УДК 341.123 (045)

АНАЛІЗ ГОЛОВНИХ СКЛАДОВИХ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

СТЕПКО Олександр Михайлович,
к.політ. н., доцент кафедри міжнародної інформації,
Інституту міжнародних відносин Національного авіаційного університету

У статті розглядаються головні складові інформаційної безпеки держави. Розглянуто комплекс питань інформаційної безпеки держави. Проаналізовано цілі, завдання та принципи інформаційної безпеки України, а також типи, джерела інформаційних загроз і основні напрями забезпечення інформаційної безпеки держави.

Ключові слова: *інформація, інформаційна безпека, інформаційні загрози.*

Метою статті є аналіз головних складових інформаційної безпеки держави. Проблема інформаційної безпеки має давнє походження і стала особливо важливою у наш час, коли використання інформаційних технологій відбувається вже практично у всіх сферах нашого життя. Розгляду питань інформаційної безпеки приділяють величезну увагу як вітчизняні, так і закордонні дослідники. Серед зарубіжних вчених вагомий внесок у розгляд цього питання внесли Г. Кіссінджер, З. Бжезинський, Л. Браун, Ч. Флавін, Х. Френч. Серед вітчизняних дослідників хотілося б відзначити праці О. Соснін а, В. Грубова, В. Домарьова, В. Ліпкана, В. Косевцова, І. Бінько, В. Мунтіяна, Г. Почепцова, О. Литвиненко та інших.

Інформаційна безпека відіграє важливу роль у забезпеченні інтересів будь-якої держави. Створення розвиненого і захищеного інформаційного середовища є неодмінною умовою розвитку суспільства та держави. Останнім часом в світі відбуваються якісні зміни у процесах управління, зумовлені інтенсивним впровадженням сучасних інформаційних технологій. Разом з цим посилюється небезпека несанкціонованого втручання в роботу інформаційних систем, і вагомість наслідків такого втручання дуже сильно зросла. Як наслідок, в багатьох країнах все більше уваги приділяється проблемам захисту інформації та пошуків шляхів її вирішення.

Країни, які не можуть забезпечити власну інформаційну безпеку, стають неконкурентоспроможними і, як наслідок, не можуть брати участь у боротьбі за розподіл ринків та ресурсів. Можна стверджувати, що зникнення великих держав відбувалося не в останню чергу через неспроможність ефективного управління на власній території та невідповідність інформаційної структури новим умовам існування. Отже, незаперечним є те, що в будь-якій розвиненій країні має існувати система забезпечення інформаційної безпеки, а функції та повноваження відповідних державних органів повинні бути закріплені законодавчо.

Поняття інформаційної безпеки включає в себе з одного боку забезпечення якісного інформування громадян та вільного доступу до різних джерел інформації, а з іншого - контроль за непоширенням таємної інформації, сприяння цілісності суспільства, захисту від негативних інформаційних впливів тощо. Рішення цієї комплексної проблеми дозволить як захистити інтереси суспільства і держави, так і сприяти реалізації права громадян на отримання всебічної та якісної інформації.

Проблема ефективного забезпечення безпеки інформації в державі передбачає вирішення таких масштабних задач, як: розроблення теоретичних основ забезпечення безпеки інформації; створення системи органів, відповідальних за безпеку інформації; вирішення проблеми керування захистом інформації і її автоматизації; створення нормативно-правової бази, що регламентує рішення всіх задач забезпечення безпеки інформації; налагодження виробництва засобів захисту інформації; організація підготовки відповідних фахівців та ін.

Комплекс питань інформаційної безпеки держави включає такі сфери державної діяльності, як: захист та обмеження обігу інформації; захист інформаційної інфраструктури держави; безпека розвитку інформаційної сфери держави; захист національного інформаційного ринку; попередження інформаційного тероризму та інформаційної війни. [1]

Існує два аспекти вивчення інформаційної безпеки в контексті національної безпеки. З одного боку, це самостійний елемент національної безпеки будь-якої країни, а з іншого - інтегрована складова будь-якої іншої безпеки: військової, економічної, політичної і т.д.

Одним з найбільш повних визначень інформаційної безпеки можна вважати наступне: це такий стан захищеності життєво важливих інтересів особистості, суспільства і держави, при якому зводиться до мінімуму завдання збитку через неповноту, невчасність і недостовірність інформації, негативний інформаційний вплив, негативні наслідки функціонування інформаційних технологій, а також

через несанкціоноване поширення інформації. Це визначення тією чи іншою мірою охоплює практично всі сфери інформаційної взаємодії суб'єктів держави.

Проблема забезпечення інформаційної безпеки України знайшла відображення в законах «Про основи національної безпеки України», «Про концепцію національної програми інформатизації», «Про національну програму інформатизації», а також у Концепції національної безпеки України. Основними складовими останньої є: національна безпека, національні інтереси, національні цілі, пріоритети і принципи задоволення і захисту національних інтересів, загрози національній безпеці і система національної безпеки. [2, с. 5] Сутність інформаційної безпеки як невід'ємної складової національної безпеки України вперше була зазначена у Законі «Про основи національної безпеки України».

Захист інформаційного суверенітету держави тісно пов'язаний із поняттям інформаційної безпеки, що може бути розглянута, як захищеність внутрішньої інформації як такої, тобто захищеність якості інформації, її надійність, захищеність різних галузей інформації від розголошення, а також захищеність інформаційних ресурсів. З іншого боку, інформаційна безпека означає контроль над інформаційними потоками, обмеження використання провокаційної, ворожої суспільної інформації, включаючи контроль над рекламою; захист національного інформаційного простору від зовнішньої інформаційної експансії.

Серед головних складових інформаційної безпеки держави виділяють: обсяг інформаційного продукту, що виробляється в державі і державою; здатність мереж витримувати зростаюче інформаційне навантаження; можливість держави керувати розвитком вироблення та розповсюдження інформації; можливість доступу народонаселення до усіх можливих інформаційних джерел, а також відкритість більшості з них. [3]

Аналізуючи дослідження вітчизняних фахівців, головні цілі політики інформаційної безпеки України можна сформулювати таким чином: реалізація конституційних прав громадян, суспільства та держави на інформацію; захист інформаційного суверенітету України, зокрема, національного інформаційного ресурсу та систем формування суспільної свідомості; забезпечення рівня інформаційної достатності для прийняття рішень державним установам, підприємствам та громадянам; належна присутність країни у світовому інформаційному просторі. [4, с.129] Крім того, розглядаючи актуальність формування, функціонування та безпеки національного інформаційного простору, експерти виділяють наступні цілі [3]: зміцнення інформаційної безпеки України, загалом її національної безпеки за рахунок більш ефективного використання національного потенціалу; підняття рівня і значення вітчизняного інформаційного продукту та технологій, національних інформаційних ресурсів, розвитку інформаційної інфраструктури України у відповідності до її національних інтересів на засадах державного суверенітету України; упорядкування інформаційних відносин у національному інформаційному просторі України, особливо зміна співвідношення розповсюдження в країні вітчизняної та зарубіжної інформаційної продукції та інформаційних технологій на користь вітчизняних; державна підтримка вітчизняних суб'єктів національного інформаційного простору, забезпечення інформаційної та духовної, культурної ідентифікації України в міжнародних інформаційних відносинах, піднесення міжнародного авторитету вітчизняного інформаційного продукту та технологій, його виробників.

Необхідність забезпечення інформаційної безпеки зумовлюється, багатьма факторами: потреба забезпечення національної безпеки України в цілому; існування загроз інформаційній сфері країни, що можуть завдати значної шкоди загальним національним інтересам; можливість впливу за допомогою інформації на свідомість і поведінку людей. Головним стратегічним завданням інформаційної безпеки України є створення потужного національного інформаційного простору, як головного аспекту присутності держави в світовому інформаційному просторі. Крім того, таке завдання включає створення системи протидії інформаційним загрозам та захист власного інформаційного простору, інформаційної інфраструктури та інформаційних ресурсів держави.

Загалом, завданнями забезпечення інформаційної безпеки держави вважають: виявлення, оцінку та прогнозування поведінки джерел загроз інформаційній безпеці, що здійснюється шляхом оперативного моніторингу інформаційної обстановки; вироблення, координацію та введення єдиної державної політики у галузі інформаційної безпеки; створення та експлуатацію систем забезпечення інформаційної безпеки; розробку, координацію та запровадження єдиної державної політики у галузі міжнародних інформаційних відносин, зокрема у напрямку формування іміджу держави. [4, с.130]

Оскільки національний інформаційний ресурс став одним з головних джерел економічної потужності держави та її суб'єктів, то необхідним є формулювання державних інтересів, факторів і загроз в інформаційній сфері, аналіз ефективності існуючої системи безпеки та можливостей її удосконалення. У контексті державної інформаційної політики мова повинна йти не тільки про права громадян,

юридичних осіб і держави в сфері інформації, але і про необхідність захисту інтелектуальної власності, державних інформаційних ресурсів та конфіденційної інформації.

Отже, рішення ключових проблем інформаційної безпеки повинне здійснюватися на основі державної політики, при цьому необхідно враховувати основні принципи забезпечення інформаційної безпеки держави. Закон України "Про основи національної безпеки України" виділяє такі з них: пріоритет прав людини; верховенство права; пріоритет договірних засобів у вирішенні інформаційних конфліктів; адекватність заходів захисту національних інтересів держави в інформаційній сфері реальним та потенційним загрозам; громадський контроль за діяльністю органів державної влади, що входять до системи забезпечення інформаційної безпеки держави; додержання балансу інтересів особи, суспільства, держави, їх взаємна відповідальність; чітке розмежування повноважень та функцій органів державної влади в системі забезпечення інформаційної безпеки та ін. [5]

Крім цього, виділяються основні положення державної політики забезпечення інформаційної безпеки: обмеження доступу до інформації є виключення з загального принципу відкритості інформації і здійснюється тільки на основі законодавства; відповідальність за зберігання, засекречення і розсекречення інформації персоніфікується; доступ до інформації, а також обмеження доступу, здійснюються з обліком обумовлених законом прав власності на цю інформацію; держава формує нормативно-правову базу, що регламентує права, обов'язки і відповідальність усіх суб'єктів, що діють в інформаційній сфері; юридичні і фізичні особи, що збирають, нагромаджують і обробляють персональні дані і конфіденційну інформацію, несуть відповідальність перед законом за їх зберігання і використання; держава законними засобами забезпечує захист суспільства від помилкової, перекрученої і недостовірної інформації, що надходить через засоби масової інформації; держава здійснює контроль за створенням і використанням засобів захисту інформації за допомогою їхньої обов'язкової сертифікації і ліцензування діяльності в області захисту інформації; держава проводить протекціоністську політику, що підтримує діяльність вітчизняних виробників засобів інформатизації і захисту інформації, і здійснює заходи для захисту внутрішнього ринку від проникнення на нього неякісних засобів інформатизації й інформаційних продуктів; держава сприяє наданню громадянам доступу до світових інформаційних ресурсів, глобальних інформаційних мереж; держава прагне до відмовлення від закордонних інформаційних технологій для інформатизації органів державної влади і управління по мірі створення конкурентоздатних вітчизняних інформаційних технологій і засобів інформатизації; держава формує програму інформаційної безпеки, що поєднує зусилля державних організацій і комерційних структур у створенні єдиної системи інформаційної безпеки; держава докладає зусиль для протидії інформаційній експансії інших країн, підтримує інтернаціоналізацію глобальних інформаційних мереж і систем. [6]

Відповідно до вищеназваних принципів і положень забезпечення інформаційної безпеки держави вимагає рішення наступних ключових проблем: розвиток науково-практичних основ інформаційної безпеки, що відповідають сучасній геополітичній ситуації та умовам політичного і соціально-економічного розвитку держави; формування законодавчої і нормативно-правової бази забезпечення інформаційної безпеки, у тому числі розробка реєстру інформаційного ресурсу, регламенту інформаційного обміну для органів державної влади, підприємств, нормативного закріплення відповідальності посадових осіб і громадян за дотримання вимог інформаційної безпеки; розробка механізмів реалізації прав громадян на інформацію; формування системи інформаційної безпеки, що є складовою частиною загальної системи національної безпеки країни; розробка сучасних методів і технічних засобів, що забезпечують комплексне рішення задач захисту інформації; розробка критеріїв і методів оцінки ефективності систем і засобів інформаційної безпеки і їх сертифікація; дослідження форм і способів цивілізованого впливу держави на формування суспільної свідомості; комплексне дослідження діяльності персоналу інформаційних систем, у тому числі методів підвищення мотивації, морально-психологічній стійкості і соціальної захищеності людей, що працюють із секретною і конфіденційною інформацією.

На національному рівні інформаційна безпека держави розглядається як система заходів, спрямованих на недопущення несанкціонованого доступу до інформації, її модифікації та порушення цілісності. Вона включає: захист політичних, державних і громадських інтересів; захист моральних цінностей; заборона інформації, яка містить ідеї агресивної війни, насилля, дискримінації та посягання на права людини.

Серед пріоритетів національних інтересів України, визначених в «Законі України Про основи національної безпеки України», можна виділити ті, що мають відношення до сфери інформації: гарантування конституційних прав і свобод людини і громадянина; збереження та зміцнення науково-технологічного потенціалу, утвердження інноваційної моделі розвитку; забезпечення розвитку і фун-

кціонування української мови як державної в усіх сферах суспільного життя на всій території України, гарантування вільного розвитку, використання і захисту російської, інших мов національних меншин України; розвиток духовності, моральних засад, інтелектуального потенціалу Українського народу.

Важливою проблемою інформаційної безпеки, як вже зазначалося, є забезпечення захисту і контролю національного інформаційного простору, а також забезпечення інформації про країну в світовому інформаційному просторі. Під інформаційним простором розуміється певне середовище, у якому здійснюється формування, збирання, збереження, опрацювання і поширення інформації, і на яке розповсюджується юрисдикція держави.

Треба наголосити, що будь-яка інформаційна технологія складається з наступних елементів: створення інформації, її обробка, зберігання та споживання. З огляду на безпеку необхідно забезпечити надійність роботи всіх елементів цієї системи. Розглядаючи проблему в такому ракурсі, можна окреслити основну мету інформаційної діяльності – створення повноцінного відкритого інформаційного простору.

Важливий елемент інформаційного простору – засоби масової інформації. Умови їх функціонування в країні, законодавче забезпечення, стан захищеності журналістів є важливими чинниками для цього сектору інформаційного простору. В країнах, що розвиваються ЗМІ відіграють вирішальну роль для всього суспільства, бо вони дозволяють при відсутності законодавчих засобів стримування маніпулювати суспільною думкою та надавати некоректну інформацію, що є важливим порушенням стану національної інформаційної безпеки. У системі національної оборони дедалі більшого значення набуває інформація, яка заповнює вільний час і формує настрій нації. Такою інформацією і забезпечують суспільство ЗМІ та інші системи формування масової свідомості. Як зазначає Г. Почепцов: “як для тоталітарного, так і для будь-якого іншого сучасного суспільства інформаційна картина світу (уявлення про світ) важливіша, ніж сам реальний світ.” [7, с. 43] Ще більшого значення набуває довгостроковий вплив ЗМІ, який є одним з основних джерел формування системи соціально-політичних настанов та стереотипів.

Відсутність відомостей, їх виключно або переважно негативний характер у сучасному світі впливає на зовнішньополітичну і економічну діяльність як держави в цілому, так і на окремих її громадян та їхніх організацій. Саме тому ця проблема набуває загальнодержавного значення, а в разі її нехтування створює загрозу національній безпеці. Саме тому створення належних умов для розширення інформаційної присутності у світовому інформаційному просторі є найважливішим завданням державної політики інформаційної безпеки.

Одним із основних елементів реалізації державної політики в інформаційній сфері є інформаційна інфраструктура, що є невід’ємною частиною стратегічних інформаційних ресурсів і має велике значення для обороноздатності держави і її інформаційного ринку. За Законом України „Про Концепцію національної програми інформатизації” до інформаційної інфраструктури входять: міжнародні та міжміські телекомунікаційні та комп’ютерні мережі; системи інформаційно-аналітичних центрів; інформаційні ресурси; інформаційні технології; системи науково-дослідних установ з проблем інформатизації; виробництво та обслуговування технічних засобів інформації; система підготовки кваліфікованих фахівців у сфері інформатизації. [8] Інформаційна інфраструктура являє собою єдність наступних компонент: системи виробництва інформаційних продуктів, системи доставки їх до споживача, системи виробництва засобів виробництва інформаційних продуктів та їх доставки, системи виробництва інформаційних технологій, системи накопичення і збереження інформаційного продукту або інформаційного ресурсу, тобто системи сервісного обслуговування елементів інфраструктури і системи підготовки кадрів.

Вдосконалення суспільних відносин великою мірою залежить від розвитку інформаційних ресурсів, які є базовими для створення ефективних моделей державного управління. Отже, цей вид ресурсів є водночас об’єктом управління і предметом діяльності державної влади та її інститутів. Інформаційні ресурси — це інформаційна інфраструктура та циркулююча в ній продукція інформаційної діяльності, яка дає змогу вирішувати відповідні завдання. [9] Найважливішим при цьому є розуміння того, що дві складові інформаційних ресурсів доповнюють одна одну і не можуть бути використані окремо.

Темпи науково-технічного та економічного розвитку країни багато в чому визначаються такими факторами, як доступність та якість інформаційного забезпечення. А рівень забезпеченості інформацією визначає успіх держави і суспільства в цілому. Важливою проблемою є налагодження збирання, аналізу та ефективного використання науково-технічної інформації іноземного походження, тому доступ до неї – одна з критичних умов забезпечення прогресу. Величезне значення в сучасних умовах

надається інформаційному забезпеченню політичної діяльності. Наприклад, в нині діючій системі збирання та аналітичної обробки інформації США вирізняються такі три складові: 1) державні інформаційні органи, зокрема розвідувальні органи, установи держдепартаменту, адміністрації Президента, Ради національної безпеки; 2) інформаційні центри "прямої підтримки", зокрема такі установи, як Rand, Військовий університет національної оборони тощо; 3) громадські центри "широкої підтримки", такі, як Центр стратегічних і міжнародних досліджень, Американський підприємницький інститут, Фонд спадщини, Атлантична Рада, Центр з національної політики та ін. [4, с.131] Перша складова системи забезпечує оперативне керівництво державою, інтереси другої зосереджені на оперативному рівні, а третя здійснює стратегічне планування зовнішньополітичної діяльності.

При розгляді проблеми інформаційної безпеки важливим кроком є виділення загроз інформаційній безпеці, а також аналіз захисту від цих загроз. Загроза інформаційній безпеці – явище, дії негативних чинників або процес, через які: соціальні об'єкти інформаційної безпеки частково або повністю втрачають можливість реалізувати свої інтереси в інформаційній сфері; а також, порушується нормальне функціонування, здійснюється руйнація або стримується розвиток технічних об'єктів інформаційної безпеки.

Як правило, виділяють такі типи інформаційних загроз: політичні; економічні; суспільні; військові та науково-технічні [1, с. 106]. В політичній сфері це: система державного управління; системи підготовки прийняття політичних рішень; виборчі системи; телекомунікаційні системи спеціального призначення. В економічній: система прийняття рішень; банківська інфраструктура; управління економічним станом в умовах надзвичайних ситуацій; система управління державними комунікаціями, які мають економічний характер; корпоративні війни і промисловий шпіонаж. В суспільній: загрози для системи формування громадської думки; системи ЗМК; структури політичних партій, громадських рухів, релігійних організацій; структури забезпечення основних прав і свобод людини. У військовій: інформаційні ресурси збройних сил; системи управління військами; системи постійного контролю і спостереження; канали надходження інформації стратегічного, оперативного і розвідувального характеру. В науково-технічній: системи накопичення ноу-хау; об'єкти інтелектуальної власності; структури фундаментальних і прикладних досліджень; структури аналізу та прогнозування тенденцій в науково-технічній сфері; бази і банки даних конфіденційного характеру.

Закон України "Про основи національної безпеки України" визначає наступні загрози національним інтересам і національній безпеці України в інформаційній сфері: прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації. [5]

Вітчизняні експерти [10] як правило, загрози інформаційній безпеці України за своєю загальною спрямованістю, поділяють на такі види: загрози конституційним правам і свободам людини і громадянина у сфері духовного життя й інформаційної діяльності, індивідуальній, груповій і суспільній свідомості, духовному відродженню України; загрози інформаційному забезпеченню державної політики України; загрози розвиткові вітчизняної індустрії інформації, включаючи індустрію засобів інформатизації, телекомунікацій і зв'язку; загрози безпеці інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, що створюються.

Серед загроз інформаційному забезпеченню державної політики України виділяють наступні: монополізація інформаційного ринку України, його окремих секторів вітчизняними і закордонними інформаційними структурами; блокування діяльності державних засобів масової інформації з інформування української і закордонної аудиторій; низька ефективність інформаційного забезпечення державної політики України внаслідок дефіциту кваліфікованих кадрів, відсутність системи формування і реалізації державної інформаційної політики.

Серед загроз розвитку вітчизняної індустрії інформації можна виділити такі: протидія доступу України до новітніх інформаційних технологій, взаємовигідній і рівноправній участі українських виробників у світовому поділі праці в індустрії інформаційних послуг, засобів інформатизації, телекомунікацій і зв'язку, інформаційних продуктів, а також створення умов для посилення технологічної залежності України в галузі сучасних інформаційних технологій; закупівля органами державної влади імпортних засобів інформатизації, телекомунікацій і зв'язку за наявності вітчизняних аналогів, що не поступаються за характеристиками закордонним зразкам; витіснення з вітчизняного ринку украї-

ських виробників засобів інформатизації, телекомунікацій і зв'язку; відтік за кордон кваліфікованих фахівців.

Загрозами для безпеки інформаційно-телекомунікаційних систем на території України, як діючих, так і тих, що створюються, можуть бути: протиправні збирання та використання інформації; порушення технології обробки інформації; впровадження в апаратні і програмні вироби компонентів, що реалізують функції, не передбачені документацією на ці вироби; розробка і поширення програм, що порушують нормальне функціонування інформаційно-телекомунікаційних систем, зокрема систем захисту інформації; знищення, пошкодження, радіоелектронне придушення або руйнування засобів і систем обробки інформації, телекомунікацій і зв'язку; вплив на парольно-ключові системи захисту автоматизованих систем обробки і передачі інформації; компрометація ключів і засобів криптографічного захисту інформації; витік інформації по технічних каналах; впровадження електронних пристроїв для перехоплення інформації в технічні засоби обробки, збереження та передачі інформації, а також у службові приміщення органів державної влади, підприємств, установ і організацій незалежно від форми власності; знищення, пошкодження, руйнування або розкрадання машинних та інших носіїв інформації; перехоплення інформації в мережах передачі даних і на лініях зв'язку, дешифрування цієї інформації і нав'язування помилкової інформації; використання несертифікованих вітчизняних і закордонних інформаційних технологій, засобів захисту інформації, засобів інформатизації, телекомунікації і зв'язку під час створення й розвитку української інформаційної інфраструктури; несанкціонований доступ до інформації, що знаходиться в банках і базах даних; порушення законних обмежень на поширення інформації. [10]

Прикладами загроз інформаційній безпеці України, є, зокрема, протизаконна приватизація державних видавництв і поліграфічних комбінатів, свавільний розподіл радіочастот тощо. [11] Найбільш вражаючим є те, що одна з головних загроз інформаційній безпеці лежить в сфері діяльності органів державної влади: невиконанні або неналежному виконанні органами державної влади своїх повноважень у інформаційній сфері. Хоча, відповідно до Конституції України "забезпечення інформаційної безпеки є однією з найважливіших функцій держави та справою всього Українського народу". [12, ст. 17]

Розглядаючи проблему інформаційних загроз неможливо обминути поняття джерел загроз інформаційній безпеці. Експерти розрізняють внутрішні та зовнішні джерела загроз. [13, с. 211] Під внутрішніми джерелами розуміють відсутність історичного, політичного та соціального досвіду життя у правовій державі, що торкається процесу практичної реалізації конституційних прав та свобод громадян, в тому числі в інформаційній сфері, а також 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. Недостатню координацію 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 сфері; 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.

В наш час стало очевидним, що під впливом інформації зростає потенційна вразливість суспільних процесів від інформаційного впливу. Інформація стала чинником, здатним призвести до великомасштабних аварій, військових конфліктів, дезорганізації державного управління тощо. Розгляд питань інформаційної безпеки дозволяє виділити чотири групи інформаційно-технологічних небезпек для суспільства і держави, зумовлених досягненнями науково-технічного прогресу. [14, с.2] Перша група пов'язана з інтенсивним розвитком нового вигляду зброї - інформаційної, здатної ефективно впливати на психіку людей і інформаційно - технологічну інфраструктуру держави. Аналіз сучасних досліджень в цій області дозволяє говорити про ефективність програмування поведінки окремих людей під впливом на комп'ютерні банки даних знань і інформації. Друга група являє собою новий вигляд соціальних злочинів, оснований на використанні досягнень сучасних інформаційних технологій: махінації з банківськими операціями; комп'ютерне хуліганство; незаконне копіювання технологічних рішень та інше. На думку провідних дослідників в цій області, комп'ютер стає провідним знаряддям злочину. Третя група виявляється у вигляді електронного контролю за життям, настроєм, планами громадян, роботою політичних організацій, тотального комп'ютерного контролю за населенням країни. Інформаційні технології дозволяють накопичувати, зберігати і використовувати величезні масиви

даних про здоров’я, соціальну активність, політичні думки, зв'язки, фінансові справи населення. Четверта група полягає у використанні інформаційних технологій в політичній боротьбі. Зростання впливу засобів масової інформації на хід і зміст політичних процесів, функціонування механізму влади - одна з домінуючих тенденцій сучасного суспільного розвитку.

Перейдемо до розгляду питання, які ж засоби використовуються для захисту інформації від вищенаведених загроз. Кожній із загроз безпеці в різних сферах інформаційного життя можна поставити у відповідність певні напрями, методи і заходи із забезпечення інформаційної безпеки. Так, Закон України «Про основи національної безпеки України» серед основних напрямів державної політики з питань національної безпеки в інформаційній сфері виділяє: забезпечення інформаційного суверенітету України; вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну; активне залучення засобів масової інформації до боротьби з корупцією, зловживаннями службовим становищем, іншими явищами, які загрожують національній безпеці України; забезпечення неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України. [5]

Враховуючи цілі та завдання політики інформаційної безпеки України, як правило, виділяють такі основні напрями забезпечення інформаційної безпеки: забезпечення інформаційної достатності для прийняття рішень; захист інформації, тобто захист інформаційного ресурсу; захист та контроль національного інформаційного простору, тобто систем формування масової свідомості; присутність у світовому інформаційному просторі. [4, с.131]

Головним завданням заходів із забезпечення інформаційної безпеки є мінімізація шкоди через неповноту, несвоєчасність або недостовірність інформації чи негативного інформаційного впливу через наслідки функціонування інформаційних технологій, а також несанкціоноване поширення інформації. [15]

Загалом, основні напрямки діяльності по забезпеченню інформаційної безпеки держави являють собою величезний комплекс заходів, до яких відносяться: розвиток науково-практичних основ інформаційної безпеки; розвиток законодавчої і нормативно-правової бази забезпечення інформаційної безпеки; розробка нормативно-правових і організаційно-методичних документів; розробка концепції інформаційної безпеки, спеціальних правових і організаційних заходів, що забезпечують збереження і розвиток інформаційних ресурсів; формування правового статусу суб'єктів системи інформаційної безпеки; розробка законодавчих і нормативних актів, що регулюють порядок ліквідації наслідків загроз інформаційній безпеці; відновлення порушеного права і ресурсів, реалізації компенсаційних мір; вдосконалення організації форм і методів запобігання і нейтралізації загроз інформаційній безпеці; розвиток сучасних методів забезпечення інформаційної безпеки. [6]

Розвиток науково-практичних основ інформаційної безпеки включає в себе: розробку стратегії забезпечення інформаційної безпеки країни; обґрунтування державної політики в умовах глобалізації інформаційних процесів, формування світових інформаційних мереж, прагнення деяких країн до домінування в розвитку і використанні світового інформаційного простору; розробку науково-практичних основ формування і проведення державної політики в області забезпечення інформаційної безпеки; обґрунтування пріоритетів національної безпеки, що відповідають довгостроковим інтересам суспільного розвитку.

Розвиток законодавчої і нормативно-правової бази забезпечення інформаційної безпеки означає визначення порядку розробки законодавчих і нормативно-правових актів, а також механізмів практичної реалізації прийнятого законодавства.

Розробка нормативно-правових і організаційно-методичних документів включає розробку документів, що регламентують: діяльність в області інформаційної безпеки органів державної влади; взаємини суб'єктів інформаційної діяльності для забезпечення інформаційної безпеки; регулювання державою процесів функціонування і розвитку ринку засобів інформації, інформаційних продуктів і послуг; інформаційні відносини в суспільстві і державі в умовах ринкової економіки тощо.

Формування правового статусу суб'єктів системи інформаційної безпеки включає формування правового статусу користувачів інформаційних і телекомунікаційних систем; визначення їхньої відповідальності за забезпечення інформаційної безпеки процедур застосування законодавства і норма-

тивних актів до суб'єктів, що скоїли злочини при роботі з закритою інформацією, а також правопорушення з використанням незахищених засобів інформації; розробку складу правопорушень з урахуванням специфіки карної, цивільної, адміністративної, дисциплінарної відповідальності.

Вдосконалення організації форм і методів запобігання і нейтралізації погроз інформаційної безпеки містить в собі: розробку нормативно-правової бази функціонування системи інформаційної безпеки, розмежування повноважень органів державної влади із забезпечення інформаційної безпеки; розробку системи моніторингу стану інформаційної безпеки; розробку пропозицій із створення сприятливих умов виходу з критичного стану вітчизняних галузей промисловості, що виробляють засоби інформатизації і захисту інформації; аналіз техніко-економічних параметрів вітчизняних і закордонних програмно-технічних засобів забезпечення інформаційної безпеки і вибір перспективних напрямків розвитку вітчизняної техніки; розробку системи економічних і статистичних показників, що характеризують ефективність функціонування системи забезпечення інформаційної безпеки; дослідження критеріїв і методів оцінки ефективності системи інформаційної безпеки тощо.

Під розвитком сучасних методів забезпечення інформаційної безпеки мається на увазі: розробка форм і способів цивілізованого впливу держави на формування суспільної свідомості і практичних рекомендацій з реалізації їх на практиці; розробка методів комплексного дослідження діяльності персоналу інформаційних систем, у тому числі методів підвищення мотивації, морально-психологічній стійкості і соціальної захищеності людей, що працюють із секретною і конфіденційною інформацією; розробка практичних рекомендацій зі збереження і зміцнення політичної стабільності в суспільстві; забезпеченню прав і свобод громадян; зміцненню законності і правопорядку методами інформаційної безпеки; формування шляхів і способів забезпечення органів державної влади, підприємств і громадян достовірною, повною і своєчасною інформацією; розробка основних напрямків діяльності із запобігання негативних інформаційних впливів на індивідуальну, групову і суспільну свідомість; розробка цивілізованих, демократичних форм і методів впливу на засоби масової інформації; розробка механізмів розвитку інформаційних відносин у сфері підприємництва і включення інформаційного ресурсу у господарські відношення; дослідження основних шляхів послаблення криміногенної обстановки, зниження числа комп'ютерних злочинів, у першу чергу - у кредитно-фінансовій сфері; розробка методів і практичних рекомендацій із контролю над експортом вітчизняних наукомістких технологій; обґрунтування напрямків протидії інформаційній зброї; удосконалення способів контролю за персоналом у захищених інформаційних системах.

Одним з найважливіших чинників національної безпеки країни є її економічний потенціал, під яким треба розуміти сукупність матеріальних і духовних сил суспільства, а також спроможність держави мобілізувати ці сили для забезпечення своєї безпеки. В свою чергу, інформація охоплює всі сфери людської діяльності і підвищує цей економічний потенціал країни, забезпечуючи зростання матеріальних і духовних сил суспільства і створюючи умови для можливостей, пов’язаних з координацією та мобілізацією. Крім того, вона створює матеріальні і інтелектуальні ресурси країни для ефективного захисту від агресивних в інформаційному відношенні держав.

З вищесказаного очевидно, що державна політика в сфері формування інформаційних ресурсів і інформатизації повинна бути спрямована на створення умов для ефективного і якісного інформаційного забезпечення рішення задач соціально-економічного розвитку країни. Серед основних напрямків державної політики в сфері інформатизації виділяють: забезпечення умов для розвитку і захисту всіх форм власності на інформаційні ресурси; формування і захист державних інформаційних ресурсів; створення і розвиток федеральних і регіональних інформаційних систем і мереж, забезпечення їхньої сумісності і взаємодії в єдиному інформаційному просторі; створення умов для якісного й ефективного інформаційного забезпечення громадян, органів державної влади, організацій і суспільних об'єднань на основі державних інформаційних ресурсів; забезпечення національної безпеки в сфері інформатизації, а також забезпечення реалізації прав громадян, організацій в умовах інформатизації; сприяння формуванню ринку інформаційних ресурсів, послуг, інформаційних систем, технологій, засобів їхнього забезпечення; формування і здійснення єдиної науково-технічної і промислової політики в сфері інформатизації з обліком сучасного світового рівня розвитку інформаційних технологій; підтримка проектів і програм інформатизації; створення й удосконалювання системи залучення інвестицій і механізму стимулювання розробки і реалізації проектів інформатизації; розвиток законодавства в сфері інформаційних процесів, інформатизації і захисту інформації. [6]

Існує багато різних засобів несанкціонованого доступу до інформації. Під захистом інформації від несанкціонованого доступу розуміють діяльність із запобігання одержання інформації, яка захищається, зацікавленим суб'єктом з порушенням установлених правовими документами чи власником інформації прав чи правил доступу до інформації, що захищається. Під системою захисту інформації

зазвичай розуміють сукупність органів і виконавців, техніку захисту інформації, а також об'єкти захисту, організовані і функціонуючі за правилами, установленими відповідними правовими, організаційно-розпорядницькими і нормативними документами про захист інформації. [16]

Вітчизняні дослідники Бондаренко В.О. та Литвиненко О.В. у загальній системі захисту інформації вирізняють такі напрями: законодавчо-нормативне забезпечення, яке передбачає розробку відповідних законодавчих актів, нагляд за виконанням законодавства з боку правоохоронних органів, судовий захист; організаційно-технічне забезпечення, що розкриває систему заходів, спрямованих на недопущення реалізації загроз безпеці інформаційного ресурсу; страхування інформаційних ризиків, що прийнятне лише для недержавних установ. [4, с.131]

Слід одразу ж відмітити, що ніякий окремо взятий засіб захисту не в змозі гарантувати адекватну безпеку. Надійний захист можливий лише за умови створення механізму комплексного забезпечення безпеки. Зазвичай, виділяють три основні складові такого комплексу: нормативно-правові; технічні; організаційні засоби.

Нормативно-правові засоби захисту визначаються законодавчими актами держави, які регламентують правила використання, обробки та передачі інформації обмеженого доступу та встановлюють ступінь відповідальності за порушення цих правил. У ст. 34 Конституції України розглядається право громадян України на інформацію, забезпечення інформаційних процесів. [12] Ця та деякі інші статті Конституції мають стати основою розвитку інформаційного законодавства. Невідповідність чинного законодавства України сучасним вимогам інформаційного розвитку є однією з основних проблем щодо захисту інформації, яка за наявності в державі потужного науково-технічного потенціалу може призвести до особливо тяжких наслідків.

Вся сукупність технічних засобів поділяється на фізичні та апаратно-програмні та включає в себе електричні, механічні, електромеханічні та електронні пристрої. Фізичні засоби реалізуються у вигляді автономних пристроїв та систем, що виконують функції загального захисту об’єктів, на яких обробляється інформація. Апаратні технічні засоби розміщують безпосередньо в обчислювальній техніці, в телекомунікаційній апаратурі чи в пристроях, що зв’язані з подібною апаратурою за допомогою стандартного інтерфейсу. Програмні засоби є програмним забезпеченням, що виконує функції захисту інформації.

Організаційні засоби захисту поділяються на організаційно-технічні та організаційно-правові, які використовуються в процесі створення та функціонування будь-якої структури. Інакше кажучи, тільки на основі нормативно-правової бази та за наявності апаратно-програмних засобів можливе ефективне керування в умовах широкого впровадження нових інформаційних технологій. Практика сьогодення свідчить про недооцінювання цих питань керівниками різних організацій. [17]

Вищесказане дозволяє зробити висновок, що необхідний рівень інформаційної безпеки держави забезпечується цілим комплексом політичних, економічних, організаційних та інших заходів, які допомагають реалізації інформаційних прав та інтересів держави і її суб’єктів.

Розгляд проблем інформаційної безпеки держави дає можливість стверджувати, що забезпечення інформаційної безпеки покладається на інформаційну організацію держави. Ця організація повинна гарантувати інформаційну безпеку держави та її суб’єктів в наш час глобалізації та зростання загроз з боку міжнародного тероризму. На жаль, в Україні існує дуже багато негативних факторів, які перешкоджають чи утруднюють створення такої інформаційної організації, і не останнім з них є неузгодженість органів державної влади щодо забезпечення інформаційної безпеки.

Отже, наукове осмислення комплексу проблем, пов’язаних з розробкою та втіленням у життя державної політики в інформаційній сфері, сьогодні набуває особливого значення, оскільки їх розв’язання сприятиме розвитку в Україні інформаційного суспільства і, таким чином - забезпеченню національної та інформаційної безпеки нашої держави.

ДЖЕРЕЛА ТА ЛІТЕРАТУРА

1. Соснін О.В. Інформаційна політика України: проблеми розбудови [Електронний ресурс] – Режим доступу: http://www.niisp.gov.ua/vydanna/panorama
2. Постанова Верховної Ради України «Про Концепцію (основи державної політики) національної безпеки України» від 16 січня 1997 р. № 3/97 ВР // Голос України. – 1997. – 4 лютого. – С. 5.
3. Інформаційна потужність держави, як складова національної безпеки. [Електронний ресурс] – Режим доступу: http://propolis.com.ua
4. Бондаренко В.О., Литвиненко О.В. Інформаційна безпека сучасної держави: концептуальні роздуми // Стратегічна панорама. – 1999. – № 1-2. – С. 127-133.
5. Закон України Про основи національної безпеки України // Відомості Верховної Ради. – 2003. – № 39. – Ст. 351.
6. Домарев В.В. Безпека інформаційних технологій. Методологія створення систем захисту. [Електронний ресурс] – Режим доступу: http://domarev.kiev.ua

7. Почепцов Г. Г. Информационные войны / С.Л. Удовик (отв.ред.). – М. : Рефл-бук, 2000. – 576 с.
8. Закон України "Про Концепцію Національної програми інформатизації" від 4 лютого 1998 р. № 75/98-ВР // Відомості Верховної Ради. – 1998. – № 27-28. – С. 182.
9. Гнатцов О.Г. Інформаційні ресурси в системі забезпечення державної безпеки. [Електронний ресурс] – Режим доступу: HTTP://WWW.NIISP.GOV.UA/VYDANNA/PANORAMA
10. Морозов О. Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності. [Електронний ресурс] – Режим доступу: http://www.viche.info
11. Тополевський Р., Захаров Є. Харківська правозахисна група. Коментарі до проекту Закону України «Про інформаційну безпеку України» (№5732 від 22 вересня 2004 р.). [Електронний ресурс] – Режим доступу: http://khpg.org.ua
12. Макаренко Е., Кирик В. Інформайційно-психологічний захист як складовий чинник інформаційної безпеки // Проблеми безпеки української нації на порозі XXI сторіччя. – К.-Чернівці, 1988.
13. Інформаційна безпека суспільства і держави. Стратегічні цілі і задачі інформаційної боротьби. [Електронний ресурс] – Режим доступу: http://www.ngo.dn.ua/doc/concept.doc
14. Галамба М., Петрик В. Інформаційна безпека України: поняття, сутність та загрози. [Електронний ресурс] – Режим доступу: http://www.justinian.com.ua
15. Концепція інформаційної безпеки держав – учасників Співдружності Незалежних Держав у військовій сфері. [Електронний ресурс] – Режим доступу: http://www.ngo.dn.ua
16. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект; Фонд «Мир», 2003. – 640 с.

Степко О. М. Анализ главных составляющих информационной безопасности страны / Институт международных отношений Национального авиационного университета.

В статье рассматриваются основные составляющие информационной безопасности страны. Рассмотрен комплекс вопросов информационной безопасности государства. Проанализированы цели, задачи и принципы информационной безопасности Украины, а также типы, источники информационных угроз и главные направления обеспечения информационной безопасности державы.

Ключевые слова: *информация, информационная безопасность, информационная безопасность страны.*

Stepko O. M. Analysis of the main parts of informational security of the state / Institute of International Relations National Aviation University.

The article concerns main parts of informational security of the state. Complex of problems of informational security of the state is considered. Basic tasks, principles and threats to informational security of Ukraine are analyzed.

Key words: *information, informational security, informational security of the state*