-технічної політики економічно розвинених держав. У змісті військових дій все більше зростає значимість інформаційного протиборства. Перевага в ступіні інформованості стає неодмінною умовою перемоги в війні, що переконливо доводить досвід збройних конфліктів і локальних війн сучасності. Зростання ролі інформаційної боротьби стирає межу між війною і миром.

Інформаційна війна ніким не оголошувалася і ніколи не припинялася, ведеться потайно і не знає кордонів у просторі й часі. Інформація стала чинником, здатним спровокувати військовий конфлікт, але і призвести до поразки у війні. Інформаційна боротьба стала обов’язковим елементом, що є об’єктивно існуючою тенденцією і стимулом розвитку матеріальної основи загальновійськової стратегії відповідно у формах і засобах збройної боротьби з’явилися такі нові наукові категорії, як "інформаційна боротьба", "засоби інформаційної боротьби", "інформаційна зброя".

Як відомо, бойовий потенціал протистоячих угруповань військ (сил) реалізується в ході військових дій в результаті взаємодії двох його основних компонентів – військового та інформаційного. Ця взаємодія відбувається в умовах постійного впливу на кожний з них з боку супротивника. При цьому правомірність використання поняття "інформаційна зброя" визначається тим, що в контексті застосування інформації в якості засобів боротьби, вона може характеризуватися такими показниками, як цілеспрямованість, розпізнавання, розосередженість, масштабність впливу, досяжність, швидкість доставки, комплексність впливу на технічні засоби, системи управління і особовий склад.

Інформаційній боротьбі притаманні такі закономірності: використання загальних об’єктивно існуючих фізичних полів для інформаційного за-

безпечення функціонування систем і засобів озброєння і військової техніки; збільшення глибини інформаційного зіткнення систем управління і значного скорочення часу на проведення операцій по добуванню, аналізу і розподілу інформації; зменшення вільних ділянок частотного діапазону і збільшення його енергетичної завантаженості; одночасне використання великої кількості функціонально об'єднаних засобів, побудованих на різноманітних фізичних принципах; комплексне застосування різнорідних систем і засобів згідно з єдиним задумом і планом у складі єдиної системи управління.

При протиборінні сторін з інтегрованими системами управління, вхідна інформація для реалізації своїх планів є єдиною, а цілі – протилежними. При такому тлумаченні конфлікт розглядають як засіб взаємодії складних систем. Задача оцінки ефективності управління (Эу) в умовах інформаційної боротьби зводиться до зменшення залежності:

$$Эу = F\ (Кбг, До, Ку, Коб, Кс, Кіб),$$

де: *Кбг, До, Ку, Коб, Кс, Кіб* – значення показників бойової готовності, оперативності, тривалості, обґрунтованості, скритності управління і готовності до інформаційної боротьби відповідно.

Для кількісної оцінки обґрунтованості управління вводиться показник, що враховує ступінь адекватності рішення, яке приймають, в обстановці, що склалася:

$$Ку = \max_{Ку} \min_{Кт} F\ (Ку, Кт, Ny, Nm)\ при\ Тр\ Трд,$$

де *Ку* – оптимальне управлінське рішення в поточній ситуації інформаційної боротьби; Ку – безліч всіх допустимих рішень по управлінню в поточній ситуації інформаційної боротьби; Кm – безліч всіх допустимих рішень супротивника за його відповідними діями; Ny (Nm) – обсяг інформації про свої війська (про супротивника), на підставі якого приймається рішення на управління; Тр – необхідний час на прийняття рішення в поточній ситуації, його доведення і виконання в умовах інформаційної боротьби; Трд – допустимий час з урахуванням необхідності реалізації рефлексивного управління в конкретній поточній ситуації.

Вибір кращої стратегії управління в умовах інформаційної боротьби залежить від реалізації переваг по одному з показників (або декільком з них) з урахуванням прогнозу на очікувану тривалість інформаційної переваги і спроможності системи управління оперативно (в масштабі часу, близькому до реального) прогнозувати зміни в стратегії і діях супротивника. В цьому зв'язку для оцінки ефективності системи управління в умо-

вах інформаційної боротьби доцільно не використовувати критерій вигляду:

П = max min Пуф (Кбг, Ке, Ку, Коб, Кс, Кіб, А, Б, З, Пут),

А і А, Б і Б,

де *Пуф і Пут* – фактично необхідний ефект від застосування систем управління;

А (Б) – стратегії управління протиборствуючих сторін А і Б своїми силами і засобами в умовах інформаційної боротьби;

З – поточні умови обстановки, використання яких дозволяло оцінити максимально можливу ефективність управління в умовах активної протидії з боку супротивника.

Ефективність функціонування системи управління військами, силами і зброєю в значному ступені залежить від адекватності, що входить в їхній склад спеціального математичного забезпечення, відбиття поглядів супротивника на застосування своїх засобів і систем озброєння і на підсилення ролі впливу на інформаційні ресурси іншою стороною як чинника забезпечення переваги в ході військових дій.

Таким чином, взаємодія систем управління протиборствуючих (що конкурують) сторін в мирний і в воєнний час має яскраво висловлений конфліктний характер на інформаційному рівні, що виявляється в боротьбі за вірогідну інформацію і в нав'язуванні протиборствуючій стороні бажаного інформаційного уявлення, що представляє суттєвість інформаційної боротьби.

Література:

1. Конституція України: Прийнята на п'ятій сесії Верховної Ради України 28 черв. 1996 р. – К.: Україна, 1996. – 54 с.
2. Закон України «Про основи національної безпеки України» від 19 червня 2003 року № 964-IV // Відомості Верховної Ради України. – 2003. – № 39. – ст. 351.
3. Закон України «Про концепцію національної програми інформатизації» від 4 лютого 1998 року № 75/98-ВР // Відомості Верховної Ради України. – 1998. – № 27–28. – ст. 182.
4. Закон України «Про національну програму інформатизації» від 4 лютого 1998 року № 74/98-ВР // Відомості Верховної Ради України. – 1998. – № 27–28. – ст. 181.
5. Указ Президента України «Про Стратегію національної безпеки України» від 12 лютого 2007 року № 105/200.
6. Жданов І. Можливі підходи до визначення основ державної політики забезпечення інформаційної безпеки України // Матеріали до кругло-

го столу “Безпека інформації в інформаційно-телекомунікаційних системах”. – К., 2001. – 28 трав.
7. Указ Президента України “Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України” від 22 січня 2002 р. № 63/2002.
8. Комп’ютерна злочинність: Навч. посіб. – К.: Атіка. – 240 с.
9. Роговец В. Информационные войны в современном мире: причины, механизмы, последствия. // Персонал. – 2000. – №5.
10. Макаренко Е., Кирик В. Інформайційно-психологічний захист як складовий чинник інформаційної безпеки // Проблеми безпеки української нації на порозі XXI сторіччя. – К.-Чернівці, 1988.
11. Цымбал В.О концепции "информационной войны" // Безопасность. – 1995. – №9.

Олена Гамкало, *аспірант*
Львівський національний університет імені Івана Франка
м. Львів, Україна

КЛАСИФІКАЦІЇ ІПОТЕЧНОГО КРЕДИТУ

Одним із важливих елементів фінансово-господарського механізму країн із розвинутою ринковою економікою є застава нерухомого майна – іпотека, за допомогою якої гарантується виконання фінансових та інших зобов’язань суб’єктів ринкових відносин.

Згідно з Законом України “Про іпотечне кредитування, операції з консолідованим іпотечним боргом та іпотечні сертифікати” – Іпотечний кредит відображає правовідносини, які виникають на підставі договору про іпотечний кредит між кредитодавцем і боржником з приводу надання коштів у користування з встановленням іпотеки.

Питання формування та розвитку іпотечного кредитування досліджували такі зарубіжні та вітчизняні вчені-економісти, як Дж. Фрідман, Н. Ордуей, В. Мінц, В. Кудрявцев, О. Кудрявцева, О. Євтух, О. Кручко, К. Поливода.

Аналіз наукових публікацій дозволяє з’ясувати застосовувану класифікацію іпотечних кредитів, ідентифікацію і сприймання операцій іпотеки. Іпотечне кредитування поділяють за:

- об”єктами нерухомості – земельні ділянки; підприємства; житлові будинки, квартири; дачі, садові будинки, гаражі та інші будівлі споживчого призначення; повітряні і морські судна; космічні об”єкти; незавершене будівництво.