

УДК 321.02: 004.056

ОСНОВНІ СУБ'ЄКТИ ТА ІНСТИТУТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

К. Захаренко, кандидат політичних наук, здобувач НПУ імені
М.П. Драгоманова

Інформаційна безпека це спроможність системи протистояти випадковим або навмисним внутрішнім і зовнішнім загрозам. Сьогодні суспільству доводиться забезпечувати захист суб'єктів від негативного інформаційного впливу. Водночас інформаційна безпека переважно пов'язується з діяльністю держави, бо саме вона за допомогою різних політичних інститутів здійснює заходи щодо убезпечення життєдіяльності громадян. Отож, доцільною є організація інформаційної безпеки суспільства, держави та окремої особистості. В систему інформаційної безпеки мають бути залучені не тільки фахівці з інформаційних технологій, але й вітчизняні вчені з різних галузей науки, а також представники бізнесових структур. до її вирішення, як складової національної безпеки. Розробляючи й упроваджуючи нові ідеї, знання і політику в сфері інформатизації, вони активно впливають на стан економічної, політичної, оборонної та інших складових національної безпеки України.

Ключові слова: людина, політика, культура, інформаційна сфера, інформаційна безпека, інформаційний суверенітет.

Актуальність проблеми. У сучасному суспільстві одним із найважливіших показників рівня цивілізованості сучасної держави є ступінь розвитку її інформаційного простору. Західні вчені й спеціалісти, стверджуючи про соціальне значення інформації, зазначають, що інформація – це не лише знання, а й влада.

Формування цілей статті. Управління інформацією є, по суті, управлінням соціальними й економічними процесами. Через це проблеми поширення інформації, широкого її використання набувають не лише суто економічного, а й політичного характеру як у межах окремої країни, так і на міжнародній арені. Інформаційні ресурси суспільства характеризують загальний рівень розвитку продуктивних сил і передусім самої людини [1, с. 127]. При таких перевагах інформатизації, як оптимізація політичних та економічних процесів, формування більш досконалих принципів взаємодії влади та суспільства, існує і її зворотний бік. Він включає в себе появу нових загроз, пов'язаних з поширенням та розвитком інформаційних технологій, а також негативні та злочинні наслідки їх використання, що визначає проблематику інформаційної безпеки в політиці як особливо актуальну [2, с.88]. Саме тому визначення і класифікація основних політичних інститутів – агентів інформаційної безпеки є об'єктом дослідження.

Виклад основного матеріалу. Значення інформації у безпеці сучасного світу важко переоцінити. Як влучно підмітив американський дослідник М. Маклуен: «Істинно тотальна війна – це війна за допомогою інформації» [3, с. 43]. А боротьба в інформаційній сфері має таку ж мету, що і збройні конфлікти, економічна експансія та інші види агресивних впливів. Новою метою часто стає розум людини, і конфлікти можуть вирішуватися не силовими методами, а за допомогою застосування тих чи інших інформаційних технологій. Сьогодні гостро постає питання забезпечення інформаційної безпеки. Саме безпека на інформаційному рівні часто є пріоритетною для країни, оскільки визначає, з одного боку, рівень захищеності і, як наслідок, стійкості основних сфер життєдіяльності суспільства (країни) щодо небезпечного інформаційного впливу (дестабілізуючого, деструктивного, уразливого тощо), а з іншого – інтенсивність розвитку суспільства в тій чи іншій сфері за рахунок ефективного використання накопичених людством знань [4, с. 41].

Як показує аналіз наукової літератури, присвяченої питанню інформаційної безпеки, більшість фахівців сходяться на думці, що інформаційна безпека – це складова частина національної безпеки та представляє собою: 1) стан захищеності життєво-важливих інтересів особи, суспільства і держави, за якого зводиться до мінімуму нанесення шкоди через неповність, несвоєчасність та недостовірність інформації або негативного інформаційного впливу через негативні наслідки функціонування інформаційних технологій, а також через несанкціоноване поширення інформації; 2) стан захищеності інформаційного середовища/простору, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави [5, с. 13].

Сьогодні з поняттям «інформаційна безпека», зокрема, з його термінологічним визначенням, склалася парадоксальна ситуація. З одного боку, термін «інформаційна безпека» широко використовується в наукових публікаціях, навчальній літературі та законодавчих документах різного рівня, з іншого боку, це поняття досі не має однозначного розуміння, а його зміст у різних джерелах має кардинальні розбіжності. Відсутність центральної дефініції у сфері інформаційної безпеки обумовлює методологічну невизначеність ряду інших положень та термінів, що приводить до полісемії і значно знижує ефективність та прикладне значення наукових розробок в області інформаційної безпеки. Офіційне визначення інформаційної безпеки зафіксоване в Законі України «Про Основні засади розвитку інформаційного

суспільства в Україні на 2007-2015 роки» [6]: «інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації». Але у науковців є багато зауважень до цього визначення [7, с. 65-66]. Крім того, часто вітчизняні дослідники запозичують основний зміст визначення терміну з міжнародних стандартів, не враховуючи те, що термін «information security» може перекладатися з англійської не тільки як «інформаційна безпека», але й як «безпека інформації», що не є синонімами в повному обсязі.

З точки зору більшості науковців, інформаційна безпека є здатністю системи протистояти випадковим або навмисним внутрішнім і зовнішнім загрозам – здатність забезпечити захист суб'єктів від негативного інформаційного впливу, тобто вона насамперед пов'язується з діяльністю держави, оскільки в більшості випадків йдеться про певні несанкціоновані дії з інформацією. Отже, беззаперечно, що головним інститутом – агентом інформаційної безпеки виступає держава, яка через низку певних політичних інституцій здійснює заходи щодо забезпечення безпеки. Серед політичних заходів інформаційної безпеки – з'ясування односторонніх та багатосторонніх інтересів шляхом обміну інформацією та проведення переговорів; об'єктивне висвітлення сутності конфліктів та кризових проблем засобами масової комунікації; створення умов для професійної діяльності ЗМК у зонах напруженості для забезпечення достовірною інформацією міжнародного співтовариства і формування відповідної світової думки; інформаційне супроводження політичних (референдумів) та виборчих процесів, проведення аналітичних моніторингів за дотриманням основних прав і свобод людини; інформаційні контакти з опозиційними групами, неурядовими організаціями з метою ефективності досягнення консенсусу між сторонами протиборства [8, с. 47]. Таким чином, агентами інформаційної безпеки є держава, державні органи та структури, що займаються її забезпеченням на державному рівні (це можуть бути органи не тільки виконавчого механізму влади, а й законодавчого, судового), а також інституціалізовані форми вироблення конкурентоспроможного інформаційного продукту. Політична складова забезпечення національної безпеки покладається на таких агентів:

– Президент України, Верховна Рада України, Кабінет Міністрів України, Рада національної безпеки і оборони України, які здійснюють загальне керівництво, координацію та контроль за реалізацією заходів у сфері національної безпеки;

– міністерства та інші центральні органи виконавчої влади; Національний банк України; суди загальної юрисдикції; прокуратура України; місцеві державні адміністрації та органи місцевого самоврядування; Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України, на які безпосередньо покладається виконання заходів у сфері національної безпеки [9].

У кожній державі об'єктами інформаційної безпеки виступають передусім люди (усі громадяни) і держава, як цілісність, а основним каналом інформаційного впливу завжди є свідомість, психіка людини, свідомість (переконання, утвердження і т. ін.) великого етносу. Коли ведуть мову про захист національного інформаційного простору, як такого, то мають на увазі насамперед державний інформаційний суверенітет, тобто належне володіння й розповсюдження всією спільнотою у державі відповідних національних інформаційних ресурсів. Інформаційний суверенітет – це виняткове право держави на формування й використання усіх інформаційних засобів, створених на засадах і за державний кошт [10, с. 60].

Таким чином, в якості об'єктів інформаційної безпеки виступають:

- особа – її права та свободи в інформаційній сфері, техніка та свідомість;
- суспільство – його духовні цінності, засади солідарної діяльності;
- держава – її конституційний лад, ефективне функціонування, суверенітет [11, с. 115].

Інформаційна безпека особистості – це стан захищеності психіки та здоров'я людини від деструктивного інформаційного впливу, який призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану. Інформаційна безпека суспільства – можливість безперешкодної реалізації суспільством та окремими його членами своїх конституційних прав, пов'язаних з можливістю вільного одержання, створення й поширення інформації, а також ступінь їхнього захисту від деструктивного інформаційного впливу. Інформаційна безпека держави – це стан її захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за

допомогою спеціальних технічних засобів, комп'ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам [12, с. 124].

З точки зору інформаційної безпеки можна виокремити три групи національних інтересів:

а) для людини: реалізація прав і свобод людини і громадянина щодо одержання, використання, поширення, зберігання інформації; забезпечення права людини на захист від маніпуляції індивідуальною свідомістю; захист права інтелектуальної власності, захист енергоінформаційної безпеки людини тощо;

б) для суспільства: побудова інформаційного суспільства; забезпечення плюралізму засобів масової інформації; захист від маніпуляції масовою свідомістю; розвиток духовності, моральних засад, інтелектуального потенціалу українського народу, зміцнення психічного здоров'я нації.

в) для держави: забезпечення інформаційного суверенітету; унеможливлення монополізації інформаційного простору іноземними компаніями або транснаціональними корпораціями; створення конкурентоспроможних інформаційних технологій та технологій зв'язку; збереження та зміцнення науково-технологічного потенціалу; інтеграція України в європейський інформаційний простір; боротьба з інформаційною злочинністю тощо [13, с. 116].

Фахівці вважають, що деякі країни з нерозвиненим інформаційним простором (до них, на жаль, сьогодні належить й Україна) можуть бути лише споживачами інформаційних продуктів, які часто не збігаються з національними інтересами. Наприклад, одним з найважливіших завдань інформаційної діяльності будь-якої країни є формування і підтримання її позитивного іміджу (образу) у світовому інформаційному полі. З цього погляду процес формування позитивного іміджу України у світі оцінюють як неефективний. По-перше, загальний обсяг інформації про Україну та її зовнішню політику незначний, неадекватний її потенціалу. Крім того, в деяких секторах світового інформаційного простору, (окремих регіонах планети, верствах світової громадськості, ділових колах тощо) такої інформації взагалі немає. По-друге, навіть наявна інформація значною мірою є застаріла і тенденційна. Водночас останніми роками іноземна інформаційна активність щодо України збільшилась у десятки разів. Особливо інформаційний потік із Заходу та Сходу в Україну не має перешкод, а зворотного, з України на Схід і Захід, по суті, не існує [14, с. 131].

Проблема інформаційної безпеки не може бути вирішена без впровадження нових ідей, нових знань, нової політики у сфері інформатизації. Концептуальними є пропозиції щодо широкого залучення саме вітчизняних вчених і виробників до її вирішення, як складової національної безпеки. Вітчизняні фахівці мають гарантувати високу якість інформаційних послуг, безпеку інформаційних технологій, сучасну систему сертифікації програмних і технічних засобів, впровадження стандартизації, створення національних баз даних, систем телекомунікації, безпеку роботи в світовому інформаційному просторі. Бо ігнорування цих проблем може призвести до ускладнень у прийнятті найважливіших політичних, економічних, соціальних, військових рішень тощо [15].

Враховуючи вищевикладене, необхідно визначити низку напрямів щодо регулювання державою, як головним агентом інформаційної безпеки регулювання інформаційної сфери:

- заохочення конкуренції, боротьба з монополізмом (передусім державний контроль за концентрацією засобів масової інформації);
- забезпечення права і технічних можливостей для доступу до інформації й інформаційних ресурсів всього населення;
- дотримання свободи слова;
- захист інтересів національних меншин, підростаючого покоління в інформаційній сфері;
- захист національної культурної спадщини, мови, протистояння культурній експансії інших країн;
- забезпечення інформаційної безпеки;
- охорона інтелектуальної власності, боротьба з піратством;
- боротьба з комп'ютерними і злочинами, пов'язаними з високими технологіями;
- впровадження електронного уряду;
- правове регулювання мережі Інтернет [16, с. 22].

Висновок. До того ж треба враховувати, що рівень інформаційної безпеки активно впливає на стан політичної, економічної, оборонної та інших складових національної безпеки України, бо найчастіше реалізація інформаційних загроз – це завдання шкоди в політичній, військовій, економічній, соціальній, екологічній сферах тощо. На жаль, нині в Україні немає реальних гарантів її інформаційної безпеки, відсутній комплекс нормативно-правових актів щодо захисту інформаційних ресурсів та інформаційної інфраструктури. А процес інформатизації має стихійну, некеровану природу з

переважним ухилом у бік використання засобів інформатизації іноземного виробництва [17].

Література

1. Хімей В. Основні сучасні проблеми інформаційної безпеки України / В. Хімей // Теле-та радіожурналістика. – 2014. – Вип. 13. – С.127-132.
2. Корольов М.В. Проблематика дослідження питань інформаційної безпеки у державному управлінні / М.В. Корольов, О.О. Скопа // Вісн. Східноукраїнського нац. ун-ту ім. В. Даля. – 2013. – № 15(1). – С.88-93.
3. Присяжнюк М. Інформаційна безпека України в сучасних умовах / М. Присяжнюк, Я. Белошевич // Вісн. Київського нац. ун-ту ім. Т. Шевченка. Військово-спеціальні науки. – 2013. – Вип. 30. – С.29-33.
4. Богуш В.М. Інформаційна безпека держави / В. М. Богуш, О. К. Юдін. – К.: МК-Прес, 2005. – 432 с.
5. Кісілевич-Чорнойван О.М. Інформаційна безпека та міжнародна інформаційна безпека: проблема визначення понять / О.М. Кісілевич-Чорнойван // Юриспруденція: теорія і практика. – 2009. – № 8. – С.11-18.
6. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» // Відомості Верховної Ради України (ВВР). – 2007. – № 12. – Ст. 102.
7. Олійник О. В. Адміністративно-правові засади інформаційної безпеки / О. В. Олійник // Європейські перспективи. – 2012. – № 4(1). – С. 65-68.
8. Макаренко Є.А. Політичні доктрини глобальної інформаційної безпеки / Макаренко Є.А. // Вісн. Ін-ту міжнародних відносин Київськ. нац. ун-ту ім. Т. Шевченка. – 2007. – № 2. – С.41-51.
9. Зайцев М.М. Суб'єкти забезпечення інформаційної безпеки України [Електронний ресурс] / М.М. Зайцев // Форум права. – 2013. – № 3. – С. 231 – 238. – Режим доступу:http://nbuv.gov.ua/j-pdf/FP_index.htm_2013_3_40.pdf
10. Кирильчук Є. О. Проблеми національної інформаційної безпеки України в контексті сучасних національних державотворчих процесів та світової інтеграції / Є. О. Кирильчук // Наукові праці МАУП. – 2013. – Вип. 1. – С.89-95.
11. Сагайдак О.В. Інформаційна безпека України в умовах глобалізаційних викликів / О.В. Сагайдак // Вісн. Луганського нац. ун-ту ім. Т. Шевченка. Соціологічні науки. – 2010. – № 12. – Т. 2(2). С.110-125.
12. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи / В. Петрик // Юридичний журнал. – 2009. – № 5. – С.122-134.
13. Сагайдак О. В. Інформаційна безпека України в умовах глобалізаційних викликів / О. В. Сагайдак // Вісн. Луганського нац. ун-ту ім. Т. Шевченка. Соціологічні науки. – 2010. – № 12. – Т. 2(2). С.110-125.
14. Хімей В. Основні сучасні проблеми інформаційної безпеки України / В. Хімей // Теле-та радіожурналістика. – 2014. – Вип. 13. – С.127-132.
15. Попов С.В. Проблеми інформаційної безпеки України [Електронний ресурс] / С.В. Попов, О.О. Бойченко // Форум права. – 2011. – № 1. – С.798-801. – Режим доступу:http://nbuv.gov.ua/j-pdf/FP_index.htm_2011_1_128.pdf
16. Малик Я.Й. Забезпечення інформаційної безпеки України у контексті світового досвіду / Я.Й. Малик, О. І. Береза // Ефективність державного управління. – 2012. – Вип. 32. – С.20-27.
17. Попов С.В. Проблеми інформаційної безпеки України [Електронний ресурс] / С.В. Попов, О.О. Бойченко // Форум права. – 2011. – № 1. – С. 798 – 801. Режим доступу:http://nbuv.gov.ua/j-pdf/FP_index.htm_2011_1_128.pdf

ОСНОВНЫЕ СУБЪЕКТЫ И ИНСТИТУТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

К. Захаренко

Информационная безопасность это способность системы противостоять случайным или преднамеренным внутренним и внешним угрозам. Сегодня обществу приходится обеспечивать защиту субъектов от негативного информационного воздействия. В то же время информационная безопасность преимущественно связывается с деятельностью государства, потому что именно она с помощью различных политических институтов осуществляет меры по обеспечению безопасности жизнедеятельности граждан. Так, целесообразной есть организация информационной безопасности общества, государства и отдельной личности. В систему информационной безопасности должны быть привлечены не только специалисты по информационным технологиям, но и отечественные ученые из разных областей науки, а также представители бизнес-структур, к ее решению, как составляющей национальной безопасности. Разрабатывая и внедряя новые идеи, знания и политику в сфере информатизации, они активно влияют на состояние экономической, политической, оборонной и других составляющих национальной безопасности Украины.

Ключевые слова: человек, политика, культура, информационная сфера, информационная безопасность, информационный суверенитет.

KEY SUBJECTS AND INSTITUTIONS OF INFORMATIONAL SECURITY

K. Zaharenko

Information security is the ability of the system to resist accidental or intentional internal and external threats. Today the society has to ensure the protection of its subjects from the negative informational effects. However, informational security is mainly associated with the activities of the state, because through the various political institutions it takes measures to the security of its citizens life. Therefore, the organization of informational security of society, the state and the individual is expedient. The system of informational security should involve not only informational technology experts, but also local scientists from different fields as well as representatives of businesses to cope with it as with part of national security. By developing and introducing new ideas, knowledge and policy in the field of informatization, they actively influence the state of economics, politics, defense and other components of national security of Ukraine. The article analyzes the degree of informational space development in modern society as one of the most important indicators of civilization level in modern state. Scientists and experts arguing about the social value of information point that information is not only a knowledge but also a power. Informational security is the ability of the system to resist accidental or intentional internal and external threats - the ability to ensure the protection of subjects from negative informational effect, thereby it is primarily associated with the activities of the state, because in most cases we are talking about some unauthorized informational activities. So, undoubtedly, the main institution - the agent of informational security - is the state that via a number of some policy institutions takes measures to ensure safety.

Key words: human, politics, culture, informational sphere, informational security, informational sovereignty.