УДК 351.862:354.61

Л. О. ЄВДОЧЕНКО

ІНФОРМАЦІЙНА БЕЗПЕКА ДЕРЖАВИ: ЕВОЛЮЦІЯ ПІДХОДІВ

***П**ростежено еволюцію розуміння поняття "інформаційна безпека держави" від античності до сучасності. Показано важливість захисту інформації в усі часи існування держави. Визначено місце інформаційної безпеки в національній безпеці держави. Проаналізовано основні підходи до здобуття інформації у сучасному світі.*

***T**he evolution of concept "information safety of the state" from antiquity up to now is considered. The importance of protection of the information in all times of existence of the state is shown. The place of information safety in national safety of the state is determined. Is analysed the basic approaches to reception of the information in the modern world.*

Ключові слова: інформаційна безпека, національна безпека, розвідка, держава, історія.

Безпека – одна з найголовніших потреб людини і суспільства, вона притаманна навіть тваринам на рівні інстинктів. Саме бажанням безпеки пояснюється створення в державі армії, поліції, служб охорони, розвідки тощо. Цим же обумовлені й наддержавні та міжнародні організації такі, наприклад, як НАТО та ООН. Недостатня організація безпеки держави може викликати найстрашніші наслідки – аж до занепаду держави, знищенням народу, кровопролиттям та іншими лихами. Держава (суспільство), в якій безпека організована погано, швидше за все, є нетривалою.

Проблема інформаційної безпеки як складова національної безпеки завжди була актуальною для будь-якої країни. Відмінність полягає в тому, що в різні періоди цьому приділялося більше менше уваги. Дослідження таких вчених, як О. Бодрук [3], О. Гончаренко [1], Б. Кормич [7], В. Кохно, В. Шкідченко [8], М. Левицька [9] дають можливість отримати загальне уявлення про генезу поняття "інформаційна безпека" серед характерних ознак національної безпеки держави.

Однак, незважаючи на актуальність теми, обсяг наукових досліджень у цій сфері, на жаль, залишається ще недостатнім (порівняно з потребами українського суспільства та з існуючими практиками європейських держав). Зокрема, не зроблено огляду глибинних коренів проблеми захисту інформації.

Виходячи з наведеного, доцільно розглянути еволюцію підходів до інформації та її місця в загальній безпеці держави в ретроспективі: від стародавніх часів – до наших днів.

Тема державної безпеки довгий час (у СРСР) була під забороною. Так навіть у "Великій радянській енциклопедії" 1970 р. була відсутня стаття "Безпека". Дане питання розглядалося лише у вузькоспеціалізованих і, як правило, засекречених

публікаціях. Ситуація змінилася лише після розпаду Радянського Союзу. Відтоді на пострадянському просторі, в тому числі і в Україні, побачила світ велика кількість праць, присвячених безпеці.

Стосовно інформаційної безпеки – складової національної безпеки держави – у "Великій Радянській Енциклопедії" так само немає згадки. Є лише визначення інформації (від лат. informatio – пояснення, викладення) – спочатку відомості, які передавалися одними людьми іншим усним, письмовим або будь-яким іншим способом (наприклад, за допомогою умовних сигналів, з використанням технічних засобів тощо), а також сам процес передачі або отримання цих відомостей [4].

В умовах, коли економічно розвинені країни намагаються завоювати країни, що розвиваються, контролювати їх інформаційні процеси, важливість інформаційної складової національної безпеки держави тяжко переоцінити. Адже метою такого впливу є поступове перетворення інформації, що передається, на політичний та ідеологічний фактор впливу, тобто фактор досягнення власних національних інтересів в інших країнах [12, с. 97]. Саме тому одним з головних завдань держави у сфері національної безпеки є захист інформації.

Історія інформаційної безпеки (хоча її раніше так і не називали) сягає корінням у глибоку давнину. Наприклад, у Біблії у вранішній молитві Давид говорить, звертаючись до Бога: "Ти погубиш тих, що говорять брехню; кровожерного і підступного гребує Господь" [17, с. 570]. Брехня ж є не чим іншим, як недостовірною інформацією. А Плутарх у праці "Древні звичаї спартанців" першим пунктом поставив звичай, що кожного, хто входив до сессітії, старший показуючи на двері, попереджав: "Жодне слово з них не виходить" [16, с. 481], що повністю відповідає розумінню конфіденційності інформації. Сенека у трагедії "Едип-цар" застерігає від використання недостовірної інформації, говорячи устами свого героя, що виявлення довіри віроломному – надання йому можливості шкодити [19, с. 142]. А фразою "безпека є попередженням шкоди" Платон фактично говорить про інформаційну розвідку [15, с. 415].

Загальновідомий вислів "знання – сила" – ні що інше, як перефразований латинський вислів "Praemonitus praemunitus" – "Хто попереджений – той озброєний".

При цьому батьківщиною розвідки вчені вважають стародавній Китай. У IV ст. до нашої ери філософ Сунь-Цзи (313 – 239 рр. до н.е.) написав першу фундаментальну працю під назвою "Мистецтво війни", де зокрема говориться: "Якщо прогресивний государ або мудрий генерал отримує перемогу над супротивниками кожного разу, коли вони переходять до дії, то це досягається завдяки попередній інформації. Так звана попередня інформація не може бути отриманою ні від духів, ані від божеств, ні за аналогією з попередніми подіями, ані шляхом розрахунків. Її необхідно отримати від людини, котра знайома із ситуацією супротивника" [20, с. 93].

Про згубну силу інформації для держави згадував і Ш. Монтеск'є у праці "Роздуми про причини величі та падіння римлян", говорячи, що найнебезпечнішим для держави зазвичай є не дійсні втрати, а уявні та занепад бойового духу, що відбирає в держави навіть ті сили, які ще залишила їй фортуна [10, с. 54]. Тобто і тут йдеться про силу інформації.

Підходи до розуміння поняття "інформація" є дуже різноманітними. Наприклад, з точки зору економіки, інформація може стати предметом торгівлі, якщо має певну вартість. Не даремно ж девізом дуже успішної компанії Міцуї є: "Інформація – кров підприємства". Причому, постановивши, що інформація має вартість, яку можна відобразити в матеріальній формі, тим самим встановлюється, що до неї можуть бути використані всі існуючі економічні закони. У тому числі твердження К. Маркса, що капітал піде на будь-який злочин заради трьохсот відсотків прибутку.

З позиції статистики інформацію розглядаємо, виходячи з класифікації джерел інформації, методики їх оцінки та принципів відбору. Так само існує окремий підхід до інформації в соціології, політології, філософії тощо.

Технології отримування та розповсюдження інформації постійно змінюються та вдосконалюються при цьому. Тотальна глобалізація підкорила собі практично всі сфери життя людей, суспільство стає все більш відкритішим та прозорішим. У цих умовах захист інформації стає надзвичайно актуальним, особливо це стосується інформаційної безпеки держави. І дана проблема ділиться на дві рівнозначні частини: 1) захист інформації; 2) захист від інформації.

Показовим є той факт, що технічні інновації в сучасному зборі даних мають багато аспектів, таких, як набуття знань за допомогою платного навчання у вищих навчальних закладах, огляд технічних публікацій тощо. Учені світу навзаєм спостерігають за всіма науковими та технологічними звітами. Наприклад, у Південній Кореї лише американські технічні публікації ретельно вивчає близько 570 перекладачів. В Японії понад 5000 інженерів і вчених проглядають іноземні технічні звіти. Майже 13 000 японських громадян навчається в університетах США (близько 1000 з них спеціалізуються на інженерній справі), тоді як не більше, ніж сім американських студентів щороку вивчають інженерну справу в Японії (дані за останні двадцять років). Окрім того, більше 50 % кандидатів на отримання вченого ступеня в США у сфері інженерії – іноземці [13, с. 13–14].

С. Паркінсон у праці "Закони Паркінсона" згадує стратегічний прийом під назвою "підхід з обходом" і говорить, що не цілком зрозуміло, наскільки вдалим є такий маневр на війні, однак будь-яке завдання вирішується за допомогою використання стратегеми, основою якої є попередній всеохоплюючий збір інформації [14, с. 45].

Поняття "стратегема" було виведене Сунь-Цзи [21]. Воно означає стратегічний принцип, якого має дотримуватися полководець у своїй діяльності. Можна стверджувати, що більшість цих принципів у підґрунті має інформаційну складову. Наприклад, "якщо знаєш ворога і знаєш себе, змагайся хоч сто разів – небезпеки не буде; якщо знаєш себе, а його – ні, одного разу переможеш, іншого – зазнаєш поразки; якщо не знаєш ні себе, ні його, кожного разу, коли будеш боротися, будеш зазнавати поразки" [21, с. 84].

Ці принципи актуальні і за наших часів, хоча сьогодні вони здебільшого застосовуються у випадках, які можна назвати полем битви лише умовно.

У плані захисту від інформації спостерігається таке. Після закінчення "холодної війни" в 1991 р. багато розвідслужб акцентували увагу саме на економічному шпигунстві. Кожна держава намагалася допомогти своїм вітчизняним компаніям

отримати комерційну інформацію і в той самий час захистити ці компанії від економічного злодійства іноземних агентів і компаній. Наприклад, у 1994 р. уряд США створив Національний центр контррозвідки (NCC) і випустив у 1995 р. Класифікацію пріоритетної інформації. Це зроблено з метою допомогти керівникам приватних компаній у моніторингу та аналізі активності світового промислового шпигунства, спрямованого до американських підприємств. Роль NCC полягає в інтеграції і координації активності національних розвідслужб, у т.ч. CIA, Департаменту захисту, ФБР, Департаменту юстиції та держави, Консультативної комісії зовнішньої безпеки і Національної ради безпеки [13, с. 12].

"Холодна війна" закінчилася, однак, на думку багатьох дослідників [1; 6], суспільство стоїть на порозі нової війни – інформаційної. Певна група осіб вже почала підготовку до таких війн, пояснюючи логіку своїх дій тим, що такі війни розпочнуться в будь-якому випадку. А хто попереджений – той озброєний. На сьогодні вже створено спеціальну організацію – Лігу Айвар Систем України. Незрозуміле слово "айвар" перестає бути таким, якщо пишеться латинськими буквами: i-war – information war – інформаційна війна. Ця Ліга була створена в ході певної Стратегічної Гри. Одним з прикладів можна назвати гру, яка проходила в 2005 р. і була присвячена парламентським виборам 2006 р. Головними термінами, які використовувалися, були такі: розпредмечування, рефлексія, стретегування. А пізніше, під час виборів події, які відбувалися у грі, були втілені на політичному полі [6].

Розвиток теоретичних досліджень процесів прийняття локальних рішень в умовах неясності і ризику підвели науковців до необхідності осмислення теорії ігор та теорії організації. Їх особливе наукове значення підтверджує те, що в 2005 р. Нобелівська премія за досягнення в економіці була присуджена Р. Ауманну та Т. Шеллінгу за праці з використанням теорії ігор у моделюванні економічних процесів прийняття рішень, які враховують взаємозалежність між державами, організація і людьми [2, с. 567].

Методи та способи поширення та отримання неправдивої інформації (такої, від якої потрібен захист) – є великою проблемою з точки зору державного управління. Історія знає чимало прикладів успішної дезінформації. До них можна віднести пропаганду часів Радянського Союзу, головною метою якої було виховування в людей, що живуть у тоталітарній державі, відчуття безпечності та замилування політикою Партії. Так само, перед війною 1999 р. в Югославії, у державах західного блоку почали з'являтися гіперболізовані повідомлення про кількість жертв "геноциду етнічних чисток" з боку сербів щодо албанського населення Косово.

Отже, правильна та правдива інформація є найважливішою передумовою правильного та адекватного сприйняття дійсності всередині держави. А це дає можливість запобігти багатьох складних ситуацій, аж до збройних конфліктів.

Сфера інформації стрімко розвивається, пропонуючи користувачеві нову філософію осмислення систем комунікацій, наприклад, надану компанією Cisco продукт комплексної системи комунікації NGN – Next Generation Network.

Феномен інформації дуже складний, його можна навіть назвати поліфункціональним. З певної точки зору інформацію як знання про світ потрібно

вважати одним з найголовніших факторів, які породжують і розвивають свідому психіку, духовну сутність людини. Вона є змістовим фактором мислення і активного творчого ставлення людини до об'єктивно існуючого світу, прямого та зворотного зв'язку цих стосунків [5, с. 693].

На сьогодні в Україні існує весь комплекс технологічних і правових передумов для переходу на новий рівень інформатизації не лише різних сфер життя сусідства (бізнесу, освіти, науки, медицини), але і держави в цілому.

Інформатизація суспільства проголошена одним з пріоритетів державної політики.

"Електронний уряд", "електронна митниця", застосування нових інформаційно-комунікаціних технологій у роботі органів державної влади і місцевого самоврядування, в усіх сферах суспільного життя – це завдання, яке вже вирішується [22, с. 22].

Термін "інформаційна безпека" використовується все частіше, двома такими найуживанішими значеннями:

– стан (якість) певного об'єкта (в якості об'єкта може виступати інформація, дані, ресурси автоматизованої системи, автоматизована система, інформаційна система підприємства, суспільства, держави тощо);

– діяльність, спрямована на забезпечення захищеного старого об'єкта (у цьому значенні частіше використовується термін "захист інформації").

Інформаційна безпека (information security) – захищеність життєво важливих інтересів особи, суспільства і держави від навмисного або ненавмисного впливу в тій чи іншій формі (інформаційна блокада, інформаційна інтервенція, інформаційна війна, дезінформація тощо). Суть інформаційної безпеки – забезпечення збереження інформаційних ресурсів держави і захищеність законних прав особистості у сфері інформації.

Класично вважається, що забезпечення безпеки інформації складається з трьох складових: конфіденційності, цілісності, доступності. Пунктами, до яких застосовується процес захисту інформації до інформаційної системи, є апаратне забезпечення, програмне забезпечення та забезпечення зв'язку (комунікації). Процедури (механізми) захисту поділяються на захист фізичного рівня, захист персоналу та організаційний рівень.

В. Северин вивів основні принципи, які є основою аналітичних досліджень (АД) у сфері захисту інформації. До них належать такі:

– приналежність до дійсності як до об'єктивної реальності (стосовно можливих каналів витоку) (МКВ) інформації, що підлягає охороні (ІПО);

– необхідність відрізняти істотні елементи від несуттєвих під час вивчення об'єктивної реальності;

– визнання стабільності та змінності елементів, які складають систему МВК ІПО та захисту ІПО;

– урахування історичності процесів та явищ, які вивчаються;

– визнання значення протиріч у розвитку явища, яке вивчається;

– конкретність і об'єктивність під час вибору об'єкта дослідження і безпосередньому проведенні АД [18, с. 13–14].

Б. Парад у своїй роботі "Комерційне шпигунство" [13, с. 15–70] систематизував технічні прийоми для збору конфіденційної інформації: перевербовування;

"оцінювання" (під виглядом різноманітних уточнень отримується інформація, яка не стосується справи); цінова війна (під виглядом різноманітних уточнень отримується інформація, яка не стосується справи); утримування виставкових зразків на різноманітних показах; "дурник"/компанія-прикриття; комп'ютерний злам; науковий обмін; відвідування; перехоплення інформації; інформаційні брокери; повітряні комунікації (прослуховування коміркових мереж); наукові презентації; підслуховування; класичне викрадення; аерофотозйомка; упровадження "крота"; співбесіда з провідними вченими щодо працевлаштування від імені неіснуючих фірм; продаж "використаного" обладнання; зміна сфери використання (з цивільної на військову); шантаж; використання жінок як агентів розвідки; іграшкові моделі військової техніки (часто точна мініатюрна копія); використання невдоволених працівників; покупці; агентства з оцінки майна; розгляд добровільно наданої ідеї (для чого спеціально ініціюються судові процеси щодо авторського права); рекламна та торгова література; уряд (ненароком та спеціально); поставщики; збереження записів; передчасне тестування або демонстрація; судові записи за тяжбами; торгові виставки; технічні публікації; завелике розповсюдження інформації; соціологічні опитування і огляди ринку; приватні розмови; консультанти; зворотній (реверсивний) інжиніринг; ліцензування; франчайзинг; спільні підприємства; реклама щодо працевлаштування; патенти; "жовті сторінки"; зустрічі акціонерів; спостереження за підприємствами і установами; торговельні публікації; місцеві газети; іноземні копії державних публікацій; бюро патентів та торгових марок; перелік власників патентів; митні брокери; дистриб'ютори і роздрібні продавці; біржові аналітики; звіти за кредитами; щорічні звіти; комісії з цінних паперів; державний архів; спостереження за керівним персоналом; фінансові та інвестиційні звіти; інтерв'ю з репортерами; комерційні бази даних; банки; державна торгова палата; іноземні торгові палати і торгові організації; аналіз сміття; іноземні людські ресурси; внутрішня інформація; фото-, відео-, аудіозапис; інтернет; консульства; подружжя та коханці; обслуговуючий персонал; перекладачі; приватні детективи.

Даний перелік створювався для конфіденційної комерційної інформації, однак може бути повністю, без застережень, використаний для будь-якої іншої державної інформації.

Видозмінюючись у часі протягом усієї історії людства (відколи з'явилася перша держава), існувало поняття, яке сьогодні називається інформаційною безпекою. Вона мала інші назви та різне наповнення, проте завжди залишається однією з найважливіших складових національної безпеки. Те, що способи, які використовуються в пошуку конфіденційної комерційної інформації можуть використовуватися (і використовуються) для отримання всіх видів інформації, свідчить про гнучкість та еволюцію підходів і спонукає до пошуку шляхів захисту державної інформації.

Перспективою подальшого дослідження може бути вивчення підходів до захисту суб'єктів держави від інформації, яка є неправдивою та небезпечною для суспільства.

Література:

1. *Алексеев А.* Война на пороге. Информационная / А. Алексеев // PR-менеджер, 2007. – № 9. – С. 56–57.

2. *Алексеров Ф. Т.* Роберт Ауман и Томас Шеллинг – Нобелевские лауреаты по экономике 2005 г. / Ф. Т. Алексеров // Экономический журнал ВШЭ. – 2005. – № 4. – С. 566–572.

3. *Бодрук О. С.* Системи національної та міжнародної безпеки в умовах формування нового світового порядку 1991 – 2001 роки : дис. … д-ра політ. наук : спец. 21.01.01 / О. С. Бодрук ; Нац. ін-т проблем міжнар. безпеки. – К., 2003. – 415 с.

4. Большая Советская Энциклопедия : в 30 т. / гл. ред. А. М. Прохоров. – Изд. 3-е. – М. : Советская Энциклопедия, 1972.

Т. 10. Ива-Италики. 1972. – С. 353.

5. Глобализация и безопасность развития : [монография] / [О. Г. Белоус, Д. Г. Лукьяненко и др.] ; рук. авт. кол. и науч. ред. О. Г. Белоус. – К. : КНЕУ, 2002. – 789 с.

6. *Кашпур А.* Информационне войны / А. Кашпур // Стратегии, 2007. – № 10. – С. 52–57.

7. *Кормич Б. А.* Організаційно-правові засади політики інформаційної безпеки України : [монографія] / Б. А. Кормич. – Одеса : Юридична література, 2003. – 472 с.

8. *Кохно В. Д.* Воєнна безпека як категорія воєнної науки та складова національної безпеки України / В. Д. Кохно, В. П. Шкідченко // Наука і оборона. – 2000. – № 2. – С. 3–7.

9. *Левицька М. Б.* Теоретико-правові аспекти забезпечення національної безпеки України органами внутрішніх справ України : дис. ... канд. юрид. наук : спец. 12.00.01 / М. Б. Левицька. – К., 2002. – 206 с.

10. *Монтескье Ш.* Избранные произведения / Ш. Монтескье. – М. : Госполитиздат, 1955. – 800 с.

11. Національна безпека України: історія і сучасність : [монографія] / [Н. П. Маслова-Лисичкина, О. С. Бодрук, В. О. Врадій та ін.]. – К. : Ін-т світової економіки і міжнар. відносин НАН України, 1993. – 120 с.

12. *Нижник Н. Р.* Національна безпека України (методологічні аспекти, стан і тенденції розвитку) : [навч. посіб.] / Н. Р. Нижник, Г. П. Ситник, В. Т. Білоус ; за заг. ред. П. В. Мельника, Н. Р. Нижник. – Ірпінь, 2000. – 304 с.

13. *Парад Б.* Коммерческий шпионаж. 79 способов, которыми конкуренты могут получить секреты любого бизнеса / Б. Парад. – М. : ТК Велби, 2005. – 160 с.

14. *Паркинсон С. Н.* Законы Паркинсона : [сборник] / С. Н. Паркинсон ; пер. с англ. ; сост. и авт. предисл. В. С. Муравьев. – М. : Прогресс, 1989. – 448 с.

15. *Платон.* Диалоги / Платон. – М. : Мысль, 1986. – 607 с.

16. *Плутарх.* Моралии : [сочинения] / Плутарх ; пер. М. Н. Ботвинник. – М. : ЗАО Изд-во ЭКСМО-Пресс ; Х. : Фолио, 1999. – 1120 с. – (Серия "Антология мысли").

17. Псалтирь // Библия. Книги священного писания Ветхого и Нового завета. – Avainsanoma ry. Helsinki, Finland, 2000. – С. 569–639.

18. *Северин В. А.* Правовое обеспечение информационной безопасности предприятия : [учеб.-практ. пособ.] / В. А. Северин ; МГУ им. М. В. Ломоносова. – М. : Городец, 2000. – 192 с.

19. *Сенека Луций Анней.* Трагедии / Сенека ; пер. с лат. С. Ошерова, коммент. Е. Рабинович. – М. : Искусство, 1991. – 494 с.

20. *Сунь-Цзы.* Искусство войны / Сунь-Цзы. – К. : ИД "София", 2008 – 224 с.

21. *Сунь-Цзы.* Искусство стратегии. Древнекитайские трактаты, ставшие

основой целого ряда управленческих теорий / Сунь-Цзы ; пер. с кит., предисл. и коммент. Н. И. Конрада. – М. : Эксмо ; СПб. : Мидгард, 2006. – 528 с.

22. *Чернышев С.* Информатизация как неизбежность / С. Чернышев // Финансовые услуги, 2007. – №3. – С. 22–23.

Надійшла до редколегії 19.03.2010 р.