МІНІСТЕРСТВО ТРАНСПОРТУ І ЗВ`ЯЗКУ УКРАЇНИ
ОДЕСЬКА НАЦІОНАЛЬНАЯ АКАДЕМІЯ ЗВ`ЯЗКУ
ім. О.С.ПОПОВА

На правах рукопису

ЗАЛЄВСЬКА Ірина Іванівна

УДК 32.001: 004.056 (477)

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В СУЧАСНИХ УМОВАХ: ПОЛІТИЧНИЙ АСПЕКТ

23.00.02 – політичні інститути і процеси

Д И С Е Р Т А Ц І Я
на здобуття наукового ступеня кандидата політичних наук

Науковий керівник –
доктор політичних наук, професор
СИЛЕНКО Алла Олексіївна

Одеса - 2011

З М І С Т

РОЗДІЛ 3

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

ВСТУП

Актуальність теми дослідження обґрунтована тим, що сучасний період життя суспільства характеризується всезростаючою роллю інформаційної сфери, яка являє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, поширення й використання інформації, а також системи регулювання суспільних відносин, що виникають при цьому. Інтенсивне впровадження інформаційних технологій в усі сфери життя й діяльності сучасного суспільства, ріст питомої ваги інформаційної безпеки в забезпеченні цілісності держави привели до того, що інформаційні ресурси почали вважатися таким же багатством країни, як і її корисні копалини, виробничі потужності та інтелектуальний потенціал. Інформаційні інновації, поряд з технічними й управлінськими, не тільки значно розширюють можливості керівництва державою, але й істотно підвищують цінність інформації як стратегічного ресурсу. Однак ефективне використання інформаційних ресурсів в інтересах України, кожного її громадянина було б неможливим без формування в країні комплексної системи інформаційної безпеки. Слід визнати, що наслідки інформаційної революції багато в чому ще не визначені, а це лише підсилює зацікавленість прогнозів, що стосуються актуальних викликів і загроз в сфері безпеки, детермінованих бурхливим розвитком інформаційно-комунікативних технологій.

Одним з найважливіших напрямків вивчення проблем інформаційної безпеки є її політологічний аналіз. Особливість такого роду аналізу полягає, насамперед, у тому, що безпека розглядається в складній системі політичних координат: через визначення стану політичної сфери суспільства, виявлення сутності владних відносин, характеристику видів і способів політичної діяльності, з'ясування змісту й спрямованості зовнішньо- і внутрішньополітичних процесів.

Зв'язок роботи з науковими програмами, планами, темами. Дослідження виконане в рамках наукової теми «Соціально-політичні й правові аспекти розвитку інформаційного суспільства в Україні» (2009-2014 рр.), яке здійснюється кафедрою політології Одеської національної академії зв'язку ім. О.С. Попова, одним з виконавців якої є дисертант.

Метою дисертаційного дослідження є політологічний аналіз сучасних проблем інформаційної безпеки України. Для досягнення даної мети були поставлені наступні дослідницькі **завдання**:

- проаналізувати сучасні наукові досягнення в дослідженні інформаційної безпеки держави;

- розглянути основні теоретико-методологічні підходи до дослідження політичних проблем інформаційної безпеки;

- з'ясувати з погляду політичної науки інтереси особистості, суспільства й держави в інформаційній сфері:

- з'ясувати сутність поняття та зміст інформаційної безпеки;

- визначити інформаційно-технічні й соціально-політичні загрози для особистості, суспільства, держави;

- обґрунтувати, чому Інтернет є джерелом нових загроз для інформаційної безпеки;

- провести дослідження національних інтересів України у сфері забезпечення інформаційної безпеки;

- виявити особливості державної політики у сфері інформаційної безпеки;

- з'ясувати механізми забезпечення інформаційної безпеки у відкритому суспільстві.

Об'єктом дослідження виступає інформаційна безпека як складова національної безпеки держави.

Предметом дослідження є політика інформаційної безпеки України в сучасних умовах, яка поєднує інформаційний компонент безпеки і політику

його практичної реалізації в діяльності органів державної влади та управління.

Методи дослідження. Науковий підхід до визначення сутності й змісту інформаційної безпеки припускає комплексний характер дослідження даного явища, системність, а також облік закономірної обумовленості його результатів сформованими політичними відносинами.

В основу дослідження покладені системний і порівняльний підходи, які дозволили комплексно розглянути зазначену проблему в єдності всіх складових значущих характеристик. Зокрема, системний підхід допоміг розглянути інформаційну безпеку як механізм, що перебуває в процесі безперервної взаємодії з навколишнім середовищем. Розгляд інформаційної безпеки з позицій системного підходу дало можливість побачити відмінність наукового розуміння цієї проблеми від повсякденного. У повсякденному житті інформаційна безпека розуміється лише як необхідність боротьби з витоком закритої (таємної) інформації, а також з поширенням неправдивих і ворожих відомостей. Осмислення нових інформаційних загроз, особливо технічного плану, у суспільстві ще не відбулося.

Застосування структурно-функціонального аналізу допомогло розглянути інформаційну безпеку як систему зі складною структурою, кожний елемент якої має певне призначення й виконує специфічні функції, спрямовані на підвищення рівня інформаційної безпеки держави.

Класифікаційний підхід застосовувався при розгляді принципів інформаційної політики держави. У результаті цього останні були поділені на загальні (найбільш важливі і принципові керівні засади державної політики в цілому) та спеціальні (науково обґрунтовані й практично апробовані керівні початки державного впливу на інформаційну сферу, які забезпечують результативність і легітимність інформаційної політики).

При проведенні даного політологічного дослідження використовувалися загальнонаукові методи: аналіз і синтез, дедукція та індукція, метод

порівняння, прогнозування, а також методи прикладної політології: аналіз статистичних даних і вивчення документів.

Теоретичну основу дисертаційного дослідження склали також матеріали дискусій, науково-практичних конференцій міжнародного й національного масштабів, автореферати та матеріали дисертацій щодо теми дослідження, публіцистичні матеріали, матеріали політологічних, соціологічних та інформаційних сайтів Інтернет. Дослідження ґрунтується на положення й висновки, категоріальний апарат політології, філософії, юриспруденції, соціології і теорії безпеки. Особливу увагу було приділено науковому аналізу відповідних положень українського законодавства, присвячених актуальним проблемам національної та інформаційної безпеки.

Наукова новизна отриманих результатів полягає в тому, що дана дисертаційна робота є одним з перших системних досліджень політичного аспекту інформаційної безпеки України в сучасних умовах. У ході проведеного дослідження отримані наукові результати, які відзначаються науковою новизною.

уперше:

запропоновано новий підхід до визначення інформаційної безпеки, суть якого полягає в тому, що інформаційна безпека являє собою соціальне, а не чисто технічне явище, як це вважалося раніше. Тобто, інформаційну безпеку не слід ототожнювати із застосуванням спеціальних технічних засобів і методів для захисту інформації від несанкціонованого доступу, викрадення, знищення й т.д. Доведено, що забезпечення інформаційної безпеки - це не тільки захист інформації, але й організаційні, політичні, правові та інші заходи, спрямовані на забезпечення стійкого, стабільного розвитку суспільства й держави;

визначено, що інформаційна безпека нерозривно пов'язана з політичною безпекою, залежить від її стану і є її прямим наслідком, тому що політичні процеси та система суспільних відносин в інформаційній сфері

сучасного суспільства є проекцією на цю сферу системи політичних відносин і процесів у соціальному суспільстві;

виявлені основні політичні фактори забезпечення інформаційної безпеки, характерні для періоду соціальної трансформації в Україні: стан інформаційної політики держави; політична культура суспільства; рівень зрілості інститутів громадського суспільства; політична й громадянська соціалізація особистості; ступінь розвиненості інформаційно-політичних, у тому числі виборчих технологій; політична роль засобів масової інформації. Основним фактором, який визначає характер, спрямованість розвитку і стан захищеності інформаційних інтересів, виступає політика інформаційної безпеки України - самостійний галузевий напрямок реалізації інтересів суспільства, держави та особистості в інформаційній сфері;

визначено, що в порівнянні з іншими сферами діяльності держави щодо реалізації реформ розвитку інформаційної сфери, у тому числі і її захищеність, відстають від інших інститутів сучасного українського суспільства. Це негативно позначається не тільки на інформаційній організації держави, але і на стані інформаційної безпеки країни, суспільства та особистості. Тому одним з найважливіших завдань модернізації української державності щодо визначення змісту й динаміки внутрішньополітичних процесів в українському суспільстві, специфіки самоідентифікації української держави, її місце і роль у світовому співтоваристві, яке трансформується, повинен стати захист інформаційного простору;

аргументовано, що інформатизація, яка формує єдиний світовий інформаційний простір і глобальне мережне суспільство, множить інтелектуальний ресурс, сприяючи стійкому розвитку, досягненню благополуччя й безпеки особистості та суспільства. З іншого боку, інформаційні технології не є абсолютним благом. Вони створюють можливості для контролю над масовою свідомістю і маніпуляції нею у внутрішній політиці, а також ефективні засоби впливу на національні

співтовариства з боку найбільш оснащених щодо цього держав, а, отже, і нові загрози національній безпеці;

обґрунтовано зростаючу політичну роль інформації, яка перетворюється в національний політико-стратегічний ресурс та критерій зрілості й розвиненості політичної системи. Це дає підставу вважати інформацію політичним капіталом нації. Показано, що прогресивна заможність і політична вага країни, її можливості ефективно впливати на світові події залежать не тільки від матеріально-силових факторів (наприклад, військової та економічної могутності), але й від можливості використовувати інтелектуальний потенціал інших країн, поширювати та впроваджувати свої духовні цінності, а також гальмувати культурну експансію інших народів, трансформувати їхні культурні цінності;

визначено, що об'єктивно зростаюча глобальність інформаційної сфери приводить до того, що створювана інформаційно-комунікаційна інфраструктура країни й національних інформаційних ресурсів виявляються об'єктами досить уразливими для впливу з боку геополітичних конкурентів, терористичних організацій, кримінальних груп і окремих зловмисників. З урахуванням цього інформаційний розвиток України повинен здійснюватися в межах системної і збалансованої державної інформаційної політики, спрямованої на активну протидію інформаційній агресії;

уточнено:

поняття «інформаційна безпека», що розглядається як стан захищеності національних інтересів України в інформаційній сфері, які складаються із сукупності збалансованих інтересів особистості, суспільства й держави, від внутрішніх і зовнішніх загроз. Відмінність даного визначення від наявних у науковій літературі полягає в тому, що воно дозволяє включити в сферу інформаційної безпеки не тільки вже наявні об'єкти та напрямки захисту, але й відображає основний принцип забезпечення безпеки - принцип дотримання збалансованих інтересів особистості, суспільства й держави;

роль інформаційної безпеки і її місце в системі національної безпеки країни, які визначаються тим, що державна інформаційна політика тісно взаємодіє з державною політикою забезпечення національної безпеки країни через систему інформаційної безпеки, де остання виступає важливою сполучною ланкою всіх основних компонентів державної політики в єдине ціле;

отримало подальший розвиток:

поняття «політика інформаційної безпеки», зміст якого містить у собі інформаційний компонент безпеки і політику його практичної реалізації в діяльності органів державної влади та управління. Таким чином, інформаційна безпека розглядається як специфічний елемент політичних відносин, процес її забезпечення трактується як один з напрямків державної інформаційної політики.

Практичне значення отриманих результатів полягає в тому, що положення і висновки дисертації не тільки дають основу для подальшого теоретичного дослідження проблем політики інформаційної безпеки, але і можуть бути використані в практичній діяльності органів державної влади, пов'язаної з питаннями забезпечення інформаційної безпеки. Зокрема, висновки дисертації можуть бути корисні при формуванні внутрішньополітичної стратегії України в області інформаційної безпеки. Науково-теоретичні напрацювання та висновки дослідження можуть знайти застосування у вузівському навчальному процесі при читанні курсів з національної безпеки, політології, державного управління.

Апробація результатів дисертаційного дослідження. Дисертація написана і обговорена на кафедрі політології Одеської національної академії зв'язку ім. О. С. Попова. Основні положення, висновки та пропозиції дисертаційного дослідження були апробовані на Міжнародної науково-практичної інтердисциплінарної конференції «Етнос, мова та культура: минуле, сьогодення, майбутнє» (м. Рівне, 18-19 березня 2011 р.), УШ-ой Всеукраїнської наукової конференції студентів і молодих вчених «Молодь:

освіта, наука, духовність» (м. Київ, 13 квітня 2011 р.), Ш-ой Міжнародної науково-практичної конференції «Роль та місце ОВС у розбудові демократичної правової держави (м. Одеса, 21 квітня 2011 р.), ІІ Міжнародній науково-практичній конференції «Економічний і соціальний розвиток посткомуністичних держав в умовах глобалізації» (Рівне, 14-15 квітня 2011 р.)

Публікації. Основні результати здійсненого дослідження викладені в 3-х наукових статтях, опублікованих у спеціальних виданнях, затверджених ВАК України.

Структура дисертації обумовлена метою і завданнями, які були покладені дисертантом у процесі науково-теоретичної розробки вибраної теми. Дослідження складається з вступу, трьох розділів, перший і третій з яких містять по три підрозділи, другий - два підрозділи, висновок та список використаних джерел. Загальний обсяг дисертації становить 177 сторінок (без списку використаних джерел). Список використаних джерел містить 263 найменувань (28 сторінок).

РОЗДІЛ 1
ТЕОРЕТИЧНІ Й МЕТОДОЛОГІЧНІ ОСНОВИ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

У даному розділі аналізуються ступінь наукового опрацювання, основні теоретико-методологічні підходи до дослідження політичних проблем інформаційної безпеки. Уточнюється понятійний апарат дослідження. Це необхідно, оскільки без детального концептуального обґрунтування наявні понятійні проблеми лише сприяють примноженню компонентного складу інформаційної безпеки й ерозії її справжнього змісту при акценті на множинність небезпек, які мають місце в умовах недостатньої стабільності сучасних державних і суспільних інститутів, виступають одним з політичних наслідків світової економічної кризи.

1.1. Сучасні наукові досягнення в дослідженні інформаційної безпеки держави

Поява й наукове закріплення дефініції «інформаційна безпека» безпосередньо пов'язані з осмисленням феномена інформатизації й вивченням змісту процесу формування інформаційного суспільства. Даній проблемі присвячені роботи зарубіжних теоретиків - Д. Белла, Э. Тоффлера, Т. Стоуньєра, А. Турена, У. Дайзарда, М. Кастельса, К. Кояма, Е. Масуди; російських дослідників - А. Возженікова, В. Голубєва, В. Пусько, В. Манілова, В. Петрова, В. Труханова; українських дослідників - В. Литвиненка, Е. Макаренка, О. Сосніна, Л. Шиманського, С. Янишевського й ін.

Правові й організаційні основи захисту інформації розкриваються в дослідженнях українських учених Б. Авер'янова, О. Баранова, О. Копиленка, Б. Кормича, В. Погорілка, Г. Почепцова й ін.

Поняття "інформаційна безпека держави" розглядали російські дослідники І. Бучило, С. Расторгуєв, А. Стрельцов і ін., українські вчені С. Баринов, В. Бонадаренко, Б. Кормич, О. Литвиненко й ін.

Взаємозв'язок систем інформаційної й національної безпеки розкривають роботи М.І. Абдурахманова, А.В. Возженікова, В.І. Голубєва, В.С. Пусько, В.Л. Манілова, В. П. Петрова, В.А. Труханова.

Ролі інформаційних систем у підвищенні ефективності управління соціальними системами, складовою частиною яких є національна складова, присвячені роботи А. Пригожина, Л. Абалкіна, Т. Заславської, Д. Гвішіані, Ю. Волкова, І. Мостової, Г. Осипова, В. Ядова й ін.

Окрему групу становлять роботи А. Білоусова, Г. Іващенка, А. Кислявського, Д. Ловцова, Т. Мєшкової, Є. Митрохіної, А. Розсошанського, В. Садовничева, А. Стрельцова - присвячені формуванню системи інформаційної безпеки сучасної держави, виявленню й класифікації існуючих загроз.

Політичні проблеми процесу інформатизації й інформаційної безпеки розглядаються в роботах російських дослідників Д. Черешкіна, Г. Смоляна, В. Цигічка. Різні аспекти захисту особистості від негативного інформаційного впливу відображені в наукових працях Г. Грачова, І. Мельника, Ю. Єрмакова, В. Лепського. Питання впливу Інтернету на розвиток особистості досліджені С. Расторгуєвим, Г. Почепцовим, А. Войскунським і ін. Основоположники нового наукового напрямку - інформаційного права І. Бачило, В. Копилов, А. Агапов, М. Розсолов, В. Лопатін, А. Морозов досліджують проблеми регулювання відносин в області доступу до інформації, охорони прав на результати інтелектуальної діяльності, захисту персональних даних і т.п.

Новій й небезпечній для громадян, суспільства й держави проблемі - необхідності протидії комп'ютерній злочинності присвячені праці Ю. Батурина, В. Крилова, Н. Шурухнова й ін.

У ряді робіт інформаційна безпека розглядається як специфічний елемент політичних відносин, процес її забезпечення трактується як один з напрямків державної інформаційної політики [22, 97, 153, 228, 244].

Політичному аналізу інформаційного протистояння, дії інформаційної зброї, основним факторам його вражаючого впливу, питанням, пов'язаним із захистом психіки людини від шкідливого інформаційного впливу; військово-політичними наслідками інформаційних воєн, розкриттям особливостей впливу Інтернету на суспільно-політичні процеси й розвиток особистості присвячені роботи таких авторів як Г. В. Грачов, В. М. Цигичко, Ю. А. Єрмаков, Г. Г. Почепцов, С. Гриняєв.

Теоретичні й методологічні основи забезпечення інформаційної безпеки Росії розкриваються в монографії А. Стрельцова «Забезпечення інформаційної безпеки Росії. Теоретичні й методологічні основи» [227]. Цінність цієї книги в тім, що автор є безпосереднім учасником розробки проекту Доктрини інформаційної безпеки й ряду документів, що конкретизують її основні положення. У цій роботі досліджуються теоретичні й методологічні основи забезпечення інформаційної безпеки Росії. А. Стрельцов пропонує оригінальні рішення проблеми взаємодії особистості, суспільства й держави з метою забезпечення безпеки національних інтересів в інформаційній сфері. Автор звертає увагу на те, що наукові проблеми інформаційної безпеки потребують комплексного рішення.

Ще одна монографія, на яку варто звернути увагу всіх, хто цікавиться проблемами інформаційної безпеки, присвячена нормативно-правовим, психологічним і технологічним прийомам її забезпечення [240]. Автори цієї книги, Ю.С. Уфімцев і Є. А. Ерофеєв переконливо показують, що на тлі не цілком адекватної до них уваги преси й російської громадськості проблеми інформаційної безпеки вже сьогодні безпосередньо торкаються інтересів

кожного громадянина, нерідко стають серйозною перешкодою успішній діяльності господарюючих суб'єктів, громадських організацій, органів державної влади, а в недалекій перспективі багато в чому будуть визначати можливість здійснення наших сподівань на краще майбутнє. Забезпечення територіальної цілісності країни, збереження й розвиток самобутності народів Росії, їхня російська ідентифікація будуть досить ускладнені без розвитку інфраструктури й підвищення цілеспрямованого використання єдиного російського інформаційного простору, накопичених інформаційних ресурсів. Можливість досягнення життєво важливих інтересів Росії в інформаційній сфері багато в чому визначається її здатністю протистояти впливу ряду негативних факторів внутрішнього й зовнішнього характеру.

Важко уявити, пишуть автори монографії, що побудова громадянського суспільства й соціально-правової держави може відбуватися без розвитку системи правового регулювання відносин в інформаційній сфері, захисту законних інтересів громадян, суспільства й держави в розвитку російського інформаційного простору. Внаслідок цього забезпечення конституційних прав і свобод громадян природно передбачає правове регулювання інформаційної діяльності як окремих громадян, так і органів державної влади, засобів масової інформації, а також організацій, що забезпечують функціонування засобів і систем середовища передачі повідомлень.

Безсумнівний науковий інтерес представляє книга Г. Л. Акопова «Глобальні проблеми й небезпеки мережної політики» [2]. Досліджуючи функціонування мережної політики, автор звертає увагу на деякі небезпечні політичні аспекти мережної діяльності й позначає можливі як позитивні, так і негативні наслідки стрімкої комп'ютеризації й інформатизації сучасного суспільства. Предметом дослідження Г.Л. Акопова стали такі найбільш значущі проблеми сучасної мережної політики як інформаційні протиборства з використанням глобальної комп'ютерної мережі, небезпеки мережного «тероризму» або «кібертероризму» й поширення несанкціонованих електронних послань («спам») як політичного, так і економічного змісту.

У монографії В. Пірумова «Інформаційне протиборство. Четвертий вимір протистояння» [180] аналізуються історичні аспекти виникнення й розвитку, основні поняття й визначення, системне бачення сучасної термінологічної бази й деякі концептуальні положення інформаційного протиборства. Багато уваги автор приділяє проблемам інформаційної війни, інформаційної боротьби й боротьби з інформаційною злочинністю, а також сутності, змісту, основним методам впливу й можливим сценарієм ведення.

Великий інтерес для нашого дослідження представляє книга А.В. Федорова «Інформаційна безпека у світовому політичному процесі» [241]. Дана робота виділяється тим, що автор на основі системного підходу досліджує нову для політичної теорії проблему міжнародної інформаційної безпеки. Проаналізувавши основні теорії інформаційного суспільства й практики державного будівництва, автор доходить висновку, що ця складова безпеки іманентна постіндустріалізму й викликана до життя природними соціальними й технічними процесами. Супроводжуючи глобалізацію й сприяючи їй, інформатизація породжує нові можливості й нові, у тому числі стратегічні, загрози. Для їхнього запобігання поки немає міжнародно-правових механізмів. Вироблення останніх, вважає А. Федоров, - актуальне завдання сучасного права й дипломатії.

В 2006 р. побачила світ книга В.Я. Асановича й Г.Г. Маньшина "Інформаційна безпека. Аналіз і прогноз інформаційного впливу" [7]. У цій роботі розглядається новий напрямок, що розвивається, кібернетики й інформатики - інформаційна безпека соціально-економічних систем і людини. Систематизовано роботи в даній області, наведена класифікація загроз інформаційній безпеці. Аналізуються принципи й проблеми забезпечення інформаційної безпеки. Вперше моделі інформаційної безпеки розглядаються комплексно, досліджуються важливі для практики аспекти моделювання інформаційно-психологічного впливу на особистість, впливи ЗМІ на динаміку політичної взаємодії, широкий спектр математичних

моделей інформаційного впливу, національної безпеки соціально-економічних систем.

У 2009 р. вийшла книга Є. Прохорова «Забезпечення інформаційної безпеки й діяльності ЗМІ» [197], в якій почата спроба системного розгляду проблем масово-інформаційної безпеки (МІБ). Дається визначення МІБ, небезпеки й загрози в цій сфері, характеризується структура діяльності в ЗМІ по збереженню й підтримці МІБ, організаційні форми, необхідні для моніторингу й подолання небезпек і погроз, для зміцнення й розвитку МІБ.

Інформаційне забезпечення національної безпеки досліджується в дисертаційній роботі І. Гальцева [52]. Метою даної роботи є політологічний аналіз інформаційного забезпечення національної безпеки сучасної Росії, виявлення актуальних проблем і обґрунтування рекомендації з їхнього вирішення. Для досягнення даної мети автор спробував вирішити такі наукові завдання: уточнити теоретичні положення інформаційності в сучасному російському суспільстві й державі в цілому; виявити основні функції інформаційного забезпечення національної безпеки; розглянути інформаційне забезпечення національної безпеки від можливих політичних і соціокультурних загроз; проаналізувати стан інформаційного забезпечення національної безпеки сучасної Росії; виявити актуальні політичні й соціокультурні проблеми інформаційного забезпечення національної безпеки й рекомендації з їхнього вирішення в Російській Федерації.

Метою дослідження в дисертаційній роботі К. Оганяна «Інформаційна політика й проблема забезпечення національної безпеки в сучасній Росії» [162] є соціально-політичний аналіз сутності й особливостей реалізації інформаційної політики як фактора забезпечення національної безпеки сучасної Росії. Автор поставив перед собою наступні основні завдання: розкриття сутності інформаційної політики як феномена інформаційного суспільства і забезпечення його безпеки; виявлення критеріїв систематизації й відповідних їм форм, видів, напрямків інформаційної політики; дослідження методологічних основ інформаційної політики, класифікація

методів оцінки, одержання, подачі інформації, здійснення інформаційної політики й ін.; аналіз ролі російських політичних інститутів, насамперед держави й політичних партій, як ключових суб'єктів реалізації інформаційної політики з метою забезпечення національної безпеки сучасної Росії; розкриття значення інформаційної безпеки при здійсненні інформаційної політики сучасної Росії.

У дисертації І. Сафронової «Політичні проблеми забезпечення міжнародної інформаційної безпеки» [212] комплексно розглянуті загрози міжнародної інформаційної безпеки (МІБ) військово-політичного, кримінального й терористичного характеру, описані їх недостатньо вивчені прояви й проаналізовані можливі взаємозв'язки між ними. Досліджено напрямки й зміст міжнародного співробітництва й переговірного процесу в області МІБ і міжнародні підходи до забезпечення інформаційної безпеки, вироблені або такі, що перебувають у стадії розробки в рамках міжнародних і регіональних організацій та форумів; дана оцінка їхньої ефективності й адекватності відносно завдань зниження існуючих загроз у цій сфері. Проаналізовано діючі міжнародні політико-правові документи й механізми, що відносяться до інформаційної безпеки з метою визначення їхньої достатності для регулювання питань забезпечення міжнародної інформаційної безпеки.

На основі цього аналізу дана оцінка перспективності продовження консультацій і переговорного процесу з цієї проблематики на двосторонньому, регіональному й міжнародному рівнях. Визначені й обґрунтовані доцільні шляхи й засоби подальшого зміцнення МІБ; при цьому виявлена пріоритетність питань, з яких можливе досягнення міжнародних домовленостей. Запропоновано основні елементи, які могли б бути включені в перспективний міжнародний політико-правовий документ, такий, як принципи діяльності або кодекс поведінки держав в області МІБ, а надалі - у проект відповідного юридично обов'язкового міжнародного договору.

Інформаційній безпеці в діяльності органів внутрішніх справ

присвячене дисертаційне дослідження М. Величка «Інформаційна безпека в діяльності органів внутрішніх справ: теоретико-правовий аспект» [41]. Метою дослідження М. Величка є уточнення теоретико-правових положень, методологічних принципів забезпечення інформаційної безпеки органів внутрішніх справ, інформаційного протиборства й ефективної інформаційної протидії кримінальним структурам із застосуванням правових і правоохоронних механізмів. Відповідно до сформульованої мети в роботі були поставлені наступні завдання: дослідити й уточнити теоретичні й методологічні основи державно-правового регулювання в сфері захисту інформації й організації інформаційної безпеки органів внутрішніх справ; визначити шляхи вдосконалювання правових механізмів захисту інформації, організаційні заходи й управлінські рішення по боротьбі з комп'ютерними злочинами; виявити роль правових і організаційних механізмів захисту інформації в системах інформаційного забезпечення діяльності органів внутрішніх справ; розробити пропозиції по формуванню організаційно-правових механізмів забезпечення інформаційної безпеки органів внутрішніх справ.

Інформаційна безпека Росії в умовах соціальної трансформації досліджується в дисертаційній роботі А. Миколаєва [154]. Метою дослідження став політологічний аналіз стану, системи й шляхів забезпечення й ефективного розвитку інформаційної безпеки російського суспільства в соціально-трансформаційних (перехідних) умовах. Для досягнення поставленої мети А. Миколаєв поставив перед собою такі завдання: визначити й розкрити зовнішні й внутрішні політичні фактори детермінації процесу інформатизації, характерні для етапу соціальної трансформації держав світового співтовариства; виявити специфіку й особливості соціальної трансформації, характерної для сучасного російського суспільства, політичні фактори впливу її на інформаційну сферу; з'ясувати сутність і зміст інформаційної безпеки сучасного російського суспільства, її залежність від політичних факторів періоду соціальної трансформації;

дослідити процес впливу політичних інститутів держави й громадянського суспільства сучасної Росії на становлення й функціонування системи інформаційної безпеки; розглянути характер подальшого розвитку, пріоритетні шляхи забезпечення й підвищення ефективності інформаційної безпеки російського суспільства.

Метою дисертаційної роботи М. Шамова «Державна стратегія й політичні технології попередження інформаційного тероризму в сучасному Російському суспільстві» [248] став аналіз соціально-політичних аспектів прояву тероризму в інформаційній сфері. Завдання даного дослідження автор сформулював в такий спосіб: виявити причини, основні напрямки використання терористами сучасних інформаційних технологій у злочинних цілях і на цій основі сформулювати шляхи вдосконалювання протидії інформаційному тероризму як частини єдиної системи загальнодержавних заходів.

Частково проблеми інформаційної безпеки розкриваються в дисертації Смагіна В. А. «Забезпечення інформаційної відкритості політичної системи Росії» [221]. Так, на думку В. Смагіна, з урахуванням уразливості мережних технологій для різного роду атак, для даного етапу розгляду нормативних актів необхідно виробити й впровадити спеціальні вимоги до інформаційної безпеки сеансів зв'язку й інформації, яка опрацьовується.

Метою дисертаційної роботи Н. Тиклюк «Проблеми забезпечення «прозорості» і доступності влади в сучасній Росії» [238] став аналіз механізмів, факторів і умов забезпечення прозорості влади й доступу громадян до суспільно-значущої інформації в умовах впровадження інформаційно-комунікативних технологій у діяльність органів влади. Для реалізації поставленої мети необхідно було вирішити наступні дослідницькі завдання: розглянути політичні наслідки входження Росії у світовий геоінформаційний простір і реалізації міжнародно-визнаних підходів до забезпечення «прозорості» і доступності для громадян органів державної влади й місцевого самоврядування; вивчити особливості застосування

сучасних інформаційних технологій для забезпечення «прозорості» й доступності для громадян органів державної влади й місцевого самоврядування; виявити специфіку реалізації державної політики в сфері захисту прав громадян в інформаційній сфері й узагальнити наявний досвід у цій сфері; проаналізувати основні перешкоди в рішенні проблеми «прозорості» влади, доступності суспільно-значущої інформації й виробити пропозиції й рекомендації; розробити авторську версію «Концепції забезпечення «прозорості» влади, ефективної інформаційної взаємодії громадян і влади, розширення доступу громадян до суспільно-значущої інформації в ході інформатизації регіону», що може бути основою для планомірної реалізації заходів у даному напрямку.

Безсумнівний науковий інтерес для нашого дослідження має дисертаційна робота Д. Прудникова «Державна інформаційна політика Російської Федерації в області оборони» [198]. Мета даного дослідження полягає в науковому осмисленні специфіки державної інформаційної політики в області оборони, обґрунтуванні її концептуальних положень і визначенні сучасних пріоритетних напрямків розвитку.

Для досягнення даної мети поставлені дослідницькі завдання, а саме: провести аналіз теоретико-концептуальних підходів до визначення державної інформаційної політики в області оборони; з'ясувати сутність, визначити структуру, основні принципи й напрямки інформаційної політики російської держави в області оборони; здійснити аналіз специфіки й факторів, що визначають сучасний зміст інформаційної політики російської держави в області оборони; обґрунтувати основні напрямки вдосконалення інформаційної політики російської держави в області оборони.

Метою дисертації Т. А. Полякової «Правове забезпечення інформаційної безпеки при побудові інформаційного суспільства в Росії» [189] є наукове осмислення фундаментальних теоретичних питань, що стосуються визначення юридичного поняття інформаційного суспільства, особливостей інформаційних правовідносин в області забезпечення інформаційної безпеки

при побудові інформаційного суспільства в період глобалізації. Рішення актуальних теоретичних і методологічних питань правового забезпечення інформаційної безпеки необхідні, на думку автора дисертації, для розробки концептуальних положень правових основ розвитку інформаційного суспільства в Росії й конкретних пропозицій по вдосконаленню законодавства Російської Федерації.

Для досягнення зазначеної мети в дисертації були поставлені наступні завдання: обґрунтувати теоретичні й методологічні питання правового забезпечення інформаційної безпеки при побудові інформаційного суспільства в Росії; на основі теорії права, інформаційного права й спеціальної наукової літератури розробити юридичне поняття інформаційного суспільства в умовах глобалізації; визначити місце й роль правового забезпечення інформаційної безпеки при побудові інформаційного суспільства в Росії; провести порівняльно-правовий аналіз законодавства Російської Федерації, міжнародних і закордонних правових актів в області правового забезпечення інформаційної безпеки при побудові інформаційного суспільства; розглянути питання формування державної політики й визначення основних напрямків удосконалювання законодавства в розглянутій області, у тому числі в сфері Інтернету, спрямованих на реалізацію Стратегії розвитку інформаційного суспільства в Російській Федерації; проаналізувати нові виклики й загрози інформаційній безпеці в умовах глобалізації й побудови інформаційного суспільства в Росії; дослідити проблеми систематизації законодавства в даній області, юридичної техніки, уніфікації термінології й сформульовані пропозиції з подальшого вдосконалення класифікатора правових актів; обґрунтувати роль Мін'юсту Росії в створенні державної системи правової інформації.

У докторській дисертації І. Юрченка «Національна й регіональна безпека як політична стратегія сучасної Росії» [256, с.19] інформаційна безпека розглядається як складова національної й регіональної безпеки. Мета даного дисертаційного дослідження - концептуалізація процесу формування

політичної стратегії національної безпеки на загальнонаціональному й регіональному рівнях. Автор спробував вирішити такі наукові завдання: розкрити евристичну значимість поліпарадигмального підходу до вивчення національної й регіональної безпеки; визначити основні методологічні проблеми моделювання в розробці й концептуалізації політичної теорії національної й регіональної безпеки; визначити місце регіональної безпеки в системі національної безпеки держави й розкрити концептуальну сутність понять «регіональна модель безпеки» і «модель регіональної безпеки»; розглянути геополітичний вимір проблем національної й регіональної безпеки на південному напрямку; конкретизувати ризики й загрози російській державності в контексті глобалізації; охарактеризувати роль макро- і мікрополітичних факторів у конфліктному політичному процесі; інтерпретувати соціально-політичну природу екстремізму як загрози національній й регіональній безпеці; провести аналіз політичного дискурсу із проблем регіональної й національної безпеки в аспекті політичної стратегії розвитку сучасної Росії; визначити ментальні основи забезпечення безпеки й особливості формування громадянської ідентичності в процесі становлення російської державності в пострадянський період; охарактеризувати зміст політико-управлінського забезпечення національної безпеки в умовах інноваційного розвитку країни; проаналізувати політико-інформаційні ресурси формування національної та регіональної безпеки.

І. Юрченко відзначає, що сучасний етап глобального інформаційного суспільства характеризується значним впливом дискурсивних феноменів, що реалізуються в конфліктних та інтеграційних параметрах, які безпосередньо впливають на рівень безпеки суспільства, особистості й держави, на виникнення нових загроз і ризиків політичного розвитку. Спостерігається дискурсивне конструювання соціальної й політичної реальності, ріст конфліктного й інтеграційного потенціалу політичного дискурсу, що має як деструктивну, так і конструктивну спрямованість у поліетнічному соціальному просторі й служить серйозним фактором вироблення й реалізації

політичної стратегії як довгострокової програми забезпечення національно-державних інтересів країни і її громадян. Диверсифікованість і диференціація політичного процесу проявляється як боротьба політичних порозумінь, при цьому боротьба є способом взаємодії, у результаті якого затверджується та або інша система захисту й безпеки. Безпека - не тільки свобода, але й примус із метою підпорядкування корисливої волі окремих особистостей і груп ідеї захищеності життєво важливих інтересів всієї соціально-політичної спільності та її конкретних представників від зовнішніх і внутрішніх погроз [256, с.18].

У докторській дисертації з історичних наук Є. Штурби «Формування й реалізація концепції національної безпеки Російської Федерації в 1992-2004 рр.» [254] поставлена мета - вивчення історичного досвіду формування й реалізації концепції національної безпеки Російської Федерації в 1992-2004 рр. Для досягнення поставленої мети, для більш повного розкриття теми автором дисертації були визначені наступні завдання: охарактеризувати ступінь наукової вивченості, початкову базу проблеми, методологічну основу її вивчення й з врахуванням цього визначити її слабо розроблені аспекти й перспективи подальшого дослідження; осмислити процес відновлення основ політичного ладу Росії й формування концепції національної безпеки в 1992-2004 рр.; здійснити комплексний аналіз зовнішньополітичних пріоритетів країни в контексті розробки й реалізації концепції національної безпеки; дослідити специфіку військових загроз національній безпеці Росії й політику в сфері зміцнення обороноздатності в 1992-2004 рр.; комплексно вивчити проблеми забезпечення економічної безпеки в умовах інтеграції Росії у світове економічне співтовариство; розглянути проблеми формування соціальної держави як важливої умови забезпечення національної безпеки країни; висвітлити кризові явища в сфері духовного життя, боротьбу держави з антигромадськими проявами, злочинністю й екстремізмом.

У дисертації А. Сапожникової «Взаємодія держави й суспільства в політиці інформаційної безпеки РФ» [208] поставлена мета - розробка підстав

теоретичної моделі інформаційної безпеки сучасної держави, що припускає теоретико-методологічне обґрунтування потенціалу й перспектив підвищення ролі громадянського суспільства, його пріоритетів та інтересів у контексті опрацювання й реалізації політики інформаційної безпеки. А. Сапожникова поставила перед собою наступні завдання: уточнити сутність і зміст поняття «безпека», суб'єкт-об'єктний вимір суспільних і владно-політичних відносин в області забезпечення безпеки сучасної держави, суспільства й особистості; виявити основні напрямки еволюції суспільно-наукового дискурсу в області проблематики безпеки, маючи на увазі зміни його ціннісних орієнтирів і пріоритетів у процесі історичного розвитку держави й громадянського суспільства; уточнити зміст основних теоретичних підходів до розуміння громадянського суспільства як суб'єкта й об'єкта відносин в області забезпечення безпеки; виявити особливості формування й реалізації політики безпеки в умовах інформаційно-комунікаційної революції й руху до інформаційного суспільства; дати комплексний аналіз основних напрямків реалізацій функцій держави по забезпеченню інформаційної безпеки, з урахуванням актуальних викликів і загроз у даній області; розкрити політико-адміністративний зміст російської моделі політики інформаційної безпеки, інституціональні механізми й процеси в даній області; сформулювати модель взаємин громадянського суспільства й держави як об'єкта і суб'єкта політики інформаційної безпеки; узагальнити наявний світовий досвід взаємодії держави й цивільного суспільства в області інформаційної безпеки; обґрунтувати потенціал і перспективи реалізації стратегій соціального партнерства й взаємовигідного співробітництва держави й цивільного суспільства; у процесах і механізмах формування політики безпеки; виробити конкретні пропозиції щодо реалізації стратегій соціального партнерства в області політики інформаційної безпеки.

Метою дослідження у дисертаційній роботі Д. Кафтанчикова «Інформаційна безпека регіонів Російської Федерації: сучасний стан і

пріоритети забезпечення» [99] є виявлення актуальних загроз інтересам особистості, суспільства й держави в інформаційній сфері й визначенні пріоритетних напрямків протидії їм на регіональному рівні державного управління. Виходячи з вибраної мети автором визначені наступні завдання дисертаційної роботи: на підставі порівняльного дослідження наукових підходів до сутності й змісту поняття "національна безпека" виявити її взаємозв'язок із процесом інформатизації й особливостями забезпечення в умовах інформаційного суспільства, що формується; проаналізувати теоретичний і нормативно-правовий зміст інформаційної безпеки, на підставі чого уточнити поняття «інформаційна безпека регіону», а також визначити причини, що формують стан і рівень захищеності інтересів особистості, суспільства й держави в інформаційній сфері; розглянути регіональний аспект у системі забезпечення інформаційної безпеки, на підставі чого визначити вплив на її стан процесів інформатизації й регіоналізації політичного простору; виявити соціально-політичну специфіку проявів загроз інформаційно-технологічного й інформаційно-психологічного характеру на регіональному рівні й визначити пріоритетні шляхи протидії їм з боку органів державного й муніципального керівництва й інститутів громадянського суспільства; на підставі аналізу стану інформаційної безпеки в суб'єктах Російської Федерації сформулювати пріоритетні завдання функціонування систем забезпечення регіональної інформаційної безпеки; розробити практичні рекомендації з удосконалювання функціонування системи протидії загрозам регіональній інформаційній безпеці в суб'єктах Російської Федерації.

Важливе значення для вивчення зазначеної проблеми представляє дисертаційне дослідження Ю. Корольова «Інформаційно-політичні імперативи регіональної безпеки (на прикладі Саратовської області)» [118]. Мета цього дослідження полягає в політологічному аналізі процесу забезпечення регіональної безпеки в контексті підвищення рівня інформаційних загроз і розвитку сучасної системи масових комунікацій.

Автор даної роботи поставив перед собою наступні наукові завдання: концептуалізувати інституційно-правові характеристики регіональної безпеки; досліджувати систему й структуру регіональної безпеки в контексті зростаючих інформаційних загроз і способів їхнього запобігання; виявити експлікацію глобальних соціально-політичних тенденцій у російському регіональному політичному процесі; виявити особливості й тенденції розвитку інформаційного простору регіону; розглянути актуальні інформаційні й політичні загрози регіональної безпеки; проаналізувати існуючу політико-правову базу забезпечення інформаційної безпеки в регіоні, дати оцінку її ефективності; проаналізувати особливості деструктивного впливу інформаційних політичних кампаній у регіоні.

Політика США в області забезпечення інформаційної безпеки як у внутрішній політиці, так і в міжнародних відносинах розглядається в дисертації П. Шарикова «Політика США в області інформаційної безпеки» [250]. Головною метою даного дослідження є аналіз політики США в області інформаційної безпеки – як на внутрішньополітичному, так і на зовнішньополітичному рівні, визначення історичних етапів становлення цієї політики, факторів, що формують інтереси США в цій області, виявлення дестабілізуючих компонентів сучасної американської концепції протидії інформаційним викликам національної безпеки, а також розробка рекомендацій, які, на думку автора, сприяли б виробленню російської політики в області протидії загрозам інформаційної безпеки.

У більш конкретному плані в дисертації поставлені наступні дослідницькі завдання: визначити основні історичні етапи формування американської політики в сфері інформаційної безпеки; виявити фактори, під впливом яких формувалася американська внутрішньо- і зовнішньополітична стратегія в області інформаційної безпеки; провести аналіз внутрішньої політики федерального уряду Сполучених Штатів у сфері інформаційної безпеки; оцінити вплив політики адміністрацій Клінтона й Буша в області інформаційної безпеки на міжнародні аспекти інформаційної безпеки й

механізми міжнародного правового регулювання цих питань; проаналізувати існуючі багатобічні спроби регулювання питань інформаційної безпеки, а також політику США в міжнародних відносинах; розробити рекомендації заходів протидії загрозам інформаційної безпеки.

Метою дослідження в дисертації В. Остапенко «Державна політика в області забезпечення інформаційної безпеки органів виконавчої влади (регіональний аспект)» [167] є аналіз і узагальнення наявної практики із забезпечення інформаційної безпеки регіональних органів виконавчої влади, визначення й обґрунтування значення інформаційної безпеки в підвищенні ефективності процесу прийняття управлінських рішень; розробка проблемних напрямків забезпечення інформаційної безпеки регіональних органів виконавчої влади, пошук оптимальних методів правового, організаційного й технічного захисту інформації в регіональних органах виконавчої влади. Автор поставив перед собою такі завдання: проаналізувати теоретико-методологічні основи, особливості й проблеми становлення інформаційного суспільства в сучасній Росії; обґрунтувати необхідність забезпечення інформаційної безпеки органів виконавчої влади в умовах переходу країни до інформаційного суспільства; визначити основні напрямки забезпечення інформаційної безпеки регіональних органів виконавчої влади; виявити показники ефективності використання інформаційних ресурсів у діяльності органів виконавчої влади, а також індикатори погроз інформаційної безпеки; визначити фактори, що перешкоджають впровадженню й ефективному використанню існуючої організаційно-правової й технічної бази інформаційної безпеки в органах виконавчої влади суб'єктів Південного федерального округу; встановити індикатори інформаційної безпеки органів виконавчої влади, а також визначити критерії готовності органів виконавчої влади до ефективного впровадження й використання сучасних інформаційно-комунікаційних технологій; проаналізувати й узагальнити досвід Адміністрації Ростовської області по створенню регіональної системи захисту інформації.

У дисертації І. Чайки «Політичні технології забезпечення інформаційної безпеки регіону (на прикладі Краснодарського краю)» [246] поставлена мета: визначити особливості застосування політичних технологій забезпечення інформаційної безпеки регіону (на матеріалах Краснодарського краю). Автор дисертації спробував вирішити наступні завдання: охарактеризувати регіон у сучасній політико-інформаційній сфері; визначити основні політичні заходи забезпечення інформаційної безпеки регіону; розкрити механізми застосування інформаційних технологій як інструмент забезпечення регіональної безпеки; виявити основні виклики й загрози безпеки Краснодарського краю в політико-інформаційній сфері; визначити основні напрямки діяльності органів державної влади по забезпеченню інформаційної безпеки в Краснодарському краю; обґрунтувати технології протидії погрозам і викликам у політико-інформаційному просторі в ході підготовки й проведення Зимових Олімпійських ігор 2014 р. у Краснодарському краю.

Безсумнівний науковий інтерес для нашого дослідження має дисертаційна робота Є. Ковальової «Забезпечення транспарентності органів місцевого самоврядування сучасної Росії в процесі інформатизації політичного управління» [109]. Метою даного дослідження є визначення й політологічна оцінка ефективності механізмів, факторів і умов забезпечення транспарентності органів місцевого самоврядування в умовах інформатизації політичного управління. Автор дисертації спробував вирішити такі дослідницькі завдання: розглянути міжнародні стандарти свободи доступу до інформації й забезпечення транспарентності органів місцевого самоврядування для громадян; розглянути стан державно-правових підходів до забезпечення інформаційної свободи в Росії; вивчити особливості забезпечення транспарентності влади на рівні органів місцевого самоврядування й узагальнити досвід у цій сфері; проаналізувати основні перешкоди в рішенні проблеми забезпечення транспарентності влади на муніципальному рівні, доступності суспільно-значимої інформації й

виробити пропозиції й рекомендації; розробити авторську версію «Концепції забезпечення транспарентності органів місцевого самоврядування в процесі інформатизації політичного керівництва регіоном», що може бути основою для планомірної реалізації заходів у даному напрямку.

У вітчизняній науці найбільш ґрунтовно проблеми інформаційної безпеки вивчені в юриспруденції. Під юридичними аспектами організаційно-правового забезпечення захисту інформації розуміється сукупність законів і інших нормативних правових актів, за допомогою яких досягалися б наступні цілі: всі правила захисту інформації є обов'язковими для дотримання всіма особами, що мають відношення до конфіденційної інформації; узаконюються всі міри відповідальності за порушення правил захисту інформації; узаконюються (здобувають юридичну чинність) техніко-математичні рішення питань організаційно-правового забезпечення захисту інформації, а також узаконюються процесуальні процедури вирішення ситуацій, що складаються в процесі функціонування системи захисту.

Розробка законодавчої бази інформаційної безпеки будь-якої держави є необхідною мірою, що задовольняє найпершу потребу в захисті інформації при визначенні соціально-економічних, політичних, військових напрямків розвитку цієї держави.

У цьому плані особливо слід виділити дисертаційне дослідження українського правознавця Б. Кормича "Організаційно-правові основи політики інформаційної безпеки України" [116], метою якого стало проведення комплексного аналізу організаційно-правових основ політики інформаційної безпеки України, охарактеризувати динаміку процесу створення системи інформаційної безпеки, з'ясувати причини відставання інституціалізації й розвитку інформаційних правовідносин у цій сфері, визначити правові методи підвищення ефективності функціонування такої системи, запропонувати перспективну модель правового захисту інформаційної безпеки. Автор поставив перед собою такі наукові завдання: сформулювати й уточнити правовий зміст основних понять і категорій

інформаційної безпеки як складової національної безпеки; створити класифікацію об'єктно-суб'єктного складу й напрямків інформаційної безпеки, придатну для застосування в нормативно-правових актах; з'ясувати особливості формування інформаційного права й правової бази інформаційної безпеки на сучасному етапі; розкрити сутність інституціонального механізму захисту інформаційної безпеки й проаналізувати основні проблеми організації його функціонування; визначити особливості застосування форм і методів державного управління в області інформаційної безпеки; досліджувати специфіку правового регулювання захисту інформаційної безпеки держави, суспільства, людини; здійснити порівняльно-правовий аналіз повноважень державних органів у сфері інформаційної безпеки; проаналізувати співвідношення національного законодавства в сфері інформаційної безпеки з міжнародно-правовими нормами й стандартами; узагальнити сучасний досвід правотворчої та правозастосовної практики щодо захисту інформаційної безпеки як важливої функції держави; визначити пріоритетні напрямки законодавчого утвердження й реалізації політики інформаційної безпеки України; окреслити перспективи розвитку системи інформаційної безпеки в Україні й теоретично обґрунтувати конкретні пропозиції й рекомендації щодо її вдосконалювання.

Мета дисертаційного дослідження Ю. Максименко «Теоретико-правові засади забезпечення інформаційної безпеки» [135] - визначення теоретичних і правових основ забезпечення інформаційної безпеки України. Здійснити системний огляд українських і закордонних науково-практичних джерел щодо наукової розробки теми. Автор даної дисертації поставив перед собою дослідницькі завдання: уточнити зміст основних понять теорії національної безпеки, а саме: "національна безпека", "національні інтереси", "національні інтереси в інформаційній сфері", "інформаційна безпека"; виділити основні підходи до визначення поняття "інформаційна безпека", зміст інформаційної безпеки України й національні інтереси в інформаційній сфері; розкрити особливості розуміння Європейським Союзом інформаційної

безпеки й проблеми євроінтеграції України в даному контексті; окреслити напрямки співробітництва Європейського Союзу й України в інформаційній сфері; охарактеризувати стан нормативно-правового забезпечення інформаційної безпеки України й окреслити головні проблеми в цій сфері; надати пропозиції по вдосконаленню національного законодавства щодо регулювання суспільних відносин у сфері інформаційної безпеки України.

Мета дисертаційного дослідження В. Козубського [110] - повний багатоаспектний і докладний аналіз стану інформаційного простору кримського регіону як значущого складового загальнонаціонального інформаційного простору періоду становлення України як незалежної самостійної держави. Автор спробував вирішити такі завдання: визначити й проаналізувати системи й засоби інформаційного впливу зовнішніх факторів у контексті україно-російських відносин і повернення репатріантів; визначити й проаналізувати роль, місце й завдання ідеологічних факторів впливу на суспільну думку; проаналізувати ступінь інформаційного впливу державних і недержавних інформаційних установ; проаналізувати місце й роль сучасних засобів масової комунікації в процесі інформаційного впливу на суспільну думку кримського регіону; розробити структуру регіонального інформаційного центру з урахуванням наявних можливостей і інфраструктури Національного космічного агентства України, розташованого в Криму.

Мета дисертаційної роботи О. Олійника «Організаційно-правові засади захисту інформаційних ресурсів України» [168] - виявлення й систематизація проблем захисту інформації як складової (підсистеми) інформаційної безпеки України, обґрунтування правових і організаційних основ, удосконалення цієї діяльності. О. Олійник поставив такі завдання дослідження: систематизувати адміністративно-правові проблеми реалізації конституційних принципів суверенності й незалежності держави в сфері внутрішньої й зовнішньої інформаційної політики; вияснити змістовну сутність, значимість поняття «захист інформації обмеженого доступу й іншої життєво важливої

інформації», визначити правовий режим інформаційного простору; проаналізувати вітчизняні й світові підходи й тенденції до рішення проблем інформаційної безпеки й захисту інформації, виявити правові й організаційні проблеми в цій сфері діяльності; визначити й обґрунтувати теоретико-методологічні основи формування й удосконалення захисту інформаційних ресурсів у процесі міждержавного співробітництва; розглянути відповідно до сучасних реалій і тенденцій методичні підходи до формування зваженої державної політики в сфері інформаційної безпеки й захисту інформації; визначити концептуальні основи вдосконалення захисту інформаційних ресурсів України й змоделювати правові механізми й організаційні заходи рішення цього завдання.

Безсумнівним внеском у вітчизняну науку й освіту став підручник Б. Кормича «Інформаційне право» [115], у якому аналізуються базові принципи й положення інформаційного права, його основні інститути, розглядається правове регулювання основних видів інформаційних відносин та інформаційної діяльності. Особливе місце в даному підручнику зайняли питання, присвячені інформаційній безпеці з позиції юридичної науки. Автор даної роботи справедливо відзначає, що інформаційна безпека останнім часом стала одним з найважливіших напрямків інформаційної діяльності, що обумовлено рядом факторів. Насамперед, це ключова організаційно-управлінська й регулятивно-контрольна функція інформаційного фактора в сучасному суспільстві. Але пропорційно до збільшення ролі цього фактора підвищується можливість суспільно-небезпечних наслідків від протиправного втручання в інформаційні відносини й процеси. Крім цього, пише автор підручника, в умовах сучасних глобалізаційних тенденцій Україна повинна бути здатною адекватно відповідати на всі виклики й небезпеки, пов'язані з побудовою глобального інформаційного суспільства [115, с.116].

Отже, можна зробити наступні висновки. Теоретико-правові проблеми забезпечення безпеки особистості, суспільства й держави, правове

регулювання організації й діяльності інститутів захисту державного ладу представлені в публікаціях вітчизняних і зарубіжних учених. У той же час, незважаючи на значну увагу, що приділяється дослідниками проблем інформаційного суспільства обговоренню питань забезпечення інформаційної безпеки України, формуванню й реалізації державної політики України в цій області, цілий ряд аспектів поки залишаються слабо розробленими, що ускладнює створення ефективно діючої системи забезпечення інформаційної безпеки держави. Зокрема, у вітчизняній і зарубіжній літературі недостатньо розробленими питаннями залишаються політичні проблеми, що впливають на інформаційну безпеку в Україні.

В основному, наявні наукові дослідження носять військово-політичний і техніко-технологічний характер і не повною мірою відображають стан політики інформаційної безпеки в умовах глобалізації. Звідси й технократичні проекти забезпечення інформаційної безпеки.

Думається, що повинен набувати вагу гуманітарний підхід до забезпечення інформаційної безпеки, в основі якого лежало б розширене розуміння інформаційних впливів і об'єктів їхнього застосування. А також акцентувати на інформаційно-психологічній стороні, що має надзвичайну актуальність у сучасних умовах.

Аналіз ступеня розробки даної проблеми показав, що соціально-політична тематика інформаційної безпеки має наступні складові. Перша проблемна область - це аналіз діяльності ЗМІ як суб'єкта забезпечення інформаційної безпеки і як джерела загроз інформаційно-психологічної безпеки людини й суспільства. Зацікавленість тут представляє стан нормативно-правової бази, роль ЗМІ в процесі формування відкритого суспільства, суспільної думки державного управління й т.д.

До цього напрямку прилучається проблематика, пов'язана з інформаційними війнами. У даному ракурсі інформаційна безпека охоплює коло питань, що стосується розробки тактики й стратегії інформаційного протиборства, відбиття інформаційних атак, захисту власного

інформаційного простору, розробки й реалізації інформаційної політики. Цей аспект стосується різноманітних суб'єктів політики й проявляється на всіх рівнях організації політичної системи: регіональному, державному й міжнародному.

Третя проблемна область пов'язана із процесами інформатизації органів державної влади й місцевого самоврядування. Тут у центрі уваги перебуває «електронний уряд» і аналіз сутності трансформацій, що відбуваються. Сюди ж можна віднести проблему цифрової нерівності й формування інформаційного суспільства.

В останні роки помітно актуалізувався науковий інтерес до проблем співвідношення інформаційної сфери суспільства й функціонування політичних відносин. У зв'язку із цим зросло значення досліджень, присвячених визначенню ролі й функціональних параметрів акторів політичного процесу, здатних виступати суб'єктами забезпечення різних аспектів національної безпеки. Цим і обумовлений вибір теми дисертантом.

1.2. Основні теоретико-методологічні підходи до дослідження політичних проблем інформаційної безпеки

Формування інформаційного суспільства стало можливим завдяки інформаційній революції, що відбулася в другій половині XX століття. Вона характеризувалася появою й стрімким поширенням якісно нових технологій, що дозволяють людству створювати, зберігати, обробляти й передавати практично будь-яку інформацію в будь-якій кількості в режимі реального часу. Винахід радіо й телебачення дозволяли транслювати інформацію серед величезної кількості людей. Однак створення й поширення персональних комп'ютерів і, головне, поява наприкінці XX століття Інтернету стали основними факторами формування загального інформаційного простору й зародження інформаційного суспільства, що поєднує людей, які проживають у найрізноманітніших куточках світу. Крім індивідів, учасниками

глобального інформаційного суспільства стають практично всі суб'єкти міжнародних відносин, починаючи від держави й закінчуючи транснаціональними злочинними угрупованнями, що використовують інформаційні технології не тільки як засіб зв'язку, але й як спосіб поширення гасел, ідей, залучення людських ресурсів і т.д.

Розуміння змін, що відбуваються під впливом інформаційної революції, у науковій літературі, вкрай неоднозначне. Можна виділити два підходи до їхнього осмислення: перший припускає досить вузьке розуміння, другий – більш широке. У першому випадку акцент робиться на технічних аспектах інформаційної революції, тобто на розвитку й поширенні засобів зв'язку, технологій роботи з інформацією, за допомогою яких забезпечується передача, обмін, зберігання й обробка інформації й даних. Поширення інформаційних технологій у сучасному світі до початку XXI століття досягло таких масштабів, що можна говорити про формування глобального інформаційного простору. Технологічно саме з ним зв'язаний розвиток можливостей роботи з інформацією. Такий підхід практикують відомчі експерти, тісно пов'язані з відповідними «силовими» структурами. Він припускає, насамперед, дослідження «вузьких», чисто технічних проблем проведення ефективних операцій.

З погляду даного підходу варто просто описати різні моделі сучасних операцій із забезпечення безпеки проти нових і нетрадиційних загроз і співставити їхню ефективність із погляду досягнення безпосередніх цілей. Саме в цьому вузьковідомчому контексті в основному існують дослідження операцій також у США й Великобританії.

Ще одним цікавим представляється другий підхід, у рамках якого відбувається більш широке й глибоке осмислення наслідків інформаційної революції. Цей підхід, умовно кажучи, можна назвати «широким» або академічним. Він полягає в дослідженні проблем забезпечення безпеки з погляду їх широкого соціально-політичного контексту й на загальному тлі функціонування державних інститутів. На Заході він розвивається в рамках

класичної університетської традиції дослідження проблем безпеки, насамперед, у контексті таких академічних дисциплін, як «міжнародні відносини», «політологія» і «конфліктологія».

Найбільша увага приділяється соціальним змінам, що відбуваються під впливом розвитку інформаційних технологій (ІТ), – формуванню інформаційного суспільства, украй залежного від інформації й ІТ і вразливого перед погрозами, що з'являються в результаті їхнього становлення й розвитку.

Соціокультурний підхід, як головний об'єкт безпеки, виділяє особистість, суспільство, державу й є орієнтований на задоволення їхніх інформаційних потреб та інтересів. Але представники цього підходу не в усьому єдині між собою. Одні з них трактують інформаційне забезпечення безпеки досить широко, розуміючи під ним захищеність потреб громадян, окремих груп і соціальних прошарків, масових об'єднань людей і населення в цілому в якісній (ціннісно-значимій) інформації, необхідній для забезпечення їхньої життєдіяльності, освіти й функціонування. При цьому інформаційне забезпечення безпеки розкривається через забезпечення інтелектуального, психологічного, культурного, світоглядного, духовно-морального й інших видів безпеки великомасштабних систем різного державного й міждержавного рівнів. Інші вважають, що в цьому трактуванні невиправдано упущені інтереси держави як самостійного об'єкта захисту.

Однак неспроможність цього підходу легко виявляється й у структурно-змістовному плані. Справа в тому, що різний ступінь зрілості соціально-економічних, політичних, соціокультурних та інших відносин у кожній конкретній державі характеризується й різним станом інформаційного забезпечення безпеки. Це у вирішальній мірі залежить від рівня інформування суб'єктів політико-економічного життя, що визначає одночасно й ступінь адекватності сприйняття ними навколишньої дійсності й, як наслідок, обґрунтованість прийнятих рішень і дій [52, с.6].

Одним з найбільш важливих наслідків інформаційної революції й формування інформаційного суспільства стало те, що інформаційний потенціал і ступінь включення в інформаційний простір і інформаційне суспільство в значній мірі визначають міць держави в міжнародних відносинах.

Знання й інформація стали одним із стратегічних ресурсів держави й суспільства, ресурсом соціально-економічного, технологічного й культурного розвитку. Масштаби використання цього ресурсу порівняні з використанням традиційних ресурсів, а величина сумарних витрат на нього вже має макроекономічну значимість.

У силу згаданої різниці між поняттями «інформаційний простір» і «інформаційне суспільство» існує різне розуміння поняття «інформаційний потенціал». У першому випадку критерієм його визначення є, насамперед, рівень технологічного розвитку держави, а також поширеність технологій серед населення. Більш широке розуміння інформаційного потенціалу містить у собі ефективність використання можливостей, що відкриваються при застосуванні інформаційних технологій. Ця ефективність стала фактором економічного зростання, підвищення добробуту населення, військової переваги й багатьох інших факторів, що визначають міць держави.

В якості критеріїв оцінки розміру інформаційного потенціалу країни й ступеня його залучення в інформаційне суспільство, як передбачається, можуть використовуватися наступні показники: масштаби виробництва й експорту високотехнологічних товарів і послуг, розміри витрат на НІОКР, число патентів на винаходи, кількість Інтернет-сайтів з доменом країни й кількість користувачів Інтернету. Звичайно, такий підхід дещо вузький, тому що, безсумнівно, повинні враховуватися й багато інших факторів, однак він дозволяє одержати загальне уявлення про сучасне співвідношення сил держав в інформаційній сфері.

Як справедливо стверджує російський дослідник Ю. Корольов, проблема інформаційної безпеки не є сьогодні вузько технологічною

категорією, а переходить в сферу концептуального обґрунтування управління суспільними процесами. Складний за будовою характер інформаційної безпеки актуалізує дослідження в різних областях. Сьогодні активно розробляється проблематика інформаційно-психологічної безпеки особистості, тематика інформаційної безпеки держави [118, с.14]. При цьому недостатня увага приділяється політологічним аспектам інформаційної безпеки.

Один із запропонованих у науковій літературі (і підтримуваний нами) підходів виходить із того, що національна безпека є продукт спільної діяльності держави й громадянського суспільства, що доповнюють один одного. Але оскільки держава й громадянське суспільство часто протипоставлені один одному, іноді не можуть знайти необхідного компромісу й прийти до якоїсь згоди з багатьох аспектів, варто виділити в рамках національної безпеки дві її форми. Одна із цих форм - політична (державна) безпека, її формування в повному обсязі ініціюється державою, саме вона відповідальна перед громадянським суспільством за забезпечення соціальних гарантій громадян. Друга форма - безпека громадян, що виступає результатом ініціативи громадянського суспільства, його ресурсів. У свою чергу, політична безпека, суб'єктом якої є державна влада, має внутрішньо- і зовнішньополітичний аспекти.

Не випадково інформаційна безпека (що являється складовою частиною національної безпеки) розглядається в контексті проблем національної безпеки. Чим вища активність громадян, організацій або держав у кіберпросторі, тим перед суспільством гостріше встають проблеми забезпечення своєї інформаційної безпеки. І сьогодні є всі підстави вважати, що національна безпека країн буде залежати від забезпечення інформаційної безпеки. У міру ж інтенсифікації технічного прогресу й посилення «електронного співробітництва» держав ця залежність буде постійно зростати [187, с.228]. Так, наприклад, український дослідник М. Галамба справедливо вважає, що «інформаційна складова не може існувати поза

цілями загальної національної безпеки, так само як і національна безпека не буде всеохоплюючою без інформаційної безпеки» [51].

Щоб з'ясувати особливості даного підходу, проаналізуємо поняття «національна безпека», що, як відомо, вперше прозвучало в посланні президента Т. Рузвельта Конгресу США в 1904 р. У даному посланні доводилася доцільність приєднання зони Панамського каналу з метою інтересів національної безпеки Сполучених Штатів Америки. Із цього моменту, мабуть, і почався процес наукового усвідомлення національних інтересів в аспекті національної безпеки [39, с.38].

Більш широке застосування поняття «національна безпека» почалося приблизно з перших десятиліть XX сторіччя. Споконвічно те, що сприймалося в основному як безпека військово-політична, яка забезпечує політичний суверенітет, згодом, у зв'язку з усе більш системним вивченням крізь призму національних інтересів, перетворилося у визнане інтегративне поняття, що включає широкий комплекс проблем внутрішнього й зовнішнього порядку [254, с.6].

«Нація, - писав У. Липман, - перебуває в стані безпеки, коли їй не доводиться приносити в жертву свої законні інтереси з метою уникнення війни й коли вона в змозі захистити при необхідності ці інтереси шляхом війни» [49].

Концепція національної безпеки, так само як зовнішньополітичні й геополітичні концепції, являє собою похідну від концепції національних інтересів. Парадигма національної безпеки будується із врахуванням як зовнішніх загроз, так і внутрішніх проблем, пов'язаних із станом самого суспільства, й кореняться в суспільстві.

Першорядне завдання концепції національної безпеки - це визначення й розробка пріоритетних напрямків, комплексу заходів і засобів запобігання, насамперед, крайніх форм зовнішньої й внутрішньої загроз - війни з іншими державами й громадянською війною.

Національна безпека - наукова й практична проблема, що характеризується станом політичних інститутів, які забезпечують ефективну діяльність з підтримки оптимальних умов існування й розвитку особистості й суспільства. Національна безпека, як категорія політичної науки, відображає зв'язок безпеки з націями, що включає суспільні відносини й суспільну свідомість, інститути суспільства і їхню діяльність, які забезпечують реалізацію національних інтересів у конкретній історично сформованій обстановці.

У сучасних вітчизняних політичних і політико-юридичних документах національна безпека характеризується як одна з головних проблем українського суспільства.

У національній безпеці виділяються три рівні безпеки: особистості, суспільства й держави. Їхнє місце й роль визначаються характером суспільних відносин, політичним устроєм (ладом), наявністю внутрішніх і зовнішніх загроз. У змістовному плані в понятті національна безпека прийнято виділяти політичну, економічну, військову, екологічну, інформаційну безпеку й безпеку культурного розвитку нації.

Ряд дослідників, в основному юристів, вважають, що дане поняття має політичне походження, «що, з одного боку, обумовлює його нерозривний зв'язок з державною діяльністю й державною політикою, а з іншого - створює певні труднощі при правовому регулюванні пов'язаних з нею питань у силу декларативності й нестабільності цілого ряду її аспектів» [116, с.14].

З погляду політологів, «національна безпека - це державна політика, спрямована на створення внутрішніх і міжнародних умов, сприятливих для збереження або зміцнення життєво важливих національних цінностей; це стан, що забезпечує захищеність інтересів народу й держави, суспільства й кожного його члена» [186, с. 316].

Російський дослідник Д. Кафтанчиков вважає, що стан національної безпеки детерміновано трансформацією політичної системи, коли впровадження інформаційних технологій ініціює мережну логіку змін усього

спектра суспільних взаємодій. Політична система, включаючи її регіональні компоненти, втрачає вид стандартної сукупності й традиційно сформованої конфігурації інститутів публічної влади й політичних партій, здобуваючи форму багатомірного співтовариства, автономні елементи якого взаємопов'язані багатогранними формальними й неформальними контактами, що виникають і знаходять стійкість завдяки революції в зоні поширення інформації, систем зв'язку й електронних комунікацій.

Завдяки цьому інформація набуває значення стратегічного ресурсу соціуму, коли саме ступінь залученості держави й громадянського суспільства в глобальний інформаційний простір розцінюється як пріоритетний критерій їхнього розвитку. Подібна ситуація, в першу чергу, обумовлена поширенням такого явища, як інформатизація, що характеризує злиття когнітивних, соціокультурних і техніко-технологічних процесів [99, с.17].

На думку українського вченого-юриста Б. Кормича, «національна безпека являє собою стан захищеності гарантованих законодавством умов життєдіяльності держави, суспільства й окремої особи від внутрішніх і зовнішніх загроз. Підтримка національної безпеки є важливим напрямком державної діяльності, що актуалізується залежно від наявності й ступеня відповідних загроз» [116, с.15].

Український дослідник Ю. Максименко пропонує визначати національну безпеку як результат управління реальними або (і) потенційними погрозами (небезпеками) з метою задоволення національних інтересів людини, суспільства й держави [135, с.9].

У законодавчій практиці України питанню національної безпеки була приділена увага в Декларації про державний суверенітет України від 16 липня 1990 р. Акт проголошення незалежності України від 24 серпня 1991 р. також містить такі поняття, як безпека й інтереси українського народу.

Тільки через сім років з'явився спеціальний нормативно-правовий акт, що стосується питань національної безпеки України. А саме: прийняття

Верховною Радою 16 січня 1997 р. Постанови «Про концепцію (основи державної політики) національної безпеки України», що була розроблена вже на основі нової Конституції України.

Як уже було сказано вище, інформаційна безпека нерозривно пов'язана з політичною безпекою, залежить від її стану і є її прямим наслідком, тому що політичні процеси й система суспільних відносин в інформаційній сфері сучасного суспільства є проекцією на цю сферу системи політичних відносин і процесів у суспільстві соціальному. З огляду на це, розглянемо поняття «політична безпека» або «безпека політичної системи суспільства» більш докладно.

Вихідним пунктом розгляду проблем безпеки, з погляду політичної науки, є з'ясування здатності суспільної системи зберігати стан динамічної рівноваги за допомогою інструментів політичного регулювання, незважаючи на несприятливі впливи зовнішнього й внутрішнього середовища. Тобто можна сказати, що з політичної точки зору безпека є способом безконфліктної взаємодії, у якому держава за допомогою політичної інституціалізації й технологій створює безконфліктні зони життєдіяльності індивідів, протидіє конфліктному способу взаємодії в суспільстві з метою створення умов, що забезпечують гідне життя й вільний розвиток людини. Держава забезпечує безпеку двояким чином. Вона конституює й формує політику, а для цього створює інститути й програми, спрямовані на створення умов для гідного життя й вільного розвитку людини, що протидіють конфлікту, виробляє технології попередження, керування й розв’язання конфлікту. Держава втримує рівень досягнутої безпеки, і, не відмовляючись від її зміни, протидіє крайнім формам прояву конфлікту, що претендує на руйнування встановленої безпеки.

Об'єктом політологічного аналізу, таким чином, повинна стати безпека особистості, суспільства й держави в усіх її різноманітних проявах, а предметом - закономірності виникнення загроз і небезпек функціонування соціальної системи в ході розвитку політичних процесів і явищ, а також

умови, спрямованість і способи регулювання суспільних відносин за допомогою політики в інтересах безпеки.

З'ясування складного комплексу питань, пов'язаних з пізнанням зазначених проблем, вимагає дослідження поля політики, що робить найбільш безпосередній вплив на стан безпеки особистості, суспільства й держави. Знання співвідношення між полем політики й сферою безпеки дозволяє визначити сутність політичного впливу на процеси, що торкаються безпеки особистості, суспільства й держави, а також роль політики, її можливості й межі у відображенні потенційних і актуальних небезпек і загроз.

Характеристика поля політики, тобто того соціального простору, що пов'язане з політичними процесами і явищами, безпосередньо випливає із сутності політики як суспільного явища. Політика знаходить свій найбільш яскравий прояв у діяльності соціальних суб'єктів, спрямованих на реалізацію суспільних інтересів за допомогою інститутів влади. Вона являє собою також відносини між соціальними групами, класами, націями й державами з приводу влади й владних відносин. Політика може бути зрозуміла як особливий тип поведінки людей, як мистецтво управління суспільними процесами. Різноманіття проявів політики не означає її невизначеності, її сутність виражається через категорію «влада». Тому, як відомо, поле політики - це область владних відносин.

У соціальній системі політика виступає як загальний і універсальний інструмент суспільного регулювання, а політичне керівництво й управління є вирішальним чинником громадської організації. Загальний організаційний початок, закладений у політику, дає можливість переборювати процеси стихійного розвитку, які властиві економічній, соціальній і духовній сферам суспільства й здатні порушити стабільний стан, викликати соціальну дезорганізацію й загрози безпеки. Більше того, політична організація доповнює соціальну самоорганізацію, надає їй осмислений, цілеспрямований характер, а в необхідних випадках – замінювати процеси самоорганізації,

якщо вони ведуть до суспільних деформацій (ріст кримінальних структур, архаїчних форм виробництва, залежності від зовнішніх факторів і т.д.).

Найважливішою, хоча й не єдиною причиною появи політики як регулятора суспільних відносин, є потреба в безпеці людського співтовариства. Необхідність в координації діяльності різноманітних елементів соціальності, у вольових відносинах між людьми в особливому ступені виникають саме тоді, коли протиріччя й конфлікти усередині соціуму створюють загрозу його існуванню. Таким чином, потреба в самозбереженні й виживанні в умовах, що становлять загрози життю як окремих індивідів, так і всього співтовариства, породжує особливий вид суспільних відносин - політичні відносини.

Політична безпека - це спосіб взаємодії в суспільстві, у якому держава, усвідомлюючи конфліктну природу безпеки, прагне відігравати провідну й визначальну роль. Правова держава з погляду безпеки є прийнятна форма інституціаліоналізації конфлікту й забезпечення безпеки громадян.

Безпека політичної системи суспільства або політичної безпеки полягає в стійкому й ефективному розвитку цієї системи, що дозволяє їй адекватно реагувати на негативні зовнішні й внутрішні впливи, зберігати цілісність соціуму і його сутнісні якості. Вона може бути охарактеризована через стан динамічної рівноваги політосфери й ефективність діяльності політичних інститутів. Стрижнем політичної безпеки є система владних відносин: через функціонування державних механізмів забезпечується необхідний ступінь стійкості як політичної сфери, так і всієї суспільної системи, здійснюється регулювання політичних процесів і спрямовується діяльність спеціальних служб. Політична безпека тісно зв'язана із здатністю владних органів забезпечувати політичний суверенітет країни, згуртованість суспільства в досягненні загальнозначущих цілей на основі балансу корінних національних цінностей, життєво важливих інтересів його громадян і основних соціальних груп.

Політична безпека має дві основні сторони: зовнішню й внутрішню. Структура внутрішньополітичної безпеки представлена такими основними компонентами: безпека інституційної підсистеми; безпека регулятивної підсистеми; безпека функціонально-комунікативної підсистеми; безпека духовно-ідеологічної підсистеми.

Перша із зазначених підсистем політичної сфери містить у собі політичну організацію суспільства, тому безпека інституційної підсистеми має особливе значення для стійкого функціонування політичної системи суспільства в цілому. Ця підсистема складається із сукупності державних органів, політичних партій і громадських організацій, за допомогою яких забезпечується регулювання всіх сторін громадського життя. Центральним елементом політичної організації виступає держава, що безпосередньо реалізує функцію захисту від загроз і небезпек.

Значення безпеки інституційної підсистеми для політичної безпеки в цілому виражається в тому, що всяка її дезорганізація несе із собою порушення організаційно-технологічних основ функціонування політичної сфери суспільства, що може бути пов'язане з падінням ефективності інститутів влади, не реалізацією політичних рішень, загальним зниженням сили й обсягу владних органів.

Безпека регулятивної підсистеми забезпечує стійкість політико-правового регулювання суспільних процесів. Оскільки ця підсистема містить у собі сформований комплекс політичних принципів і правових норм, основ конституційного ладу й способи їхньої реалізації, то дезорганізаційні явища, що порушують нормальне функціонування політико-правової сфери, завдають значної шкоди політичній безпеці.

Виникнення істотних протиріч у політико-правовій основі життєдіяльності суспільства веде до зниження соціальної цінності права, його можливостей як засобу регулювання соціально-політичних відносин і інструменту розв’язання конфліктів. Все це може породити тенденції до використання неправових методів у діяльності політичних інститутів, а

також масштабні прояви правового нігілізму. Ослаблення регулятивної підсистеми політичної сфери суспільства здатне викликати зростання політичної апатії законослухняних громадян при одночасному посиленні активності екстремістських сил, політична поведінка яких виходить за конституційні рамки.

Безпека функціонально-комунікативної підсистеми відіграє важливу роль у збереженні стійкості політичних відносин на основі суспільної й громадянської згоди.

У структурі політичної безпеки особливо виділяється безпека духовно-ідеологічної підсистеми, що містить у собі сукупність політичних цінностей, тип політичної культури, укорінені в суспільстві політичні ідеології. Стійкість духовно-ідеологічного компоненту політичної системи багато в чому визначає стабільність всієї політичної сфери суспільства.

Зовнішньополітичний аспект політичної безпеки містить у собі здатність політичної системи суспільства протистояти негативному впливу ззовні. Цей вплив може виражатися в спробах дестабілізації внутрішньополітичної обстановки, зміни конституційного ладу, забезпечення зовнішнього впливу на прийняття важливих державних рішень, порушення територіальної цілісності країни й в інших діях, що суперечать національним інтересам.

Зовнішній вплив, спрямований на ослаблення політичної безпеки країни, може здійснюватися різними напрямками і виражатися в різних формах. У сучасних умовах спроби домогтися політичних змін шляхом зовнішнього тиску не обов'язково припускають військово-силові методи, хоча й не виключають їх з арсеналу засобів, що використовуються.

Забезпечення політичної безпеки є найважливішим завданням, рішення якого створює необхідні передумови для ефективної діяльності всієї системи захисту особистості, суспільства й держави від зовнішніх і внутрішніх загроз. Тільки на цій основі можлива ефективна діяльність державних та інших

політичних інститутів, пов'язана із забезпеченням безпеки в інших сферах громадського життя.

Безпека виступає в політиці не тільки як насущна потреба, але і як найважливіша життєва цінність: вона виступає об'єктом людських бажань і устремлінь, необхідною нормою буття. У той же час безпека вимагає необхідної суспільної регуляції. На основі ціннісних подань про безпеку в сфері політики здійснюються й розгортаються системи нормативного контролю й відповідні політичні інститути. З їхньою допомогою забезпечується об'єднання розрізнених зусиль індивідів, різних прошарків, груп і суспільства в цілому для рішення насущних завдань в інтересах самозбереження, виживання й розвитку.

Головна мета політики полягає в забезпеченні цілісності соціальної системи, в ефективній суспільній інтеграції. У системі політичного цілеспрямування безпека виступає провідним компонентом, оскільки створення сприятливих зовнішніх і внутрішніх умов для суспільного розвитку повністю збігається з інтересами забезпечення безпеки й завданнями конструктивної політики.

Внутрішній взаємозв'язок політики й безпеки як суспільних феноменів породжує значний збіг сфери їхнього прояву. Сфера безпеки й поле політики визначаються, насамперед, конфліктним середовищем, і в цьому проявляється єдність того соціального простору, на яке вони поширюються. Дійсно, поле політики являє собою область конфліктних соціальних взаємин, а сама політика виступає інструментом їхньої оптимізації: завдання політики полягає в розв’язанні суспільного конфлікту й переведенні соціальної взаємодії в русло згоди. У той же час загроза безпеки особистості, суспільства й держави виникає в тому конфліктному середовищі, що накопичує в собі потенціал руйнування, тому сфера безпеки охоплює, насамперед, і переважно все ту ж область конфліктних взаємовідносин.

Інформаційна безпека, як і політична безпека, є складовою загальної безпеки й стрімко розвивається як в усьому світі, так і в Україні, глобальна

інформатизація охоплює всі сфери держави: економічну, військову, політичну, промислову й т.п. Крім усього, обчислювальна техніка стає невід'ємною частиною життєдіяльності людини. Інформаційна безпека, як і будь-який інший об'єкт, має загрози, що зазіхають як на цілісність фізичну, так і її похідні.

Процеси перебудови в політичному житті України, що відбуваються в сучасних умовах, безпосередньо впливають на стан інформаційної безпеки держави. При цьому виникають нові фактори, які необхідно враховувати при оцінці реального стану інформаційної безпеки й визначенні ключових проблем у цій області. Їх можна розділити на політичні, економічні й організаційно-технічні.

До політичних факторів відносяться:

- зміна геополітичної обстановки внаслідок фундаментальних змін у різних регіонах світу, зведення до мінімуму ймовірності світової ядерної й звичайної війн;

- інформаційна експансія Росії, США й інших розвинених країн, що здійснюють глобальний моніторинг світових політичних, економічних, військових, екологічних й інших процесів, що поширюють інформацію з метою одержання односторонніх переваг;

- становлення нової української державності на основі принципів демократії, законності й інформаційній відкритості;

- руйнування раніше існуючої командно-адміністративної державної системи управління, а також сформованої системи забезпечення безпеки країни;

- порушення інформаційних зв'язків внаслідок утворення незалежних держав на території колишнього СРСР;

- прагнення України до більш тісного співробітництва із зарубіжними країнами в процесі проведення реформ на основі максимальної відкритості сторін;

- низька загальна правова й інформаційна культура в українському суспільстві.

У політичному аспекті розвиток інформаційного суспільства в Україні повинен привести до формування й розвитку єдиного інформаційного простору як необхідної умови політичного й духовного об'єднання українського народу й входженню країни у світове інформаційне співтовариство; вдосконалюванню й розвитку ЗМІ, створенню сприятливого суспільно-політичного клімату в країні, розвитку інформаційних потреб і інформаційної культури населення; удосконалюванню системи забезпечення особистої й суспільної безпеки в інформаційній сфері, запобіганню загроз використання нових інформаційних технологій як зброї, інформаційного тероризму й інформаційного криміналу.

В економічній сфері зростає вразливість економічних структур від недостовірності, запізнювання й незаконного використання економічної інформації.

У сфері духовного життя виникає небезпека розвитку в суспільстві за допомогою електронних засобів масової інформації агресивної споживчої ідеології, поширення ідей насильства й нетерпимості й інших негативних впливів на свідомість і психіку людини [158].

Інформаційні зв'язки в системі національної безпеки такі ж складні й багаторівневі, як і її структура. В узагальненому вигляді їх можна представити як сукупність груп взаємозв'язків.

По-перше, це обмін інформацією між суб'єктами охорони національної безпеки, що забезпечують утворення організаційної цілісності системи.

По-друге, інформаційні зв'язки між людьми, діяльність яких безпосередньо й опосередковано пов'язана із забезпеченням функціонування системи національної безпеки.

По-третє, інформаційні зв'язки між технічними компонентами системи, оскільки частина інформаційних функцій, надлишкових для людини, але

необхідних для забезпечення національної безпеки, у сучасних умовах передається різноманітним технічним засобам.

Особливе місце надається інформаційним ресурсам в умовах ринкової економіки. У конкурентній боротьбі широко поширені різноманітні дії, спрямовані на одержання конфіденційної інформації різними способами. Установлено, що сьогодні у світі 47% відомостей, що охороняються, добуваються за допомогою технічних засобів промислового шпигунства [187, с.303]. У цих умовах захисту інформації від неправомірного оволодіння нею відводиться значна й всезростаюча роль.

Інформаційна безпека є найважливішим критерієм оцінки стабільності системи соціальних, духовних, політичних відносин сучасного суспільства в інформаційній сфері, що розглядається державою як особливе поле діяльності. Поява й реалізація концепції так званого «електронного уряду», формування на законодавчому рівні основ державної інформаційної політики дозволяє говорити про те, що в наш час іде процес активної інтеграції державних структур і органів влади в інформаційний простір, їхня адаптація до нових умов діяльності, що пов'язана зі значними змінами їхньої первісної структури (так, виконавча влада в інформаційному просторі існує не у вигляді звичних для постіндустріального суспільства міністерств і відомств, а у вигляді «електронного уряду»), що, у свою чергу, говорить про те, що держава стає основним фактором, що регулює суспільні відносини в інформаційній сфері. Одночасно із все посилюючою регулюючою роллю держави в інформаційній сфері все більшу вагу в загальному обсязі суспільних відносин здобувають відносини винятково політичні - відносини між соціальними групами, класами, націями й державами з приводу влади й владних відносин, що існують і розвиваються в рамках законів віртуального інформаційного простору й реалізовані за допомогою інструментів (методів) інформаційного впливу. Це, у свою чергу, породжує в межах інформаційної сфери власну сферу політичних відносин, що тісно змикаються (і частково перекриваються) із традиційною сферою політичних відносин суспільства

постіндустріального. Можна також говорити, що з переходом суспільства від індустріальної стадії розвитку до інформаційної відбувається трансформація його політичної сфери, окремі частини якої прямо включаються в інформаційну політичну сферу, а інші стають основою для її подальшого розвитку. Поява в інформаційній сфері власної політичної сфери й вивчення політичних процесів, що відбуваються в ній, стає основою для появи нового напрямку політики - інформаційної.

В аналізі змісту й специфіки впливу захищеності сегмента глобальної мережі Інтернет на забезпечення інформаційної безпеки принципово важливим є виявлення найбільш важливих з погляду політичних відносин параметрів зазначеного процесу. При дослідженні такого роду відносин необхідно розглядати обидва явища з позицій системного аналізу, що припускає не простий вплив одного явища на інше, а й навпаки, тобто враховувати їхню взаємодію, взаємовплив, а також дію на розглянуті явища інших явищ, подій, процесів. Значну роль у ході дослідження взаємного впливу зазначених явищ має виявлення мотивації впливу або, іншими словами, факторів впливу як основної характеристики їхнього причинно-наслідкового зв'язку, що визначають умови, спрямованість і зміст досліджуваних процесів. Тому визначення змісту й специфіки впливу захищеності сегмента глобальної мережі Інтернет на забезпечення інформаційної безпеки необхідно розглянути через призму впливу факторів, які його зумовлюють [173].

Безумовно, стосовно сфери інформаційної безпеки такою “силою” виступає захист інформаційного простору, як політичне явище й процес, за допомогою якого багато в чому й визначається стан, зміст, а також перспективи даного виду безпеки держави. Більше того, відповідно до даного визначення, а також з урахуванням вищезгаданих підходів, поняттям “фактор”, що стосується до захисту інформаційного простору в процесі його впливу на інформаційну безпеку держави, доцільно позначати також і те, що

в інших випадках може позначатися поняттями “рушійна сила”, “причина”, “умова”.

Фактор - це поняття, що служить для позначення джерела впливу, надаваного на той чи інший об'єкт, що має певне значення для його функціонування й у даних конкретних умовах представляє особливий дослідницький інтерес. Все це повною мірою можна застосувати, як вище було відзначено, до аналізу впливу на стан інформаційної безпеки, що надається з боку процесу захисту інформаційного простору.

Якщо розглядати в якості об'єкта, що випробовує вплив різноманітних факторів і розвивається під впливом цих факторів, сам процес впливу захисту інформаційного простору на інформаційну безпеку держави, то нам необхідно розглянути досить широкий спектр зазначених факторів (Пеньков І.А. Вплив захищеності…).

Багатоплановість і неоднозначність впливу різних факторів на взаємодію захисту інформаційного простору й інформаційної безпеки логічно підштовхує до їхнього угрупування й типологізації. Насамперед, варто виділити групи факторів об'єктивного й суб'єктивного характеру.

У цьому плані представляється, що об'єктивні фактори являють собою багаторівневу систему (глобального, регіонального й національно-державного рівнів) внутрішніх і зовнішніх параметрів, що впливають на суб'єкти формування й реалізації інформаційної політики держави.

До числа найбільш значущих об'єктивних факторів у сучасних умовах, що обумовлюють вплив захисту інформаційного простору на інформаційну безпеку, відносяться геополітичні фактори - геополітичні параметри (умови, ресурси, можливості), що визначають стан і розвиток держав, регіонів і світу в цілому.

Геополітичні параметри держави є визначальними в дихотомії “захист інформаційного простору - інформаційна безпека”, оскільки саме вони визначають в умовах формування нового світового порядку специфіку й

можливості держави здійснювати захист інформаційного простору й відповідно забезпечувати свою інформаційну безпеку.

Будь-яка держава, приступаючи до формування своєї інформаційної політики або вносячи в неї корективи, повинна враховувати вплив геополітичних факторів і тих загроз, які вони провокують. Сама ж геополітична обстановка стосовно питань забезпечення інформаційної безпеки держави здобуває геостратегічне значення.

До об'єктивних факторів з повною підставою можна віднести також кліматичні умови, демографічну ситуацію в країні й цілий ряд інших параметрів, що об'єктивно визначають місце держави у світовому співтоваристві. Тому аналіз "відмінних початків" держави й відповідності їм інформаційної системи держави є важливою умовою дослідження процесу впливу захисту інформаційного простору на інформаційну безпеку [173].

Поряд з об'єктивними факторами досліджуваного процесу на нього мають вплив також фактори суб'єктивної властивості, що представляють собою результати багатопланової діяльності суб'єктів інформаційної політики (захисту інформаційного простору) конкретної держави (групи держав) в області її (їх) інформаційної безпеки.

У цьому випадку мова йде, насамперед, про політичну діяльність і практичні дії конкретних держав, політичних сил і різних організацій (у тому числі й екстремістських, терористичних), що негативно впливають на політичну обстановку у світі, країні, визначаючи стан небезпек і загроз інформаційній безпеці конкретної держави. Крім цього, до факторів суб'єктивного порядку відносяться також діяльність суб'єктів інформаційної політики даної держави (органів державної влади, структур інформаційної організації й систем, що забезпечують її життєдіяльність і розвиток), що здійснює захист інформаційного простору й реалізує завдання забезпечення інформаційної безпеки. Вплив суб'єктивних факторів у цьому випадку припускає результат усвідомленої діяльності суб'єктів політики в процесі

їхнього впливу на інформаційну безпеку держави, опосередковану специфікою, змістом і результатами захисту інформаційного простору.

Таким чином, найголовнішими аспектами, що визначають характер і зміст впливу захисту інформаційного простору на інформаційну безпеку держави, є наступні.

Перший – інформаційна безпека сучасної держави детермінована сукупністю об'єктивних і суб'єктивних факторів глобального, регіонального й національно-державного характеру.

Другий – у числі об'єктивних факторів провідне місце займають фактори геостратегічного рівня, які обумовлюють генезис вихідної складової політики захисту інформаційного простору -інформаційно-інтелектуальний потенціал, інформаційні ресурси й можливості захисту інформаційного простору в інтересах забезпечення інформаційної безпеки.

Третій – забезпечення інформаційної безпеки сучасної держави в значній мірі обумовлено дією суб'єктивного фактора, пов'язаного з політичними пріоритетами в діяльності керівників органів державної влади й керівництва, в першу чергу так званих “силових структур” як основних суб'єктів політики, що визначають цілі, завдання, методи й способи вирішення проблем в області захисту інформації.

Глобальне використання інформаційних технологій і телекомунікацій, з одного боку, спричиняє залежність національної безпеки держави від захищеності інформаційної інфраструктури, що визначає ступінь уразливості від впливу недружніх держав, терористичних організацій, кримінальних співтовариств і окремих осіб через інформаційний простір.

З іншого боку, вирішальне значення для національної безпеки країни має рівень розвитку інформаційної інфраструктури, що повинен забезпечувати ефективність проведення державної політики. Під цим слід розуміти ряд заходів: забезпечення органів державної влади й управління повною, достовірною й своєчасною інформацією для прийняття обґрунтованих рішень; забезпечення сучасних інформаційних відносин у

сфері бізнесу для становлення й розвитку цивілізованого ринку; реалізація ефективного механізму зарахування інформаційного ресурсу в господарський оборот для рішення соціально-економічних завдань; забезпечення прав громадян на інформацію для підтримки соціальної й політичної стабільності в суспільстві й інше.

До найважливіших об'єктів національної безпеки в інформаційній сфері, крім інформаційної інфраструктури, відносяться інформаційні ресурси і, в першу чергу, - державні інформаційні ресурси.

Отже, однією з основних складових системи забезпечення національної безпеки є інформаційна безпека, що виступає важливою сполучною ланкою всіх основних компонентів державної політики в єдине ціле. При цьому цілком очевидно, що роль інформаційної безпеки і її місце в системі національної безпеки країни стає все вагомішою. Це відбувається в силу наступних причин: національні інтереси, загрози їм і забезпечення захисту від цих загроз у всіх областях національної безпеки виражаються, реалізуються й здійснюються через інформацію й інформаційну сферу; людина і її права, інформація й інформаційні системи й права на них - це основні об'єкти не тільки інформаційної безпеки, але й основні елементи всіх об'єктів безпеки в усіх її сферах; вирішення завдань національної безпеки пов'язане з використанням інформаційного підходу як основного науково-практичного методу; проблема національної безпеки має яскраво виражений інформаційний характер [84].

Аналіз наукових підходів дозволив розділити існуючі поняття інформаційної безпеки на кілька груп. По-перше, інформаційна безпека безпосередньо як стан захищеності інтересів, особистості, суспільства й держави в інформаційній сфері. По-друге, інформаційна безпека як стан соціально-політичного середовища, при якому забезпечується захист особистості, суспільства, держави. По-третє, інформаційна безпека як право, гарантія одержання достовірної інформації.

У чому суть поняття «інформаційна безпека», з'ясуємо в наступному підрозділі.

1.3. Поняття й зміст інформаційної безпеки

Правителям і воєначальникам усіх часів потрібна була інформація про сильні й слабкі сторони їхніх ворогів, про наміри їхніх супротивників або суперників. Із цієї причини розвідка (або шпигунство) мають настільки ж довгу історію, що й сама цивілізація. Ще п'ять століть до нашої ери древній китайський стратег Сан Цу писав у своїй класичній книзі "Мистецтво війни" про велике значення розвідки й розвідувальних мереж у стані супротивника. Навіть у Біблії міститься більше сотні спогадів про шпигунів і випадки збору розвідувальної інформації.

В XVI - XVII століттях правителі європейських монархій у боротьбі за збереження й зміцнення своєї влади буквально загрузли в інтригах. Утворився інститут іноземних посольств, від яких вимагали не тільки виконання офіційних представницьких функцій, але й поєднання їх із шпигунством і підривною діяльністю. Створені в той час розвідувальні служби з великою ефективністю використовувалися такими видатними політиками, як кардинал Ришельє у Франції (1585 - 1642) і сер Френсіс Волсингем в Англії (1537 - 1590).

Незважаючи на постійний технічний прогрес, "технологія" шпигунства за своєю суттю мало змінилася із часу епохи Відродження: для досягнення успіху агент повинен, насамперед, одержати доступ до секретної інформації, потім викрасти або скопіювати її. Після цього треба непоміченим вибратися "на волю", встановити контакт зі своїм "куратором" і передати йому добуті матеріали.

Політичні, світоглядні й культурні зміни, що відбувалися в той час у Європі, стимулювали розвиток "технології" збору розвідувальної інформації. Цікаво, що основні принципи так званих "багато алфавітних" шифрів, що

склалися протягом XV століття, продовжували використовуватися навіть на початку XX сторіччя. З того часу технічні засоби й методи шпигунства досягли такої досконалості, про яке старі розвідники не могли навіть мріяти.

Були створені різноманітні хитромудрі апарати й пристосування: від пристроїв, що підслуховують, і апаратів для таємної фотозйомки, до зв'язного й шифрувального устаткування, контейнерів, схованок, відмичок і навіть спеціальної зброї. Весь цей арсенал може бути легко захований або замаскований, забезпечуючи тим самим безпеку розвідника. Більше того, навіть після знаходження в схованці протягом декількох років він залишається цілком придатним до роботи.

А оскільки в другій половині XX століття кадровим співробітникам розвідки і їхнім агентам доводиться діяти у винятково складних умовах, для них часом спеціально розробляються унікальні вироби [142].

Вражаючі досягнення науково-технічної революції, особливо створення й поширення ракетно-ядерної зброї масового знищення, змусили по-новому дивитися на корінні проблеми війни й миру, безпеки й міжнародного співробітництва. Розробка високоточних засобів спостереження й контролю буквально революціонізувала збір розвідувальної інформації й верифікацію міжнародних угод. Завдяки можливостям, що з'явилися, вести спостереження за рівнем озброєння супротивника в конкретний період часу, зміною в його розміщенні, внутрішніми комунікаціями, пересуваннями військ практично запобігає раптовий напад або несподівані зміни в розкладі сил супротивника.

У класичному вигляді проблема забезпечення інформаційної безпеки стала усвідомлюватися тільки в другій половині XX в. разом з формуванням концепції «інформаційного суспільства», що прийшла на зміну теоріям «індустріального» і «постіндустріального» суспільства. Саме до того періоду застосування інформаційних технологій стає визначальною умовою перетворення всіх новітніх наукомістких видів діяльності, а інформація перетворилася у вирішальний фактор соціального розвитку. Відбулося

усвідомлення глибокої залежності всіх сфер життєдіяльності суспільства від інформації [140, с.38].

Таким чином, історично інформація завжди мала величезне значення в побуті людей і завжди їй надавалося особливе місце в ньому, багато уваги приділялося розвиткові засобів і методів її захисту. Аналіз процесу розвитку цих засобів і методів захисту інформації дозволяє розділити його на три відносно самостійних періоди. В основі такого розподілу лежить еволюція видів носіїв інформації.

Перший період визначається початком створення осмислених і самостійних засобів і методів захисту інформації й пов'язаний з появою можливості фіксації інформаційних повідомлень на твердих носіях, тобто з винаходом писемності. Разом з незаперечною перевагою збереження й переміщення даних виникла проблема забезпечення збереження в таємниці існуючої вже окремо від джерела конфіденційної інформації. Тому практично одночасно з появою писемності виникли такі методи захисту інформації, як шифрування й приховування [34].

За твердженням ряду фахівців, криптографія за віком – ровесник єгипетських пірамід. У документах древніх цивілізацій – Індії, Єгипту, Месопотамії – є відомості про системи й способи складання шифрованих листів. У древніх релігійних книгах Індії вказується, що сам Будда знав кілька десятків способів письма, серед яких були наявні шифри перестановки (за сучасною класифікацією). Один із найстаріших шифрованих тестів з Месопотамії (XX в. до н.е.) являє собою глиняну табличку, що містить рецепт виготовлення глазурі в гончарному виробництві, у якому ігнорувалися деякі голосні й приголосні й вживалися числа замість імен [34].

Другий період (приблизно із середини XIX століття) характеризується появою технічних засобів обробки інформації й можливістю збереження й передачі повідомлень за допомогою таких носіїв, як електричні сигнали й електромагнітні поля (наприклад, телефон, телеграф, радіо). Виникли проблеми захисту від так званих технічних каналів витоку (побічних

випромінювань, наводок і ін.). З'явилися способи шифрування повідомлень у реальному масштабі часу (у процесі передачі телефонними і телеграфними каналами зв'язку) і т.д. Крім того, це період активного розвитку технічних засобів розвідки, що багаторазово збільшує можливості ведення промислового й державного шпигунства. Величезні, всезростаючі збитки підприємств і фірм сприяли науково-технічному прогресу в створенні нових і вдосконалюванні старих засобів і методів захисту інформації [34].

Найбільш інтенсивний розвиток цих методів припадає на період масової інформатизації суспільства (третій період). Тому історія найбільш інтенсивного розвитку проблеми захисту інформації пов'язана із впровадженням автоматизованих систем обробки інформації й вимірюється періодом у більше ніж 40 років. В 1960-х роках на Заході стала з'являтися велика кількість відкритих публікацій з різних аспектів захисту інформації. Така увага до цієї проблеми, в першу чергу, була викликана всезростаючими фінансовими втратами фірм і державних організацій від злочинів у комп'ютерній сфері [34].

Інформаційна сфера в сучасних умовах є системостворюючою областю життя суспільства. Із цієї причини вона активно впливає на стан політичної, економічної, оборонної сфер, а також інших складових національної безпеки. У політичній сфері все більшу значимість здобуває інформаційно-психологічний вплив з метою формування відносин у суспільстві, його реакції на процеси, що відбуваються.

Усе більше зростає політична роль інформації, що перетворюється в національний політико-стратегічний ресурс і критерій зрілості й розвиненості політичної системи. Сьогодні в науковому світі інформація цілком обґрунтовано вважається політичним капіталом нації. Прогресивна спроможність і політична вага країни, її можливості ефективно впливати на світові події залежать не тільки від матеріально-силових факторів (наприклад, військової й економічної моці), але й від можливості використовувати інтелектуальний потенціал інших країн, поширювати й

впроваджувати свої духовні цінності, а також гальмувати культурну експансію інших народів, трансформувати їхні культурні цінності [154, с.3].

Вперше аналіз безпеки не як фізичного, а як соціального явища був проведений англійським філософом XVII століття Томасом Гоббсом, що вказав на взаємозв'язок і взаємозумовленість безпеки людини, суспільства й безпеки держави. Розглядаючи безпеку як соціальне явище, Т. Гоббс установив її соціальну природу, зв'язав ефективність забезпечення безпеки з опрацьованими суспільством нормами поведінки, що виробляються суспільством [249].

На думку ряду дослідників, цей термін досить вузький, під яким варто розуміти набір апаратних і програмних засобів для забезпечення збереженості, доступності й конфіденційності даних у комп'ютерних мережах. Те, що в 1970-их рр. називалося комп'ютерною безпекою, а в 1980-і – безпекою даних, зараз, як уважають ці дослідники, і є інформаційна безпека. Інформаційною безпекою вони називають «заходи щодо захисту інформації від неавторизованого доступу, руйнування, модифікації, розкриття й затримок у доступі», при цьому використовується термін «критичні дані», під яким розуміють дані, що вимагають захисту через імовірність нанесення (ризику) збитку і його величини в тому випадку, якщо відбудеться випадкове або навмисне розкриття, зміна або руйнування даних. Так, наприклад, українські дослідники М. Галамба й В. Петрик вважають, що «інформаційна безпека держави - це стан її інформаційної захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії й таємного зняття інформації (за допомогою спеціальних технічних засобів), інформаційний тероризм і комп'ютерні злочини не завдають істотної шкоди національним інтересам» [51]. А російські дослідники В. Мельников, С. Клейменов, А. Петраков пропонують під інформаційною безпекою розуміти захищеність інформації й підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть завдати неприпустимої

шкоди суб'єктам інформаційних відносин, у тому числі власникам і користувачам інформації й підтримуючої інфраструктури [с.12].

Відповідно до цієї логіки метою інформаційної безпеки є: убезпечити цінності системи, захистити й гарантувати точність і цілісність інформації й мінімізувати руйнування, які можуть мати місце, якщо інформація буде модифікована або зруйнована. Інформаційна безпека дає гарантію того, що досягаються наступні цілі: конфіденційність критичної інформації, цілісність інформації й пов'язаних з нею процесів (створення, введення, обробки й виводу), доступність інформації, коли вона потрібна, облік всіх процесів, пов'язаних з інформацією [245, с. 23].

Інші дослідники під інформаційною безпекою розуміють «захищеність інформації й підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, здатних завдати збитків власникам або користувачам інформації й підтримуючої інфраструктури», виділяючи тим самим уже два об'єкти захисту – інформацію й інформаційну інфраструктуру [124, с. 12].

Здається, що варто погодитися з думкою російського дослідника А. Сапожникової, яка пропонує позбутися від переважаючого винятково технологічного сприйняття інформаційної безпеки. Комплексне розуміння природи безпеки сучасного суспільства припускає застосування інструментарію не тільки технічного, але й ідеологічного характеру. Ключовим елементом політики інформаційної безпеки може стати культивування цінностей і пріоритетів громадянського суспільства, стратегій соціального партнерства й інформаційної взаємодії [208, с.13].

Останнім часом в Україні й Росії вийшла досить велика кількість публікацій, присвячених питанням забезпечення інформаційної безпеки, однак мають місце неоднозначні судження, висновки й пропозиції з вдосконалення цієї діяльності. Окремі теоретичні положення щодо поняття «інформаційна безпека» мають різні тлумачення.

Як вважають автори відомого російського підручника «Політичні комунікації», під інформаційною безпекою варто розуміти захищеність інформації й підтримуючої її інфраструктури від випадкових або навмисних впливів, здатних завдати збитків як власникам або користувачам інформації, так і відповідним технічним структурам, причому незалежно від того, чи носять ці дії природний, чи штучний характер [187, С.303].

Науковий інтерес викликає визначення А. Алексенцева, відповідно до якого «Інформаційна безпека - стан інформаційного середовища, що забезпечує задоволення інформаційних потреб суб'єктів інформаційних відносин, безпека інформації й захист суб'єктів від негативного інформаційного впливу» На думку А. Алексенцева, інформаційна безпека включає три складові: 1) задоволення інформаційних потреб суб'єктів, які увійшли в інформаційне середовище; 2) забезпечення безпеки інформації; 3) забезпечення захисту суб'єктів інформаційних відносин від негативного інформаційного впливу [3, с.48]. Об'єктами інформаційної безпеки варто вважати: свідомість, психіку людей; інформаційно-технічні системи різного масштабу й призначення. Якщо ж говорити про соціальні об'єкти інформаційної безпеки, то до них можна віднести особистість, колектив, суспільство, державу, світове співтовариство. Суб'єктами інформаційної безпеки є ті органи й структури, які займаються її забезпеченням.

Значення поняття «інформаційна безпека» відбито в статті 17 Конституції України, відповідно до якої «захист суверенітету й територіальної цілісності України, забезпечення її ... інформаційної безпеки є найважливішими функціями держави, справою всього українського народу» [113, с.11].

Відповідно до Концепції Національної програми інформатизації (затвердженої Законом України від 4 лютого 1998 року № 75/ 98-ВР): «інформаційна безпека» - невід'ємна частина політичної, економічної, оборонної й інших складових національної безпеки. Об'єктами інформаційної безпеки є інформаційні ресурси, канали інформаційного обміну й

телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж та інші елементи інформаційної інфраструктури країни».

Як випливає із Закону України «Про основні принципи розвитку інформаційного суспільства в Україні»: «Інформаційна безпека - стан захищеності життєво важливих інтересів людини, суспільства й держави, при якому запобігається нанесення шкоди через: неповноту, несвоєчасність й невірогідність використовуваної інформації; негативного інформаційного впливу; негативних наслідків застосування інформаційних технологій; несанкціонованого поширення, використання й порушення цілісності, конфіденційності й доступності інформації» [82].

На думку В. Гавловського, «Зміст категорії "інформаційна безпека" знаходить розвиток у комплексі нормативно-правових документів щодо використання засобів обчислювальної (комп'ютерної) техніки для обробки й зберігання інформації обмеженого доступу; державних стандартів на документування, супровід, використання, сертифікаційних випробувань комп'ютерних програмних засобів захисту інформації; банку засобів діагностики, локалізації й профілактики комп'ютерних вірусів; нові технології захисту інформації з використанням спектральних методів; високонадійні криптографічні методи захисту інформації й т.п.» [48].

Менш широким і містким за змістом ніж інформаційна безпека є поняття «безпека інформації». Цю категорію можна «розкласти» на дві складові: безпека змістовної частини (змісту) інформації й захищеність інформації від зовнішніх впливів (спроб неправомірного копіювання, поширення, модифікації (зміни змісту) або знищення. Друга складова частина поняття «безпеки інформації» являє собою захист інформації.

Таким чином, змістовна частина категорії «інформаційна безпека» вибудовується в лінію із трьох наукових категорій: інформаційна безпека, безпека інформації й захист інформації. При цьому кожна наступна категорія є складовою частиною попередньої [84].

Зміст діючого інформаційного законодавства України свідчить, що український законодавець значною мірою зв'язує сутність категорії "інформаційна безпека" з категорією "захист інформації в автоматизованих системах". Ця категорія також має визначення на законодавчому рівні, як системостворюючий фактор (об'єкт) правовідносин - правового регулювання суспільних інформаційних відносин, пов'язаних з використанням автоматизованих (комп'ютерних) систем (АСС). У нашій країні системостворюючим фактором цієї області суспільних відносин виступає Закон України "Про захист інформації в автоматизованих системах", затверджений 5 липня 1994 року.

Аналіз наявних визначень поняття «інформаційна безпека» показав, що багато з них мають потребу в конкретизації, додатковому тлумаченні. Вважається, що визначення інформаційної безпеки необхідно формулювати на основі чинного законодавства, зокрема, Доктрини інформаційної безпеки України, що являє собою сукупність офіційних поглядів на мету, завдання, принципи й основні напрямки забезпечення інформаційної безпеки.

Наприклад, відповідно до Доктрини інформаційної безпеки Російської Федерації інформаційна безпека - це стан захищеності її національних інтересів в інформаційній сфері, що визначається сукупністю збалансованих інтересів особистості, суспільства й держави [65].

Особистість, суспільство й держава виступають як об'єкти й суб'єкти інформаційної безпеки на міждержавних, регіональних, національно-державному рівнях. У багатьох країнах існує певна невідповідність між інформаційною безпекою держави й правами особистості на свободу слова в ньому. Це очевидно, тому що інтереси особистості й інтереси держави далеко не завжди схожі.

Інформаційна безпека суспільства, держави характеризується ступенем їхньої захищеності й, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості й т.д.) стосовно небезпечних, дестабілізуючих,

інструктивних, що ущемлюють інтереси країни інформаційним впливам на рівні як впровадження, так і витягу інформації. Інформаційна безпека визначається здатністю нейтралізувати такі впливи.

Інтереси суспільства в інформаційній сфері полягають у забезпеченні інтересів особистості в цій сфері, зміцненні демократії, створенні правової соціальної держави, досягненні й підтримці громадянської згоди, у духовному відновленні України.

Інформаційна безпека особистості характеризується захищеністю психіки й свідомості від небезпечних інформаційних впливів: маніпулювання, дезінформування, спонукання до самогубства, образ і т.п. Необхідно відзначити, що інформаційні впливи небезпечні (або корисні) не стільки самі по собі, скільки тим, що “запускають” потужні матеріально-енергетичні процеси, керують ними. Суть впливу інформації саме й полягає в її здатності “запускати” і контролювати матеріально-енергетичні процеси, параметри яких на багато порядків вищі самої інформації [173].

У науковій літературі пропонується досить багато трактувань поняття «інформаційне забезпечення національної безпеки». Російський дослідник І. Гальцев виділяє два напрямки: технологічне й соціокультурне. Технологічне - інформаційне забезпечення безпеки - це сукупність апаратних і програмних засобів, що забезпечують доступ, конфіденційність, збереження інформації в сучасних інформаційних (комп'ютерних) мережах. Мова йде про специфічний соціотехнічний феномен, що в 1970-і роки іменувався «комп'ютерною безпекою», в 1980-і роки - «безпекою даних», а сьогодні одержав назву «інформаційної безпеки» або «інформаційного забезпечення безпеки». Властиво «інформаційним забезпеченням безпеки» називають заходи щодо захисту інформації від неавторизованого доступу, руйнування, модифікації, розкриття й затримок у доступі, в результаті чого її метою стає забезпечення безпеки функціонування інформаційних систем, а головним об'єктом захисту - сама інформація, також поряд з інформацією - другий об'єкт захисту - інформаційна інфраструктура [52, с.9].

Висновки до розділу 1

Інформаційні потоки пронизують всі сфери життя людства й відіграють все більш зростаючу роль в умовах глобалізації світового співтовариства. Розвиток і поширення інформаційно-комунікаційних технологій, їхнє проникнення практично в усі сфери життєдіяльності, з одного боку, є важливим чинником світової інтеграції, соціального розвитку й економічного росту; з іншого боку, будучи найсильнішим каталізатором інформаційного обміну, ці технології несуть у собі також безліч як видимих, так і прихованих загроз. Надзвичайну значимість у зв'язку із цим набувають питання забезпечення інформаційної безпеки.

Таким чином, інформаційна безпека в сучасних умовах здобуває все більшу актуальність і значимість, є одним із пріоритетних напрямків забезпечення національної безпеки України, а також міжнародної безпеки, що вимагає теоретичного осмислення основних положень інформаційної безпеки для вдосконалювання правової бази й політичної практики.

Чим вища активність громадян, організацій або держав у кіберпросторі, тим гостріше перед суспільством встають проблеми забезпечення своєї інформаційної безпеки. І сьогодні є всі підстави думати, що національна безпека країн буде залежати від забезпечення інформаційної безпеки. В міру ж інтенсифікації технічного прогресу й посилення «електронного співробітництва» держав ця залежність буде постійно зростати.

До сьогоднішнього дня серед учених, що досліджують проблеми безпеки, не вироблено загального підходу до визначення основного понятійного апарата із зазначеної проблематики.

Дослідники виділяють два напрямки у вивченні проблем інформаційної безпеки. Відповідно до одного з них поняття можна визначити як безпеку самих інформаційних ресурсів – інформації й технологій. До забезпечення

інформаційної безпеки в цьому випадку відносять забезпечення стабільного функціонування інформаційної інфраструктури, захист від несанкціонованого доступу, шкідливих програм та ін. Тобто, даний аспект в основному торкається технічних проблем, обмежується питаннями захисту інформаційного простору від навмисного або випадкового впливу на інформацію або інформаційну інфраструктуру у тих сферах безпеки, в яких вони використовуються.

Другий напрямок включає, в першу чергу, такі питання: значення інформаційних ресурсів у забезпеченні безпеки в цілому, ефективність застосування інформаційних технологій та ін. Інформаційні технології знайшли широке застосування практично в усіх аспектах національної безпеки, з чим зв'язана критичність і актуальність питань захисту інформаційних ресурсів. Вплив на інформацію або інформаційну інфраструктуру має катастрофічні наслідки для тої сфери, у якій вони застосовуються (тому існує безліч прикладів, розглянутих у дослідженні). Таким чином, до другого аспекту варто віднести питання застосування цих ресурсів для забезпечення різних аспектів національної безпеки.

Безумовно, що обидва ці напрямки важливі й тісно взаємозв’язані між собою. Адже інформаційні ресурси відіграють найважливішу роль у розвитку особистості, суспільства, бізнесу, держави й міжнародних відносин у цілому, а інформаційні технології знайшли широке застосування у військовій, економічній, соціальній, енергетичній та інших сферах безпеки.

У результаті дослідження дисертант доходить висновку, що при побудові інформаційного суспільства зростає число суб'єктів, все більша кількість членів суспільства здійснюють інформаційно-правову діяльність. Особливості цих правовідносин визначаються змістом інформаційної безпеки як станом захищеності збалансованих інтересів особистості, суспільства й держави в інформаційній сфері від внутрішніх і зовнішніх небезпек.

Національна безпека України істотно залежить від забезпечення інформаційної безпеки, причому в ході технічного прогресу ця залежність буде ще більше зростати. Це змушує з особливою увагою поставитися до загроз національної безпеки, що здійснюються в інформаційній сфері, глобальних проблем забезпечення безпеки інформації. Про інформаційно-технічні й соціально-політичні загрози для особистості, суспільства, держави - у наступному розділі.

РОЗДІЛ 2
БЕЗПЕКА В УМОВАХ ГЛОБАЛЬНОЇ ІНФОРМАТИЗАЦІЇ: НОВІ ВИКЛИКИ Й НОВІ МОЖЛИВОСТІ

Розвиток і поширення інформаційно-комунікаційних технологій, їхнє проникнення практично в усі сфери життєдіяльності, з одного боку, є важливим чинником світової інтеграції, соціального розвитку й економічного зростання. З іншого боку, будучи найсильнішим каталізатором інформаційного обміну, ці технології несуть у собі також безліч як явних, так і прихованих загроз.

Даний розділ присвячений розгляду можливих інформаційно-технічних і соціально-політичних загроз для особистості, суспільства й держави. Окремий підрозділ присвячений Інтернету.

2.1. Інформаційно-технічні й соціально-політичні загрози для особистості, суспільства, держави

Доводиться визнати, що чим вищі технологічні можливості держави й чим більше число його взаємодій з іншими групами (включаючи внутрішні групи) або державами, тим більше держава вразлива в інформаційній війні. Ця вразливість буде зростати в міру збільшення розмірів мереж або числа й обсягу транзакцій.

Після 11 вересня світ знайшов розуміння того, що найбільш уразливою крапкою безпеки держави стає національна інформаційна інфраструктура (НДІ). З'явився спектр нових інформаційних загроз, здійснюваних за допомогою спеціально підібраної системи інформації й спрямованих на дестабілізацію суспільства. У політичній сфері з'являються нові можливості для маніпулювання суспільною свідомістю, політичними установками й орієнтаціями різних соціальних груп. Технологічні досягнення, їхнє широке

проникнення й фактична доступність ведуть до формування особливого світовідчуття. Віртуальна реальність істотно трансформує сучасну політичну дійсність [1].

Як показує практика, у єдиному інформаційному просторі сучасні держави не можуть діяти як абсолютно відкриті структури. Надмірна інформаційна відкритість може завдати шкоди інтересам держави й суспільства, а в деяких випадках поставити під сумнів існування правлячого режиму. Все це змушує державу піклуватися про інформаційний захист своїх інтересів, вибірково підходити до оцінки транспарентності своєї політики, постійно знижувати вразливість своїх об'єктів. Причому політика інформаційної безпеки поширюється не тільки на взаємодію держави із зарубіжними партнерами або зі ЗМІ, але й на відносини з окремими корпораціями й громадянами.

Чималу роль у зміцненні інформаційної безпеки відіграють і інформаційна залежність окремих державних інститутів від закордонних технологій, нові типи злочинів у кіберпросторі, небезпека терористичних акцій та інші аналогічні фактори.

Як відзначає російський дослідник І. Юрченко: «В умовах відкритого глобального суспільства актуалізувалося завдання забезпечення інформаційної безпеки в поліетнічному просторі, де простежуються елементи інформаційного хаосу, інформаційного тероризму, розпалення ворожнечі з використанням механізмів «м'якої (інформаційної) війни» і сугестивних технологій. Найважливішою тенденцією розвитку політико-інформаційного простору сучасного суспільства є конфліктний та інтеграційний потенціал інформаційних ресурсів» [256, с.19].

Тому не випадково, практично у всіх розвинених країнах нині створені або створюються спеціальні державні організації з її захисту [221, с.25].

Також варто враховувати ще один не менш важливий момент: демократії не є менш вразливими, ніж тоталітарні режими, хоча демократичні соціальні системи, такі як групи, можуть бути дещо більш

стійкими до виведення з ладу. Але апарат управління економікою вразливий. Банки, фінанси, торгівля, подорожі й управління повітряним рухом стають усе більше залежними від інформаційної технології [251].

Більше того, розвиток технологій, що підвищують інформаційну й ідеологічну вразливість політичної системи, викликає відповідну реакцію держав і транснаціональних структур, які всіма доступними методами - і юридичними, і апаратно-програмними - намагаються підсилити контроль за цими технологіями. У підсумку поступово вибудовується своєрідна система «загальної піднаглядності», керування свідомістю й поведінкою як конкретного індивіда, так і соціальних груп і цілих націй, що підготовляє фундамент для активізації в найближчі десятиліття неототалітарних політичних процесів. Комп'ютерні технології відкривають нові можливості для контролю над суспільством. Жодна зі спроб створити діючу систему захисту конфіденційності електронної пошти або повідомлень мобільного телефонного зв'язку поки не увінчалася успіхом [141, с.139].

Як витікає із Закону України «Про принципи розвитку інформаційного суспільства в Україні», одним із шляхів рішення проблеми інформаційної безпеки є підвищення рівня координації діяльності державних органів з виявлення, оцінки й прогнозування загроз інформаційної безпеки, попередження таких загроз і забезпечення ліквідації їхніх наслідків, здійснення міжнародного співробітництва із цих питань [82]. Розглянемо, які ж є інформаційні загрози?

Сьогодні можна виділити наступні найбільш істотні групи інформаційно-технічних небезпек, обумовлених досягненнями науково-технічного прогресу.

Перша група пов'язана з бурхливим розвитком нового класу зброї - інформаційного, котре здатне ефективно впливати й на психіку, свідомість людей, і на інформаційно-технічну інфраструктуру суспільства й армії. На сьогоднішній день створено багато нових засобів впливу на психіку людей, управління їхньою поведінкою. Правда, за даними закордонних джерел,

стійких і прогнозованих способів керівництва колективною поведінкою людей поки не знайдено, але такі дослідження ведуться. У пресі періодично з'являється інформація про американську програму “ Мк-Ультра”, а також про аналогічні програми у Франції, Японії й інших країнах. Досягнення в цій області такі, що вже зараз можна говорити про ефективність зомбування (програмування поведінки, діяльності) окремих людей. З цією метою створені й використовуються не тільки фармакологічні засоби, але й психотропні генератори.

Можливості засобів радіоелектронної протидії достатньо відомі. В останні роки в їхньому розвитку відбуваються революційні зміни. Головний напрямок прогресу в електроніці - комп'ютеризація. Тому особливо швидко й з разючими успіхами розробляються методи впливу на комп'ютерні системи. Наприкінці 1990 р. за замовленням ДАРПА (управління НІОКР Пентагона) була підготовлена доповідь “Комп'ютери в небезпеці” і зроблено висновок, що США стоять на порозі катастрофи в комп'ютерних мережах, а також рекомендовано посилити заходи інформаційної безпеки. І ЦРУ, і АНБ досліджують можливості зараження інформаційно-технічних систем інших країн комп'ютерними вірусами, пастками, логічними бомбами й т.д. Для боротьби з подібними діями з боку інших держав у США створена служба “Комп’ютерно-вірусні контрзаходи” [173].

Цілком очевидно, що відповідні служби розвинених в області інформатики держав ведуть підготовку до “комп'ютерної війни”, розробляють і апробують способи, прийоми впливу на комп'ютерні системи. Відомості про це з'являються у відкритій пресі. Захист інформаційної безпеки включає як технічні питання, так і організаційно-правові. І якщо технічна складова інформаційної безпеки змінюється з удосконалюванням технологій, то організаційно-правова повинна забезпечувати стан інформаційної безпеки.

У США створена найбільш завершена система взаємодії державних органів із забезпечення інформаційної безпеки. Питання інформаційної

безпеки й захисту особистої інформації, насамперед, вирішуються на рівні агентств, які розробляють відповідні програми. Вони звітують перед директором адміністративного й бюджетного керівництва, а той, у свою чергу, перед комітетами палат Конгресу. Директор керує федеральним центром інцидентів у сфері інформаційної безпеки. Центр збирає й вивчає відомості про події, що можуть загрожувати інформаційній безпеці, попереджає про загрозу в цій сфері, а при необхідності - надає технічну допомогу агентствам. Оскільки така система була остаточно закріплена вище згадуваним законом про електронну державу 2002 р., говорити про її ефективність зараз важко. Але стурбовані можливістю "Електронного 11 вересня" американці продовжують удосконалювати створену систему. З 2003 р. вони перейшли на систему державного контролю над дотриманням інформаційної безпеки в державних структурах і бізнесі. Останні повинні надавати відповідні матеріали про інформаційної безпеки, що застосовуються. У США існує Центр комп'ютерної безпеки (Пентагон), створений ще в 1981 р., є спеціально підібрані урядові групи експертів, які стежать за рівнем захищеності зовсім секретних комп'ютерних систем. Нема сумніву, що ефективність комп'ютерного протиборства буде надзвичайно високою. Про це, наприклад, свідчить факт неможливості застосування Іраком проти багатонаціональних сил систем ПВО, закуплених у Франції. Їхнє програмне забезпечення містило логічні бомби, які були активізовані з початком бойових дій. Використанням такої бомби або вірусу, очевидно, можна буде досягати тих же результатів, що й звичайним бомбардуванням органу державного керівництва, пункту (центру) бойового керування. Тому комп'ютерні системи державного управління й військового призначення (у першу чергу всі скільки-небудь важливі системи й мережі) будуть намагатися “замінувати” логічними бомбами, “заразити” вірусами, що чекають своєї години. З'явиться й інформаційний тероризм. До всього цього треба спеціально готуватися й передбачати контрзаходи [173].

В останні роки на розробку методів і засобів інформаційної безпеки в США витрачається близько 5 млрд. доларів у рік. У нашій країні подібні роботи ще тільки розгортається. Адже в основному програмне забезпечення в країні або запозичене, або побудоване із включенням запозичених модулів. Близько 70% програмного забезпечення, яке продається у світі, створене в США. Крім того, у країну надходить маса інформаційної техніки, виготовленої за рубежем. Вона часто містить спеціальні компоненти знімання й передачі інформації.

Друга група інформаційно-технічних небезпек для особистості, суспільства, держави - це новий клас соціальних злочинів, заснованих на використанні сучасної інформаційної технології (махінації з електронними грошима, комп'ютерне хуліганство й ін.). На думку фахівців, комп'ютер стає найбільш багатообіцяючим знаряддям злочину. У розвинених країнах практично всі грошові операції проводяться через комп'ютерні системи й мережі. Широке поширення одержали кредитні картки, що заміняють звичайні гроші. Їхня підробка, злодійство за допомогою ЕОМ прийняли характер справжнього нещастя в США, Італії, інших країнах. Компанії, особливо банки, прагнуть приховати факти комп'ютерного злодійства, оскільки побоюються падіння довіри вкладників, акціонерів, партнерів. Тому в офіційній статистиці масштаби втрат часто не реєструються. Та й жертви часто не підозрюють, що їх обікрали. Експерти думають, що в США за допомогою ЕОМ з банків викрадають учетверо більше, ніж при збройних пограбуваннях. За останні 10 років щорічні втрати зросли більш ніж в 20 разів і становлять десятки мільярдів доларів.

Швидкими темпами розвивається промислове шпигунство й контршпіонаж. Утворено спеціальні служби, що співпрацюють у цій області з державною розвідкою, створено навіть “Американське співтовариство з промислової безпеки”. Існує й розвивається напрямок інформатики, що обслуговує цю діяльність, що розробляє законні й незаконні методи й засоби одержання інформації про секрети конкурентів. Комп'ютерна боротьба стала

звичайним явищем у світі ринкових відносин, у тому числі й у зовнішній торгівлі. Оскільки інформаційно-обчислювальні мережі розвинених держав об’єднуються, можливості впровадження логічних бомб розширюються. Їх закладають у програмне забезпечення ще при розробці як засіб боротьби з незаконним копіюванням. Комп'ютерна боротьба доповнила електронне шпигунство, зробила його активним. Зрозуміло, що вона розгортається й на міжнародній економічній арені. З'явилися нові злочини проти особистості. Так, у комп'ютерних відеофільмах зображення реально існуючих акторів виконують за бажанням програміста те, що він вважає потрібним. Однак методів і засобів розслідування злочинів такого роду поки нема, та й законодавство не відповідає вимогам дня. Юристам доводиться ламати голову над новою проблемою - класифікацією незаконного підключення до електронного банку даних [173].

Третя група інформаційно-технічних небезпек - електронний контроль за життям, настроями, планами громадян, політичних організацій. Правлячі кола не тільки використовують підслуховування телефонних розмов, але й здійснюють контроль за перепискою, використовують детектори неправди, тотальний комп'ютерний контроль, кібернагляд за населенням. Особливо щільний “електронний ковпак” над людьми встановлений, на думку американців, у США. Кількість комп'ютерних банків даних про громадян, компанії, партії збільшується в Сполучених Штатах дуже швидко. Вони використовуються для вирішення різних питань: кадрових, адміністративних, охорони порядку й судочинства, соціального забезпечення. Правда, картотеки в США велися й раніше. Сучасна ж інформація привела до якісного стрибка в можливостях “висвітити” особисте життя будь-якої людини. Справа в тому, що комп'ютерні мережі дозволяють накопичувати, зберігати й використовувати величезну кількість даних про здоров'я, соціальну активність, політичні думки, зв'язки, фінансові справи американців. Швидкий і зручний доступ до всієї інформації про конкретну людину, її централізована обробка, систематизація й узагальнення дають у

руки владі потужну зброю з метою припинення небажаних дій з боку цієї людини, причому збирати інформацію із всіх наявних досьє можна швидко й практично непомітно для суспільства.

Кібернагляд застосовується й у політичній боротьбі. “Уотер-Гейт” яскраво це продемонстрував. Подібний інцидент відбувся й у Канаді. В умовах низької політичної культури населення інформатизація на словах може подаватися як засіб демократизації, розширення свободи і т.п., а насправді використовуватися для зловживання владою, таємного порушення конституційних свобод, поступової еволюції демократичної держави в тоталітарну [173].

Четверта група інформаційних небезпек - використання нової інформаційної технології в політичних цілях. Спроби впровадження інформаційного тоталітаризму (експансіонізму, колоніалізму) цілком зрозумілі. Адже ріст впливу засобів масової інформації (ЗМІ) на хід і зміст політичних процесів, функціонування механізму влади - одна з домінуючих тенденцій сучасного суспільного розвитку. Боротьба за контроль над новими засобами масової інформації й інформаційною структурою, їх використання для обліку й обробки суспільної думки стали центральною проблемою у внутрішньополітичному житті держав, особливо під час виборчих кампаній. Наприклад, комп'ютер комітету Республіканської партії США не тільки збирав і обробляв інформацію, але й безпосередньо впливав на виборців. Через автоматизовану телефонну систему цей комп'ютер зв'язався з 25 млн. абонентів у різних штатах, закликаючи їх голосувати за певні кандидатури. Питання впливу інформації на політичну владу, її розподіл є, мабуть, центральним у західному політичному житті. Можна стверджувати, що за рахунок концентрації інформації, більш широких можливостей її використання відбувається посилення виконавчої влади, влади державного апарату в порівнянні з владою виборних представників. Використання комп'ютерних мереж розширює можливості апарату в маніпулюванні масами. У багатьох державах, що розвиваються, індустріально розвинені

країни захопили ключові позиції в економічній і науково-технічній інформатиці. Передача інформаційної технології неминуче веде до передачі відповідних адміністративних процедур, форм обліку, методів керівництва й контролю, до необхідності існування інституту радників. Все це поступово перетворює передану інформаційну технологію в політичний та ідеологічний фактор, що робить тиск на економіку країн, які розвиваються. У хід ідуть і такі засоби, як логічні бомби в програмному забезпеченні. Тому вимога встановлення "нового інформаційного порядку" означає рівноправність і незалежність у всьому міжнародному інформаційному обміні, тобто в обміні економічною, науково-технічною, політичною, культурною й пропагандистською (ідеологічною) інформацією, а не тільки останньою, як це іноді подається [173].

Що стосується соціально-політичних загроз, що мають інформаційну природу, то їх можна підрозділити на системні й периферійні загрози. Загрози першого типу носять цілеспрямований, структурований і централізований характер і є наслідком упорядкованих дій владних і навколоелітних структур, наприклад, скоординованої інформаційно-психологічної атаки на конкретну політичну систему або її сегмент із боку конкуруючої держави (цивілізації, транснаціональної структури) або деструктивних акцій внутрішньодержавних кваліеліт, проведених відповідними методами. Разом з тим варто враховувати, що в сучасних умовах реальний збиток тій або іншій країні можуть нанести навіть збір і комп'ютеризований експертний аналіз відкритої інформації.

Не менш серйозну небезпеку представляють і загрози другого типу, які пов'язані з діяльністю широкого спектра позасистемних сил - від міжнародних терористичних організацій до всіляких хакерських груп. Неструктурованість, дифузність і непрогнозоване виникнення периферійних інформаційних загроз украй утруднює вироблення діючої стратегії захисту від них.

Аналіз наукової літератури, присвяченої інформаційному тероризму, показує, що обговорення проблем протидії військово-політичній загрозі, яка проявляється у використанні інформаційно-комунікаційних технологій для досягнення політичних цілей у наш час має пріоритетне значення. Ймовірно, це можна пояснити тим, що, з одного боку, питання протидії загрозам кіберзлочинності, включаючи кібертероризм, уже досить широко обговорюються на різних міжнародних форумах, а з іншого боку - інформаційно-комунікаційні технології поступово трансформуються в принципово новий і досить потужний засіб руйнуючого впливу. Він може бути спрямований на об'єкти виробничої й економічної сфер, соціальної інфраструктури, державного керівництва.

Ці загрози можуть проявлятися у вигляді порушення стійкості функціонування складових інформаційної інфраструктури, несанкціонованого доступу до інформації, що охороняється законом, економічно й соціально значимих структур з боку злочинних, у тому числі терористичних, організацій. Об'єктами реалізації таких загроз можуть виступати інформаційні системи енергетичної, транспортної й деяких інших інфраструктур. Потенціал так званої " кіберзлочинності" досить високий. Тенденція росту цього виду злочинів спостерігається в багатьох країнах. Загрози в даній області можуть проявлятися у вигляді спроб здійснення шахрайських операцій з використанням глобальних або вітчизняних інформаційно-телекомунікаційних систем, відмивання фінансових засобів, отриманих протиправним шляхом, одержання неправомірного доступу до фінансової, банківської та іншої інформації, що може бути використана з корисливою метою. Загрози також можуть проявлятися й у вигляді нанесення збитків інформаційній інфраструктурі з метою змушення політичного керівництва країни до прийняття певних, вигідних терористам рішень.

Це перетворює розглянуті технології в засіб боротьби, що здатний сприяти рішенню завдань міждержавного протиборства на тактичному, оперативному й стратегічному рівнях.

У цій якості інформаційно-комунікаційні технології набувають якості зброї, вражаючі властивості якої будуть зростати в міру подальшого вдосконалювання ІКТ, розширення їхнього повсюдного використання, розвитку інформаційної інфраструктури суспільства й держави, інформатизації озброєння й військової техніки [234].

Таким чином, для продовження інтенсивного розвитку інформаційного суспільства необхідно забезпечити ефективну протидію загрозам використання сучасних інформаційних технологій. І хоча домогтися рішучого перелому в протидії загрозі інформаційного тероризму поки ще не вдалося, певні позитивні тенденції в цій області все-таки є.

Не секрет, що сучасні інформаційні технології інтенсивно використовуються для підготовки, планування й здійснення терористичних актів, вербування нових членів терористичних організацій, пропаганди екстремістської, у тому числі, терористичної ідеології. Так, останнім часом інформаційний простір усе активніше використовується терористами для координації своєї діяльності, організації зв'язку й залучення фінансування. Усвідомлюючи потенціал, яким володіють нові інформаційні технології, ряд міжнародних терористичних організацій останнім часом намагаються встановлювати зв'язки із глобальними мережними співтовариствами хакерів. Терористами ведеться робота з можливого їхнього залучення в майбутньому для планування й проведення терористичних актів. Доведено, що терористи Аль-Каїди координували свою діяльність саме шляхом використання глобальних мереж. Установлення робочих контактів між терористами й хакерами загрожує різким стрибком у технологічному розвитку терористів, що може привести до того, що терористи набудуть здатність проведення масштабних терактів в інформаційній сфері вже в найближчі роки [61].

Мішенями терористів стають комп'ютери й створені на їхній основі спеціалізовані системи - банківські, біржові, архівні, дослідницькі, управлінські, а також засоби комунікації - від супутників безпосереднього телемовлення й зв'язку до радіотелефонів і пейджерів.

Новою тенденцією в еволюції тероризму став кібертероризм. Його політична мета - нагнітання суспільної напруженості, страху, дестабілізації обстановки, дискредитації офіційної влади. Фактичною метою його атак виступають комп'ютерні системи управління критичною інфраструктурою, тобто транспортом, атомними електростанціями, водопостачанням і енергетикою. Кібертероризм - це, насамперед, вид політичного тероризму, завдання якого завжди зводиться до спроби змінити суспільство за допомогою сили.

На думку І. Додіна, під кібертероризмом доцільно розуміти дії окремих осіб або їхніх груп по дезорганізації роботи автоматизованих інформаційних систем і мереж зв'язку, що створюють небезпеку загибелі людей, заподіяння значного майнового збитку або наступу інших суспільно небезпечних наслідків.

До кібертероризму можна віднести також деструктивні дії стосовно інформаційних систем, що створюють умови для здійснення актів тероризму [63].

Саме дана форма тероризму викликає сьогодні особливу заклопотаність в експертів у зв'язку з високою вразливістю існуючих систем управління. Сучасні злочинні кіберугрупування працюють за принципами, що подібні до звичайних реальних компаній. Завдяки значним прибуткам, вони швидко розвиваються й ростуть. Індивідуальне хакерство й невеликі групи хакерів відходять у минуле. Сьогодні найбільшою небезпекою є ієрархічно організовані об'єднання кіберзлочинців, де кожний учасник має свою роль і систему винагород. Спрямовані атаки проти фінансових установ, підприємств і урядів у поєднанні із досконалим управлінням краденими

даними роблять цей «бізнес» дуже успішним, а кожну організацію, що використовує Інтернет, - вразливою [105].

Зовсім недавно в розпал передвиборної кампанії, що почалася в країні, жертвою кіберзлочинців став Президент Франції Ніколя Саркозі. Хакери зламали сторінку французького лідера в соціальній мережі Facebook і "від його імені" заявили, що глава держави на майбутніх в 2012 році президентських виборах не буде балотуватися на другий термін. «Дорогі співвітчизники, у силу виняткових обставин, про які відомо всій країні, я прийняв рішення не висувати свою кандидатуру для переобрання на пост президента в 2012 році», - говорилося в повідомленні інтернет-зломників.

Разом із заявою на сторінці було розміщене запрошення в тільки що створену групу Facebook. Її учасникам пропонувалося взяти участь (із нагоди відходу Саркозі у відставку) у фуршеті, що нібито повинен пройти 6 травня 2012 року [89].

До загрози кібертероризму тісно примикає кібервійна. Однак якщо кібертероризм уже став загрозою сучасності, то кібервійна - це проблема майбутнього. Поняття кібервійни пов'язане з військовою галуззю. Воно розвиває й уточнює природу військового конфлікту в епоху інформатизації.

Ще однієї наростаючою за актуалізацією проблемою, прямо пов'язаною із процесом інформатизації суспільства, є можливість за допомогою Інтернету керувати протестною поведінкою активних користувачів мережі. Причому дана діяльність абсолютно не підконтрольна державним органам.

До першорядних, на думку І. Додіна, загроз відносяться інформаційні війни (інформаційно-психологічні війни), як крайні форми інформаційного протиборства, з використанням нових ІКТ і особливо Інтернету. Це обумовлюється тим, що вони є фактично постійними в часі й масштабними за охопленням аудиторії. Крім того, регулювання їхнього протікання в Інтернеті вкрай проблематичне [63, с.180].

Гостроту проблеми підтверджує те, як на неї реагує міжнародне співтовариство. Відомо, що створення інформаційного суспільства стало розглядатися як першорядне завдання Ради Європи з кінця 1993 р., коли була випущена Біла книга «Економічне зростання, конкуренція, зайнятість - завдання й шляхи їхнього рішення на порозі XXI століття» [38, с.6]. У червні 1994 року Радою Європи був прийнятий план дій «Шлях Європи в інформаційне суспільство», що передбачає ряд механізмів, які дозволяють створити умови для вільного доступу до інформації й одночасно оберігають особистість і суспільство.

Таким чином, одним із джерел загроз інтересам суспільства в інформаційній сфері є безперервне ускладнення інформаційних і телекомунікаційних систем, мереж зв'язку, інформаційної складової критично важливих об'єктів інфраструктури життя суспільства.

До зовнішніх джерел загроз відносяться: недружня політика іноземної держави в сфері глобального інформаційного моніторингу, поширення інформації й нових інформаційних технологій; діяльність іноземних розвідувальних і спеціальних служб; діяльність іноземних політичних і економічних структур, спрямована проти інтересів України; злочинні дії міжнародних груп, формувань і окремих осіб; стихійні лиха й катастрофи.

Внутрішніми джерелами загроз є: протизаконна діяльність політичних і економічних структур в області формування, поширення й використання інформації; неправомірні дії державних структур, що приводять до порушення законних прав громадян і організацій в інформаційній сфері; порушення встановлених регламентом збору, обробки й передачі інформації; навмисні дії й ненавмисні помилки персоналу інформаційних систем; відмови технічних засобів і збої програмного забезпечення в інформаційних і телекомунікаційних системах [34].

До основних проблем, які несуть ризики й загрози національній безпеці України, експерти відносять такі явища, що властиві багатьом державам, як: боротьба за енергоресурси, техногенні катастрофи, міжнаціональні й

міжконфесійні конфлікти, тероризм, наркоторгівля, організована злочинність і корупція, нелегальна міграція, торгівля людьми, демографічні проблеми й т.п.. Особливу небезпеку представляють тенденції консолідації національних і міжнародних злочинних угруповань, об'єднання кримінальної злочинності з націоналістичними й екстремістськими угрупуваннями.

Більш конкретно: проблема хронічного економічного відставання України, що передається багато років у спадщину від однієї влади до іншої, неконкурентоспроможності, згортання ринків. Невизначеність зовнішньополітичного курсу, незважаючи на підтвердження позаблокового статусу. Тобто, статус заявили, але конкретним змістом не наповнили. Відсутність системності й механізмів соціальної амортизації у внутрішніх економічних реформах, що приводить до росту соціальної напруженості й протестних настроїв. Необхідність проведення адміністративної реформи, оскільки модель керівництва, що зберігається, не тільки гальмує розвиток країни, але й є джерелом корупції, яку президент недавно назвав однієї з головних загроз національній безпеці. Крім того, проблеми в гуманітарній сфері, що роз'єднують суспільство, несподіване зростання популярності націоналістичних партій, невизначеність із датою чергових парламентських виборів, від чого залежить рівень політичної стабільності в країні [146].

Основними факторами, що створюють загрозу безпеки в інформаційній сфері, є поширення недостовірної або навмисне перекрученої інформації, спрямоване на руйнування громадської згоди, духовних і моральних цінностей суспільства, а також на порушення національної релігійної ворожнечі, соціальної ворожнечі.

Д. Кафтанчиков робить висновок про амбівалентний характер впливу процесу інформатизації на стан різних аспектів національної безпеки. З одного боку, поширення інформаційних технологій і телекомунікаційних систем надає в розпорядження органів державного управління більш ефективні засоби, технології й прийоми забезпечення національних інтересів. Разом з тим інформатизація висуває підвищені вимоги до функціонування

системи забезпечення національної безпеки: по-перше, у даній сфері життєдіяльності можуть виникати протиріччя й формуватися інтереси, протилежні інтересам особистості, суспільства й держави; по-друге, інформаційна сфера, виконуючи комунікативну функцію, здатна в ситуації політичної нестабільності виступати ретранслятором загроз і небезпек, що формуються в інших сферах соціального буття [99, с.28].

Реальні й потенційні загрози інформаційної безпеки України відображені в Доктрині інформаційної безпеки України, затвердженої Указом Президента України 8 липня 2009 р. Загрози інформаційної безпеки, відповідно до Доктрини, підрозділяються на кілька класів:

На сучасному етапі основними реальними й потенційними загрозами інформаційної безпеки України є:

1) у зовнішньополітичній сфері:

поширення у світовому інформаційному просторі перекрученої, недостовірної й упередженої інформації, що завдає шкоди національним інтересам України;

прояв комп'ютерної злочинності, комп'ютерного тероризму, які загрожують постійному й безпечному функціонуванню національних інформаційно-телекомунікаційних систем;

зовнішні негативні інформаційні впливи на суспільну свідомість через засоби масової інформації, а також мережа Інтернет;

2) у сфері державної безпеки:

негативні інформаційні впливи, спрямовані на підрив конституційного порядку, суверенітету, територіальної цілісності й недоторканності кордонів України;

використання засобів масової інформації, а також мережі Інтернет для пропаганди сепаратизму за етнічною, мовною, релігійною та іншими ознаками;

несанкціонований доступ до інформаційних ресурсів органів державної влади;

розголошення інформації, що представляє державну й іншу передбачену законодавством таємницю, а також конфіденційної інформації, що є власністю держави;

3) у військовій сфері:

порушення встановленого регламенту збору, обробки, зберігання й передачі інформації з обмеженим доступом в органах військового керівництва й на підприємствах оборонно-промислового комплексу України;

несанкціонований доступ до інформаційних ресурсів, незаконний збір і використання інформації з питань оборони;

реалізація програмно-математичних заходів з метою порушення функціонування інформаційних систем у сфері оборони України;

перехоплення інформації в телекомунікаційних мережах, радіоелектронне глушіння засобів зв'язку й керування;

інформаційно-психологічний вплив на населення України, у тому числі на особовий склад військових формувань, з метою ослаблення їхньої готовності до оборони держави та погіршення іміджу військової служби;

4) у внутрішньополітичній сфері:

недостатня розвиненість інститутів цивільного суспільства, недосконаліть партійно-політичної системи, непрозорість політичної й суспільної діяльності, що створює передумови для обмеження свободи слова, маніпулювання суспільною свідомістю;

негативні інформаційні впливи, у тому числі із застосуванням спеціальних засобів, на індивідуальну й суспільну свідомість;

поширення суб'єктами інформаційної діяльності перекрученої, недостовірної й упередженої інформації;

5) в економічній сфері:

відставання вітчизняних наукомістких і високотехнологічних виробництв, особливо в сфері телекомунікаційних засобів і технологій;

недостатній рівень інформатизації економічної сфери, зокрема кредитно-фінансової системи, промисловості, сільського господарства, сфери державних закупівель;

несанкціонований доступ, порушення встановленого порядку роботи з інформаційними ресурсами в галузях національної економіки, перекручування інформації в таких ресурсах;

використання неліцензованого й несертифікованого програмного забезпечення, засобів і комплексів обробки інформації;

недостатній рівень розвитку національної інформаційної інфраструктури;

6) у соціальній і гуманітарній сферах:

відставання України від розвинених держав за рівнем інформатизації соціальної й гуманітарної сфер, насамперед, освіти, охорони здоров'я, соціального забезпечення, культури;

недотримання прав людини й громадянина на одержання інформації, необхідної для захисту їхніх соціально-економічних прав;

поширення в засобах масової інформації невластивих українській культурній традиції цінностей і способу життя, культу насильства, жорстокості, порнографії, зневажливого відношення до людської й національної гідності;

тенденція до витіснення з інформаційного простору й молодіжної культури українських художніх творів, народних традицій і форм дозвілля;

послаблення суспільно-політичної, міжетнічної й міжконфесійної єдності суспільства;

відставання рівня розвитку українського кінематографа, книговидання, книгорозповсюдження й бібліотечної справи від рівня розвинених держав;

7) у науково-технологічній сфері:

зниження наукового потенціалу в області інформатизації й зв'язку;

низька конкурентоспроможність вітчизняної інформаційної продукції на світовому ринку;

відтік за кордон наукових кадрів і суб'єктів права інтелектуальної власності;

недостатній захист від несанкціонованого доступу до інформації внаслідок використання іноземних інформаційних технологій і техніки;

неконтрольована експансія сучасних інформаційних технологій, що створює передумови технологічної залежності України;

8) в екологічній сфері:

втаємничення, несвоєчасне надання інформації або надання недостовірної інформації населенню про надзвичайні екологічні ситуації або надзвичайні ситуації техногенного й природного характеру;

недостатня надійність інформаційно-телекомунікаційних систем збору, обробки та передачі інформації в умовах надзвичайних ситуацій;

низький рівень інформатизації органів державної влади, що унеможливлює здійснення оперативного контролю й аналізу стану потенційно небезпечних об'єктів і територій, завчасного прогнозування та реагування на надзвичайні ситуації [64].

Як справедливо вважає російський дослідник П. Шариков, протидія інформаційним загрозам повинна досягатися, насамперед, відповідними нормами міжнародного права. Загрози міжнародній інформаційній безпеці – виклик, унікальний тільки для сучасного етапу розвитку міжнародних відносин, що не має аналогів в історії. Протидія всім існуючим раніше глобальним загрозам, таким як поширення зброї масового знищення, організована злочинність, екологічні погрози й ін., носили силовий і правовий характер. Міжнародним співтовариством були розроблені механізми силової й правової протидії таким загрозам. Крім того, практично будь-який механізм протидії міжнародним загрозам опирається на політичні методи верифікації дотримання договору, а також передбачає міри покарання за недотримання норм права [250, с.19].

Специфіка загроз міжнародній інформаційній безпеці значно утрудняє використання досвіду протидії іншим загрозам порушення міжнародної

стабільності. У першу чергу це пов'язане з тим, що ресурси, необхідні для створення інформаційної загрози, не можуть контролюватися державою. Для створення зброї масового знищення, необхідні значні фінансові ресурси для розробки технологій, придбання особливих матеріалів і устаткування, поширення яких у міжнародній торгівлі регулюється системами експортного контролю. Для створення можливостей використання інформаційних ресурсів, як загрози міжнародній безпеці, достатньо застосування технологій, наявних у вільному продажу.

На основі викладеного представляється доцільним виділити кілька основних напрямків здійснення роботи з формування системи протидії загрозам інформаційної безпеки.

Одним з таких напрямків є вдосконалювання вітчизняного законодавства, що регулює відношення в інформаційній сфері, і системи міжнародних домовленостей з питань протидії погрозам безпеки інформаційного суспільства. Другий напрямок - удосконалювання системи організації правоохоронної й судової діяльності в області забезпечення безпеки законних інтересів громадян, суспільства й держави в інформаційній сфері як в Україні, так і на міжнародному рівні. Третій напрямок пов'язаний з удосконалюванням технологічного забезпечення безпеки інформаційної інфраструктури, засобів захисту інформації, проведення оперативно-слідчих заходів, включаючи їхнє нормативне забезпечення. Четвертий напрямок - удосконалювання системи підготовки кадрів для реалізації функцій забезпечення безпеки інформаційної сфери суспільства. І, нарешті, створення системи культурно-освітнього забезпечення безпеки інформаційної сфери.

На нашу думку, ці напрямки в основному перекривають проблемне поле, пов'язане з досягненням довгострокової стратегічної мети державної інформаційної політики України - формуванням відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору як простору цілісної держави, його інтеграції у світовий інформаційний простір з урахуванням національних особливостей та інтересів при забезпеченні

інформаційної безпеки на внутрішньодержавному й міжнародному рівнях. Для досягнення зазначеної мети в процесі докорінного реформування основ української державності необхідно реалізувати основний стратегічний напрямок державної інформаційної політики, який можна визначити як «формування й розвиток відкритого інформаційного простору держави при неодмінній умові забезпечення його цілісності та єдності, його інтеграція у світовий інформаційний простір з урахуванням національних інтересів і особливостей при забезпеченні інформаційної безпеки на внутрішньодержавному й міжнародному рівнях» [156, с. 109].

Отже, у міру розвитку науково-технічного прогресу роль інформаційної безпеки особистості, суспільства, держави збільшується, і її забезпечення повинно зайняти належне місце в політиці держави, у тому числі й військової. Інформація стала фактором, здатним привести до великомасштабних аварій, військових конфліктів і поразки в них, дезорганізувати державне управління, фінансову систему, роботу наукових центрів. І чим вищий рівень інтелектуалізації й інформатизації суспільства, тим надійнішою повинна бути його інформаційна безпека.

Відставання в інформатиці може привести в перспективі до вразливості комп'ютерних мереж країни і в цілому всієї її інформаційної, управлінської інфраструктури.

Аналіз загроз, пов'язаних з використанням інформаційно-комунікаційних технологій у політичному житті, дав можливість класифікувати їх як: загрози особистості й демократизації суспільних відносин; загрози нормальному функціонуванню структур державної влади; загрози політичним лідерам і партіям.

Обґрунтований висновок про те, що в сучасних умовах поряд із традиційними загрозами безпеки особистості й суспільства зростає значення такого компонента безпеки як інформаційно-психологічна безпека, тобто безпека особистості від негативного й деструктивного інформаційного впливу. У сучасному світі індивід більшою мірою залежить від інформації,

однак інтенсивне зростання кількості надаваної інформації утрудняє процес усвідомленої, раціональної оцінки останньої. Глобальний характер негативних наслідків, які можуть бути викликані загрозами інформаційно-психологічної безпеки громадян, а також те, що індивіди, нездатні самостійно забезпечувати інформаційно-психологічну безпеку, мають на увазі, що дана область є сферою державного контролю й регулювання.

2.2. Інтернет як джерело нових загроз для інформаційної безпеки

Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що представляє собою сукупність інформації, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, поширення й використання інформації, а також системи регулювання відносин, що виникають при цьому.

Стрімке зростання комп'ютеризації основних сфер людської діяльності, що охоплює управління державою, збройними силами, роботою ядерних реакторів, хімічних заводів, фінансово-банківську діяльність, вивчення космосу й подібне, з одного боку, дозволило забезпечити високі досягнення в галузі науки, техніки, культури, управління й організації життєдіяльності суспільства в цілому. З іншої сторони, наявність глобальних комп'ютерних мереж і недостатня їхня захищеність від збоїв техніки, викликаних всілякими причинами, від неправомірних дій людей, здійснених навмисно або з необережності, можуть викликати найбільш непередбачені, шкідливі для людини й суспільства наслідки.

Віру громадян у швидкий наступ інформаційного суспільства підривають і дії комп'ютерних хуліганів, здатних порушувати нормальну роботу стратегічно важливих державних об'єктів. Можна згадати випадок, коли група хуліганів спробувала розбудувати систему управління польотами Франкфуртського міжнародного аеропорту (серед найбільш підозрюваних - союз «Ніякого зв'язку»). Зловмисники, які володіли необхідними

спеціальними знаннями, паралізували роботу систем попередження й вивели з ладу кабельні лінії, по яких забезпечувався комп'ютерний, факсимільний й телефонний зв'язок між трьома рознесеними у просторі станціями спостереження. Перший у ФРН напад комп'ютерних терористів не привів, на щастя, до серйозних наслідків: графік руху повітряних суден порушився лише на дуже незначний інтервал часу, а системи управління й комунікації були швидко відновлені. Але вже через два місяці після цього інциденту ланцюг збоїв в електронній системі Бундесбана (Управління залізниць у Німеччині) вивів з рівноваги десятки тисяч пасажирів, подорож яких на ділянці дороги «Гамбург-Алтона» раптово призупинилася. Причиною події виявився невідрегульований комп'ютер у системі управління рухом, побудований фірмою «Сіменс» [152, с.98].

Мало хто знає про те, що розрекламована Телекомом широколінійна система зв'язку ISDN з її волоконно-оптичними лініями працює тільки при наявності зовнішнього джерела електроенергії і повністю залежить від справності місцевої електромережі. Колишня аналогова система телефонного зв'язку з її мідними кабелями була щодо цього надійніша й не вимикалася при нетривалих ушкодженнях ліній електропередач, зв'язаних, скажемо, з розрядами блискавок. Громадяни, знайомлячись із такими «сюрпризами» і аваріями, починають розуміти, що неприємності й розчарування «комп'ютерного світу майбутнього» уже запрограмовані.

Як написав Г. Бехманн, «Інтернет - своєрідна сполучна тканина або павутина нашого життя. Це не майбутнє - це сьогодення. Інтернет став медіумом для всього, що вступає у взаємодію із суспільством як цілісністю. І хоча у своїх соціально релевантних формах він ще дуже молодий (Інтернет виник між 1969 і 1994 р. у міру розвитку браузера World Wide Web), уже не потрібно занадто довго пояснювати, що це таке» [21, с.23].

Інтернет як унікальний, вільний канал комунікації відкриває інноваційні можливості політичної взаємодії й обміну інформацією. Інтернет, маючи технічні особливості, спрощує умови комунікації як однобічної, так і

двосторонньої, забезпечує можливість ведення діалогів і постійного зв'язку із громадськістю, скорочує при цьому тимчасові й матеріальні витрати.

У науковій літературі аналізуються наступні функції цього унікального явища. Функції Інтернету як політичної технології детермінуються унікальністю комунікаційних характеристик Інтернету. Комунікативна функція Інтернету включає функцію однобічної, двосторонньої комунікації, а так само двосторонньої масової комунікації. Особливість функції легітимації влади обумовлена використанням у державному управлінні системи «електронний уряд», здатної скоротити тимчасові, бюрократичні, матеріальні витрати взаємодії влади із громадянами, бізнесом і державними структурами, сформувати клімат довіри, скорегувати політичні позиції й дії.

Функція оперативного реагування в кризових ситуаціях здійснюється завдяки технічній можливості як швидкого одержання, так і миттєвого розміщення інформації в Мережі. Так само серед функцій Інтернету виділяються: функція тиражування інформації журналістами, формування суспільної думки, політичної соціалізації, інформативна, функція обліку зворотного зв'язку, формування іміджу, рекламна функція й функція позиціонування. Так само розглянуті зміст політичних кампаній в Інтернеті, види сайтів, види Інтернет-Реклами [112].

Уже стало очевидним, що поширення Інтернет-Технологій у політику розширює можливості політичної участі населення і є кроком до громадянського суспільства.

Разом з тим, простір Інтернет породжує й нові злочини. Поява електронних мереж створила якісно нові умови й для пропаганди терористами своїх ідей, для ведення ними відкритої полеміки з офіційними державними структурами, дискредитації й дезавуювання заяв офіційної влади. Не слід забувати й ту обставину, що з комп'ютеризацією адміністративно-управлінських процесів терористи одержали можливість використовувати у своїх цілях відносно дешеві й доступні методи

інформаційно-комп'ютерних диверсій. Поки під удар потрапляють найбільш розвинені країни, у яких широко поширені відкриті електронні системи. Насамперед, це відноситься до США й Канади.

Науково-технічний прогрес розширює можливості міжнародного тероризму до провокування ядерних, екологічних, інформаційних та інших глобальних катастроф. Тому винятково більшу небезпеку в сучасних умовах представляє технологічний тероризм, що включає в себе інформаційний тероризм (кібертероризм, біотероризм, «ядерний тероризм») і можливе використання ядерних матеріалів, що розщеплюються, і хімічної зброї.

Політична мета кібертероризму - нагнітання суспільної напруженості, страху, дестабілізація обстановки, дискредитація офіційної влади. Фактичною метою його атак виступають комп'ютерні системи управління критичною інфраструктурою, тобто транспортом, атомними електростанціями, водопостачанням і енергетикою.

Інтернет-Технології надають екстремістам унікальну можливість ведення інформаційної війни з державою методом безпосереднього й безконтрольного поширення своїх ідей, гасел, закликів у вигляді звертань до широкої аудиторії через сайти, форуми й чати, файлообмінні мережі. Головна небезпека полягає в тому, що до Інтернету підключена в основному молодь, тобто соціальна група, найбільш сприйнятлива до екстремізму. Екстремістські інформаційні ресурси в Інтернеті при грамотному їхньому розміщенні оперативно придушити досить складно, тому що треба зв'язатися із представниками влади тої країни, де розташований сервер,що обслуговує екстремістів, виконати всі відповідні юридичні формальності - все це вимагає часу й фінансових витрат. Навіть швидке ознайомлення з каталогом ресурсів радикалів в українській мережі показує, що багато які із сайтів розташовані за межами зони UA. У цьому зв'язку зростає роль служб, відповідальних за безпеку держави й протидію кібертероризму.

Отже, у ході глобальної інформатизації виникло принципово нове середовище протиборства конкуруючих держав - кіберпростір. Якщо у світі

до теперішнього часу склався в тому або іншому ступені стратегічний баланс сил в області звичайних озброєнь і зброї масового знищення, то питання про паритет у кіберпросторі залишається відкритим.

У процесі формування кіберпростору відбувається конвергенція військових і цивільних комп'ютерних систем і технологій. Державні органи усе ширше закуповують для рішення військових та інших спеціальних завдань апаратно-програмні засоби, розроблені комерційними виробниками для широкого кола користувачів.

Росте також потреба в сумісності громадянської інформаційної інфраструктури з урядовою й військовою. У зв'язку із цим відбувається їх технологічне й організаційне злиття. Так, 95% ліній зв'язку комп'ютерних мереж Міністерства оборони США розгорнуто на базі загальнодоступних телефонних каналів, а понад 150 тис. комп'ютерів підключені до мережі Інтернет, що робить їх надзвичайно вразливими.

Весь стандартизований комп'ютерний комплекс може бути швидко виведений з ладу застосуванням одного конкретного засобу, атакою, орієнтованою на загальний для стандартизованої мережі вразливий елемент, наприклад, операційну систему або протокол зв'язку.

Зазначена обставина може бути ефективно використана радіоелектронною розвідкою країни-розроблювача цих уніфікованих платформ.

Лідируюче положення в цій області займають США, що розглядають світову інформаційну інфраструктуру як сферу, контроль над якою дозволить здійснити стратегічні цілі глобального домінування. У формуванні їхньої зовнішньої політики з'явився новий підхід, пов'язаний з поняттям "інформаційної парасольки", коли США беруть на себе забезпечення інформаційної безпеки своїх союзників.

Ця позиція зустрічає протидію з боку розвинених країн. Наприклад, Японія вважає, що введення інформаційної парасольки може привести до втрати суверенітету країни.

Американська адміністрація вважає, що формування єдиної глобальної інформаційної інфраструктури під контролем США дозволить їм вирішити завдання стратегічного використання інформаційної зброї "аж до блокування телекомунікаційних мереж держав, що не визнає реалії сучасної міжнародної системи".

На думку західних аналітиків, ЦРУ й військова розвідка США вивчають можливості й методи проникнення в комп'ютерні мережі своїх потенційних супротивників. Для цього, зокрема, розробляються технології впровадження електронних вірусів і «логічних бомб», які, не проявляючи себе у звичайний час, здатні активізуватися по команді.

У кризовій ситуації «електронні диверсанти» можуть дезорганізувати оборонну систему управління, транспорт, енергетику, фінансову систему іншої держави. Перспективними для таких цілей уважаються "заражені" мікросхеми, що впроваджені в експортовану Сполученими Штатами обчислювальну техніку.

За наявними даними, у цей час більше 30 країн займаються розробкою інформаційної зброї. Провідні країни світу розширюють і створюють у збройних силах і спецслужбах підрозділи, які повинні забезпечити розвиток наступальних можливостей у кіберпросторі. Це дозволяє говорити про початок витка гонки озброєнь у кіберпросторі.

Так, у Пентагоні активно дискутуються питання створення й використання електронних і комп'ютерних засобів атаки на військову техніку й об'єкти військової інфраструктури ймовірного супротивника.

Причому справа не обмежується теоретичною дискусією. Один з головних ентузіастів кіберзброї в Пентагоні М. Уінн створив в 2007 році кіберкомандування для проведення операцій у кіберпросторі, включаючи в тому числі й наступальні (перехоплення контролю над безпілотними літальними апаратами супротивника, виведення з ладу ворожих літаків у польоті, супровід авіаударів електронною атакою на системи ПВО й т.д.).

Крім того, Міністерство оборони США активізувало розробку підходів до ведення бойових дій у кібернетичному просторі.

Основною метою зусиль, що вживаються, є формування вигляду майбутніх сил ведення бойових дій у кіберпросторі й визначення їхніх бойових можливостей на тлі прискореного розвитку технологій мережних комп'ютерних операцій, радіоелектронної боротьби, радіоелектронної розвідки, а також зброї спрямованої енергії.

І все це - для контролю над кіберпростором, що обіцяє в недалекому майбутньому військову перевагу США над супротивниками.

У європейській пресі з'явилася інформація, що командування збройних сил Німеччини приступило до створення служби мережних операцій з конкретною метою - здійснення впливу на комп'ютерні мережі супротивника,які спрямовані на використання, перекручування, підміну або знищення інформації, що втримується в базах даних комп'ютерів і інформаційних мереж, а також зниження ефективності їхнього функціонування або виведення з ладу.

У ФРН була припинена спроба проникнення в бази даних німецького уряду. Німецькі експерти не сумніваються в тому що за цією кібератакою стоять не групи комп'ютерних фанатів, а китайські спецслужби. Про це повідомив віце-президент Федерального відомства з охорони Конституції ФРН (BFV) Х.-Э. Ремберг, який підготував відповідний рапорт для уряду.

Фахівці BFV установили, що комп'ютерні атаки здійснювалися з міст Ланчжоу, Кантон і Пекін. При цьому з метою маскування хакери діяли через проміжний сервер мережі Інтернет у Південній Кореї.

Для проникнення в урядову мережу ФРН зловмисники встановили таємний контроль за сайтами Word-Datei і Powerpoint у мережі Інтернет. При заході на ці сайти з персонального комп'ютера будь-якого урядового об'єкта цей ПК заражався вірусом, що пізніше міг проникнути у внутрішню мережу установи.

Можливо, метою цієї акції була перевірка ступеня захищеності урядової мережі ФРН.

Таким чином, Пекін виступає ще одним суб'єктом, що активно освоює кіберпростір у військових цілях. Інститут стратегічних досліджень Heritage Foundation підготував для конгресу США доповідь про діяльність спеціальних підрозділів Народно-визвольної армії Китаю (НВАК) у кіберпросторі, що представляє небезпеку для США.

Аналітики виділяють два основних напрямки діяльності китайських підрозділів з ведення бойових операцій у кіберпросторі - "перевірка на міцність" захисту мереж оборонного відомства й розвід співтовариства США й викрадення передових технологій. НВАК успішно використовує інтегрованість підконтрольних їй корпорацій в американську IT-Індустрію.

Експерти стверджують, що останнім часом число мережних нападів, здійснених китайськими військовими на американську інформаційно-телекомунікаційну інфраструктуру, збільшилося втроє. Як основний об'єкт впливу НВАК, як і колись, вибрала комп'ютерні системи збройних сил США.

На них здійснено понад 80 тисяч атак, що дозволили нападаючій стороні переслати на свої сервери 20 Терабайт даних закритого характеру з мережі NIRPNet, а також розробити й впровадити програмне забезпечення для її дистанційного виводу з ладу. Міністерство внутрішньої безпеки США зафіксувало факт несанкціонованого копіювання конфіденційної інформації із власної мережі, що, як думають співробітники Heritage Foundation, через Інтернет був здійснений фахівцями НВАК.

Канадські вчені виявили мережу електронних шпигунів, розташованих переважно в Китаї, які відслідковують вміст комп’ютерів, розміщених в урядових закладах по всьому світу. За словами вчених з Університету Торонто, вірус-шпигун відслідковував уміст 1295 комп'ютерів в 103 країнах. Зараженими виявилися й комп'ютери, якими користується тибетський далай-лама [106].

Китайські спецслужби, у свою чергу, останнім часом відзначають різку активізацію спроб різних сепаратистських і екстремістських організацій використовувати будь-які інформаційні канали для ведення антиурядової пропаганди серед населення країни.

Наприклад, з моменту виникнення масових хвилювань у Тибетському автономному районі з-за кордону було організовано широкомасштабне вкидання в інформаційне поле Китаю коментарів і повідомлень, що повністю спотворюють реальний хід подій і обстановку в цілому. Антикитайські організації з використанням каналів стільникового телефонного зв'язку, радіомовлення й мережі Інтернет відкрито закликали громадян країни до проведення протибетських демонстрацій, мітингів і антиурядових виступів [106].

Слід зазначити, що США раніше від інших держав усвідомили важливість побудови кіберзахисту, у той же час формуючи потужний потенціал для інформаційної агресії.

За океаном інтенсивно розробляються засоби й методи активного впливу на інформаційні інфраструктури потенційних супротивників. У цих цілях використовується продана за рубіж обчислювальна техніка, програмні й програмно-апаратні засоби, що містять відповідні закладки, а також прив'язка потенційних супротивників до глобальних інформаційно-телекомунікаційних мереж, що перебувають під контролем США.

Якщо раніше вектор державної політики в області забезпечення інформаційної безпеки був більш орієнтований на загрозу, що у кіберпросторі можуть представляти терористичні й кримінальні угрупування,

- спецслужби очікували інспірованих катастроф літаків і поїздів, техногенних аварій, то тепер акценти в сфері міжнародної безпеки змістилися убік повномасштабної системи захисту інформації.

Головними суперниками оголошені не хакери-одинаки, а спеціально створені служби на державному рівні. Матеріальний збиток від викраденої інформації оцінюється в мільярди доларів. Відповідно до досліджень Пентагона, проведених торік, найбільша кібератака на США могла б позбавити електрики кілька штатів, перервати роботу банків і цифрових комунікаційних систем.

Президент Барак Обама вже на самому початку виконання функцій глави держави ввів посаду директора з кіберпростору в радах з національної і внутрішньої безпеки США. Також він розпорядився протягом двох місяців підготувати доповідь про стан безпеки комп'ютерних мереж [106].

За останні роки США домоглися істотних успіхів у створенні нових засобів ведення "інформаційної війни". У ході проведення воєнних операцій проти Іраку і Югославії ними були практично випробувані найрізноманітніші види "інформаційної зброї", починаючи від спроб силового придушення командних пунктів і центрів управління за допомогою високоточної зброї й кінчаючи застосуванням широкого спектра інформаційно-психологічного впливу на населення.

На відміну від традиційних озброєнь, засоби протиборства в інформаційному просторі можуть ефективно використовуватися й у мирний час. Важливою особливістю цих засобів є та обставина, що вони доступні не тільки державним, але й терористичним, кримінальним структурам, а також окремим особам.

Так, на думку експертів американської розвідки, терористи, крім використання широко розповсюджених каналів зв'язку в так званих "Інтернет-Форумах", перейшли на спілкування один з одним під прикриттям учасників мережних комп'ютерних ігор. Передбачається, що вони

використовують сценарії даних ігор для координації дій, установки контактів і репетицій можливих атак на віртуальних моделях [106].

Американські служби, що спеціалізуються на протидії інформаційній діяльності терористичних організацій, зізнаються, що і зараз не здатні ефективно протистояти пропагандистській активності "Аль-Каїди" у глобальній мережі Інтернет.

Проте технологічне лідерство США в глобальному інформаційному просторі створює передумови для його використання на шкоду інтересам інших країн, у тому числі для їхнього витіснення з ринків інформаційних технологій, організації інформаційної блокади, проведення наступальних операцій у рамках інформаційної війни.

Поява нових загроз породила політичну необхідність контролю (регулювання) кіберпростору, прийняття відповідних норм. Пріоритетність питань кібербезпеки для подальшого розвитку Інтернету визнана на Всесвітньому саміті з інформаційного суспільства.

Необхідно відзначити, що застосування інформаційних технологій у військових цілях не регулюється міжнародним правом. Все це дозволяє зв'язати швидкий прогрес у розвитку інформаційних технологій з виникненням нових факторів міжнародної безпеки.

Відповідно, питання про контроль над інформаційним простором стає актуальним питанням міжнародної політики. На думку експертів, ці питання повинні розглядатися й зважуватися на багатобічній основі за участю всіх зацікавлених сторін.

Причому управління інформаційним простором необхідне не тільки для забезпечення національної безпеки абсолютного IT-Лідера - США, але й міжнародної безпеки в цілому.

Група експертів НАТО на чолі з екс-держсекретарем США Мадлен Олбрайт дійшла висновку, що комп'ютерна атака проти життєво важливих інфраструктур країн альянсу повинна прирівнюватися до збройного нападу, що виправдує відповідний удар військовими засобами.

На думку експертів, "великомасштабна (кібернетична) атака на командні й контрольні системи альянсу або на енергетичні мережі може привести до відповідних колективних оборонних дій у відповідності зі статтею 5-ою". Це положення Північноатлантичного договору трактує напад на один із членів альянсу як напад на всіх його учасників.

Юристи НАТО думають, що, оскільки наслідки кібератаки можуть бути схожими з військовим нападом, немає необхідності вносити які-небудь корективи в договір для виправдання удару відплати. [255]. Важливість питання підтверджує той факт, що до порядку денного листопадового саміту альянсу в Португалії було внесене питання про можливість нанесення відповідного збройного удару у відповідь на кібератаку, а також наскільки серйозним й масштабним він повинен бути, щоб виправдати застосування військових дій.

Так, зовсім недавно, у листопаді 2010 р. скандально відомим сайтом WikiLeaks були оприлюднені матеріали http://www.newsru.com/world/ 29nov2010/wiki.html, у яких подається переписка Держдепартаменту з посольствами США за рубежем. Як з'ясувалося, дипломати обговорювали не тільки лідерів інших держав, але також членів їхніх родин. Глава відомства Хілларі Клінтон виступила зі спеціальною заявою, у якій назвала витоки, що відбуваються, атакою на світове співтовариство.

"WikiLeaks" одержав документи від джерела, що мало доступ до секретного онлайн-архіву Держдепартаменту США й Пентагона. Це переписка американських посольств по усьому світі з Державним департаментом США. Наприклад, плани по створенню на корейському півострові єдиної держави після падіння КНДР, подробиці про спонсорів " Аль-Каїди", про американське стеження за керівництвом ООН, про таємне прохання Саудівської Аравії нанести авіаудар по Ірану й багато чого іншого. У Вашингтоні оприлюднення документів різко засудили. На думку експертів, під загрозою виявилися не тільки американські дипломати й розвідники, а й

весь ланцюжок людей, що працюють із США по дипломатичних каналах [199].

У зв'язку з тим, що відбулося, Пентагон уже заявив, що підсилить захист своїх комп'ютерних систем. Втім в американських ЗМІ вже не перший раз публікуються факти, що свідчать про проникнення хакерів у комп'ютерні мережі Пентагона. Основними винуватцями атак називалися Китай і Росія.

Усього ж, за словами представників американського Міноборони, понад 100 іноземних розвідок працюють над тим, щоб проникнути в американські комп'ютерні мережі, не говорячи вже про промислове шпигунство, терористичних і злочинних угрупуваннях [230].

У рамках ООН іде процес переговорів з правового режиму міжнародної інформаційної безпеки. Починаючи з 1998 р., проблеми, пов'язані з інформаційною безпекою, зокрема питання, що стосуються понятійного апарата в даній сфері суспільних відносин, а також розробки міжнародно-правового режиму інформаційної безпеки, неодноразово обговорювалися на сесіях Генеральної Асамблеї ООН.

Виробленням механізмів рішення питань кіберзлочинності займаються такі організації, як Форум з управління Інтернетом, створений за підсумками Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства, Міжнародний союз електрозв'язку, ряд недержавних організацій, експертне співтовариство.

У грудні 1997 р. на зустрічі міністрів внутрішніх справ і юстиції держав «вісімки» у США був підписаний документ «Принципи й план дій по боротьбі з високотехнологічними злочинами». У травні 2002 р. на зустрічі її представників у Парижі була досягнена домовленість про прийняття країнами «вісімки» аналогічних законів по боротьбі з кіберзлочинністю на національному рівні. У листопаді 2001 р. на конференції в Будапешті представниками 30 країн (у тому числі 26 держав - членів Ради Європи, а також США, Канади, Японії й ПАР) була підписана Конвенція по кіберзлочинності. Відповідно до неї створений спеціальний міждержавний

орган, що працює в цілодобовому режимі (тобто в режимі Інтернет-Часу) і має повноваження з видалення матеріалів не залежно від фізичного місцезнаходження Інтернет-Ресурсу. Узгоджувались національні законодавства, режим пошукових заходів, також передбачалася розробка системи покарання злочинців. Фактично малося на увазі створення міжнародної кіберполіції з найширшими правами.

Аналіз міжнародних актів показує, що, починаючи з 2000 р., прийняті такі найважливіші акти, як Окинавська хартія глобального інформаційного суспільства, підсумкові документи Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства в грудні 2003 р. у Женеві й у листопаді 2005 р. у Тунісі, спрямовані на прискорення формування постіндустріальних тенденцій в економічній, соціально-політичній і духовній сферах життя суспільства. Декларація принципів з питань інформаційного суспільства, прийнята в Женеві в 2003 р., проголосила побудову інформаційного суспільства як глобальне завдання в новому тисячолітті й визначила принцип забезпечення підвищення довіри й безпеки при використанні інформаційних технологій як один із ключових. Для побудови інформаційного суспільства важливе значення мають розвиток інфраструктури, створення людського потенціалу, інформаційна безпека при дотриманні принципу верховенства права, протидія новим викликам і погрозам, що виникають у результаті використання інформаційно-комунікаційних технологій у злочинних і терористичних цілях.

В 2005 р. у Тунісі в ході заключного етапу Всесвітньої Зустрічі на вищому рівні з питань інформаційного суспільства (ВВУІО) було досягнуто загального розуміння необхідності забезпечення міжнародної інформаційної безпеки, запобігання використання інформаційних технологій у терористичних і злочинних цілях, а також обліку принципів міжнародного права й національного суверенітету при побудові глобального інформаційного суспільства.

В 2005 р. у Греції було створено Європейське агентство мережної й інформаційної безпеки (ENISA) у рамках адміністрації Євросоюзу. Агентству доручили складати звіти про останні вразливості, що загрожують країнам-учасницям, і накопичувати досвід найбільш ефективних способів боротьби із проблемами інформаційної безпеки.

Специфіка інформаційного тероризму не у фізичному знищенні людей, ліквідації матеріальних цінностей, руйнуванні життєво важливих об'єктів, а в порушенні роботи інформаційно-комунікативних мереж. Так, за інформацією глави Кіберкомандування США генерала Кіта Александера мережі міністерства оборони США витримують шість мільйонів хакерських атак у день. У числі основних джерел мережної загрози генерал назвав терористів, злочинні угрупування й окремих хакерів. При цьому Александер підсумував, що інтереси країни перебувають у небезпеці через наявність "значних вразливостей" і загроз. Генерал навів як приклад хакерські DDo-Атаки на урядові ресурси Естонії й Грузії в 2007 і 2008 роках. Він також повідомив, що з тих пір з'явилися й нові загрози безпеки. У даний момент безпеку 15 тисяч мереж Пентагона забезпечують понад 7 мільйонів систем [213].

М. Величко виділяє такі відмінні риси інформаційного тероризму, як дешевизна й складність виявлення. Система Internet, що зв'язала комп'ютерні мережі по всій планеті, змінила правила, що стосуються сучасної зброї. Анонімність, забезпечувана Internetом, дозволяє терористові стати невидимим, як наслідок, практично невразливим і нічим (у першу чергу життям) не ризикує при проведенні злочинної акції [41, с. 18].

Є навіть думка, що сучасні Інтернет-Технології стають, наприклад, для ісламських екстремістів більш зручним способом збору розвідданих, ніж традиційне шпигунство. Так, найбільшу небезпеку представляють онлайн-відеосистеми, які дозволяють спостерігати за різними куточками світу й дають можливість одержання точних даних про обрану місцевість у режимі реального часу.

У той же час відомо, що керівництво США поблажливо ставиться до мережної активності радикальних ісламістів, обґрунтовуючи це тим, що існування подібних ресурсів свідчить про високий ступінь свободи в американському сегменті Інтернету. Крім того, спецслужби використовують сайти екстремістів як джерело інформації про їхню діяльність [90].

На думку комісара ЄС по засобах комунікацій та інформаційному товариству Вівіани Рединг, компанії Євросоюзу витрачають занадто мало грошей на захист своїх інформаційних інфраструктур, у той час як активність хакерів продовжує залишатися дуже високою.

За її інформацією лише від 5 до 13% витрат на IT ідуть на захист мереж та інформації, що не може не викликати тривоги. Рединг упевнена, що з ростом масштабів і складності мереж і систем Європу чекає безпрецедентно велика кількість проблем [105].

Викладене дозволяє зробити висновок про те, що в українських умовах істотну небезпеку стабільності політичної системи несе Інтернет. Це зв'язано головним чином з відсутністю ефективних правових механізмів, що регулюють життя в Інтернет-Просторі. У результаті під впливом ІКТ система інформаційно-політичних відносин трансформується не просто в поле інформаційного протиборства, тобто суперництва політичних сил з приводу впливу на ключові сфери соціальних відносин і встановлення контролю над джерелом стратегічних ресурсів [136, с.345], а війну компроматів, де не останнє місце займає «чорний піар». Поряд з офіційними сайтами органів державної влади, політичних партій, громадських організацій в Інтернеті створюються інформаційні площадки для «вкидання» у суспільство компромату на ту або іншу політичну силу, тому що практично ніяких обмежень на характер інформації, що вноситься у Мережу, не існує.

Більше того, сучасні Інтернет-Технології сприяють розростанню міжнародного тероризму й виникненню принципово нового високотехнологічного кібертероризму. При цьому можуть застосовуватися як інформаційно-комп'ютерні, так і інформаційно-психологічні засоби. Інтернет

же все активніше використовується для поширення ідеології тероризму, залучення в протиправну діяльність нових членів, про що красномовно свідчить наявність великої кількості відповідних сайтів.

Всі ці обставини свідчать про гостру потребу держави постійно зміцнювати інформаційну безпеку її політичної сфери, сприяти усуненню загроз, пов'язаних з використанням ІКТ.

Висновки до розділу 2

Не є секретом той факт, що організаційні форми політичної боротьби перманентно модифікуються, все частіше комбінують застосування технологій, призначених для непрямого й прихованого примусу індивідів і соціальних груп. Різні політичні й соціальні сили як в Україні, так і за рубежем використовують інформацію як засіб для збереження влади, здійснення експансії в різних сферах життєдіяльності. З цією метою застосовуються такі види протиправного впливу проти інтересів особистості, суспільства й держави, як інформаційно-технологічне й інформаційно-психологічне.

Один з висновків дисертації полягає в тому, що деформації політичного процесу в Україні надають широкі можливості для розгортання деструктивного інформаційно-психологічного впливу. Наслідки глобалізації заохочують вільний комунікаційний обмін між етнічними, конфесійними, культурологічними елітами, фінансово-промисловими групами в Україні та їхніми закордонними партнерами, що реалізують проекти інформаційного й культурного співробітництва. Можливості інформатизації надають субнаціональним і місцевим елітам технологічні засоби й ідеологічні обґрунтування для встановлення контактів і зв'язків із впливовими акторами політичних відносин, сприяючи мімікрії їх світоглядних і геополітичних орієнтацій.

Підвищується вразливість масової свідомості для деструктивного впливу, реалізованого за допомогою можливостей процесу інформатизації.

Прийнято вважати, що рівень використання ІКТ в Україні істотно нижчий, ніж у західних країнах. Однак не можна не враховувати той факт, що вже сьогодні в країні майже всі системи життєзабезпечення суспільства й держави базуються на широкому використанні єдиної інформаційної інфраструктури України. Відповідно, виведення з ладу будь-якого істотного елемента інформаційної інфраструктури може привести до непоправного збитку й катастрофічних наслідків, економічних і соціально-політичних.

Можна зробити висновок, що в умовах розвитку постіндустріального суспільства політична стратегія української держави в області інформаційної безпеки має потребу в удосконалюванні з метою зміцнення імунітету перед виникаючими інформаційними небезпеками.

Інтереси держави в інформаційній сфері полягають у використанні інформації й інформаційної інфраструктури для управління справами суспільства, роз'яснення населенню країни й міжнародній громадськості змісту й спрямованості державної політики, у створенні умов для гармонійного розвитку інформаційної інфраструктури країни, у безумовному виконанні законодавства, у підтримці правопорядку, у розвитку міжнародного співробітництва на основі партнерства.

Актуалізація проблеми захисту інформаційного простору і його впливу на інформаційну безпеку безпосередньо пов'язана з існуючими реальними й потенційними загрозами й викликами безпеки держави, рівень і масштаби яких в останнє десятиліття істотно зросли й придбали досить небезпечний характер.

У результаті впливу загроз інформаційній безпеці може бути нанесений серйозний збиток життєво важливим інтересам України в політичній, економічній, оборонній та іншій сферах діяльності держави, заподіяний соціально-економічний збиток суспільству й окремим громадянам.

Наслідком такого впливу можуть бути: створення перешкод на шляху рівноправного співробітництва України з розвиненими країнами й дружніми державами; утруднення прийняття найважливіших політичних, економічних та інших рішень; підрив державного авторитету України на міжнародній арені; створення атмосфери напруженості й політичної нестабільності в суспільстві; порушення балансу інтересів особистості, суспільства й держави; дискредитація органів державної влади й керівництво; провокування соціальних, національних і релігійних конфліктів; ініціювання страйків і масових безладів; порушення функціонування системи державного управління, а також систем управління військами, озброєнням і військовою технікою, об'єктами підвищеної небезпеки.

Також наслідком впливу загроз може бути зниження темпів науково-технічного розвитку країни, втрата культурної спадщини, прояв бездуховності й аморальності. Досить істотний економічний збиток у різних областях громадського життя й у сфері бізнесу може бути заподіяний у результаті порушень законодавства в інформаційній сфері й комп'ютерних злочинів.

Загрози інформаційній безпеці можуть нанести фізичний, матеріальний і моральний збиток громадянам, викликати неадекватну соціальну або кримінальну поведінку груп людей або окремих осіб, вплинути на процеси утворення й формування особистості.

Оскільки інформація - важливий елемент життєдіяльності суспільства, забезпечення інформаційної безпеки є однієї із пріоритетних складових національної безпеки України й впливає на захищеність національних інтересів Української держави в різних сферах життєдіяльності суспільства й держави. У період зростаючої ролі інформаційних технологій, появи нових глобальних викликів і погроз в інформаційній сфері зростає значення такої функції держави, як забезпечення інформаційної безпеки, як функції, що випливають з потреб суспільства в захисті прав та інтересів особистості, суспільства й держави в інформаційній сфері.

Виходячи з того, що інформаційна безпека на рубежі третього тисячолітті виходить на перше місце в системі національної безпеки, формування й проведення єдиної державної політики в цій сфері здобуває пріоритетне значення. Про це в наступному розділі.

РОЗДІЛ 3
ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Мета даного розділу полягає в обґрунтуванні пріоритетів державної політики в сфері протидії загрозам інформаційної безпеки, а також визначенні параметрів і функціонального призначення системи її забезпечення, рівнів і елементів останньої. На думку автора, це повинно сприяти раціональному розподілу й використанню сил, засобів і ресурсів суспільства, що застосовуються для захисту національних інтересів у всіх областях життєдіяльності індивідів і соціальних агрегацій.

3.1. Національні інтереси України в сфері забезпечення інформаційної безпеки

При переході від індустріального суспільства до інформаційного поряд із традиційними ресурсами (матеріальними, енергетичними, технічними й ін.) роль ресурсів інформаційних й інтелектуальних різко зростає. Знання й інформація стають стратегічним ресурсом суспільства, що визначає перспективи його економічного, соціального, культурного розвитку в новому тисячолітті. Крім того, інформаційні ресурси - об'єкт власності конкретних юридичних і фізичних осіб, вони потребують захисту, забезпечення правового режиму їхнього володіння, розпорядження й користування.

Сучасний етап розвитку суспільства характеризується зростаючою роллю інформаційної сфери, що є важливим фактором громадського життя. Це обумовлено, насамперед, наступними обставинами:

- в умовах реалізації конституційних прав громадян на свободу економічної, інформаційної й інтелектуальної діяльності істотно збільшуються потреби соціально активної частини суспільства в розширенні інформаційної взаємодії як усередині країни, так і з зовнішнім світом;

- інтенсивний розвиток інформаційної інфраструктури й, насамперед, інформаційно-телекомунікаційних систем, засобів і систем зв'язку, а також інформатизація практично всіх сторін громадського життя, діяльності органів державної влади й керівництва істотно підсилили залежність ефективності функціонування суспільства й держави від стану інформаційної сфери;

- індивідуальна, групова й масова свідомість людей усе більшою мірою залежать від діяльності засобів масової інформації й масових комунікацій.

Дані обставини визначили зміст національних інтересів України в інформаційній сфері й потреби держави в забезпеченні їхньої безпеки, а практика останніх років показала необхідність концептуальних документів, що визначають політику держави в цій сфері.

На думку Д. Кафтанчикова, «Вплив фактора інформатизації на розвиток суспільних відносин не тільки актуалізує завдання забезпечення інформаційної безпеки, але й підвищує вимоги до стану всього спектра проблем, пов'язаних із захистом національних інтересів у політичній, економічній, соціальній, військовій, екологічній та інших областях залежно від ступеня їх залученості в систему інформаційного простору» [99, с.13].

Поява поняття «національні інтереси» більшість дослідників відносить до XVII століття. Це час утворення національних держав у Європі. Термін «національні інтереси» або попередні до нього й близькі за змістом «державний розрахунок» («raison d'etat»), «воля государя» («will of prince») й інші спорідненні поняття можна зустріти вже в працях Н. Макіавеллі, Т. Гоббса, Дж. Локка. Виникнення даного поняття зв'язується, з одного боку, з усвідомленням своєї спільності людьми, що проживають на певній території, та, з іншого боку, осмисленням часткової розбіжності інтересів цієї спільності з інтересами династичних правителів, що панували над даними людьми.

Однак саме поняття «національного інтересу» увійшло в науковий оборот порівняно недавно. Лише в 1934 році побачила світло книга видатного економіста й політолога Ч. Бирда, у якій він запропонував

використовувати національний інтерес для наукового опису зовнішньополітичної діяльності держав. А в 1935 році термін «національний інтерес» одержав наукове визнання й «право громадянства» в Оксфордській енциклопедії соціальних наук [143].

Ю. Касперович справедливо відзначає, що «Національні інтереси в значній мірі реалізуються в результаті цілеспрямованої діяльності всіх суб'єктів державного регулювання суспільних відносин, і в них фактично закріплюються відношення індивідуумів, соціальних груп, усього суспільства до тої або іншої сукупності соціальних інститутів.

Політика соціального розвитку визначає мету діяльності з реалізації цих інтересів, а стратегія, що випливає із цієї політики, визначає практику їхньої реалізації й досягнення поставлених цілей» [98, с.3].

Пріоритети сучасного незалежного розвитку будь-якої держави в значній мірі залежать від того, наскільки чітко й недвозначно сформульовані його національні інтереси, а також від правильного розуміння шляхів і засобів реалізації цих інтересів. Серед пріоритетних цілей стійкого розвитку держави на першому місці стоїть забезпечення національної безпеки в усіх її формах і проявах [205].

Сам факт широкого використання поняття "національний інтерес" представниками різних політичних напрямків заслуговує на увагу з двох причин. По-перше, правильно зрозумілий національний інтерес допускає визнання права на існування будь-якої держави, а також обов'язкове прийняття до уваги й повагу інтересів всіх взаємодіючих сторін. По-друге, реалістична позиція щодо поняття "національний інтерес" і сьогодні залишається важливою складовою частиною юридичної науки в цілому й міжнародно-правової науки зокрема [205].

Комплекс дій держави виходить із подань про його національні інтереси, причому не тільки в інформаційній, але й більш широкій соціально-політичній області. Ці інтереси можуть носити як прагматичний характер (що спонукає держави прагнути одержати конкретні вигоди у різних сферах

діяльності), так і міфологічний (що передбачає наявність якоїсь керівної доктрини, ідеї, ідеології, що спрямовує всю діяльність цього інституту). Стосовно інформаційної сфери можна сказати, що саме характер розуміння такого роду інтересів визначає стилістику дій, загальне відношення до проблем державної безпеки.

Як відзначає А. І. Соловйов, «національний інтерес являє собою найбільш важливий орієнтир самостійної політичної діяльності національно орієнтованих сил у сфері державної влади. Національний інтерес є однією з основних умов знаходження людьми національної й культурної ідентичності, крім того, він у концентрованій формі виражає ті інтереси й способи їхнього досягнення, які закріплюють за національними рухами той або інший політичний статус як усередині країни, так і на міжнародній арені. Нарешті, як підстава діяльності національної держави національний інтерес виступає і як показник визначеності зовнішньої й внутрішньої політики країни» [224, с.183].

На думку К. Гаджиєва, «Національний інтерес - категорія абстрактна й суб'єктивна, оскільки її параметри визначаються картиною світу й ціннісною системою, що панує в даному суспільстві й державі. Як відзначав Дж. Розенау, "визначення національного інтересу ніколи не може бути нічим іншим як системою розумних висновків, що виходять із аналітичної й ціннісної бази політики". Реальність національного інтересу виявляється в процесі й у ступені його здійснення. А це, у свою чергу, припускає наявність вольового й дієвого початку, а також засобів для реалізації поставлених державою завдань. З даної точки зору політику можна розглядати як найважливіший засіб реалізації національних інтересів» [50].

Характеризуючи поняття національних інтересів, український учений Б. Кормич вважає, що інтерес взагалі - це «об'єктивно обумовлений мотив діяльності окремої людини, соціальної спільності, суспільства в цілому, спрямований на досягнення мети. Він має таку структуру: конкретні об'єктивні умови існування суб'єкта цього інтересу, суб'єктивна система

цінностей, що обумовлює конкретні завдання й необхідність їхнього досягнення й, нарешті, конкретна мета (завдання), що стоїть перед суб'єктом. Таким чином, якщо поняття національної безпеки виражає стан захищеності держави, її громадян від різних загроз, то поняття національних інтересів - зміст основних цінностей, цілей і устремлінь суспільства й держави на конкретно-історичному етапі розвитку» [115, с.122]. Національні інтереси - це «інтегральне вираження інтересів всіх членів суспільства, які реалізуються через політичну систему відповідної держави, як компроміс в об'єднанні запитів кожної людини й суспільства в цілому» [186, с.322].

«Державна політика завжди виражає й представляє певний суспільний інтерес. У формуванні державної політики виражаються інтереси держави й суспільства взагалі (національні інтереси) та інтереси окремих фізичних і юридичних осіб» [115, с.122].

Національні інтереси мають об'єктивно-суб'єктивну природу. Їхня об'єктивність обумовлена реальними потребами особистості, суспільства й держави в забезпеченні економічної, політичної, соціальної й духовно-моральної стабільності в суспільстві, міцного суверенітету держави, його територіальної цілісності й міжнародного авторитету.

Суб'єктивна сторона національних інтересів полягає в тому, що їхніми носіями й конкретними виразниками є індивіди (особистості), держава й суспільство із властивими тільки їм соціальними цінностями й потребами, прагненнями й установками в забезпеченні власної безпеки й умов для розвитку [220, с.10].

У науковій літературі виділяються кілька основних джерел загроз безпеки інформаційного суспільства, що торкаються як соціальних інтересів людини, так й інтересів суспільства і держави.

Так, соціальні інтереси людини, які необхідно охороняти в інформаційному суспільстві, полягають, насамперед, у реальному забезпеченні прав і свобод людини на доступ до відкритої інформації, на використання інформації в інтересах здійснення не забороненої законом

діяльності, а також у захисті інформації, що забезпечує особисту безпеку, духовний та інтелектуальний розвиток. Найнебезпечнішим джерелом загроз цим інтересам є істотне розширення можливості маніпулювання свідомістю людини за рахунок формування навколо неї індивідуального "віртуального інформаційного простору", а також можливості використання технологій впливу на її психічну діяльність.

Другим небезпечним джерелом загроз соціальним інтересам людини є використання на шкоду її інтересам персональних даних, що накопичуються різними структурами, у тому числі органами державної влади, а також розширення можливостей таємного збору інформації, що становить її особисту й сімейну таємницю, відомостей про її приватне життя. Це обумовлено подальшими успіхами в області мініатюризації засобів таємного збору й передачі інформації. Для протидії погрозам соціальним інтересам людини необхідно розробити й реалізувати діючі правові механізми охорони цих відомостей.

Величезне значення має зовнішньополітичний аспект безпеки України, пов'язаний із створенням оптимальних можливостей для розвитку міжнародного співробітництва на основі партнерства в умовах міцного миру.

Не секрет, що провідні країни світу продовжують модернізувати свої розвідувальні служби, удосконалюють технічну розвідку, нарощують її можливості. Увага до України як об'єкту розвідки підсилилася. При цьому головними пріоритетами іноземних розвідок є процеси становлення України як самостійної держави в структурі світового співтовариства, її внутрішні й зовнішні політичні орієнтири, військова політика й шляхи її практичної реалізації, економічні перетворення, що відбуваються, спрямованість наукових досліджень і технічних експериментів, оцінка українського ринку у всіх його складових.

Розвідувальна діяльність іноземних держав у наш час відрізняється більшою розмаїтістю використовуваних сил і засобів. Це: багатофункціональні розвідувальні космічні системи, наземні центри

радіотехнічної й радіолокаційної розвідки, стратегічні літаки-розвідники, морські системи й комплекси технічної розвідки й ін. Витрати на розвідувальну діяльність іноземних держав не скорочуються (наприклад, у США вони становлять щорічно близько 30 млрд. доларів). У сферу інтересів технічних розвідок потрапляють навіть союзники. Досить згадати стурбованість європейських партнерів і союзників США тим, як активно впроваджується в їх політичну, економічну й, можливо, приватне життя горезвісна американська система «Ешелон», що використовує глобальну мережу космічної радіо- і комп'ютерної розвідки.

Інтереси держави в інформаційній сфері полягають у створенні умов для гармонійного розвитку української інформаційної інфраструктури, для реалізації конституційних прав і свобод людини й громадянина в області одержання інформації й користування нею з метою забезпечення непорушності конституційного ладу, суверенітету й територіальної цілісності України, політичної, економічної й соціальної стабільності, у безумовному забезпеченні законності й правопорядку, розвитку рівноправного й взаємовигідного міжнародного співробітництва.

Проблематика національних інтересів України в інформаційній сфері піднімається в офіційних нормативно-правових документах, наукових дослідженнях і публікаціях, розробках різних відомств і служб, де на концептуальному рівні представлені позиції й погляди в цій області, а також є предметом обговорення в органах державної влади й у ході наукових дискусій.

Базовим концептуальним документом, що визначає політику держави в сфері інформаційної безпеки, є Доктрина інформаційної безпеки України, затверджена Указом Президента України 8 липня 2009 р.

Доктрина інформаційної безпеки України являє собою сукупність офіційних поглядів на цілі, завдання, принципи й основні напрямки забезпечення інформаційної безпеки України. Вона є основою для формування державної політики в області забезпечення інформаційної

безпеки Української держави, підготовки пропозицій по вдосконалюванню правового, методичного, науково-технічного й організаційного забезпечення інформаційної безпеки України, а також розробки цільових програм забезпечення інформаційної безпеки України.

У Доктрині інформаційної безпеки України закріплені чотири основні складові національних інтересів України в інформаційній сфері.

Перша складова національних інтересів України в інформаційній сфері містить у собі дотримання конституційних прав людини й громадянина в області одержання інформації та її використання, забезпечення духовного відновлення України, збереження й зміцнення моральних цінностей суспільства, традицій патріотизму й гуманізму, культурного й наукового потенціалу країни.

Друга складова - це інформаційне забезпечення державної політики України, пов'язане з доведенням до української й міжнародної громадськості достовірної інформації про державну політику України, її офіційної позиції відносно значущих подій українського й міжнародного життя, із забезпеченням доступу громадян до відкритих державних інформаційних ресурсів.

Третя складова інтересів України в інформаційній сфері включає розвиток сучасних інформаційних технологій, вітчизняної індустрії інформації, у тому числі індустрії засобів інформатизації, телекомунікації й зв'язку, забезпечення потреб внутрішнього ринку її продукцією й вихід цієї продукції на світовий ринок, а також забезпечення накопичення, збереження й ефективного використання вітчизняних інформаційних ресурсів.

До четвертої складової національних інтересів відносяться: захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки інформаційних і телекомунікаційних систем як уже розгорнутих, так і створюваних на території України [64].

Для реалізації тої групи інтересів, які пов'язані з дотриманням конституційних прав і свобод людини й громадянина в області одержання

інформації й користування нею, забезпеченням духовного відновлення України, збереженням і зміцненням моральних цінностей суспільства, традицій патріотизму й гуманізму, культурного й наукового потенціалу країни, у першу чергу потрібно підвищити ефективність використання інформаційної інфраструктури в інтересах суспільного розвитку, консолідації суспільства, духовного відродження багатонаціонального народу України, що саме по собі представляє тепер непросте завдання. Адже не секрет, що в умовах розколу суспільства на «бідних» і «багатих» досить складно забезпечити рівні можливості користування передовими інформаційними технологіями для всіх членів суспільства. Тому держава повинна передбачати створення й розвиток відповідних соціальних інститутів підтримки з цих питань певної частини населення.

Необхідно далі вдосконалювати систему формування, збереження й раціонального використання інформаційних ресурсів, що становлять основу науково-технічного й духовного потенціалу України й одночасно забезпечити конституційні права й свободи людини й громадянина вільно шукати, одержувати, передавати, виробляти й поширювати інформацію будь-яким законним способом.

І навпаки: право вільного доступу до інформації не повинно вести до порушення конституційного права людини й громадянина на особисту й сімейну таємницю, таємницю листування, телефонних переговорів, поштових, телеграфних і інших повідомлень, на захист своєї честі й свого доброго імені. Необхідно також гарантувати свободу масовій інформації, заборону цензури й одночасно зміцнювати механізми правового регулювання відносин в галузі охорони інтелектуальної власності, створити умови для дотримання встановлених законодавством обмежень на доступ до конфіденційної інформації.

Д. Кафтанчиков робить справедливий висновок про амбівалентний характер впливу процесу інформатизації на стан різних аспектів національної безпеки. З одного боку, поширення інформаційних технологій і

телекомунікаційних систем надає в розпорядження органів державного управління більш ефективні засоби, технології й прийоми забезпечення національних інтересів. Разом з тим інформатизація висуває підвищені вимоги до функціонування системи забезпечення національної безпеки: по-перше, у даній області життєдіяльності можуть виникати протиріччя й формуватися інтереси, протилежні інтересам особистості, суспільства й держави; по-друге, інформаційна сфера, виконуючи комунікативну функцію, здатна в ситуації політичної нестабільності виступати ретранслятором загроз і небезпек, що формуються в інших областях соціального буття [99, с.18].

Формування інформаційного суспільства й розвиток інформаційних технологій, що триває, значно впливають на відносини в сфері військової безпеки – інформаційні технології активно використовуються не тільки в комерційній, але й у військовій області.

Не випадково, багато авторитетних дослідників уважають, що забезпечення військової безпеки в XX1 столітті усе більше буде залежати від інформаційних факторів. Так, відомий американський футуролог О. Тоффлер у своїй книзі «Війна й антивійна» [263, p.45] відзначає, що інформація стає найважливішим воєнно-стратегічним ресурсом, не менш, а то й більш важливим, ніж традиційні види озброєнь і військової техніки. Тобто, у формуванні оборонного потенціалу й військової могутності держави значне місце повинно бути приділене регулюванню інформаційних відносин, розвитку інформаційних технологій, удосконалюванню методів інформаційної боротьби й т.д. [198, с.10].

Як відомо, стан військової сфери є найбільш показовим прикладом уразливості національних інтересів. І це не випадково, оскільки розвиток і поширення інформаційних технологій досягло тут критичної маси. Тому, приміром, відсутність засобів захисту від застосування інформаційно ємних технологічних досягнень у військовій сфері (високоточної зброї, технології «стелс», радіоелектронних засобів бойового й розвідувального призначення, нових засобів командування, контролю й комунікації, засобів космічного

базування, віртуальних стимуляторів і систем підготовки персоналу й, нарешті, футуристичних, з погляду обивателя, розробок в області роботизації й автоматизації бойових засобів) може мати найсерйозніші наслідки для національної безпеки країни.

Застосування інформаційних технологій військовими відкрило нові можливості в забезпеченні оборони держави. Нові технології надали нові можливості одержання інформації про супротивника, а відповідно й попередження про можливі конфлікти й напади. Застосування інформаційних технологій у системах озброєння дозволило істотно збільшити ефективність їхнього використання. Нарешті, інформаційні технології самі по собі можуть бути використані як засіб поразки інформаційних систем супротивника.

Дані обставини свідчать про те, що інформаційна безпека, а точніше оборона (як елемент національної безпеки, у тому числі й в інформаційній сфері) може бути забезпечена не тільки пасивними, але й активними засобами.

При цьому, процес впровадження інновацій, необхідних для збройних сил потужної держави, украй складний. Комерційні компанії мають більш вдосконалені фінансові ресурси для розробки й впровадження нових технологій. На думку багатьох експертів, будь-яка невелика армія, вільна від бюрократичних обмежень, з ефективною системою поставок нового обладнання, здатною швидко освоїти й прийняти на озброєння нові комерційні технології, може мати переваги в порівнянні з американською армією. У цьому полягає одне з основних джерел загрози військової інформаційної безпеки в сучасному світі [250, с.15].

Крім того, технології роботи з інформацією, доступні військовим, як правило, доступні й у цивільній сфері, тобто в наш час одержати доступ до засобів активної й пасивної оборони інформаційного простору можуть практично всі бажаючі. Очевидно, що для створення подібних технологій необхідна фахова освіта й володіння багатьма специфічними знаннями й

навичками роботи з інформацією, але для їхнього використання, як правило, подібних навичок не потрібно.

Російський дослідник Д. Прудников справедливо підтверджує, що історія збройних конфліктів і воєн двадцятого й початку двадцять першого століття свідчить про безумовне зростання ролі інформаційного фактора в забезпеченні оборонної безпеки. Сьогодні будь-які збройні конфлікти супроводжуються сильним інформаційним протиборством, в орбіту якого втягуються не тільки спеціальні інформаційні служби конфліктуючих сторін, але й практично вся інформаційна інфраструктура держави й суспільства [198, с.10]. Як уважає військовий експерт С. Гриняєв, сьогодні істотна частка всіх протиріч між державами перенесена в інформаційну сферу. Дана обставина привела до трансформації підходів до поняття «військової сили». На зміну «грубій силі» зброї приходить «м'яка сила» переконання й психологічної маніпуляції. Реалізація цього принципу вимагає перегляду підходів до формування військової стратегії нової епохи. Домінуюча роль інформації й інформаційних технологій, а також орієнтація на відбиття принципово нових загроз інформаційної епохи, змусили керівництво ряду західних країн, і насамперед США, активніше впроваджувати нові концепції будівництва збройних сил [61].

Таким чином, ефективна інформаційна діяльність може істотно поліпшити зусилля держави з мирного розв’язання кризової ситуації. І навпаки, ігнорування інформаційних факторів, а часто й навмисно змінена інформація здатні спровокувати найрадикальніші настрої, спалахи ворожості й привести до катастрофічних наслідків. Володіння інформаційними ресурсами та їхнім захистом у військовій сфері стане таким же неодмінним атрибутом, як озброєння, боєприпаси, транспорт і т.п. Виграш в інформаційному протиборстві в ході безконтактних воєн може сприяти досягненню їхніх стратегічних цілей [198, с.10].

Інформаційна безпека у військовій справі - це досить традиційна область. Військові структури завжди захищалися від засобів розвідки всіма способами: пасивними й активними.

На думку вітчизняних і зарубіжних фахівців, бойові дії в сучасних (і майбутніх) війнах, насамперед, ведуться не для розгрому сухопутних військових угрупувань супротивника. Вони мають на меті дезорганізацію політичного, економічного й військового управління відповідними структурами протиборчої сторони. Про те, що змінилися мета й характер бойових дій, свідчить досвід локальних воєн останнього часу (після В'єтнаму). Зараз наступає новий етап. Намітилася тенденція переходу від зброї масового знищення до високоточної «інформаційної зброї». Так, у США створений центр з реалізації концепції «Інформаційна війна». Новий орган буде розробляти положення з організації й ведення боротьби в новій сфері військового протиборства, вирішувати завдання з підготовки фахівців у даній області, а також визначати пріоритети в НІОКР і закупівлях призначених для цих цілей озброєнь і апаратури.

Інформаційна зброя може істотно змінити характер майбутніх воєн. Іноді стверджується, що майбутні війни можуть перетворитися по суті в «комп'ютерні війни» з масовим застосуванням комп'ютеризованих роботів, роботизованої зброї й військової техніки. Передбачається, що основу бойового екіпірування солдата в майбутньому становитиме бойовий комп'ютер. Крім аналізу навколишнього оточення, комп'ютер за рахунок відповідного програмного забезпечення й сенсорів буде здійснювати медичний контроль за станом солдата й видавати лікувальні рекомендації.

У свою чергу, елементом впливу на сили й засоби супротивника в майбутній війні може стати комп'ютерна зброя. Вона може бути реалізована, зокрема, у вигляді деструктивних програм, які можуть змінювати або знищувати програми комп'ютерів, що керують зброєю, військовою технікою й військами.

Досвід воєнних дій останніх років (на Близькому Сході, у Югославії, Іраку) показав, що різко зрослі технічні можливості засобів розвідки зробили неефективними багато традиційних методів і засобів захисту інформації. Наприклад, дані космічних засобів розвідки оперативно використовувалися безпосередньо на полі бою для керування високоточною зброєю, навіть для боротьби з іракськими оперативно-тактичними ракетами СКАД. Це значить, що такі традиційні методи приховання інформації про дислокацію ракетних комплексів, як просторове маневрування в позиційному районі, уже неефективні.

Зрослі оперативні можливості технічних розвідок і використання їхніх даних дозволило віднести радіоелектронну боротьбу вже не до засобів бойового забезпечення, а до етапу бойових дій. Відповідно зросла роль захисту інформації.

Сьогодні одним з найбільш істотних об'єктів безпеки в оборонній сфері є інформаційні ресурси й інформаційна структура оборонного потенціалу країни (збройних сил і військово-промислового комплексу). Важливо, що всі сучасні засоби озброєння, військової техніки, системи управління військами й зброєю є системами критичних додатків з високим рівнем комп'ютеризації. Ці системи можуть виявитися досить уразливими з погляду впливу інформаційної зброї як у військовий, так і в мирний час. Останнє може привести до того, що до загрозливого періоду зброя стримування країни виявиться повністю або частково заблокованою за рахунок таємного впровадження їм в програмне забезпечення систем керування програмних закладок. Про реальність такої ситуації свідчить досвід локальних воєн останніх років.

Одні учасники інформаційного простору, які в різному ступені володіють навичками роботи з інформацією, можуть використовувати доступні їм інформаційні ресурси для зміни властивостей інформації, тобто являти загрозу іншим учасникам інформаційного простору.

Велику небезпеку представляє не тільки можливість несанкціонованого одержання конфіденційної інформації, але й запобігання вільного доступу до інформації, що повинна бути поширена й відома [250, с.16].

Як відзначає В. Пірумов, «інформаційний простір практично став театром воєнних дій, де кожна із протиборчих сторін прагне одержати і як можна довше втримувати перевагу, а якщо буде потреба - розгромити супротивника. Стає очевидним, що сторона, яка не розуміє або недооцінює зазначену обставину, приречена виявитися на узбіччі стовпової дороги цивілізаційного розвитку» [180, с.544].

Отже, національні інтереси України вимагають забезпечення сприятливих умов для політичного розвитку країни. Так, інтереси особистості перебувають в реальному забезпеченні політичних прав і свобод громадян, суспільство потребує зміцнення демократії, а інтереси держави виражаються в необхідності ефективного захисту конституційного ладу суверенітету й територіальної цілісності країни, встановлення й підтримки політичної стабільності, включаючи стабільність державної влади і її інститутів. На думку дисертанта, інтереси особистості в інформаційній сфері полягають у реалізації конституційних прав людини й громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного й інтелектуального розвитку, а також у захисті інформації, що забезпечує особисту безпеку.

На основі національних інтересів України в інформаційній сфері формуються стратегічні й поточні завдання політики держави з забезпечення інформаційної безпеки.

3.2. Особливості державної політики в області інформаційної безпеки

Суспільно-політичні проблеми в інформаційній сфері, що є системоутворюючим фактором життя суспільства, активно впливають на

стан соціально-політичної ситуації в країні, оскільки інформаційна функція державних органів являє собою реалізацію їхньої компетенції, прав і обов'язків відповідно до місця й призначення у державному механізмі й політичній системі суспільства. Проте тривалий час розкриттю суспільно-політичного значення інформаційної функції держави в наукових працях не приділялося уваги. Лише порівняно недавно російський дослідник Л.А. Морозова констатувала, що «на функції держави впливають також процеси інформатизації суспільства, створення загальнопланетарного інформаційного простору», і відзначила інформаційну функцію як основну функцію держави [238, с.9].

Держава завжди має певні ресурси й можливості для охорони свого інформаційного простору. До найважливіших напрямків такої діяльності можна віднести правове, організаційно-технічне й фінансово-економічне.

У правовій області держава вирішує завдання забезпечення своєї інформаційної безпеки в основному за рахунок розробки нормативних актів, що регламентують взаємини держави зі своїми контрагентами (як поза, так і всередині держави) в інформаційній сфері. У даному аспекті найбільш ефективні дії - внесення змін і доповнень у законодавство країни, що регулює це коло питань; усунення внутрішніх протиріч, пов'язаних з урегулюванням інформаційних відносин центра й регіонів, а також участі держави в міжнародних угодах; законодавчого розмежування повноважень в області забезпечення інформаційної безпеки між органами влади й управління, а також визначення мети участі в цій діяльності громадських організацій і окремих громадян; розробки актів, що встановлюють відповідальність юридичних і фізичних осіб за несанкціонований доступ до інформації; її протиправне копіювання, перекручування й протизаконне використання, навмисне поширення недостовірної інформації; розкриття конфіденційної інформації; використання в злочинних цілях службової інформації, що містить державну й комерційну таємницю; уточнення статусу іноземних закордонних агентств, ЗМІ й журналістів, а також інвесторів при залученні

ними іноземних інвестицій для розвитку інформаційної інфраструктури країни; визначення правового статусу організацій, що беруть участь в інформаційних обмінах в умовах глобалізації.

Організаційно-технічні методи забезпечення інформаційної безпеки включають: розробку й використання засобів захисту інформації й засобів контролю за їхньою ефективністю; розвиток захищених телекомунікаційних систем, підвищення надійності їхнього програмного забезпечення; створення засобів запобігання несанкціонованого доступу до інформації, що обробляється й спеціальних впливів, які спричиняють руйнування й перекручування інформації (боротьба з вірусами); виявлення технічних пристроїв, що представляють небезпеку для нормального функціонування інформаційних систем, запобігання й перехоплення інформації; удосконалювання засобів захисту при передачі, зберіганні й обробки інформації; сертифікацію засобів захисту інформації й стандартизацію цих способів; контроль за діями персоналу в інформаційних системах, які захищають; підвищення рівня професійної й спеціальної підготовки користувачів інформаційних систем і т.д. [187, с.240].

Фінансово-економічні методи передбачають: розробку програм забезпечення інформаційної безпеки й своєчасного фінансово-матеріального забезпечення функціонування систем захисту інформації; удосконалювання системи фінансування робіт, пов'язаних з реалізацією правових і організаційно-технічних методів захисту інформації; створення системи страхування інформаційних ризиків фізичних і юридичних осіб [187, с.240].

Суб'єкти інформаційної сфери й окремі елементи її інфраструктури можна об'єднати поняттям "інформаційна система", якою забезпечується одержання й обробка даних, видача результату або зміна власного зовнішнього стану [212].

Системний підхід до інформаційної безпеки вимагає визначення її суб'єктів, засобів і об'єктів, принципів забезпечення, джерел небезпеки, спрямованості небезпечних інформаційних потоків.

Суб'єктами інформаційної безпеки слід вважати ті органи й структури, які займаються її забезпеченням. Це можуть бути органи не тільки виконавчої, але й законодавчої, судової влади.

Основними елементами організаційної основи системи забезпечення інформаційної безпеки в Україні є Президент України, Верховна Рада України, Кабінет Міністрів України, Рада національної безпеки й оборони України, міністерства й інші центральні органи виконавчої влади, Національний банк України, суди загальної юрисдикції, прокуратура України, міські державні адміністрації й органи місцевого самоврядування, Збройні Сили України, Служба безпеки України, Державна прикордонна служба України й інші військові формування, створені відповідно до законів України.

Одним з найбільш важливих суб'єктів інформаційних відносин є держава. Звісно, що держава, будучи одним з головних суб'єктів процесу формування інформаційного суспільства, одночасно повинна бути гарантом її інформаційної безпеки. Органи державної влади й управління, у компетенцію яких входить регулювання соціально-політичних відносин в інформаційно-психологічній сфері, а також недержавні суб'єкти даної діяльності, що залучаються органами державної влади й управління для рішення завдань державного регулювання в інформаційно-психологічній сфері, виступають як суб'єкти державної інформаційної політики.

Держава займає особливе місце як серед суб'єктів державної інформаційної політики, так і серед суб'єктів забезпечення інформаційної безпеки, оскільки вона володіє унікальними засобами й силами протидії загрозам у даній сфері. Свою діяльність держава здійснює разом з індивідами й суспільством, але при цьому вплив держави на забезпечення безпеки є визначальним. Це положення закріплене законодавчо.

У той же час необхідно брати до уваги сутнісний дуалізм взаємовідносин особистості, суспільства й держави в області забезпечення безпеки. З одного боку, головна функція політики безпеки сучасної держави -

захист інтересів суспільства й громадянина, хоча історія знає чимало прикладів того, як держава, у свою чергу, виступала джерелом загроз безпеки особистості й суспільства. З іншого боку, особистість як об'єкт безпеки має двоїсту природу - вона має потребу в захисті й, у свою чергу, може виступати в ролі джерела загроз і викликів безпеки [208, с.13].

Суб'єкти державної інформаційної політики можна розділити на дві основні категорії: а) державні суб'єкти державної інформаційної політики; б) суб'єкти масового інформування й комунікації. У системі суб'єктів державної інформаційної політики державні суб'єкти розділяються на групи за наступними категоріями: 1) рівні влади й управління (центральний, регіональний, місцевий); 2) галузі державної влади (законодавча, виконавча, судова); 3) напрямки діяльності органів влади (органи громадянського, економічного управління, силові відомства, культура, зовнішньополітичні відомства).

У системі суб'єктів державної інформаційної політики суб'єкти масового інформування й комунікації розподіляються на групи за станом власності (державні ЗМІ й МК, контрольовані українськими фізичними й юридичними особами; недержавні ЗМІ й МК, контрольовані іноземними фізичними і юридичними особами) і за способами поширення інформації (електронні ЗМІ й МК, друковані ЗМІ й МК, Internet-ЗМІ й Internet-МК).

Як уважає російський дослідник А. Стрільцов, основний тягар реалізації державної політики в області забезпечення інформаційної безпеки лягає на органи виконавчої влади, що здійснюють на основі законодавства адміністративно-державне керівництво. Особливість реалізації функції забезпечення інформаційної безпеки полягає в тому, що кожний орган держави здійснює свою діяльність на базі використання інформаційної інфраструктури суспільства, виробляє й споживає інформаційні ресурси, має певні відносини із громадянами як представник власника державних інформаційних ресурсів, повинен уживати певні дії по забезпеченню зберігання ресурсів і безпеки функціонування інформаційних і

телекомунікаційних систем, мереж зв'язку, систем автоматизації управління [227, с.149-153].

На думку А. Сапожникової, «Необхідною умовою успішної реалізації державної політики безпеки є наявність стійкої системи взаємодії владно-політичних і соціально-економічних інститутів суспільства. Особливе значення в цьому плані мають добре налагоджені відносини між органами управління, силовими структурами й структурами громадянського суспільства. У демократичній політичній системі рольові й функціональні позиції всіх складових комплексу інститутів і процесів в області політики безпеки повинні бути сумісними із ціннісними пріоритетами громадянського суспільства, нормами прозорості й підзвітності, забезпечуючи ефективні можливості суспільної участі й контролю» [208, с.14].

В Україні політика інформаційної безпеки реалізується як системою інститутів публічної влади, так і інститутами громадянського суспільства, до компетенції яких відноситься вирішення питань про створення безпечних умов функціонування й розвитку інформаційної сфери. Тому, як уважає Б. Кормич, одним з факторів негативного впливу на ефективність захисту інформаційної безпеки є недостатній розвиток та інституціалізація громадянського суспільства в Україні, що могло б бути інструментом контролю за діяльністю органів публічної влади, механізмом, що забезпечує визначення й репрезентація національних інтересів усього українського суспільства. «Основні завдання все-таки вирішуються в рамках формалізованої складової механізму інформаційної безпеки, що представлена органами публічної влади. Так, серед дослідників існує думка, що рівень ефективності забезпечення безпеки перебуває в прямій залежності від здатності координувати зусилля різних відомств і формування певного «міжвідомчого співтовариства», діяльність якого спрямована на рішення конкретних поставлених завдань» [115, с.141].

Об'єктами небезпечного інформаційного впливу й, отже, інформаційної безпеки можуть бути: свідомість, психіка людей; інформаційно-технічні

системи різного масштабу й призначення. Якщо ж говорити про соціальні об'єкти інформаційної безпеки, то до них можна віднести особистість, колектив, суспільство, державу, світове співтовариство.

Зміст інформаційної політики досить об'ємний і містить у собі цілий комплекс складних процесів: від правового регулювання, свободи слова й доступу до джерел інформації до морально-етичних характеристик медіапродукції, її впливу на масову свідомість та інформаційну безпеку. Найпоширенішим можна вважати визначення інформаційної політики, дане В.Д. Поповим: «Інформаційна політика - це здатність і можливість суб'єктів політики впливати на свідомість, психіку людей, їхню поведінку й діяльність за допомогою інформації в інтересах держави й громадянського суспільства» [94, с. 24]. Її об'єктом є інформаційні суспільні відносини або відносини між суб'єктами, що здійснюють збір, формування, аналіз, поширення й використання інформації в інтересах особистості, суспільства й держави.

У більш вузькому розумінні об'єктом інформаційної політики як науки виступають масова свідомість, система засобів масової інформації й масової комунікації, інформаційні процеси, які відбивають, виражають, захищають права особистості й політику держави.

Предметом же інформаційної політики як галузі наукових знань вважають тенденції, закономірності розвитку інформаційної сфери, інформаційних процесів, методи аналізу й прогнозу їхнього розвитку, виявлення ефекту впливу ЗМІ й масових комунікацій на масову свідомість, на громадянське суспільство й державу.

Основними завданнями, що стоять перед інформаційною політикою як науковою дисципліною, можна вважати аналіз і прогнозування сучасних інформаційних процесів, розробку теоретико-практичних методів інформаційно-аналітичної роботи, а також забезпечення інформаційно-психологічної безпеки. Крім цього, інформаційна політика покликана розкрити фактори й механізми сприйняття, засвоєння, переробки,

осмислення людьми одержуваної інформації й вироблення ними своєї диспозиції, мотиву діяльності.

Поняття «інформаційна політика» звичайно трактується як спосіб поведінки з наявними інформаційними потоками й ресурсами з боку різних інституціональних суб'єктів (наприклад, держави або державних органів, або окремих організацій і установ, які можуть мати свої бачення та інтереси при роботі з інформацією). У рамках даного підходу інформація виконує чисто технічну функцію поряд з іншими ресурсами діяльності. У подібному контексті інформаційна політика, по суті, зводиться до чисто кількісного контролю за перебігом інформаційних потоків або контролю за розподілом потоку інформації для того, щоб інформація досягла наміченої цільової групи й набула заздалегідь запланований ефект.

При такому розумінні інформаційної політики інтереси її суб'єктів лежать за межами власне інформаційного простору. У рамках цих інтересів досягаються політичні, комерційні й будь-які інші цілі, у досягненні яких нові інформаційні можливості розглядаються як допоміжний засіб, що не змінює якісні характеристики цих інтересів і цілей. Інший підхід до визначення інформаційної політики полягає в розгляді її в аспекті впливу факторів матеріальної й віртуальної реальності епохи інформаційного суспільства. При цьому підході ключовим фактором виступає, насамперед, інформаційний простір (інформаційна дійсність). Саме виникнення в процесі переходу до побудови інформаційного суспільства особливого роду простору, у якому починають складатися свої специфічні форми поведінки й діяльності, якісно відмінні від тих, що існували на попередньому етапі суспільного розвитку, є одним з ознак глобального соціально-культурного перевороту другої половини XX століття. Специфіка цього простору виражається не стільки в багаторазовому збільшенні обсягу доступної інформації, скільки в характерних саме для нього правилах і учасниках, що відбуваються (віддзеркалюються) у ньому процесів.

Державна інформаційна політика повинна базуватися на концептуальних, наукових і методологічних розробках, систематизованих і об'єднаних у єдину концепцію, і її слід формувати як сукупність цілей, що відбивають національні інтереси в інформаційній сфері; стратегії й тактики управлінських рішень і методів їхньої реалізації, що розробляються і реалізуються державною владою для регулювання й удосконалювання як безпосередньо процесів інформаційної взаємодії у всіх сферах життєдіяльності суспільства й держави, так і процесів (у широкому змісті) технологічного забезпечення такої взаємодії [155, с.11–12].

Якщо в традиційних підходах до інформаційної політики питання природи інформації й форм її присутності у світі, як правило, не є головними при формуванні інформаційної політики, то визнання інформаційного простору як фактора глобальних змін на всіх рівнях соціальної модернізації робить їх ключовими при вибудовуванні стратегій діяльності й формуванні особливої політики в інформаційному полі. Серед факторів впливу сучасного інформаційного простору на якісні характеристики інформаційної політики можна виділити наступні: особливий тип знань, що забезпечує оформлення інформації в тих або інших мозаїчних конфігураціях; особливий тип комунікації, що задає способи поведінки в просторі інформаційних потоків і обмінів; особливий тип суб'єктів (учасників), що формує ціннісну й цільову структуру інформаційного простору [43, с.56].

Як вважають деякі політологи, є всі підстави визнати необхідним існування автономного політико-галузевого напрямку за назвою «політика інформаційної безпеки», що об'єднало б інформаційний компонент безпеки й політику його практичної реалізації в діяльності органів державної влади й керівництва [154, с.3].

З розвитком взаємозалежності, властивої сучасному світу, зберігаються міждержавні протиріччя, які є джерелами нестабільності й конфліктів. У сучасних міжнародних відносинах традиційні методи міждержавного протиборства трансформуються під впливом інформаційних технологій.

Об'єктивно зростаюча глобальність інформаційної сфери приводить до того, що створювана інформаційно-комунікаційна інфраструктура країни й національних інформаційних ресурсів виявляються об'єктами, досить вразливими для впливу з боку геополітичних конкурентів, терористичних організацій, кримінальних груп і окремих зловмисників.

З урахуванням цих факторів інформаційний розвиток України, який поки що помітно відстає від провідних промислово-розвинених країн, повинен здійснюватися в рамках системної й збалансованої державної інформаційної політики, спрямованої на активну протидію інформаційній агресії. У зв'язку з цим вважається необхідним розробити й прийняти Закон України «Про інформаційну безпеку», що відповідає Доктринам національної й інформаційної безпеки України.

Як витікає з Доктрини інформаційної безпеки України, діяльність органів виконавчої влади в сфері забезпечення інформаційної безпеки України повинна бути зосереджена на конструктивному об'єднанні діяльності держави, громадянського суспільства й людини по трьох головних напрямках: інформаційно-психологічному, зокрема відносно забезпечення конституційних прав і свобод людини й громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі заради утвердження загальнолюдських та національних моральних цінностей; технологічного розвитку, зокрема розвитку та інноваційного відновлення національних інформаційних ресурсів, впровадження новітніх технологій, створення, обробки та поширення інформації; захисту інформації, зокрема, забезпечення конфіденційності, цілісності й доступності інформації, у тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак [64].

На сучасному етапі актуалізувалася проблема захисту персональних даних та інформаційної недоторканності громадянина від несанкціонованого доступу до них. Державна політика, реалізована в цьому напрямку, крім

ідеологічної й правової основи, повинна мати організаційну складову. Варто прагнути до більш чіткого розмежування повноважень державних, суспільних і комерційних організацій, відповідальних за інформаційне забезпечення й контроль ситуації в цій сфері, побудові на законній основі в країні концептуально єдиної системи інформаційної безпеки.

Поки що формування інформаційної культури громадян у країні перебуває на початковій фазі, і суспільство потребує захисту від зазіхань на його інформаційну свободу. До числа проблем, що вимагають державного втручання, можуть бути віднесені, наприклад, відповідальність за поширення матеріалів, що ганьблять людську гідність, використання брудних інформаційних технологій для дестабілізації життя суспільства й т.п.

Аналіз нормативно-правової бази інформаційної безпеки свідчить про те, що багато документів містять протиріччя, неоднозначність тлумачень, декларативність і ін.

Незважаючи на те, що в останні роки здійснено ряд заходів, створено цілісні системи захисту державної таємниці й інформації, системи ліцензування діяльності організацій в області захисту інформації й системи сертифікації засобів захисту інформації, ця область, на думку фахівців, розвивається все ще вкрай нерівномірно. Фактично в Україні вже сьогодні проводиться певна технологічна модернізація інфокомунікаційного середовища й поступово розширюється сфера застосування нових інформаційно-комп'ютерних технологій, однак, цій діяльності приділяється слабка увага з боку виконавчої й законодавчої влади.

Форми й способи забезпечення інформаційної безпеки утворять той інструмент, за допомогою якого сили інформаційної безпеки вирішують весь комплекс завдань із захисту життєво важливих інтересів особистості й суспільства. Тому необхідне чітке юридичне оформлення при опрацюванні нормативних актів, що регулюють діяльність органів інформаційної безпеки.

Найважливіша вимога до обґрунтування способів, форм і механізмів їхньої реалізації полягає в абсолютному верховенстві права в кожній, у тому

числі й політичній діяльності. У свою чергу, кожний суб'єкт інформаційного процесу повинен мати відповідну правосвідомість, бути законослухняним, добре уявляти наслідки своїх дій і ступінь відповідальності у випадку порушення життєвих інтересів особистості, суспільства й держави. І це принципово, тому що застосування тих або інших способів залежить від того, чи є інформаційні загрози наслідком ненавмисних чи навмисних дій суб'єктів інформаційного процесу.

У першому випадку забезпечення інформаційної безпеки, як правило, здійснюється у формах інформаційного патронату й інформаційної кооперації, а в другому - у формі інформаційного протиборства.

Інформаційний патронат - основна форма забезпечення інформаційної безпеки фізичних і юридичних осіб з боку держави. Він має на увазі забезпечення органів управління державної системи інформаційної безпеки відомостями про дестабілізуючі фактори і загрози стану інформованості фізичних і юридичних осіб (інформаційне забезпечення) і захист життєво важливих інтересів цих осіб від інформаційних загроз (інформаційний захист).

При цьому інформаційне забезпечення включає збір (добування) відомостей про дестабілізуючі фактори й інформаційні загрози, їхню обробку, обмін інформацією між органами управління, силами й засобами системи інформаційної безпеки. Його основу становить збір (добування) необхідних відомостей, здійснюваний у процесі розвідувальної, контррозвідувальної і оперативно-інформаційної діяльності. Інформаційний захист досягається шляхом внесення в порядку законодавчої ініціативи законопроектів, що підпадають під юрисдикцію органів інформаційної безпеки, здійснення судового захисту, проведення оперативних заходів силами й засобами інформаційної безпеки.

Інформаційна кооперація є формою забезпечення інформаційної безпеки між рівноправними суб'єктами інформаційного процесу (фізичними, юридичними, міжнародними) і включає сукупність їхніх

взаємопогоджуваних дій для одержання відомостей про дестабілізуючі фактори та інформаційні загрози й захист від них доступними законними способами й засобами.

Для конкретного суб'єкта інформаційного процесу такими способами й засобами можуть бути:

- судовий захист прав і свобод у використанні інформації;

- адміністративний захист її життєво важливих інтересів в інформуванні з боку територіальних або відомчих органів безпеки;

- автономний захист прав і свобод в основному із застосуванням технічних засобів захисту особистої, сімейної й професійної таємниці.

У теперішній час, звичайно, більше розвинені способи й засоби захисту державної таємниці - той арсенал, із застосуванням якого повинна забезпечуватися інформаційна безпека держави як інституту політичної системи і як національно-територіального утворення. Основними способами її забезпечення в рамках міжнародного інформаційного співтовариства, мабуть, повинні стати юридичний захист важливих інтересів держави в області інформації з боку Міжнародного суду ООН і захист цих інтересів у рамках системи колективної безпеки з боку Ради Безпеки ООН.

Особливе місце в системі забезпечення інформаційної безпеки займає інформаційне протиборство. Корінна його відмінність полягає в тому, що воно ведеться державними органами інформаційної безпеки з формуваннями, які мають різне суспільне (державне) положення (фізичні особи, юридичні особи, суб'єкти міжнародного права) і зловмисно створюють інформаційні загрози життєво важливим інтересам особистості й суспільства. Ця обставина обумовлює значимість його цілей і більш широкий арсенал способів і засобів, що застосовуються для їхнього досягнення. У зміст інформаційного протиборства, крім інформаційного забезпечення й інформаційного захисту, входить комплекс заходів інформаційної протидії, спрямованих на блокування інформації, що цікавить різного роду зловмисників, і доведення до них неправдивих відомостей.

Внутрішньодержавні процеси переходу України до нових соціально-економічних відносин і політичного життя ставлять специфічні проблеми забезпечення інформаційної безпеки.

Стає очевидним, що посилання на внутрішні законодавства деяких західних країн, що забезпечують «безмежну» свободу інформатизації, не завжди підтверджуються на практиці. Скоріше навпаки, всі держави в тій чи іншій мірі регулюють порядок поширення й зміст інформації, що передається на їхній території. На перше місце в цьому випадку, як правило, виноситься необхідність забезпечення національної безпеки. Наприклад, у США діє ціла система норм, що забезпечують відповідальність засобів інформації. У США зросло число судових процесів проти засобів масової інформації за обвинуваченням у наклепі й перекручуванні фактів, великі інформаційні компанії все частіше притягуються до відповідальності.

Свобода одержувати й поширювати інформацію обмежена міркуваннями національної безпеки й в інших країнах [53].

Джерела інформаційних небезпек можуть бути природними (об'єктивними) й умисними. Перші виникають у результаті ненавмисних помилок і несправностей, випадкових факторів, стихійних лих і ін. Відомо, наприклад, що системи ПВО періодично видають помилкові сигнали тривоги через різноманітні технічні збої, але через ці сигнали приводяться у високий ступінь боєздатності стратегічні ракети, літаки - носії ядерної зброї. Навмисні інформаційні впливи здійснюються свідомо й цілеспрямовано. При цьому часто використовуються засоби масової інформації, радіоелектронної боротьби (РЕБ), спеціальні програмні засоби для комп'ютерів. Вони настільки ефективні, що їх можна виділити як новий клас зброї - інформаційний.

Виходячи з того, що інформаційна безпека на рубежі третього тисячоліття виходить на перше місце в системі національної безпеки, формування й проведення єдиної державної політики в цій сфері вимагає пріоритетного розгляду.

Оскільки всяка політика в правовій державі повинна будуватися на основі права, надто важливо визначити такі правові основи. Поки можна констатувати, що розвиток суспільних відносин у цій сфері істотно випереджає розвиток права із цих питань.

Так, наприклад, поки не прийнятий закон про публічну інформацію. Хоча спроби вже є. 2 листопада 2010 року у Верховній раді був зареєстрований законопроект "Про внесення змін у деякі законодавчі акти України про забезпечення доступу до публічної інформації)".

Проект закону (№ 7321), зокрема, пропонує викласти в новій редакції визначення поняття "Інформація", а саме: "Інформацією є будь-які відомості й/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді" (зміна статті 200 Цивільного кодексу).

Крім цього, документом передбачається викласти чинний закон "Про інформацію" у новій редакції. Зокрема, визначаються загальні правові основи реалізації права кожного на інформацію у всіх сферах життя як можливості вільно створювати, збирати, одержувати, передавати, виробляти й поширювати інформацію усно, письмово або іншим способом, а також обов'язок органів державної влади й місцевого самоврядування надавати доступ до офіційної інформації й так далі.

Відповідно до законопроекту, доступ до інформації про діяльність і рішення суб'єктів владних повноважень повинен здійснюватися в такий спосіб: оприлюднення інформації в засобах масової інформації та в офіційних друкованих виданнях, надання інформації по запитах, розміщення інформації на офіційному веб-сайті в мережі Інтернет, надання інформації через інформаційні служби суб'єктів владних повноважень.

Проектом пропонується встановити, що "обов'язковому оприлюдненню суб'єктами владних повноважень підлягають:

- інформація про діяльність суб'єктів владних повноважень, зокрема: основні завдання, повноваження, функції, організаційна структура й

нормативно-правові основи діяльності, крім випадків, коли ці відомості віднесені до інформації з обмеженим доступом;

- місцезнаходження, поштова адреса, номер телефону, факсу, адреса офіційного сайту в мережі Інтернет і електронної пошти, прізвище, ім'я та по батькові, номер службового телефону, адреса електронної пошти керівника органу, а також керівників структурних підрозділів;

- основні функції структурних підрозділів, розпорядок роботи й час прийому громадян;

- відомості про вакансії, порядок і умови проходження конкурсу на заміщення вакантних посад;

- перелік і умови одержання послуг, що надаються ними, форми й зразки документів, правила їхнього заповнення, перелік підприємств, установ і організацій, що належать до сфери управління;

- порядок складання, подачі запиту на інформацію, оскарження рішень суб'єктів владних повноважень, дій або бездіяльності, рішення суб'єктів владних повноважень".

Проект закону передбачає також контроль за забезпеченням доступу до публічної інформації, що повинен здійснюватися спеціальними органами, які визначають Верховна рада України й Президент України.

Документом пропонується встановити заборону на створення яких-небудь органів державної влади, установ, введення посад, на які покладають повноваження по здійсненню контролю за змістом інформації, розповсюджуваної засобами масової інформації. Також передбачено, що навмисне перешкоджання законній професійній діяльності журналістів і/або переслідування журналіста за виконання професійних обов'язків, за критику, що здійснюється посадовою особою або групою осіб за попередньою змовою, тягне за собою відповідальність відповідно до законів України.

Проектом закону визначаються також принципи діяльності ЗМІ й порядок акредитації журналістів.

Сьогодні склалися дві тенденції в органах державної влади у визначенні поняття й структури інформаційної безпеки. Представники гуманітарного напрямку зв'язують інформаційну безпеку тільки з інститутом таємниці. Представники силових структур пропонують поширити сферу інформаційної безпеки практично на всі питання й відносини в інформаційній сфері, по суті, ототожнюючи інформаційну безпеку з інформаційною сферою.

Інформаційна безпека суспільства, держави характеризується ступенем їхньої захищеності й, отже, стійкістю основних сфер життєдіяльності (економіки, науки, техносфери, сфери управління, військової справи, суспільної свідомості й т.д.) стосовно небезпечних, дестабілізуючих, інструктивних, що обмежують інтереси країни інформаційним впливам на рівні як впровадження, так і витягу інформації. Інформаційна безпека визначається здатністю нейтралізувати такі впливи.

На думку глави Служби безпеки України Валерія Хорошковського**,** в Україні є «належна система інформаційного забезпечення різних терористичних проявів. На сьогоднішній день опрацьовуються будь-які сигнали, які можуть, так чи інакше, впливати на цю ситуацію, на цю обстановку. Тобто, фактично ми в щоденному режимі опрацьовуємо цю проблематику».

Глава СБУ відзначив, що Україна готовить оновлену стратегію безпеки, яка повинна стати частиною європейської стратегії [239].

Формування комунікативної компетентності, здатності політиків і державних службовців звертатися з інформацією, ефективно реалізовувати її в національних інтересах, повинно бути пріоритетним завданням для нашої країни.

Як і будь-яка політика, політика в області інформаційної безпеки ґрунтується на певних принципах: 1) дотримання Конституції й законодавства України, а також загальновизнаних принципів і норм міжнародного права; 2) відкритість у реалізації функцій органів державної

влади, що передбачає інформування суспільства про їхню діяльність із урахуванням обмежень, установлених законодавством України; 3) правова рівність всіх учасників процесу інформаційної взаємодії поза залежністю від їх політичного, соціального й економічного статусу; 4) пріоритетний розвиток вітчизняних сучасних інформаційних і телекомунікаційних технологій.

Можна зробити висновок, що в основу єдиної державної системи інформаційної безпеки України повинні бути покладені наступні принципи:

1) законність, дотримання балансу інтересів особистості, суспільства й держави;

2) взаємна відповідальність суб'єктів забезпечення безпеки;

3) інтеграція систем національної й міжнародної безпеки.

Отже, в наш час довгостроковою стратегічною метою державної інформаційної політики України повинно стати формування відкритого інформаційного суспільства на основі розвитку єдиного інформаційного простору як простору цілісної держави, її інтеграція у світовий інформаційний простір з урахуванням національних особливостей та інтересів при забезпеченні інформаційної безпеки на внутрішньодержавному й міжнародному рівнях.

Процес формування й розвитку інформаційного суспільства свідчить, що його важливими політичними ознаками є подолання відчуження особистості від влади, взяття громадянським суспільством політичних інститутів під правовий контроль, перетворення держави в соціально відповідальний інститут суспільства, заснований на принципах відкритості, демократизму влади й соціального партнерства. Побудова демократичної правової держави можлива тільки при наявності налагодженої системи інформаційної взаємодії між державою й суспільством. Отже, держава, її структури й представники повинні виступати як споживачі й джерела інформації [238, с.22].

Сучасний стан забезпечення національної й інформаційної безпеки України потребує розробки науково обґрунтованої державної політики й стратегії в цій області, визначення системи національних цінностей, життєво важливих інтересів особистості, суспільства й держави, визначення зовнішніх і внутрішніх загроз цим інтересам, пошуку ефективних заходів для забезпечення безпеки в усіх її сферах.

Викладене дозволяє зробити висновок про те, що в забезпеченні інформаційної безпеки зацікавлена не тільки держава, але й суспільство в цілому. На думку Д. Кафтанчикова, недосконаліть державної інформаційної політики приводить до виникнення атомізованого мережного простору, коли державні, відомчі, корпоративні, муніципальні інформаційні мережі й системи виявляються дезінтегровані, а це на порядок ускладнює забезпечення їхнього захисту від протиправного впливу [99, с.23].

Сьогодні завданням першорядної важливості необхідно вважати створення надійної системи інформаційної безпеки, що повинна забезпечити захист як країни в цілому, так і кожного її громадянина від небажаних інформаційних впливів. Зокрема, ця система повинна відгородити населення країни від інформаційних впливів, що спотворюють об'єктивне сприйняття дійсності, а також забезпечити захист вищого керівництва країни від перекрученої, недостовірної інформації, яка утруднює або робить неможливим прийняття політичних або соціально-економічних рішень, адекватних реальній обстановці.

Можливе протистояння в інформаційній області виражається в спрямованому інформаційному впливі на громадян іншої країни для зниження конкурентоспроможності цієї країни у світовому просторі. Тому мета забезпечення безпеки населення України від неконтрольованого зовнішнього інформаційного впливу має першорядну важливість.

Це значить, що необхідне розширення правового поля, яке регулює суспільні відносини, пов'язані з одержанням, поширенням і використанням інформації, а, отже, - формування й подальший розвиток інформаційного

права як окремої галузі з міцною законодавчою базою, що зможе стати фундаментом для інтеграції України у світовий інформаційний простір. Пріоритет особистості, що знайшов відображення в законодавчій базі, можна розглядати як ознаку демократичності, що складається в українському суспільстві.

Велике значення мають подальші розробки інформаційного законодавства, що є основним інструментом реалізації й однією з основних сфер формування державної інформаційної політики. Насамперед, це стосується права громадян на свободу одержання інформації, відповідальності за ненадання й приховання інформації, за поширення недостовірної інформації й дифамацію, порядку й умов використання інформації обмеженого доступу, включаючи персональні дані, комерційну, службову й інші види таємниць, проблем інформаційного забезпечення формування громадянського суспільства й діяльності органів державної влади й місцевого самоврядування, розвитку засобів масової інформації, масової комунікації й зв'язку в умовах ринкової економіки, регулювання ринку інформаційної продукції й послуг і т.д.

Особливість сучасної державної політики в області забезпечення інформаційної безпеки полягає в тому, що, з одного боку, ця політика повинна перешкоджати поширенню політичних і релігійних поглядів, які загрожують стабільності суспільства, адекватно реагувати на інформаційні загрози. З іншого боку - забезпечувати дотримання конституційних прав і свобод людини й громадянина в області одержання інформації й користування нею, збереження й зміцнення моральних цінностей суспільства.

3.3. Відкрите суспільство: механізми забезпечення інформаційної безпеки

Основними напрямками забезпечення інформаційної безпеки є формування відкритого суспільства й усунення цифрової нерівності. Ці напрямки зв'язані між собою, й кожен з них включає цілий комплекс механізмів забезпечення інформаційної безпеки.

Формування відкритого суспільства пов'язане з розробкою механізмів діяльності органів, що забезпечують прозорість влади, доступу громадян до соціально й політично значимої інформації, регулювання суспільних відносин у мережі Інтернет і т.д.

Сучасне суспільство неможливе без інформаційного забезпечення всіх сфер його життєдіяльності. Один із ключових моментів у реалізації права на інформацію - доступ до неї. Держава забезпечує доступ шляхом офіційної публікації інформації, поширення її через ЗМІ, а також безпосереднім наданням документів і матеріалів зацікавленим особам, у тому числі відомостей, на основі яких ухвалені рішення, що стосуються права й свободи громадян. За своєю значущістю інформаційні ресурси є одним із ключових моментів реформування країни на сучасному етапі й формування «електронного громадянина».

У той же час функціонування державної служби в рамках демократії припускає, що державні службовці повинні виступати як споживачі інформації, тому що ефективно здійснювати процеси керівництва можливо тільки маючи достатню інформацію, споживаючи інформацію, що приходить від громадян, із засобів масової інформації. Державні службовці таким чином одержують можливість проводити коректування своєї діяльності, звіряючи управлінські рішення й дії з реакцією суспільства, в інтересах якого вони функціонують [238, с.22].

У Загальній декларації прав людини 1948 р. записано, що кожна людина має право на: життя, свободу й на особисту недоторканність (ст. 3); свободу думки, совісті й релігії; це право включає свободу міняти свою релігію або переконання й свободу сповідати свою релігію або переконання як одноосібно, так і спільно з іншими, публічним або приватним порядком у

навчанні, богослужінні й виконанні релігійних і ритуальних обрядів (ст. 18); свободу переконань і на вільне вираження їх; це право включає свободу безперешкодно дотримуватися своїх переконань і свободу шукати, одержувати й поширювати інформацію й ідеї будь-якими засобами й незалежно від державних кордонів (ст. 19).

Пізніше ці права й свободи знайшли своє відображення в ряді міжнародних договорів. Так у статті 10 Європейської конвенції про захист прав людини й основних свобод 1950 р. додатково було зазначено, що «свобода одержання і поширення інформації реалізується без будь-якого втручання з боку державних органів» (ст. 10). У статті 19 Міжнародного пакту про громадянські й політичні права (прийнятого в 1966 і вступив у силу в 1976 році) уточнюється, що «ці свободи відносяться до всякого роду інформацій, ідей та способів їхнього поширення». Ці права й свободи одержали також своє підтвердження в Конвенції СНД про права й основні свободи людини.

На кожному новому етапі науково-технічного прогресу людство стикається із черговими викликами інформаційної безпеки, вважає директор Російського наукового центру «Курчатовський інститут» з наукового розвитку Олексій Солдатов. Із цієї причини сьогодні роль захисту інформації підвищується до не баченого раніше рівня. На думку О. Солдатова, шукати рішення завдання забезпечення інформаційної безпеки доцільно не на шляху інформаційної непроникливості, а, навпаки, активно беручи участь в інформаційному обміні [73].

Дискусія навколо проекту Закону України «Про внесення змін у деякі законодавчі акти України про забезпечення доступу до публічної інформації», а також відкриття Радою Європи для підписання Конвенції про доступ до офіційних документів знову привернули увагу громадськості, у тому числі наукової, до проблем доступу до державної інформації.

Як відомо, Декларація принципів інформаційного суспільства необхідним елементом відкритого для всіх інформаційного суспільства

визначає забезпечення кожному можливості мати доступ до інформації, ідей і знань та вносити в ці області свій внесок. Цим обумовлена важливість розвитку законодавства в цій області й рішення правових проблем у зазначеній сфері кожною державою, що поставила собі за мету рух до інформаційного суспільства, основу якого становлять принципи відкритості й доступності кожному достовірної й актуальної інформації.

«Чим більше інформації для публічного доступу виходить від державних органів і стосується їхньої діяльності, тим менша ймовірність того, що таке суспільство зможе приховати випадки беззаконня, корупції або сваволі.

Відкрите й необмежене поширення інформації для публічного доступу підвищує безпеку й здоров'я суспільства, а також сприяє підвищенню рівня життя, тому що в громадян з'являється більше можливостей для прийняття усвідомлених рішень із питань власного повсякденного життя, навколишнього середовища й майбутнього.

Інформація для публічного доступу, створювана державними органами, може також сприяти науково-технічному прогресу суспільства. Бази фактичних даних, багато з яких створюються й поповнюються державними органами або на державні асигнування, є основою передових наукових досліджень, технологічних нововведень і функціонування ефективної освітньої системи» [109, с.14].

Дотримання конституційних прав і свобод людини й громадянина в області одержання й використання інформації віднесено до перших складових національних інтересів України в інформаційній сфері в Доктрині інформаційної безпеки України.

Як справедливо відзначає А. Таїров, «Відкритість влади є важливою ознакою демократичності політичного режиму, а потім і держави. Питання відкритості влади є багатоаспектним і складним, воно стосується багатьох напрямків функціонування системи державної влади, але серед його елементів основною є проблема забезпечення інформаційної відкритості,

тобто створення умов для доступу кожного громадянина до інформації щодо діяльності органів державної влади. Відкритість і прозорість державної влади є найважливішими характеристиками демократичної держави, а забезпечення відкритості - фактором існування будь-якого демократичного суспільства» [231, с.138].

Рішення проблеми прозорості починається із введення інституту розкриття державної інформації. Для розкриття інформації необхідно в рамках інформаційного регулювання визначити, яка інформація держави підлягає обов'язковому публічному розкриттю, а яка є інформацією з обмеженим доступом, наприклад, тільки для державних органів контролю. Існуюче законодавство поки не вирішує ці завдання у повній мірі і повинно бути скоректоване в ході експертної й суспільної дискусії. Після однозначного визначення складу публічної інформації вона повинна стати доступною не за іменним запитом, який розглядається оператором-чиновником, а через Інтернет, без участі людини, юридично достовірною, у будь-який момент часу й будь-якій особі, що звернулася.

У зарубіжній літературі доступ до офіційної інформації обговорюється у зв'язку з такими поняттями, як свобода інформації й транспарентність (прозорість) уряду [12].

Дослідники навіть пропонують використовувати спеціальний термін е-прозорість. Мова іде про ідею максимально можливої доступності інформації й діяльності державного апарату й формуванні механізму суспільного впливу на сферу приватного й державного адміністрування за допомогою представницьких інститутів [231, с.142].

В умовах інформаційного суспільства, як справедливо вважає І. Бачило, питання про прозорість діяльності органів виконавчої влади має особливе значення. Даний автор указує на той вплив, що має принцип прозорості на стан інформаційної й державної безпеки в цілому, на реальність інституту відповідальності як органів державної влади, так і державних службовців [14, с.288].

Інститут доступу до інформації природно зв'язний з таким основним принципом демократії, як свобода слова й друку. Але шлях від завоювання цієї свободи до забезпечення доступу до офіційної інформації був досить тривалим. У міру зміцнення громадянського суспільства найбільш розвинені країни й ті, які виникли після Другої світової війни (під їхнім впливом) міжнародні організації, йшли від проголошення свободи слова до прийняття положень про право на інформацію, на її пошук і вільне поширення.

Як відзначають експерти, навіть прийняття цього принципу ще не означає гарантованого доступу до відповідної інформації. Держава лише «допускає» суспільство до інформації, погоджуючись не перешкоджати доступу до неї і її поширенню, але не ставила за обов'язок державним органам і чиновникам вжити конкретних заходів для забезпечення такого доступу. І лише в останні десятиліття в законодавстві й практиці ряду провідних країн, а також у різного роду міжнародних документах відбувся перехід не тільки до проголошення, але й до забезпечення гарантій доступу до інформації, що встановлює обов'язки державних органів і їхніх представників, які випливають із цього принципу [8, с.56].

Дослідження закордонного законодавства показує, що особливо важливим є облік у національному законодавстві принципів, закріплених у міжнародних правових актах (таких, як Резолюція 2450 (XXIII) від 12.12.1968 Генеральною Асамблеєю ООН): принципу свободи обміну інформацією, принципів і процедур інформування громадськості про діяльність державних структур, а також принципу контролю держав над комунікаційною діяльністю, здійснюваною під їхньою юрисдикцією, регламентації порядку діяльності й здійснення контролю за комунікаціями, включаючи комплексну розробку державної політики в цій сфері. За останні 20 років закони про доступ громадян до інформації прийняті у Франції, Греції, Данії, Голландії, Бельгії, Португалії, Іспанії, Фінляндії й Італії. Для зарубіжних країн з різними правовими традиціями характерний підхід до проблеми інформаційної

безпеки із врахуванням таких загальних понять, як «автентичність», «доступність», «цілісність», «конфіденційність».

У ряді країн Європи (Нідерланди, Іспанія, Португалія, Австрія, Угорщина, Естонія, Бельгія й Румунія) право громадян на доступ до офіційної інформації закріплено конституційно. У Франції, Греції й Італії це право закріплене законодавчо. Удосконалювання законодавства в названій сфері активно йде у Великобританії, Німеччині, Естонії, Молдові, Польщі й ряді інших країн.

Положення про недоторканність приватного життя, про захист персональних даних утримуються в різних законодавчих актах, особливо в законах, що регламентують ведення медичних записів, зберігання інформації про споживчі кредити й ін.

Як показує практика зарубіжних країн, прийняття спеціальних законів про доступ до інформації істотно поліпшує ситуацію в сфері забезпечення права громадян на інформацію й інформаційну відкритість державних органів і установ. Однак один закон не вичерпує всю проблематику забезпечення транспарентності влади. Необхідний ефективний правозастосовний механізм нормативно й функціонально відрегульованих процедур і правил по забезпеченню свободи доступу до інформації.

Більшість країн, що мають відповідний досвід, вибудовують багато в чому подібну систему забезпечення свободи доступу до інформації, за допомогою якої здійснюється збалансована взаємодія державного апарату із громадянським суспільством.

Схеми взаємин у більшості країн дуже схожі: прийняті закони, що закріплюють право на доступ до інформації, законодавчо передбачений і функціонує спеціальний орган, що здійснює контроль за дотриманням законодавства й дає рекомендації з дотримання процедур при наданні інформації [109, с.14].

Державні органи самостійно ухвалюють рішення щодо надання або приховання інформації. У всіх державах законодавчо передбачається

категорія закритої інформації, що не підлягає поширенню. У більшості країн під дану категорію інформації підпадають: відомості, отримані секретним шляхом від іноземних держав, міжнародних організацій, місцевих і муніципальних регіональних утворень; інформація, що впливає на погіршення міжрегіональних і міжнародних відносин; інформація, що торкається інтересів національної безпеки; комерційна таємниця; таємниця приватного життя; фінансова, комерційна, наукова й технічна інформація, що належить уряду або представляє матеріальні загрозі інтересам держави [109, с.15].

Порівняльний аналіз законодавства показує, що правове регулювання інформаційної безпеки є найбільш ефективним, коли сформовані правові основи інформаційного суспільства, а інформаційна безпека в силу глобального характеру мереж зв'язку може бути забезпечена лише при міжнародній взаємодії [189, с. 18-19].

На думку дослідників, мова йде про загальносвітову тенденцію, про якісне зрушення в області забезпечення прав людини. Це зрушення є відповіддю на сучасну кризу демократії.

Здійсненню демократичних ідеалів народовладдя заважає, з одного боку, егоїзм індивідів, з іншого боку - спеціалізація й професіоналізація політики, високотехнологічні маніпуляції суспільною думкою.

Рух до забезпечення доступу до інформації відбувається завдяки тиску «знизу», з боку громадянського суспільства. Звичайно, важливе значення має прийняття відповідних законодавчих положень у розвинених країнах, закріплення цих новацій у численних документах ООН, Ради Європи й інших наднаціональних органах. Сприяє процесу розширення технічних можливостей доступу до інформації, надаваних Інтернетом, розвиток інтерактивних форм зв'язку [8, с.25].

Українська наукова література з питання, яке розглядається, носить головним чином юридичний характер, у чому ми мали можливість переконатися, аналізуючи ступінь вивченості проблеми. В основному це

роботи фахівців з різних галузей права, насамперед, з конституційного й інформаційного права. Аналіз показав, що українські дослідники-юристи явно віддають перевагу праву на інформацію. Варто відзначити, що Рекомендація 2002 р. Комітету Міністрів Ради Європи й відкрита в 2009 р. для підписання Конвенція Ради Європи присвячена саме доступу до офіційної інформації (офіційних документів), Так само - про доступ до інформації - називається, наприклад, закон, що уже майже тридцять років успішно працює й удосконалюється в Канаді.

Рівень інформування громадян про всі явища економічної, політичної, соціальної й правової дійсності, інформацією про які володіють відповідні державні й суспільні структури, є одним з показників рівня цивілізованості сучасного суспільства. Право на інформацію перебуває в ряді найважливіших конституційних прав і свобод людини й громадянина, які визнаються й гарантуються в Україні.

Сьогодні право людини вільно шукати, одержувати, передавати й поширювати інформацію займає почесне місце в ряді конституційних прав і свобод, проголошених Конституцією України. Визнання й гарантії права на інформацію в Українській державі відображають тенденцію наслідування вимогам міжнародних принципів і стандартів з прав людини. Ці принципи й стандарти знайшли своє втілення в основних міжнародних угодах про захист прав і свобод людини.

Сьогодні в Україні діє досить багато нормативних правових актів різного рівня, які стосуються питань формування різних видів загальнодоступних інформаційних ресурсів і доступу користувачів до відкритої інформації. Однак правове регулювання не покриває всього різноманіття сформованих відносин з реалізації права на доступ до інформації. Можна навіть сказати, що інформаційна сфера є безумовним лідером у кількості законів, які нею регулюють, - понад 20. Однак переважна їхня кількість в умовах швидкого розвитку новітніх технологій морально застаріла, і часто вони суперечать один одному.

Серед невирішених проблем у сфері забезпечення права на доступ до інформації, у першу чергу, слід зазначити відсутність єдиного нормативного правового акту, що закріплює основні права громадян і організацій в області доступу до інформації, основні принципи надання інформації й механізм реалізації права на доступ до інформації; чіткої регламентації завдань і функцій органів державної влади при формуванні відкритих державних інформаційних ресурсів і забезпеченні доступу до них громадян і організацій; єдиного порядку інформаційного обміну органів державної влади з громадянами й організаціями за допомогою використання інформаційних систем загального користування.

Це приводить до недостатньої ефективності правових норм, що регламентують питання доступу до відкритих інформаційних ресурсів, відсутності гарантій забезпечення права на доступ до інформації й говорить про необхідність законодавчого закріплення правової норми про доступність відкритої інформації, що утримується в інформаційних ресурсах. Розмаїтість видів відкритої інформації робить украй важким вироблення загальних критеріїв, на підставі яких інформація може бути віднесена до загальнодоступної. Вважається доцільним вирішувати питання про доступність інформації шляхом закріплення в нормативних правових актах, що регламентують створення й використання різних інформаційних ресурсів і систем, правових норм, які встановлюють відкритий доступ до конкретних видів інформації із складу цих ресурсів, при закріпленні загального принципу про відкритість інформації, не віднесеної, відповідно до закону, до категорії обмеженого доступу у відповідному законі. Крім того, при правовому регулюванні відносин, пов'язаних із забезпеченням доступу до інформації, необхідно акцентувати увагу на змістовному аспекті інформації й говорити про доступ до інформації як можливості сприйняти конкретний зміст.

Закріплене сьогодні в Конституції України право на інформацію, маючи особливу значимість і фундаментальний характер, тісно пов'язане з рядом інших основних прав і свобод людини. Це відноситься, насамперед, до

права на недоторканність приватного життя, особисту й сімейну таємницю, права на таємницю листування, телефонних переговорів, поштових, телеграфних та інших повідомлень, права на свободу думки й слова, на свободу масової інформації, права кожного на достовірну інформацію про стан навколишнього середовища, свободу всіх видів творчості й викладання, права на доступ до культурних цінностей.

Надаючи громадянам право на інформацію, Конституція України припускає певні обов'язки й відповідальність держави перед громадянами. Це відбивається, насамперед, у передбачених Конституцією України гарантіях прав і свобод людини й знаходить свій розвиток в обов'язках органів державної влади й місцевого самоврядування у безперешкодному здійсненню гарантованого права. Під гарантіями в юридичній науці звичайно розуміють систему соціально-економічних, політичних, моральних, юридичних, організаційних передумов, умов, засобів і способів, що створюють рівні можливості особистості для здійснення своїх прав. Їхньою найважливішою функцією є сприяння реалізації прав особистості, з боку суб’єкта, що їх гарантує, й, насамперед, держави.

25 липня 2008 р. Кабінет Міністрів України схвалив Концепцію проекту Закону України «Про доступ до публічної інформації». Необхідність такого закону викликана тим, що в Україні ще непоодинокі випадки, коли громадяни не можуть реалізувати своє право на інформацію, тому що в цьому їм відмовляють органи влади. Крім цього, деякій інформації, що перебуває в користуванні органів державної влади або органів місцевого самоврядування, надається статус конфіденційності. А це суперечить нормам Конституції України, Конвенції про захист прав людини й основних свобод 1950 року. У відповідності до статті 10 цієї Конвенції, кожна людина має право на свободу поглядів, одержання й передачі інформації без втручання органів державної влади.

Резолюцією Парламентської Асамблеї Ради Європи від 5 жовтня 2005 р. № 1566 «Про виконання обов'язків і зобов'язань Україною» органи

української влади покликані вдосконалити порядок правового регулювання доступу до інформації й розсекретити всі офіційні документи, закриті для загального доступу.

Планом заходів щодо виконання зобов'язань України, які випливають із її членства в Раді Європи, передбачене створення необхідних правових умов для реалізації права кожного на свободу вираження поглядів і доступ до інформації.

Доступ до інформації передбачений Законами України «Про доступ до публічної інформації» і «Про інформацію». 13 січня Верховна Рада прийняла в цілому закони про доступ до публічної інформації й про внесення змін у деякі законодавчі акти щодо забезпечення доступу до публічної інформації.

За основу законопроект «Про доступ до публічної інформації» був прийнятий 30 листопада 2010 року.

Закон про доступ до публічної інформації передбачає 5-денний строк відповіді на інформаційний запит або ж 48-годинний - у випадку надзвичайної ситуації.

Крім того, ці закони передбачають необхідність створення підрозділів або відповідальних у різних установах державної влади.

Відповідно до закону, доступ до інформації про діяльність і рішення суб'єктів владних повноважень повинен здійснюватися в такий спосіб: оприлюднення інформації в засобах масової інформації й в офіційних друкованих виданнях, надання інформації по запитах; розміщення інформації на офіційному веб-сайті, надання інформації через інформаційні служби суб'єктів владних повноважень.

Документ установлює, що «обов'язковому оприлюдненню суб'єктами владних повноважень підлягають: інформація про діяльність суб'єктів владних повноважень».

Закон передбачає контроль за забезпеченням доступу до публічної інформації, що повинен здійснюватися спеціальними органами, які визначають Верховна Рада й Президент України.

Документ забороняє створення органів державної влади, установ, введення посад, на які покладають повноваження по здійсненню контролю за змістом інформації, розповсюджуваної засобами масової інформації.

Також передбачено, що навмисне перешкоджання законній професійній діяльності журналістів і/або переслідування журналіста за виконання професійних обов'язків, за критику, здійснювану по відношенню до посадової особи або групи осіб за попередньою змовою, несуть відповідальність, передбачену законами України.

Закон також визначає принципи діяльності ЗМІ й порядок акредитації журналістів [259].

Відповідно до сучасних концепцій держава розглядається як інститут, що обслуговує суспільство, якому суспільство доручає виконувати необхідні для себе повноваження.

Така держава повинна забезпечувати широкий доступ своїх громадян і бізнесу до урядової інформації, насамперед, у сфері освіти, зайнятості, медичного обслуговування й соціального забезпечення, оподатковування, ліцензування й ведення бізнесу, державних закупівель і держзамовлення, міжнародних торговельних операцій, тобто доступ до правил гри, що визначають відносини між громадянами й бізнесом, з одного боку, і державою - з іншого. Її діяльність повинна бути прозорою, оскільки прозорість - єдиний спосіб мінімізувати корупцію й забезпечити належну відповідальність держави перед громадянами. Держава повинна надати громадянам канали комунікації, що дозволяють їм брати участь у виробленні самих правил гри й здійснювати контроль з їх дотримання, що повинно повернути довіру суспільства, підвищити якість і результативність прийнятих рішень. Сьогодні ця концепція домінує в реформах державного управління [71, с.87].

У наш час у багатьох державах розробляються й реалізуються концепції «електронного уряду», які ґрунтуються на створенні державних інформаційних ресурсів і на доступі до інформації про діяльність державних

органів влади. Лідерами серед таких країн є США, Сінгапур, Австралія, Нова Зеландія.

Ведеться активна робота зі створення «електронного уряду» і в Україні. Електронний уряд повинен забезпечити інтерактивну комунікацію між суспільством і владою, особисту участь громадян у процедурах формування й експертизи рішень, відкритість інформації про діяльність органів державної влади, розширення можливості доступу до неї.

Деякі дослідники розглядають проект «Електронний уряд» як інформаційну технологію, що дозволяє оптимізувати процедуру прийняття управлінських рішень і зробити її більш «прозорою» для громадян. У той же час інформаційно-комунікаційні технології входять у зону підвищеного ризику, що вимагає забезпечення інформаційної безпеки. Зокрема, можна говорити про формування ризиків, обумовлених процесом інформатизації й розширенням доступу до колосальної кількості різноманітних даних.

Аналіз зарубіжного досвіду створення «електронної держави» або «електронного уряду» показує, що вже біля десяти років у розвинених зарубіжних державах для реалізації національних інтересів створюються «електронні уряди», оскільки одночасно з розвитком інформаційного суспільства необхідні системні, добре опрацьовані зміни й у державному управлінні [189, с.28].

Значимість проектів «електронного уряду» полягає в скороченні витрат, витрат часу простих громадян, часу й засобів бізнесменів і в тій доданій вартості, яку приносять ці системи суспільству. Становлення інформаційного суспільства в ряді країн світу свідчить, що саме в даному напрямку відбувається розвиток новітніх технологій функціонування державної служби. У той же час регламенти роботи органів державної влади практично не підтримують оперативне інформаційне обновлення інтернет-сайтів, які нерідко не містять необхідних відомостей про порядок і умови надання послуг громадянам і організаціям. Відсутній доступний єдиний реєстр

державних послуг з інформацією про умови їхнього одержання, а також загальна інформаційно-довідкова система із взаємодії населення з органами влади [189, с.28].

Той факт, що розвиток і поширення інформаційно-комунікаційних технологій носить нерівномірний, дискретний характер, є причиною нової форми соціальної нерівності - цифрової нерівності. Її суть полягає в тому, що середовище, яке виникло в ході інформатизації, виявляється в різному ступені доступним як людям і організаціям, так і країнам міжнародного співтовариства в цілому. При цьому ті, хто має можливість і здатний ефективно використовувати нове інформаційне середовище для свого розвитку, одержують перевагу перед тими, хто цього зробити не може.

Мова йде про те, що в ході інформаційної революції виникає й навіть збільшується розрив між тими, хто зміг скористатися благами інформаційних ресурсів, й іншими, які в силу особливостей свого історичного розвитку не мають доступу або можливості користуватися ресурсами інформаційного суспільства, а тому й не можуть стати його учасниками. Це явище прийнято називати «цифровим розривом». Однак проблема освоєння інформаційних ресурсів існує не тільки між розвиненими державами й країнами, що розвиваються, але й усередині кожної держави. Розвиток інформаційних технологій відбувається настільки стрімко, що «цифровий розрив» збільшується гігантськими темпами, зміцнюючи нерівність у світі й тим самим створюючи нові загрози й проблеми світового розвитку. Головною причиною «цифрового розриву» є стихійність і не контрольованість технологічного розвитку. Нерівномірний розподіл інформаційних ресурсів є одним із джерел загрози інформаційній безпеці. Ефективне застосування ІТ, насамперед у виробництві товарів і послуг, надає деяким країнам істотні конкурентні переваги, що впливають на загальне економічне зростання держави.

Усунення цифрової нерівності означає вирівнювання можливостей регіонів у сфері використання інформаційно-комунікативних технологій, має

на увазі створення єдиного інформаційного простору, інформатизацію органів державної влади, створення загальнодоступних інформаційних центрів загального доступу, підвищення комп'ютерної грамотності й доступності інформаційних технологій для населення.

М.А. Болокова пише, що монополія на переважаючий доступ до інформації веде до посилення соціальної нерівності. Нерівномірний розподіл інформації, що спостерігається в суспільстві, її неоднакова доступність для різних індивідуумів приводять до того, що одні індивідууми одержують інформаційну перевагу перед іншими, котра поступово трансформується в економічну, соціальну або політичну переваги [26, с.4].

Концентрація засобів інформації й комунікації в руках інформаційно й матеріально забезпечених шарів суспільства може привести до монопольного впливу на політичні інститути й суспільну думку, до розширення можливості маніпулювання свідомістю людей, до загроз інформаційно-психологічної безпеки особистості.

Зв'язок проблеми цифрової нерівності із проблемою стійкого розвитку полягає в тому, що політична система стає стійкою, коли її основні параметри, її критерії пропорційно зв'язані між собою. Якщо відбувається деформація критеріїв, тобто, одні коефіцієнти системи набагато перевищують задані обмеження, то система стає нестійкою [29, с.6]. Поряд із цим є й інші причини, що перешкоджають розвитку відкритого суспільства. Не менш важливою є небезпека залежності державного апарату від інформаційних комунікацій, що використовуються ним. Впровадження в систему управління ІКТ супроводжується появою безлічі варіантів для зовнішнього втручання в роботу органів державної влади й місцевого самоврядування, неузгодженості їхньої діяльності, дестабілізації загальної політичної обстановки в регіоні. Кожний будь-який значимий вплив ззовні неминуче приведе до дестабілізації роботи органів державної влади на всіх рівнях.

Одночасно із захистом інформаційних систем і засобів комунікації важливою є проблема захисту самої інформації, запобігання загрози несанкціонованого доступу й витоку персональних даних, що накопичуються різними структурами, у тому числі органами державної влади, а також таємного збору інформації, що становить особисту й сімейну таємницю, відомостей про приватне життя.

Законодавство європейських країн, дотримуючись вимог Європейського союзу, установлює, що збір особистої інформації проводиться тільки в законних цілях: особи, інформація про які збирається, повинні бути оповіщені й мати право доступу до інформації, що їх стосується, можливість змінити або вилучити неправильну інформацію, право на відшкодування збитку в судовому порядку у випадку порушень їхніх прав. Національні закони захищають особисту інформацію, насамперед, в області охорони здоров'я, фінансів.

Європейське законодавство припускає створення органів, що контролюють автоматизовану обробку особистих даних, розгляд скарг на порушення прав. Такі органи діють незалежно й мають право припиняти збір даних, якщо виявлені порушення прав і свобод. У більшості країн, де прийняли подібні закони, встановлена посада Уповноваженого в сфері інформації.

Керівництво інформаційними відносинами, що формуються, вимагає більшої погодженості у взаємодії державних структур. В умовах переходу до інформаційного суспільства держава змушена перебудовувати державний апарат, створювати нові структури, що забезпечують однаковість інформаційної політики державних структур.

Також в якості цілей комп'ютерних атак найчастіше є: виведення з ладу основних комунікаційних вузлів урядової інформаційної інфраструктури (як правило, за допомогою використання «мережних черв’яків» і вірусних атак); знищення небажаної інформації на урядових серверах; підміна інформаційних ресурсів або цілих сторінок на веб-серверах; порушення

конфіденційності урядового зв'язку; здійснення несанкціонованого доступу до ресурсів Інтернету. Як показує практика, дані цілі часто комбінуються, що може викликати не тільки неузгодженість діяльності державних установ, але й урядову кризу.

Не можна забувати про те, що «культурна стандартизація, будучи наслідком інформаційної відкритості, підриває колись замкнуті культурні ідентичності. Виживають лише ті культури, які здатні адаптуватися до мінливого світу, до сприйняття новітніх досягнень світової цивілізації, не втрачаючи при цьому своєї самобутності. Яскравий приклад такої адаптації - японська культура. Хоча є й протилежні приклади: це й іспанська, і турецька, і мексиканська, і аргентинська, і багато інших культур, що не витримали зіткнення з натиском культурної уніфікації. Вони збереглися лише як культури, умовно говорячи, фольклорні: іспанська корида, мексиканська кухня, аргентинське танго» [122, с.10]. «Крім того, глобалізація наполягає на універсалізації ціннісних орієнтирів. За допомогою масових інформаційних технологій (у першу чергу телебачення й Інтернету) вона наочно демонструє переваги західної моделі розвитку й, відповідно, західних цінностей: індивідуальної свободи, прав людини, демократичних механізмів, ринкової економіки, правової держави, громадянського суспільства, що наймає цю державу.

Глобалізація створює переваги для найбільш розвинених у соціально-економічному й технологічному змісті держав (США, країн Євросоюзу, Японії), що веде до зростаючого розриву між ними й економіками, що розвиваються. З іншого боку, саме розвинені країни - у силу накопиченого багатства, способу життя, цінностей і поведінкових стереотипів - стали в умовах глобалізації й створення мережного суспільства найбільш вразливими для нових викликів і загроз національній безпеці. Поширення телебачення, що зробило загальнодоступними образи й стандарти недосяжно багатого західного суспільства, стимулювало в деяких бідних країнах (насамперед мусульманського світу) хвилю антизахідних настроїв» [122, с.11].

Таким чином, у сучасному глобалізованому світі держави, що підтримують національні «ринки лояльностей», або, іншими словами, що прагнуть зберегти національну й культурну ідентичність як заставу соціальної й політичної стабільності, стикаються із проблемами інформаційної експансії з боку інших держав і транснаціональних ЗМІ. Поширення Інтернету, кабельного й супутникового телебачення ускладнює контроль держави над інформаційними потоками. М. Прайс відзначає, що існує два можливих типи реагування держави на даний виклик. Саме М. Прайс увів у науковий оборот понятті «ринок реальностей» - особливий ринок, суб'єкти якого використовують регулювання інформаційних потоків, створюючи свого роду «інформаційний картель». Держава є найважливішим учасником «ринку лояльностей». Кожна держава, як стверджує М. Прайс, «веде зі своїми громадянами розмову про законність свого існування. У цій розмові держава займається самовиправданням, жадаючи від громадян лояльності». Підмостки для цього постійного діалогу й надають ЗМІ. Звідси - прагнення держави контролювати їх.

По-перше, держава прагне захистити свій інформаційний простір від небажаного інформаційного впливу за допомогою різноманітних протекціоністських заходів, підтримки національних мовців і правових обмежень діяльності зовнішніх ЗМІ в межах власних державних кордонів.

По-друге, держава прагне впливати на інформаційний простір інших держав. Ці цілі досягаються різними способами: від вироблення домовленостей і все більш ефективного використання новітніх технологій до силових методів впливу [194, с.24].

Після відомих подій 11 вересня 2001 року проблема державного контролю ЗМІ загострилася з новою силою, і держави активізували свої зусилля в цьому напрямку. Як відзначає В. Орлова, «Сьогодні держава стає все більш активною в інформаційній сфері... Політичні стратегії урядів реалізуються за допомогою втручання в медіапростір інших держав, і метою стратегічної інформаційної інтервенції є зміна політичного клімату й

суспільних настроїв у країні-мішені... З іншого боку, як показує практика, уряди розвинених країн можуть контролювати, обмежувати в доступі на території інших держав глобальні телемережі новин і Інтернет. Так, CNN ледве було не зняли із супутникових систем в Ізраїлі в 2002 р.: ізраїльська влада була не задоволена висвітленням близькосхідної кризи американською телекомпанією, вважаючи, що CNN активно підтримує палестинців. BBC World протягом шести років (з 1994 по 2000 р.) залишалася практично закритою для Китаю, після того як допустила критику на адресу китайського уряду. У Китаї закритий доступ до деяких онлайнових ЗМІ. В 2001 р. за допомогою дипломатичних переговорів із владою Катару уряд США намагався «приборкати» арабську телемережу новин AL-Jazeera. Війна в Іраку 2003 р. остаточно утвердила можливість силового рішення у відношенні небажаних ЗМІ: цілями американських військ стали іракське телебачення й радіо, а відкриття англомовного сайту AL-Jazeera, намічене на березень 2003 р., було припинене (за офіційною версією, через збиток, нанесений хакерами) [160, с.54].

На початку 2011 р. під час політичної кризи в Єгипті невдоволення єгипетської влади також викликала діяльність телеканалу AL-Jazeera, у результаті чого шість журналістів цього каналу навіть були затримані.

Китайська влада має намір за допомогою інтернет-рейдів припинити поширення інформації "закордонними ворожими силами", передає Associated Press. За словами представника китайського уряду, Пекін має намір підсилити блокування шкідливої інформації з інших країн. Він не повідомив, якого роду ресурси збираються блокувати чиновники.

Нове рішення є частиною великої програми у боротьбі з мережною порнографією, азартними іграми й шахрайством. У рамках цієї програми вже були закриті тисячі ресурсів у китайському сегменті Мережі.

Крім того, фільтрація трафіка широко використовується в боротьбі з опозицією й критикою уряду. Так, розвідувачі, що перебувають у материковому Китаї, зобов'язані піддавати цензурі свої результати. У березні

з китайського ринку пішов Google, що відмовився від фільтрації своєї пошукової видачі.

У китайському сегменті Інтернету налічується понад 400 мільйонів користувачів. У середині квітня в країні створене нове відомство з Інтернет-Цензури. Воно стежить за повідомленнями в соціальних мережах, блогах і форумах [108].

Що стосується країн пострадянського простору, то тут найбільш радикальну політику в інформаційній сфері проводиться Білорусією. У Білорусі оголошена обов'язкова - до 1 липня 2010 р. - державна реєстрація всіх онлайн-ресурсів, а робота будь-якого сайту в країні, що не пройшов реєстрацію, буде вважатися незаконною, відповідно до постанови білоруської Ради міністрів.

Всі власники ресурсів, які хочуть пройти реєстрацію й працювати з 1 липня в рамках закону, повинні подати в Міністерство зв'язку й інформатизації Білорусі заяву, у якій вказати: найменування юридичної особи або прізвище, ім'я, по батькові (ПІБ) індивідуального підприємця, код країни (мається на увазі країна, у якій зареєстроване доменне ім'я), ПІБ керівника, місце знаходження юридичної особи, адреса індивідуального підприємця, контактний телефон, адреса електронної пошти, відомості з Єдиного державного регістра юридичних осіб і індивідуальних підприємців (ЄДР), договір власника ресурсу з постачальником інтернет-послуг, дані про права юридичної особи або індивідуального підприємця на зазначені ресурси. Для інтернет-сайту вказуються: опис ресурсу, використовувані мережні (IP) адреси, доменні імена ресурсу, реєстраційний номер центру обробки даних, який здійснює хостинг ресурсу, тип хостинга, що використовує ресурс.

Подібні заяви на реєстрацію будуть подавати не тільки власники сайтів, але й постачальники інтернет-послуг, а також власники центрів обробки даних [19].

А з 1 липня 2010 року уряд Білорусі зобов'язав власників комп'ютерних клубів і інтернет-кафе збирати й зберігати дані про особистих відвідувачів. Відповідно до постанови, користуватися послугами інтернет-кафе буде дозволено тільки тим, хто пред'явить документи. При цьому дані про особистість відвідувача персонал закладу зобов'язаний фіксувати й зберігати. Крім того, персоналу пропонується вести електронний журнал, у який включаються відомості про "доменні імена або IP-Адреси інтернет-ресурсів, з якими користувач здійснив з'єднання". Дані про відвідувачів адміністрація інтернет-кафе зобов'язана зберігати відповідно до підписаного на початку 2010 року указу. В указі також порушується тема контролю за відвідувачами інтернет-кафе, щоправда, вимоги до власників закладу були менш конкретні.

Положення указу стали об'єктом критики з боку журналістів і правозахисників. На їхню думку, влада, зокрема, створила умови для обмеження доступу громадян до опозиційних сайтів і блокування цих ресурсів [18].

Що стосується України, то в телевізійних кабельних мережах, якими користується понад 20 мільйонів громадян України, частка іноземних телепрограм перевищує 66 %. За даними Національної ради України з питань телебачення й радіомовлення, частка творів українських авторів і виконавців у радіоефірі становить 50 % - а це гранично низький, відповідно до Закону, рівень. Частка творів, що виконується державною мовою, менша третини - 30 % [67].

А в лютому 2011 р. Верховна рада України скасувала 50-відсоткову квоту музичних творів українських авторів у теле- і радіоефірі. Представники музичних медіа вважають, що скасування квот активізує розвиток вітчизняного шоу-бізнесу, однак продюсери побоюються витіснення з ефіру національного продукту. Це не перша спроба заперечити 50-відсоткову квоту на національний аудіовізуальний контент. В 2006 році власник радіокомпанії "Гала" Джозеф Лемир подав в Арбітражний трибунал при Міжнародному центрі за рішенням інвестиційних суперечок (ICSID) позов до уряду України.

Пан Лемир, зокрема, хотів заперечити норми закону "Про телебачення й радіомовлення", які квотують музичні здобутки українських виконавців. Але своїм рішенням від 14 січня 2010 року трибунал відмовив йому в задоволенні цієї частини позову, визнавши право держави на підтримку національної культури [199].

Щоденник «Коментарі» у результаті дослідження на тему «Коли вмре українська мова?» дійшов висновку, що «Катастрофічність процесу буде підсилюватися тим, що все нові й нові регіони в результаті їхньої русифікації будуть перетворюватися в русифікаторські. Критичну риску в 50% уже в 2012 році може перейти Запорізька область, в 2019 році - Одеська, в 2021 році - Харківщина. Приблизно в 2042 році наступить черга Дніпропетровщини, в 2045 році - Миколаївщини, в 2053 році - Херсонщини. (У той же час Сумщина вподібниться нинішній Миколаївщині, а Полтавщина - Херсону). ДО 2056 року в цілому по Україні частка, яка називає рідною мовою українську, стане менше частки тих, хто буде вважати себе русифікованими» [104].

Таким чином, необхідність захисту власного інформаційного простору повинна стати одним із пріоритетних напрямків державної політики по забезпеченню інформаційної безпеки України.

Висновки до розділу 3

Основними компонентами системи інформаційної безпеки виступають: загрози життєво важливим інтересам суспільства в інформаційній сфері, а також пов'язані з ними небезпеки, виклики й ризики; і життєво найважливіші інтереси суспільства, держави й особистості, що підлягають інформаційному захисту; основні заходи, проведені суб'єктами держави й громадянського суспільства, з нейтралізації загроз, небезпек і ризиків у сфері інформаційної безпеки. У системному вираженні інформаційна безпека України виступає частиною загальної системи національної безпеки, що

нейтралізує й запобігає загрози, небезпеки й ризики, які виникають в інформаційній сфері розвитку пострадянської України.

Нейтралізувати вплив інформаційних загроз покликана єдина державна система інформаційної безпеки України. Державна система інформаційної безпеки – це організаційне об'єднання державних органів, сил і засобів інформаційної безпеки, що здійснюють свої функції на основі закону й під контролем і захистом судової влади. У завдання цієї системи входить: виявлення й прогнозування появи дестабілізуючих факторів і інформаційних загроз життєво важливим інтересам особистості, суспільства й держави; здійснення комплексу довгострокових і оперативних заходів для їхнього попередження й усунення; створення й підтримка в готовності сил і засобів забезпечення інформаційної безпеки [180, с.544].

Інформаційна безпека визначається здатністю держави, суспільства, особистості: забезпечувати з певною ймовірністю достатні й захищені інформаційні ресурси й інформаційні потоки для підтримки своєї життєдіяльності й життєздатності, стійкого функціонування й розвитку; протистояти інформаційним небезпекам і погрозам, негативним інформаційним впливам на індивідуальну й суспільну свідомість і психіку людей, а також на комп'ютерні мережі й інші технічні джерела інформації; виробляти особистісні й групові навички й уміння безпечної поведінки; підтримувати постійну готовність до адекватних заходів в інформаційному протиборстві, ким би воно не було нав'язано.

Держава в силу своїх універсальних можливостей повинна стати головним учасником політики в сфері інформаційних технологій. Тому що саме сучасна держава, маючи у своєму розпорядженні широкі асортименти прийомів і засобів, здатна робити як стимулюючий, так і обмежуючий вплив на розвиток інформаційно-комунікаційних технологій для забезпечення інтересів людини, суспільства й держави. Роль держави в даному контексті полягає у своєчасній і ефективній профілактиці окремих інформаційно-

комунікаційних процесів з метою нейтралізації потенційної небезпеки деяких з них для людини, суспільства й держави.

Дослідження питань інформаційної безпеки України показало, що її рівень повинен відповідати потребам держави й громадянського суспільства. Для цього необхідно перебороти ряд об'єктивних і суб'єктивних проблем. Зокрема, об'єктивними проблемами варто вважати відставання вітчизняної інформаційної інфраструктури, технологій від передових закордонних зразків, безсистемне поширення на території країни глобальних електронних комунікацій.

До суб'єктивних проблем варто віднести: деструктивну активність закордонних суб'єктів політики, позасистемної політичної опозиції, транснаціональної злочинності, а також недостатній рівень організаційної, ідеологічної й технологічної готовності органів державного й муніципального управління протистояти загрозам, які виникають.

Автор виділяє принципи, на основі яких повинна реалізовуватися державна інформаційна політика:

– баланс інтересів особистості, суспільства й держави в інформаційній сфері;

– дотримання Конституції України, законодавства України, загальновизнаних принципів і норм міжнародного права;

– відкритість у реалізації функцій органів державної влади і суспільних об'єднань;

– правова рівність всіх учасників процесу інформаційної взаємодії незалежно від їх політичного, соціального й економічного статусу, що ґрунтується на конституційному праві громадян на вільний збір, одержання, передачу, виробництво й поширення інформації будь-яким законним способом;

– пріоритет розвитку вітчизняних сучасних інформаційних і телекомунікаційних технологій, виробництва технічних і програмних засобів, спрямованих на вдосконалення національних телекомунікаційних мереж,

їхнє підключення до глобальних інформаційних мереж з метою дотримання життєво важливих інтересів України.

Проаналізувавши сучасний стан українського суспільства, можна помітити, що теоретично сформульовані принципи державної політики в сфері забезпечення інформаційної безпеки далеко не повністю реалізовані. Наприклад, що стосується другого принципу (дотримання Конституції й законодавства, норм міжнародного права), то вважається, що тут стан найбільш задовільний. Однак невирішених проблем ще досить багато. Правда, прикладів з порушенням безпосередньо норм Конституції (принаймні, значимого характеру) не виявляється, але що стосується законодавства, то такі приклади є (наприклад, робота тих або інших фірм в галузі захисту інформації без передбачених законодавством ліцензій, і причому не завжди в цьому винні самі фірми).

Що ж стосується дотримання норм міжнародного права, то отут чимало проблем, пов'язаних з необхідністю гармонізації українського законодавства з міжнародним. Причому робити це треба без шкоди для національної безпеки країни, що в ряді випадків досить непросто.

Особливо слід відзначити другий принцип - відкритість інформації в діяльності органів влади. Хоча твердий режим закритого суспільства в нас у країні давно вже відмінений (точніше зруйнований), нам все-таки ще далеко до того ступеня відкритості органів влади перед суспільством, що характерний для справді демократичних держав. Відповідні приклади із цієї області дуже часто подаються в ЗМІ.

Ще одна проблема, що не знайшла, на нашу думку, свого рішення в рамках даного принципового положення. Вона стосується громадянського контролю за діяльністю державних органів в інформаційній сфері. Тим часом з метою забезпечення своєї безпеки суспільство повинно цілеспрямовано домагатися активної участі у формуванні політики безпеки (у тому числі інформаційної), розширювати соціальний контроль за державними органами, інститутами й силами забезпечення національної безпеки в різних її аспектах.

Не можна не погодитися з думкою російського дослідника Н. І. Зінченка, відповідно до якої здійснення соціального контролю за ними - основна проблема сучасного російського суспільства, що довгий час не допускався державою в цю сферу [88, с.183].

Ще один принцип - правова рівність учасників інформаційних відносин. Практично завжди у відповідних документах нормативно-правового характеру ця теза декларується, але ефективних механізмів її реалізації чи часто нема, чи вони недосконалі. Візьмемо, наприклад, питання про рівний доступ всіх членів суспільства до відкритої інформації. У плані нашого руху до інформаційного суспільства, коли інформація стає одним з найбільш значущих ресурсів, це положення приймає найбільш принципове значення. Однак його реалізація напряму практично неможлива. Так, інформація, на створення якої власник затратив певні засоби, природно й поширюється за плату. Звідси не всі члени суспільства однаковою мірою можуть нею користуватися. Отже, тут потрібні якісь соціальні інститути вирівнювання прав.

Наступний принцип - пріоритетний розвиток вітчизняних сучасних інформаційних і телекомунікаційних технологій. З одного боку, на сучасному етапі, важко уявити собі могутніший важіль для підйому економіки країни в цілому, ніж ця найбільш наукомістка й динамічна галузь, що розвивається. З іншого боку, без власних інформаційно-комунікаційних технологій нам справжню незалежність і безпеку України не забезпечити. Поки ми в цій області не вийшли на передові позиції.

Таким чином, оскільки навіть на принциповому рівні Доктрину інформаційної безпеки не можна вважати цілком реалізованою, то це веде до досить критичних оцінок інформаційної політики.

Отже, можна зробити висновок, що діяльність держави як суб'єкта розвитку інформаційних відносин і забезпечення інформаційної безпеки за останні роки здійснювалася не зовсім активно й послідовно.

Утвердження Доктрини інформаційної безпеки закріпило офіційну систему поглядів на зміст стратегічних національних інтересів України в інформаційній сфері, загроз цим інтересам, методи протидії загрозам і систему забезпечення інформаційної безпеки в довгостроковій перспективі. Доктрина створила політичну основу узгодження діяльності органів державної влади з питань реалізації національних інтересів в інформаційній сфері й захисті їх від зовнішніх і внутрішніх загроз. Вона намітила напрямки державної політики по забезпеченню практичної участі України в діяльності міжнародного співтовариства з досягнення цілей, намічених Окинавською хартією глобального інформаційного суспільства [166].

Реалізація національних інтересів в інформаційній сфері, закріплених у Доктрині, на думку її розробників, повинна знаменувати створення матеріальних, економічних і соціальних умов, що забезпечують стійкий розвиток українського суспільства і його інститутів на базі інформатизації духовної, політичної й соціальної сфер суспільного життя.

Актуалізація проблеми захисту інформаційного простору і його впливу на інформаційну безпеку безпосередньо пов'язана з існуючими реальними й потенційними загрозами й викликами безпеці держави, рівень і масштаби яких в останнє десятиліття істотно зросли й придбали досить небезпечний характер. Виходячи з того, що інформаційна безпека на рубежі третього тисячоліття виходить на перше місце в системі національної безпеки, формування й проведення єдиної державної політики в цій сфері здобуває пріоритетне значення.

У результаті проведеного дослідження, автор доходить висновку, що необхідно розробити й прийняти довгострокову програму із забезпечення виходу України на рівень провідних країн світу в області створення систем інформатики й управління, заснованих на новітніх інформаційних технологіях.

В інтересах формування громадянського суспільства, демократичної правової держави, розвитку науки й культури необхідно проводити політику

по забезпеченню свободи одержання й поширення інформації громадянами, іншими суб'єктами суспільних відносин.

Інформаційний потенціал України (тобто сукупності інформації, що забезпечує національні інтереси країни; систем її одержання, зберігання, переробки й поширення; його суб'єктів) потребує надійного захисту від неправомірного його використання на шкоду інтересам особистості, суспільства й держави, які охороняються законом.

Також вважається важливим здійснення контролю за експортом із країни інтелектуальної продукції, а також інформаційних банків даних.

Велике значення має організація ефективної системи підготовки й перепідготовки кадрів в сфері забезпечення інформаційної безпеки.

Варто розвивати взаємодію державних і недержавних систем інформаційного забезпечення з метою більш ефективного використання інформаційних ресурсів України.

Необхідно вдосконалювати систему нормативно-правових актів, що регулюють відносини власності й дотримання балансу інтересів особистості, суспільства й держави в сфері формування, зберігання й використання інформаційних ресурсів.

Необхідно докласти зусиль з протидії цілеспрямованим заходам по дезінформації органів влади, населення країни, використанню каналів інформаційного обміну з метою порушення систем управління різними сферами життєдіяльності держави.

Дисертант вважає за доцільне створення загального інформаційного простору країн СНД в інтересах сприяння інтеграційним процесам, підвищення ефективності взаємодії в реалізації спільних інтересів.

Одним з важливих завдань інформаційної політики держави повинно стати введення України в міжнародну систему інформаційного обміну з урахуванням забезпечення українських національних інтересів і протидії акціями інформаційної інтервенції.

ВИСНОВОК

Інформаційна сфера як сукупність інформації, засобів її виробництва, обробки й зберігання, інформаційної інфраструктури, суб'єктів, що здійснюють збір, формування, поширення й використання інформації, а також системи регулювання суспільних відносин, що при цьому виникають, будучи системостворюючим фактором життя суспільства, активно впливає на стан політичної, економічної, оборонної й інших складових безпеки України, і тому національна безпека Української держави істотно залежить від забезпечення інформаційної безпеки, причому, очевидно, що в ході технічного прогресу ця залежність буде зростати.

Аналіз стану інформаційної безпеки України показує, що її рівень поки не повною мірою відповідає життєво важливим потребам особистості, суспільства й держави. Сьогоднішні умови політичного й соціально-економічного розвитку країни викликають загострення протиріч між потребами суспільства в розширенні вільного обміну інформацією й необхідністю збереження окремих обмежень на її поширення. Відсутність діючих механізмів регулювання інформаційних відносин у суспільстві й державі приводить до цілого ряду негативних наслідків.

Гарантувати безпека (не тільки інформаційну) держава може тільки в тому випадку, якщо вона має можливість максимального контролю над ресурсами або управління ними. Однак інформаційний простір глобальний, тому окрема держава не може взяти на себе відповідальність по забезпеченню інформаційної безпеки навіть у рамках своїх національних кордонів.

Незабезпеченість прав громадян на доступ до інформації, маніпулювання інформацією викликають негативну реакцію населення, що в ряді випадків веде до дестабілізації соціально-політичної обстановки в суспільстві.

Закріплені в Конституції України права громадян на недоторканність приватного життя, особисту й сімейну таємницю, таємницю листування поки ще практично не мають достатнього правового, організаційного й технічного забезпечення. Незадовільно організований захист даних про фізичні особи (персональних даних), що збираються органами державної влади.

Немає чіткості при проведенні державної політики в області формування українського інформаційного простору, розвитку системи масової інформації, організації міжнародного інформаційного обміну в інтеграції інформаційного простору України у світовий інформаційний простір, що створює умови для витіснення українських інформаційних агентств, засобів масової інформації із внутрішнього інформаційного ринку в деформації міжнародного інформаційного обміну.

Недостатня державна підтримка українських інформаційних агентств з просування їхньої продукції на зарубіжний інформаційний ринок.

Погіршується ситуація із забезпеченням збереження відомостей, що становлять державну таємницю.

Серйозна втрата нанесена кадровому потенціалу наукових і виробничих колективів, що діють в області створення засобів інформатизації, телекомунікації й зв'язку, в результаті масового відтоку із цих колективів найбільш кваліфікованих фахівців. Особливу небезпеку представляє факт відтоку фахівців з інформаційної безпеки, яких і так катастрофічно не вистачає. Варто враховувати, що ці люди є також носіями знань про системи інформаційної безпеки, що використовуються у нашій країні.

Відставання вітчизняних інформаційних технологій змушує органи державної влади йти шляхом закупівель імпортної техніки й залучення іноземних фірм, через що підвищується ймовірність несанкціонованого доступу до інформації, що опрацьовується, й зростає залежність України від зарубіжних виробників комп'ютерної й телекомунікаційної техніки, а також програмного забезпечення.

Дослідження підтвердило, що Україна є під впливом серйозних загроз і викликів, пов'язаних з територіальною цілісністю, збереженням економічних і соціальних зв'язків, комунікаціями. Особливо важливим представляється адекватна відповідь на вплив різного роду інформаційних загроз. Серед них можна виділити як технологічні (недостатній транспортний зв'язок української території, нерівність у доступі до сучасних засобів комунікації і, як наслідок, обмежені можливості одержання соціально значимої інформації й т.п.), так і соціально-політичні (наявність різкої диференціації в рівні життя населення різних регіонів, нестійкість інституційної системи держави, слабкий контроль суспільства над публічною владою, постійні конфлікти правлячої політичної еліти, масові політичні маніпуляції в ЗМІ й ін.). Крім того, традиційними загрозами є збір і використання інформації засобами технічної розвідки в інтересах іноземних держав або приватних компаній, які наносять економічну шкоду Україні, що загрожує безпеці її громадян.

Таким чином, сучасне суспільство набуває практично повну залежність від стану своєї інформаційної інфраструктури, що робить його досить вразливим від різних загроз через його інформаційний простір. З огляду на це, забезпечення національної безпеки в інформаційній сфері стає одним з вищих пріоритетів держави.

Розглянувши міжнародно-правові акти, що стосуються протидії новим викликам і загрозам в інформаційній сфері, а також впливу глобалізації на визначення національної стратегії розвитку інформаційного суспільства, автор доходить висновку про необхідність подальшої імплементації положень міжнародних правових актів, що стосуються, зокрема, забезпечення доступу до публічної й судової інформації, боротьби з корупцією, тероризмом і екстремізмом, кіберзлочинністю й гармонізації законодавства України в області забезпечення міжнародної інформаційної безпеки. Тільки прийняття скоординованих і взаємодоповнюючих заходів на двосторонньому, регіональному й міжнародному рівнях дозволить адекватно протистояти сучасним викликам і загрозам безпеки в інформаційній сфері.

Конкретизовані з погляду політичної науки інтереси особистості, суспільства й держави в інформаційній сфері. Аргументовано, що інтереси особистості полягають у реалізації конституційних прав людини й громадянина на доступ до інформації, на використання інформації в інтересах здійснення не забороненої законом діяльності, фізичного, духовного й інтелектуального розвитку, а також у захисті інформації, що забезпечує особисту безпеку; інтереси суспільства - у забезпеченні інтересів особистості в цій сфері, зміцненні демократії, створенні правової соціальної держави, досягненні й підтримці громадської згоди, у духовному відновленні України; інтереси держави - в створенні умов для гармонійного розвитку української інформаційної інфраструктури, для реалізації конституційних прав і свобод людини й громадянина в області одержання інформації й користування нею з метою забезпечення непорушності конституційного ладу, суверенітету й територіальної цілісності України, політичної, економічної й соціальної стабільності, у безумовному забезпеченні законності й правопорядку, розвитку рівноправного й взаємовигідного міжнародного співробітництва.

Автор доходить висновку про необхідність розвитку інформаційної політики в напрямку вдосконалювання механізмів координації діяльності органів влади різних рівнів між собою, із правоохоронними органами, інститутами цивільного суспільства й засобами масової інформації.

Актуальним є прийняття державної цільової програми з розробки й впровадження вітчизняних конкурентоспроможних продуктів в інформаційно-комунікаційній сфері.

Також необхідно в найкоротший термін удосконалити інформаційне законодавство. На наш погляд, інформаційне законодавство, що включає нормативні правові акти, повністю присвячені питанням правового регулювання в інформаційній сфері, і окремі норми з даного предмета в інших нормативних правових актах, є одночасно основним інструментом реалізації й однією з основних сфер формування державної інформаційної

політики. Як відомо, у цей час уже прийнятий і діє ряд базових законів, що регулюють відносини в інформаційній сфері. Однак проблеми формування інформаційного законодавства продовжують залишатися досить актуальними, оскільки досить широке коло правових відносин в інформаційній сфері так і залишається не врегульованим.

В Україні необхідні умови для зміни спрямованості й методології політичної діяльності з питань розвитку інформаційної сфери держави, що, в першу чергу, пов'язане з необхідністю пошуку нових і більш ефективних шляхів забезпечення національної й інформаційної безпеки. Діяльність органів державної влади країни з реалізації повноважень в області інформаційної безпеки також повинна бути раціонально обґрунтована. Розробка й застосування наукової методології діяльності суб'єктів політики в зазначеній сфері є найважливішим напрямком оптимізації механізму захисту інформаційного простору, забезпечення інформаційної безпеки.

У результаті дослідження виявлені механізми формування відкритого суспільства, серед яких варто виділити доступ до інформації, відкритість органів державної влади, у тому числі через технології електронного уряду, подолання цифрової нерівності.

Аналіз політичного аспекту проблеми інформаційної безпеки дозволяє зробити висновок про все більший зсув центру ваги від силових факторів до більш утаємничених і тонких, що базуються на інформаційному впливі.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Акаев Д. В. Особенности использования современных информационных технологий в политическом процессе [Електронний ресурс]. – Режим доступу: http://jurnal.org/articles/2007/art.php?art=polit11.htm.

2. Акопов Г.Л. Глобальные проблемы и опасности сетевой политики / Г.Л. Акопов. - [Електронний ресурс] - Режим доступа: http://www.problem.politnet.ru/oglavlen.html

3. Алексенцев А.И. Сущность и соотношение понятий «защита информации», «безопасность информации», «информационная безопасность» // Безопасность информационных технологий. 1999. № 1. - С.4

4. Алешенков М. Основы национальной безопасности / М.Алешенков // Основы безопасности жизни.- 2005.- № 11.- С.5-10.

5. Андреев Э. М. Социальные проблемы интеллектуальной уязвимости и информационной безопасности / Э.М. Андреев, А.В. Миронов //Социально-гуманитарные знания.- 2000.- № 4.- С.169-180.

6. Арапова Н.П. Социально-информациологический подход к теории информационных войн. – М.: РАГС, 2007. – 234 с.

7. Асанович В.Я. Информационная безопасность. Анализ и прогноз информационного воздействия / В.Я. Асанович, Г.Г. Маньшин. – М.: Амалфея, 2006. – 204 с.

8. Афанасьева О. В. Наш доступ к информации, которой владеет государство / О. Афанасьева, М. Афанасьев. - М. : [Либеральная миссия], 2010. – 187 с.

9. Багиров Р.З. Информационное обеспечение военной безопасности государства / Р.З. Багиров // Власть. – 2006. - № 12. – С.86-89.

10. Багиров Р.З. Политическая коммуникация в обеспечении военной безопасности Российской федерации : автореф. дис. на соискание науч.

степени канд. полит. наук наук : спец. 23.00.02 «Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии» / Р.З. Багиров. –М., 2009. – 21 с.

11. Балуев Д.Г. Личностная и государственная безопасность: международно-политическое измерение / Д.Г. Балуев: Монография. Н. Новгород: Изд-во Нижегородского госуниверситета, 2004. – 231 с.

12. Банисар Д. Свобода информации в мире. Общий обзор законодательства по доступу к правительственной информации в мире [Електронний ресурс]. – Режим доступу: www.privacyinternational.org/foi/foisurvey2006rus.pdf

13. Баринов А. Информационный суверенитет или информационная безопасность? / А. Баринов // Національна безпека і оборона. – 2001. – № 1. – С. 70-76.

14. Бачило И.Л. Информационное право. Основы практической информатики. Учебное пособие / И.Л. Бачило // Институт государства и права РАН. – М., 2001. – 352 с.

15. Безопасность личности, общества, государства. Монография. В 2 т. Под общей редакцией академика О.А. Колобова.- Нижний Новгород: ФМО/ИСИ ННГУ, 2008. – Т.1- 522с.; Т.2- 608с.

16. Безопасность России: проблемы и пути решения. - Клуб «Реалисты», 2004. - 340 с.

17. Белл Д. Социальные рамки информационного общества / Д. Белл // Новая технократическая волна на Западе / Под ред. П. С. Гуревича. М., 1988.

18. Белорусские интернет-кафе обязали собирать данные о посетителях [Электронный ресурс]. – Режим доступа: http://podrobnosti.ua/internet/2010/05/05/683934.html

19. Белорусские сайты обязали пройти регистрацию [Электронный ресурс]. – Режим доступа: http://podrobnosti.ua/internet/2010/05/07/684195.html

20. Беляков К.И. Управление и право в период информатизации / К.И. Беляков. – К.: Изд. «КВІЦ», 2001 – 308 с.

21. Бехманн Г. Современное общество. Общество риска, информационное общество, общество знаний / Г. Бехманн. – М.: Логос, 2010. – 248 с.

22. Бойко Ю. Политика государства в информационной сфере. //Обозреватель. – 2006. – № 7. – С.24-26.

23. Бойченко О.В. Політика інформаційної безпеки в системі інформаційного забезпечення ОВС України / О.В. Бойченко // Форум права. – 2009.- № 1. - [Електронний ресурс]. - Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2009-1/09bovzou.pdf

24. Боровський В. Інформаційне забезпечення органів державної влади та місцевого самоврядування / В. Боровський // Ефективність державного управління.- 2008.-Вип. 16/17.- С. 264-271.

25. Борисов В.А. Связи с общественностью в политике / В.А. Борисов. – СпбГУ, 2000. – 85 с.

26. Болокова М.А. Информационные потоки в системе массовой культуры : автореф. дис… канд. фил. наук : спец. 24.00.01- теория и история культуры / М.А. Болокова. – Ростов-на-Дону, 2006. – 23 с.

27. Бондаренко В.О., Литвиненко О.В. Інформаційна безпека сучасної держави: концептуальні роздуми / В.О. Бондаренко, О.В. Литвиненко // Стратег. панорама. – 1999. – № 1-2. – С. 127-133.

28. Бондаренко В.О. Інформаційні впливи і операції / В.О. Бондаренко, О.В. Лиьвиненко // Стратег. панорама. – 1999. – № 4. – С. 134-140.

29. Бордюже В. Ликвидация цифрового неравенства как предпосылка устойчивого развития регионов. Научный доклад / В. Бордюже, И. Болото. – М., 2003. – 54 с.

30. Брандман Э. М. Глобализация и информационная безопасность общества/ Э.М.Брандман //Философия и общество.- 2006.-№ 1.- С.31-41.

31. Брандман Э. М. Цивилизационные императивы и приоритеты информационной безопасности общества /Э.М. Брандман //Философия и общество. - 2006.-№ 3.- С.60-77.

32. Брушлинский А.В. Проблемы информационно-психологической безопасности : (сб. ст.и материалов конф.) / А.В. Брушлинский ; Рос. акад. наук, Ин-т психологии ; Лаб.психологии рефлексив. процессов ; под. ред. А.В. Брушлинского и В.Е. Лепского. - М., 1996. - 98 с.

33. Бубнов А.В. Информационная безопасность России в условиях глобализации : автореф. дис… канд. полит. наук : спец. 23.00.02 – «Политические институты, процессы и технологии» /А.В. Бубнов – М., 2005. – 24 с.

34. Булатов С.А. Проблема информационной безопасности в Российской Федерации [Електронний ресурс]. – Режим доступу: http://vestnik.uapa.ru/issue/2010/02/02/

35. Буркин А.И. Национальная безопасность России в контексте современных политических процессов. Издание второе, дополненное / А.И. Буркин, А.В. Возженików, Н.В. Синеок // Под общ. ред. А.В. Возженикова. - М.: Изд-во РАГС, 2008. - 480 с.

36. Бучило И.Л. Информационное право: основы практической информации / И.Л. Бучило. – М., 2001 – 253 с.

37. Быченко Ю. Г. Важнейший показатель человеческого капитала / Ю.Г. Быченко // Человеческие ресурсы. 2001. - № 3.

38. Бюллетень Комиссии по свободе доступа к информации «Право знать». М., 1997. - Вып. 10. - С. 6.

39. Варфоломеев М. Проблема национальной безопасности в современном политическом процессе / М. Варфоломеев // Власть. – 2008. – С.38-40.

40. Вахромеев В. О целесообразности информационной активности политической элиты современной России / В. Вахромеев // Власть. – 2008. - № 7. – С.86-88.

41. Величко М.Ю. Информационная безопасность в деятельности органов внутренних дел: теоретико-правовой аспект : автореф. дис… канд. юрид. наук : спец. 12.00.01 – теория и история права и государства; история

учений о праве и государстве / М.Ю. Величко. – Казань, 2007. – 26 с.

42. Вербенко Б.В. Информационная безопасность России в контексте современного политического процесса: сущность, проблемы обеспечения : автореф. дис. ... канд. полит. наук. : спец. 23.00.02 – «Политические институты, процессы и технологии» / Б.В. Вербенко – М., 2005. – 24 с.

43. Вепринцев В.Б. Информационная политика в условиях глобализации / В.Б. Вепринцев : Аттестационная работа, РАГС, 2002. – 98 с.

44. Владимиров А. Информационное оружие: миф или реальность / А. Владимиров // Красная звезда. – 1991. – 5 октября.

45. Возженников А.В. Государственное управление и национальная безопасность России / А.В. Возженников, А.А. Прохожев. – М.: РАГС, 1999. – 132 с.

46. Возженников А.В. Национальная безопасность в контексте современного политического процесса России: Теория и политика обеспечения : дис... докт. полит наук : спец.23.00.02 - политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии / А.В. Возженников. - М., 2002. – 346 с.

47. Волковский Н.Л. История информационных войн / Н.Л. Волковский. – СПб.: Полигон, 2003.- 135 с.

48. Гавловський В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект) /В. Гавловський [Електронний ресурс]. – Режим доступу: www. bezpeka.com/ru/lib/spec/law.html

49. Гаджиев К.С. Введение в геополитику [Електронний ресурс]. Режим доступу: http://www.politology.vuzlib.net/book_o061_page_89.html

50. Гаджиев К. Введение в геополитику. Проблемы национальной безопасности. Концепция национального интереса [Електронний ресурс]. – Режим доступу: http://society.polbu.ru/gadzhiev_geopolitics/ch70_all.html

51. Галамба М. Інформаційна безпека України: поняття, сутність та загрози / М. Галамба, В. Петрик [Електронний ресурс]. – Режим доступу: http://www.nbu.gov.ua/infan/arxiv/arxiv0/2007/01/28

52. Гальцев И. И.. Информационное обеспечение национальной безопасности России: политический и социокультурный аспекты : автореф. дис. ... канд. полит. наук : 23.00.02 : М., 2005 – 22 с.

53. Горбенко А.Н. Информационное противоборство в современном мире / А.Н. Горбенко [Електронний ресурс]. – Режим доступу: http://www.lihachev.ru/chten/6006/6125/6127/?bpage=0

54. Грачев Г. Информационно-психологическая безопасность личности [Электронный ресурс] / Г. Грачев, И. Мельник. – 2004. - URL: http://www.koob.ru/grachev_melnik/psy_defence

55. Грачев Г.В. Информационно-психологическая безопасность личности: состояние и возможности психологической защиты / Г.В. Грачев ; Рос. акад. гос. службы при Президенте Рос. Федерации. - М. : Изд-во РАГС, 1998. - 123 с. ; То же [Электронный ресурс]. – URL: http://www.i-u.ru/biblio/archive/grachev%5Finfo/ (16.01.08).

56. Грачев Г.В. Информационно-психологическая безопасность личности: теория и технология психологической защиты : автореф. дис. ... д-ра психол. наук / Г.В. Грачев ; [Рос. акад. гос. службы при Президенте Рос. Федерации]. - М., 2000. - 56 с.

57. Грачев Г.В. Личность и общество: информационно-психологическая безопасность и психологическая защита / Г.В. Грачев. - М. : ПЕР СЭ, 2003. - 303 с.

58. Грачев С.И. Терроризм. Вопросы теории: Монография / С.И. Грачев. – Н. Новгород: Издательство ННГУ им. Н.И. Лобачевского, 2007. – 269 с.

59. Грачев С.И. Терроризм и контртерроризм в условиях глобализма: Монография / С.И. Грачев. – Н. Новгород: Издательство ННГУ им. Н.И. Лобачевского, 2007. – 354 с.

60. Грачев С.И. Спаси себя сам: практикум личной безопасности: Учебное пособие / С.И. Грачев. – Н. Новгород: Институт стратегических исследований ННГУ им. Н.И. Лобачевского, 2005. – 151 с.

61. Гриняев С. Россия в глобальном информационном обществе: угрозы, риски и возможные пути их нейтрализации [Електронний ресурс]. – Режим доступу: http://www.fondiv.ru/articles/3/335/

62. Добрынин А. И. Человеческий капитал. Методические аспекты анализа / А.И. Добрынин, С.А. Дятлов, С.А. Курганский. - СПб.: СПбГУЭФ, 1999. – 132 с.

63. Додин И.С. Информационно-коммуникационные технологии в системе государственного управления регионом : автореф. дис. канд. полит. наук : спец. 23.00.02. - политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии (по политическим наукам) / И.С. Додин. – Саратов, 2007. – 26 с.

64. Доктрина інформаційной безпеки України [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/9570.html

65. Доктрина информационной безопасности // Средства массовой информации постсоветской России: Учеб. пособие /Я.Н. Засурский, Е. Л. Вартанова, И.И. Засурский.- М., 2002 - С.262-301.

66. Доповідь про стан та перспективи розвитку інформатизації та інформаційного суспільства в Україні за 2009 рік [Электронный ресурс]. Режим доступа: http://www.dki.gov.ua/repository/36/file/PD2009.

67. Доповідь Секретаря РНБОУ Раїси Богатирьової щодо питання забезпечення національної безпеки в інформаційній сфері [Електронний ресурс]. – Режим доступу: **http://www.bogatyrova.org.ua/press/news/47e757ea070f7/view_print/**

68. Дубас О.П. Інформаційний розвиток сучасної України у світовому контексті: політологічний аналіз : автореф. дис. канд.. політ. наук : спец. 23.00.02 – політичні інститути та процеси / О.П. Дубас. – К., 2004. - 20 с.

69. Егозина В. Смотреть нельзя запретить (агрессивная информационная среда как угроза для безопасности) / В. Егозина, Н. Овчинников // ОБЖ.-2003. - № 4.- С.15-18.

70. Еляков А.Д. Информационная свобода человека /А.Д.Еляков // Социально-гуманитарные знания.- 2005. - №3. - С.125-141.

71. Емельяненко Е.М. Электронное правительство: инновационные подходы к политике и управлению в информационном обществе. – Дис… канд. полит. наук : спец. 23.00.02. – политические институты и процессы / Е.М. Емельяненко - О., 2008. – 194 с.

72. Емельянов Г.В. Проблемы обеспечения информационно-психологической безопасности России / Г.В. Емельянов, В.Е. Лепский, А.А. Стрельцов // Информ. общество. - 1999. - Вып. 3. - С. 47–51.

73. ЕС обратил внимание на информационную безопасность [Електронний ресурс]. – Режим доступу: http://www.polit.ru/news/2006/06/02/security.html

74. Журавлёва Н.Н. Информационная политика государства по продвижению национальной культуры за рубежом (на примере России и Франции) : автореф. дис… канд. полит. наук : спец. 10.01.10 – Журналистика / Н.Н. Журавлева. – Санкт-Петербург, 2007. – 23 с.

75. Журин А. А. Информационная безопасность как педагогическая проблема / А.А. Журин // Педагогика.- 2001. - №4.- С.48-55.

76. Забузов О.Н. Интернет как средство реализации военно-информационной политики Российского государства : автореф. дис. на соискание науч. степени канд. полит. наук наук : спец. 23.00.02 «Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии» / О.Н. Забузов. – М., 2008. – 26 с.

77. Забузов О.Н. Военно-информационная политика: модель и особенности ее реализации Минобороны России / О.Н. Забузов // Вестник

Тамбовского государственного технического университета. – Тамбов. – 2006. – Том 12. – № 4Б. – С. 1223–1227.

78. Закон України “Про державну таємницю” в редакції Закону “Про внесення змін до Закону України “Про державну таємницю” від 21 вересня 1999 року, http//www.rada.kiev.ua (5 січня 2006 р.

79. Закон України «Про інформацію», прийнятий Верховною Радою України 2 жовтня 1992 року // Відомості Верховної Ради України (ВВР). – 1992. – № 48. – ст. 651; Із змінами від 06.04.2000, ВВР. – 2000. – № 27, – ст. 213; від 07.02.2002, ВВР. – 2002. – № 29, – ст. 194; від 03.04.2003, ВВР. – 2003. – № 28. – Ст. 214.

80. Закон України “Про Концепцію Національної програми інформатизації” від 4 лютого 1998 р. № 75/98-ВР// Відомості Верховної Ради. – 1998. – № 27-28. – С. 182.

81. Закон України «Про основи національної безпеки України» // Відомості Верховної Ради України. – 2003. – № 39. – Ст. – 351. Із змінами, внесеними згідно із Законом № 3200-IV (3200-15) від 15.12.2005. ВВР. – 2006. – № 14. – Ст. 116.

82. Закон України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» // Відомості Верховної Ради України (ВВР). – 2007. – № 12. – Ст. 102.

83. Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» // Відомості Верховної Ради. – 1997. - № 49. – Ст.299.

84. Закупень Т. Понятие и сущность информационной безопасности, и ее место в системе обеспечения национальной безопасности РФ / Т. Закупень // «Информационные Ресурсы России» №4, 2009 [Електронний ресурс]. – Режим доступу: http://www.aselibrary.ru/digital_resources/journal/irr/2009/number_4/number_4_5/number_4_5965/).

85.

86.

87.

88. Зинченко Н. И. Обеспечение безопасности личности, общества и государства: концептуально-теоретический аспект / Н.И. Зинченко // Социально-гуманитарные знания. 2006. № 6. - С. 183-186.

89. Из-за хакеров Саркози "отказался" от участия в выборах [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/power/2011/01/24/749001.html

90. Интернет - лучший способ разведки для экстремистов [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/internet/2010/11/02/728020.html

91. Інформатизація та відкритість влади як засоби демократизації суспільства: Матеріали «круглого столу». — К: Альтерпрес, 2003. — 160 с.

92. Інформаційна безпека держави у контексті протидії інформаційним війнам: Навчальний посібник // За заг. ред. В. Б. Толубка. – К.: НАОУ, 2004. – 315 с.

93. Інформаційна безпека України. Проблеми і шляхи вирішення. Заочний круглий стіл // Національна безпека і оборона. – 2001. – № 1. – С. 24-29.

94. Информационная безопасность России / Ю.С. Уфимцев, Е.А. Ерофеев и др. – М.: Экзамен, 2003. – 560 с.

95. Информационная политика: Учебник/ Под общ. ред. В.Д. Попова. М., 2003.- 235 с.

96. Информационные вызовы национальной и международной безопасности // Под общ. ред. А.В. Федорова, В.Н. Цыгичко. – М., 2001. 0 345 с.

97. Калинин А. Управление информационной безопасностью России: проблемы и стратегия времени / А. Калинин // Власть. – 2007. – № 11. – С.58-61.

98. Касперович Ю.Н. Национальный интерес в контексте современной российской национальной политики (социально-философский анализ) : автореф. дис… канд. фил. наук : спец. 09.00.11 – социальная философия / Ю.Н. Касперович. – Краснодар, 2008. – 16 с.

99. Кафтанчиков Д.П. Информационная безопасность регионов Российской Федерации: современное состояние и приоритеты обеспечения : автореф. дис… канд. полит. наук : спец. 23.00.02 – политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии / Д.П. Кафтанчиков. – Орел, 2009. – 28 с.

100. Кафтанчиков, Д.П. Обеспечение информационной безопасности региона в условиях информатизации российского общества: актуальные проблемы и опыт ЦФО [Текст] / Д.П. Кафтанчиков // Среднерусский вестник общественных наук. – 2008. – № 2 (7) – С. 64–72.

101. Кафтанчиков, Д.П. Как противостоять информационной агрессии [Текст] /Д.П.Кафтанчиков, Д.Л. Цыбаков // Государственная служба. – 2008. – № 5. – С. 64–70. (авт.- 0,4 п.л.)

102. Кафтанчиков, Д.П. Современные угрозы региональной информационной безопасности [Текст] / Д.П. Кафтанчиков // Социология власти. – 2008. – № 6. – С. 141–148.

103. Кафтанчиков, Д.П. Состояние информационной безопасности в условиях процесса регионализации [Текст] / Д.П. Кафтанчиков //Среднерусский вестник общественных наук – 2009. – № 2 (11). – С. 105–109.

104. К 2056 году исчезновение украинского языка станет необратимым [Електронний ресурс]. - Режим доступу: http://podrobnosti.ua/society/2011/01/31/750479.html

105. Киберпреступность растет быстрее других видов преступности [Електронний ресурс]. – Режим доступу: http://antimalware.ru/news/2009-12-11/2076

106. Киберпространство: новые угрозы [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/newstext.php?news_id=60111

107. Кирьянов А.Ю. Сущность информационного аспекта национальной безопасности / А.Ю. Кирьянов // Государственная служба и местное самоуправление. – 2005. – № 6. – С.56-58.

108. Китай начинает войну в Интернете [Электронный ресурс]. – Режим доступа http://podrobnosti.ua/internet/2010/05/03/683579.html

109. Ковалева Е.В. Обеспечение транспарентности органов местного самоуправления современной России в процессе информатизации политического управления : автореф. дис… канд. полит. наук : спец. 23.00.02 – «Политические институты, процессы и технологии» / Е.В. Ковалева. – Саратов, 2010. – 26 с.

110. Козубський В.О. Інформаційна безпека держави: кримський регіон : автореф. дис… канд.. політ. наук : спец. 23.00.02 – Політичні інститути та процеси / В.О. Козубський. - Сімферополь – 2005 – 19 с.

111. Колобов О.А. Контртерроризм и информационная безопасность: Монография / О.А. Колобов, В.Н. Ясенев / Под ред. проф. Р.Г. Стронгина. – Н. Новгород: Изд-во ННГУ, 2004.- 431 с.

112. Кондрашина Н.В. Интернет-технологии как инструмент взаимодействия политической власти и общества в современной России : автореф. дис… канд. полит. наук : спец. 23.00.02 - политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии / Н.В. Кондрашина. – Астрахань, 2009. – 26 с.

113. Конституція України: Офіц. Видання. – К.: Видавничий Дім «Ін Юре», 2007. – 136 с.

114. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. Посібник / Б. А. Кормич. – К.: Кондор, 2004. – 384 с.

115. Кормич Б.А. Інформаційне право. Підручник / Б.А. Кормич. – Харків: БУРУН і К, 2011. – 334 с.

116. Кормич Б.А. Організаційно-правові основи політики

інформаційної безпеки України : автореф. дис… док. юрид. наук : спец. Спеціальність 12.00.07 - теорія управління; адміністративне право і процес; фінансове право; інформаційне право / Б.А. Кормич. – Харків, 2004. – 42 с.

117. Корнилов А.А. Безопасность превыше всего. Концепции внешней политики и национальной безопасности Государства Израиль: Монография / А.А. Корнилов.- Нижний Новгород: изд-во ННГУ, 2005. – 140 с.

118. Королев Ю.А. Информационно-политические императивы региональной безопасности (на примере Саратовской области) : автореф. дис. канд… полит. наук : спец. 23.00.02 - политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии / Ю.А. Королев. – Саратов, 2009. – 23 с.

119. Королев Ю.А. Некоторые особенности нового гражданского законодательства России.// Право и современность Сборник научно-практических статей Саратов, 2008,СЮИ МВД Выпуск 3 Часть 1. С. 172-175.

120. Королев Ю.А. Проблема информационной безопасности: влияние факторов политической системы. // Актуальные проблемы социально-экономического развития России Сборник научных трудов. Саратов: Изд. СГСЭУ, 2008. Выпуск 11. С.45-49.

121. Королев Ю.А. Теоретические подходы исследования информационной безопасности. // Традиции и новации времени: актуальные проблемы современного общества. Сборник научных трудов. Саратов. 2009. Изд. СГСЭУ. Выпуск 14. С.93-97.

122. Кортунов С.В. Диалектика национальной и международной безопасности: некоторые методологические проблемы / С.В. Кортунов // Политические исследования. – 2009. - № 1. – С.10-15.

123. Корчагин Ю. А. Российский человеческий капитал: фактор развития или деградации? / Ю.А. Корчагин. - Воронеж: ЦИРЭ, 2005.

124. Краковский Ю.М. Информационная безопасность и защита информации. М., 2008. – 276 с.

125. Крутий И. А. Человеческий капитал: эволюция представлений / И.А. Крутий, О.В. Красина [Електронний ресурс]. – Режим доступу: http://2008.isras.ru/files/File/Socis/2007-08/krasina_krutiy.pdf

126. Крысько В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) / В.Г. Крысько. – Минск: Харвест, 1999. – 189 с.

127. Кулагин В.М.Международная безопасность: Учебное пособие для студентов вузов / В. М. Кулагин. — М.: Аспект Пресс, 2006. — 319 с.

128. Лазарев И.А. Информация и безопасность. Композиционная технология / И.А. Лазарев. – М.: Изд-во Московского городского центра научно-технической информации, 2002. – 334 с.

129. Лапин Н. И. Социальная информатика: основания, методы, перспективы / Н.И. Лапин. - М., 2006. – 324 с.

130. Лепехин А. Н. Расследование преступлений против информационной безопасности. Теоретико-правовые и прикладные аспекты / А.Н. Лепехин. – М.: Тесей, 2008. – 176 с.

131. Литвиненко О.В. Інформаційна відкритість української влади: Аналітична доповідь, Національний інститут стратегічних досліджень / О.В. Литвиненко, В.М. Паламарчук, С.О. Янішевський, В.В. Жигалюк, О.В. Сахаренко. - К, 2002. – 67 с.

132. Лопатин В.Н. Информационная безопасность России : дис. на соискание ученой степени доктора юрид. наук: 12.00.01 / В.Н. Лопатин - СПб.: СПбУМВД России, 2000. - 433 с.

133. Лопатин В. Н. Информационная безопасность России: Человек, общество, государство Серия: Безопасность человека и общества. – М.: 2007. – 428 с.

134. Лукацкий А. Технологии информационной безопасности вчера и сегодня (тема номера) /А. Лукацкий // Компьютер пресс.-2004.-№ 4 /апрель/ .- С.8-11.

135. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки : автореф. дис… канд.. юрид. наук : спец. 12.00.01 –

теорія та історія держави і права, історія політичних і правових учень / Ю.Є. Максименко. – Київ, 2007. – 22 с.

136. Манойло А.В. Государственная информационная политика в условиях информационно-психологической войны / А.В. Манойло, А.И. Петренко, Д.Б. Фролов. – М.: Телеком, 2003. – 384 с.

137. Мельников В. П. Информационная безопасность / В.П. Мельников, С.А. Клейменов, А. М. Петраков. - М.: Academia, 2007. – 145 с.

138. Местное телевидение, власть, население: информационная открытость как основа социального партнерства /сост. Дзялошинский И. - М.: КСДИ, 2001. – 134 с.

139. Миэринь Л. А. Образование — системообразующий фактор информационного общества / Л.А. Миэринь, А.И. Попов // Известия СПбГУЭФ. 2003. № 1.

140. Моисеев Н.Н. Информационное общество как этап новейшей истории // Свободная мысль. 1996. № 1. - С. 38.-41.

141. Морозов И.Л. Информационная безопасность политической системы / И.Л. Морозов. – Полис. – 2002. - № 5. – С.134-145.

142. Музей истории шпионской техники [Електронний ресурс]. – Режим доступу: Кита Мэлтона http://www.photohistory.ru/1207248179548035.html

143. Мухаметов Р.С. Национальные интересы России: официальная трактовка / Р.С. Мухаметов [Електронний ресурс]. – Режим доступу: http://beztemy.usu.ru/?base=mag/0004(02_2007)&xsln=showArticle.xslt&id=a09&doc=../content.jsp

144. Нанадзе И. Информационная безопасность в период политической модернизации / И. Нанадзе // Обозреватель. – 2007. – №7. – С.56-59.

145. Нарис теорії і практики інформаційно-психологічних операцій / Дзюба М. Т., Жарков Я. М., Ольховой І. О., Онищук М. І.: Навч. Посібник // За заг. ред. В.В. Балабіна. – К.: ВІТІ НТУУ «КПІ», 2006. – 468 с.

146. НГ: Украина определила главные угрозы на 2011 год [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/outeropinion/2010/11/19/732293.html

147. Недбай В.В. Інтернет як засіб політичної комунікації // Сучасна українська політика. Політики і політологи про неї. Спецвипуск. – К., 2008. – С.134-138.

148. Недбай В.В. Інтернет-комунікації – нові можливості та нові проблеми / В. Недбай // Політологічний вісник. Зб-к наук. праць. – К.: «ІНТАС», 2009. – Вип. 39. - С.379-388 .

149. Недбай В.В. Интернет - новый постмодернистский вид медиа / В.В. Недбай // Актуальні проблеми політики. – Одеса, 2009. – Вип. 37.

150. Недбай В.В. Комунікації органів державної влади: поняття та сутність / В.В. Недбай // Актуальні проблеми політики. Вип. 36,- Одеса. 2009. – С.79-87.

151. Недбай В.В. Політична відповідальність та функції ЗМІ в демократичному суспільстві / В.В. Недбай // Актуальні проблеми політики. Вип. 31.- Одеса, 2007. – С.312-319.

152. Недбай В.В. Социально-политические последствия развития информационного общества: Дис. … канд. полит. наук : спец. 23.00.02 – политические институты и процессы / В.В. Недбай. – О., 2004. – 202 с.

153. Николаев А. Государственно – идеологическая компонента информационной безопасности / А. Николаев // Власть. – 2007.– № 4. – С.38-41.

154. Николаев А.А. Информационная безопасность России в условиях социальной трансформации (политологический анализ) : автореф. дис... канд. полит. наук : спец. 23.00.02 – политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии / А.А. Николаев. – Москва, 2007. – 21 с.

155. Нисневич Ю.А. Информация и власть / Ю.А. Нисневич. - М.: Мысль, 2000. – 156 с.

156. Нисневич Ю. А. Программа курса «Государственная информационная политика» // Вестник Российского университета дружбы народов. Сер.: Политология. 2003. № 4. - С. 109-114.

157. Ницевич В.Ф. Военно-информационная политика государства: теория, императивы, приоритеты. – М.:Изд-во ВУ, 2001.

158. Ноговицын А. В центре внимания – информационная безопасность / А. Ноговицын [Електронний ресурс]. – Режим доступу: http://www.redstar.ru/2009/02/27_02/1_06.html

159. Нойманн Ф. Методика экономической оценки человеческого капитала / Ф. Нойман // Тезисы докладов международной научно-практической конференции. Государственное управление: трансформационные процессы в современном мире. Ч. 2. Минск: Академия управления при Президенте Республики Беларусь, 2002.

160. Нос А.И. Политическая коммуникация в современной России : автореф. дис. на соискание науч. степени канд. полит. наук : спец. 23.00.02. «Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии» / А.И. Нос. – Ставрополь, 2004. – 28 с.

161. Общая теория национальной безопасности: Учебник / Под общ. ред. А.А. Прохожева. Изд. 2-е, доп. — М.: Изд-во РАГС, 2005. — 344 с.

162. Оганян К.А. Информационная политика и проблема обеспечения национальной безопасности в современной России : автореф. дис… канд. полит. наук : спец. 23.00.02 – политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии) / К.А. Оганян. – М., 2006. – 24 с.

163. Оганян К.А. Интернет как политическая коммуникация / К.А. Оганян // Объединенный научный журнал. – М., 2005.- № 8.- С.24-27.

164. Оганян К.А. Направления глобального информационного наступления США / К.А. Оганян // США, Канада: экономика, политика, культура. – М., 2006. - № 12. – С.42-43.

165. Оганян К.А. Политические институты как основное звено механизма реализации внутренней информационной политики / К.А. Оганян // Вопросы гуманитарных наук. – М., 2006.- № 1.- С.57-59.

166. Окинавская Хартия глобального информационного общества от 22.07.2000 // Международное право. 2000. - № 3.

167. Остапенко В.С. Государственная политика в области обеспечения информационной безопасности органов исполнительной власти (региональный аспект) : автореф. дис… канд. полит. наук : специальность 23.00.02 – политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии / В.С. Остапенко. – Ростов-на-Дону, 2009. – 26 с.

168. Олійник О.В. Організаційно-правові засади захисту інформаційних ресурсів України : автореф. дис. канд.. політ. наук : спеціальність: 12.00.07. – теорія управління; адміністративне право і процес; фінансове право; інформаційне право / О.В. Олійник. – К., 2006. – 22 с.

169. Орлова В.В. Глобальные телесети новостей на информационном рынке / В.В, Орлова. – М.: Изд-во «РИП-Холдинг», 2003. – С. 54.

170. Отчет компании McConnell International Risk E-Business: Seizing the Opportunity of Global E-Readiness (EN), август 2000 г. http://www.microsoft.com/Rus/ Government/newsletters/issue7/02.mspx

171. Панарин И.Н. Информационная война, PR и мировая политика / И.Н. Панарин. – М.: Горячая линия – Телеком, 2006. – 352 с.

172. Панарин И.Н. Технология информационной войны. – М: Издательство «КСП+», 2003. – 176 с.

173. Пеньков И.А. Влияние защищенности российского сегмента глобальной сети Интернет на состояние информационной безопасности государства [Електронний ресурс]. - Режим доступу: http://www.budgetrf.ru/Publications/Magazines/VestnikSF/2005/vestniksf261-09/vestniksf261-09060.htm

174. Петренко С. А. Политики информационной безопасности / С.А. Петренко, В.А. Курбатов. – М.: Компания АйТи, 2006. – 400 с.

175. Петрик В. М. Информационно-психологическая безопасность в эпоху глобализации: Учеб. пособ. / В.М. Петрик, В.В. Остроухов, А.А. Штоквиш и др. // Под. ред. В. В. Остроухова. – К., 2008. – 544 с.

176. Петрик В. Небезпеки особистості в інформаційному просторі / В. Петрик, Я. Жарков, М. Дзюба // Юридичний журнал. – 2007. – № 2. – С. 45–46 (www:justinian.com.ua).

177. Петрик В. М. Соціально-правові основи інформаційної безпеки: Навчальний посібник / В.М. Петрик, А.М. Кузьменко, В.В. Остроухов та ін. // За ред. В. В. Остроухова. – К.: Росава, 2007. – 496 с.

178. Петрик В.М. Сучасні технології та засоби маніпулювання свідомістю, ведення інформаційних війн і спеціальних інформаційних операцій: Навчальний посібник / В.М. Петрик, В.В. Остроухов та ін.. – К.: Росава, 2006. – 208 с.

179. Петрик В. М. Щодо визначення інформаційної безпеки та її різновидів // Форми та методи забезпечення інформаційної безпеки держави: Збірник матеріалів міжнародної науково-практичної конференції (м. Київ, 13 березня 2008 р.). – К.: Видавець Захаренко В. О., 2008. – С. 160–164.

180. Пирумов В.С. Информационное противоборство. Четвертое измерение противостояния / В.С. Пирумов. - М.: Издательский дом «Оружие и технологии», 2003. – С.542.

181. Піщевська Е.В. Інтернет у контексті інформаційної безпеки / Е.В. Піщевська // Вісник ХНУ імені В.Н. Карабіна, серія «Питання політології». - № 912. – С.152-158.

182. Політологічний енциклопедичний словник. – К.: Генеза, 1997. – С. 34.

183. Поляков В.П. Информационная безопасность в курсе информатики /В.П.Поляков // Информатика и образование. - 2006. - № 10.- С.116-119.

184. Поляков В. П. Практическое занятие по изучению вопросов информационной безопасности /В.П.Поляков / /Информатика и образование. – 2006. -№ 11.- С.75-80.

185. Попов В.Б. Основы информационной безопасности. Информационные технологии и право / В.Б. Попов // Основы компьютерных технологий. - .-М., 2002.- С.175-187.

186. Політологія / За ред. О.В. Бабкіної, В.П. Горбатенка. – К.: Академія, 1998. – 387 с.

187. Политические коммуникации / ред. А.И. Соловьев. – М.: Аспект Пресс, 2004. – 332 с.

188. Полякова Т.А. Информационная безопасность в условиях построения информационного общества в России / Т.А. Полякова. – М.: РПА Министерства юстиции России, 2007. – 246 с.

189. Полякова Т.А. Правовое обеспечение информационной безопасности при построении информационного общества в России : автореф. дис… докт. юрид. наук : спец. 12.00.14 – Административное право; финансовое право; информационное право / Т.А. Полякова. – М., 2008. – 42 с.

190. 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.

191. Почепцов Г.Г. Стратегические коммуникации. Стратегические коммуникации в политике, бизнесе и государственном управлении / Г.Г. Почепцов. – Киев: Альтерпрес, 2008. – 224 с.

192. Почепцов Г.Г. Теория коммуникации / Г.Г. Почепцов. – М.: Изд-во SmartBook, 2009. – 651 с.

193. Правове забезпечення інформаційної діяльності в Україні / За заг. ред. Ю.С. Шемшученка, І.С. Чижа. – К.: ТОВ «Видавництво «Юридична думка, 2006. – 384 с.

194. Прайс М. Телевидение, телекоммуникации и переходный период: право, общество и национальная идентичность. – М.: Изд-во МГУ, 2000. – 156 с.

195. Програма інтеграції України до Європейського союзу, http//www.rada.kiev.ua (10 грудня 2005 р).

196. Прокофьев В. Ф. Тайное оружие информационной войны / Прокофьев В. Ф. - М. : СИНТЕГ, 1999. - 152 с.

197. Прохоров Е.П. Обеспечение информационной безопасности и деятельности СМИ / Е.П. Прохоров. - М.: Факультет журналистики МГУ имени М.В. Ломоносова, 2009

198. Прудников Д.П. Государственная информационная политика Российской Федерации в области обороны : автореф. дис… канд. полит. наук : спец. 23.00.02 – «Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии» / Д.Н. Прудников. – Москва, 2008. – 24 с.

199. Рада отменяет 50-процентную квоту украинской музыки на ТВ и радио [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/power/2011/02/02/750791.html

199а. Разоблачения ресурса Wikileaks спровоцировали скандал [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/podrobnosti/2010/11/29/734743.html

200. Раскладкина М.К. Интернет как средство организации информационно-политического пространства России : автореф. дис. на соискание науч. степени канд. полит. наук : спец. 10.01.10 «Журналистика» / М.К. Раскладкина. – Санкт-Петербург, 2006. – 30 с.

201. Рішення всеукраїнської науково-практичної конференції «Стан та вдосконалення безпеки інформаційно-телекомунікаційних систем **(**Коблево**,** 15-17 вересня 2009 р.) [Електронний ресурс]. – Режим доступу: **http://www.afa.biz.ua/news**

202. Родичев Ю. Информационная безопасность: Нормативно-правовые аспекты Ю. Родичев. - СПб.: Питер, 2008. – 272 с.

203. Роменков А.В. Влияние Интернет-технологий на политический процесс в России : автореф. дис… канд. полит. наук : спец. 23.00.02 - Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии / А.В. Роменков. - Саратов, 2009. – 20 с.

204. Рыбалкин Н.Н. Философия безопасности: учебное пособие / Н.Н. Рыбалкин. – М.: Московский психолого-социальный институт, 2006. – 296 с.

205. Саидов А.Х. Национальная безопасность и национальные интересы: взаимосвязь и взаимодействие / А.Х. Саидов, Л.Ф. Кашинская [Електронний ресурс]. – Режим доступу: http://www.lawmix.ru/comm/24/

206. Самара Н. Борьба с бедностью с помощью спутников / Н. Самара // Newslink. – 1999. -№ 1. – С. 12-14.

207. Сапожникова А.С. Взаимодействие государства и общества в политике информационной безопасности / А.С. Сапожникова // Государственное управление. Электронный вестник. – 2009. - № 19. [Электронный ресурс]. -Режим доступу: http://e-journal.spa.msu.ru/Publ.html.

208. Сапожникова А. С. Взаимодействие государства и общества в политике информационной безопасности РФ : автореф. дис… канд. полит. наук : спец. 23.00.02 – политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии / А.С. Сапожникова. – М., 2009. – 23 с.

209. Сапожникова А. Информационно-психологическая безопасность России: состояние и тенденции / А. Сапожникова // Власть, № 2, 2009. – С.54-58.

210. Сапожникова А.С. Кадровый аспект проблемы информационной безопасности: обеспечение информационной безопасности и управление персоналом компании / А.С. Сапожникова // Теория и практика управления:

новые подходы. М.: Издательство Университетский гуманитарный лицей. - 2007. – № 8. - С.23-25.

211. Сафронова И.Л. Политические проблемы обеспечения международной информационной безопасности : дис. ... канд. полит. наук : спец. 23.00.04 / И.Л. Сафронова. – М., 2006. – 211 с.

212. Сащук Г. Інформаційна безпека в системі забезпечення національної безпеки / Г. Сащук [Електронний ресурс]. – Режим доступу: http://journ.univ.kiev.ua/trk/publikacii/satshuk_publ.php

213. Сети Пентагона атакуют шесть миллионов раз в день [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/newstext.php?news_id=67603

214. Сіленко А. Політичний вплив технологій інформаційного суспільства / А.О. Сіленко // Соціальна психологія. Спеціальний випуск. – 2007. – С.53-62.

215. Сіленко А. Розвиток інформаційного суспільства в Україні: позитиви та ризики / А.О. Сіленко // Сучасна українська політика. Політики та політологи про неї. – Вип..10. - К., 2007. – С.197-207.

216. Сіленко А.О. Соціально-політичні наслідки інформаційної революції / А.О. Сіленко // Політичний менеджмент. – 2005. - № 5. – С.61-75.

217. Сіленко А. Розвиток інформаційного суспільства в Україні: позитиви та ризики // Сучасна українська політика. Політики та політологи про неї. – Вип..10. - К., 2007. – С.197-207.

218. Сіленко А. Цифрова нерівність як глобальна соціально-політична проблема / А. Сіленко // Політичний менеджмент. – 2006. - № 3. – С.51-62.

219. Скворцов Л. В. Информационная культура в контексте глобализации / Л.В. Скворцов // Теория и практика общественно-научной информатики. М., 2003. Вып. 18.

220. Слиньков С.В. Национальные интересы России на юге Африки: политологический анализ : автореф. дис… канд. полит. наук : спец. 23.00.02

– Политические институты, процессы и технологии / С.В. Слиньков. – М., 2010. – 23 с.

221. Смагин В.А. Обеспечение информационной открытости политической системы России : автореф. дис. канд. полит. наук : спец. 23.00.02 - политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии /В.А. Смагин. – Саратов, 2007. – 27 с.

222. Снытников А.А. Обеспечение и защита права на информацию / А.А. Снытников, Л.В. Туманова. – М.: Городец-издат, 2001 – 344 с.

223. Соболев В. Информация и переходная инфраструктуры / В. Соболев // Бизнес. Информ. – 1999 – № 3-4. – С. 36-39.

224. Соловьев А. И. Политология: Политическая теория, политические технологии / А.И. Соловьев. - М., 2001. - С. 183.

225. Соснін О.В. Державна політика в галузі управління інформаційним ресурсом України : автореф. дис. докт. політ. наук : спец. 23.00.02 Політичні інститути та процеси / О.В. Соснін – О., 2005. – 36 с.

226. Стрельцов А.А. Направление совершенствования правового обеспечения информационной безопасности Российской Федерации / А.А. Стрельцов // Информационное общество. – 1999 – № 6. – С. 15-21.

227. Стрельцов А.А. Обеспечение информационной безопасности России. Теоретические и методологические основы / Под ред. В.А. Садовничего и В.П. Шерстюка. - М.: МЦНМО, 2002. - 296 с.

228. Судоргин О.А. Императивы и приоритеты политики обеспечения информационной безопасности России : автореф. дис ... канд. полит. наук : спец. 23.00.02 – «Политические институты, процессы и технологии» / О.А. Судоргин – М., 2005. – 28 с.

229. Судоргин О.А. Теоретические основы и механизмы государственной информационной политики. – Москва - Орел: Изд-во ОРАГС, 2007.

230. США впервые поддержали идею переговоров по кибератакам [Електронний ресурс]. – Режим доступу: **http://www.itsec.ru/newstext.php?news_id=67614**

231. Таиров А.И. Информационное обеспечение функционирования органов государственной власти : дис… канд. полит. наук / А.И. Таиров. – Киев, 2010. – 185 с.

232. Тамайко Л.Л. Средства массовой информации как субъект предупреждения терроризма и экстремизма: монография / Л.Л. Тамайко.- Н. Новгород: ННГУ им. Н.И. Лобачевского, 2007. - 140 с.

233. Твирова Ю.А. Политическая коммуникация как фактор трансформации политической системы современной России : автореф. дис. на соискание науч. степени канд. полит. наук наук : спец. 23.00.02 «Политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии» / Ю.А. Твирова. – Тула; Орел, 2003. – 23 с.

234. Тезисы выступления директора Института проблем информационной безопасности МГУ им. М.В.Ломоносова В.П.Шерстюка [Електронний ресурс]. – Режим доступу: http://www.iisi.msu.ru/news/news35/

235. Термінологічний словник з питань технічного захисту інформації /за ред. Проф. В.О. Хорошка – 3-є видання. – К.: Поліграф Колсалтинг, 2003 – 268 с.

236. Титоренко О.В. Становление современного информационного пространства российской региональной политики : автореф. дис… канд. полит. наук : : спец. 23.00.02 – «Политические институты, процессы и технологии» /О.В. Титоренко – Саратов, 2003. – 26 с.

237. Трахименок С.А. Безопасность государства. Методолого-правовые аспекты / Трахименок. – Мн.: «Хата», 2007. – 192 с.

238. Тыклюк Н.В. Проблемы обеспечения «прозрачности» и доступности власти в современной России : автореф. дис… канд. полит. наук : спец. 23.00.02. – политические институты, этнополитическая

конфликтология, национальные и политические процессы и технологии (по политическим наукам) / Н.В. Тыклюк. – Саратов, 2007. – 29 с.

239. Украина готовит новую стратегию безопасности [Електронний ресурс]. – Режим доступу: http://podrobnosti.ua/podrobnosti/2010/11/14/731123.html

240. Уфимцев Ю.С. Информационная безопасность России / Ю.С. Уфимцев, Е.А. Ерофеев. - М.: Экзамен, 2003. - 560 с.

241. Федоров А.В. Информационная безопасность в мировом политическом процессе / А.В. Федоров. – М.: МГИМО, 2006. – 220 с

242. Федоров В.В. Власть в информационном обществе / В.В. Федоров // Обществознание: Глобальный мир в XX1 веке. Книга для учителя. – М.: ВЦИОМ, 2007. – 234 с.

243. Федорищенко П.А. Информационно-коммуникационные технологии управления (социологический анализ Интернета) : автореф. дис. канд. соц. наук : спец. 22.00.08 – Социология управления / П.А. Федорищенко. – Ростов-на-Дону, 2008. – 22 с.

244. Халипов В.Ф. Введение в науку власти. – М.: Технологическая школа бизнеса, 1995.

245. Церлов В.Л. Основы информационной безопасности. Ростов н/Д, 2008. - С. 23.

246. Чайка И.Г. Политические технологии обеспечения информационной безопасности региона (на примере Краснодарского края) : автореф. дис… канд. полит. наук : спец. 23.00.02 – Политические институты, процессы и технологии / И.Г. Чайка. – Краснодар, 2010. – 29 с.

247. Чернов А.А. Становление глобального информационного общества: проблемы и перспективы / А.А, Чернов. – М.: «Дашков и К», 2008. – 232 с.

248. Шамов М.И. Государственная стратегия и политические технологии предупреждения информационного терроризма в современном Российском обществе : автореф. дис… канд. полит. наук : спец. 23.00.02 –

политические институты, этнополитическая конфликтология, национальные и политические процессы и технологии / М.И. Шамов. – Нижний Новгород, 2007. – 27 с.

249. Шамсуев М.Х. Теоретические аспекты изучения информационной безопасности [Електронний ресурс]. – Режим доступу: http://www.teoria-practica.ru/index.php/2010-2/215-politologia/485-2010-07-02-12-21-16

250. Шариков П.А. Политика США в области информационной безопасности : автореф. дис… канд. полит. наук : спец. 23.00.04 – политические проблемы международных отношений и международного развития / П.А. Шариков. – М., 2009. – 38 с.

251. Шафрански Р. Теория информационного оружия [Електронний ресурс]. – Режим доступу: http://lib.hive.kiev.ua/SECURITY/kvn/shafran.txt

252. Шерстюк В.П. Информационная безопасность в системе обеспечения национальной безопасности России: федеральный и региональный аспекты обеспечения информационной безопасности / В.П. Шерстюк // Информационное общество. – 1999. – № 5. – С. 3-5.

253. Шкурлатов Р. Государство будет ввергнуто в хаос если его «нервные центры» подвергнутся кибератакам /Р.Шкурлатов // Основы безопасности жизнедеятельности.- 2005.- № 9.- С.22-27.

254. Штурба Е.В. Формирование и реализация концепции национальной безопасности Российской Федерации в 1992-2004 гг. : автореф. дис… докт. истор. наук : спец. 07.00.02 – Отечественная история / Е.В, Штурба. – Москва, 2009. – 25 с.

255. Эксперты НАТО: кибератака должна приравниваться к вооруженному нападению [Електронний ресурс]. – Режим доступу: http://www.itsec.ru/newstext.php?news_id=67643

256. Юрченко И.В. Национальная и региональная безопасность как политическая стратегия современной России : автореф. дис… докт. полит. наук : спец. 23.00.02 – Политические институты, этнополитическая

конфликтология, национальные и политические процессы и технологии / И.В. Юрченко. – Ставрополь, 2009. – 55 с.

257. Юсупов Р.М. Наука и национальная безопасность / Р.М. Юсупов.- СПб.: Наука, 2006.- 290с.

258. Якушев М.В. Информационное общество и правовое регулирование: новые проблемы теории и практики / М.В. Якушев // Информационное общество. – 1999. – № 1. – С. 40-43.

259. Янукович дал доступ к публичной информации [Електронний ресурс]. – Режим доступу: http://www.pravda.com.ua/rus/news/2011/02/3/5876245/

260. Ярочкин В.И. Теория безопасности / В.И. Ярочкин, Я.В. Бузанова. - М.: Академический Проект: Фонд «Мир», 2005. - 176 с.

261. Cleveland. The knowledge executive. Leadership in an information society/ - New York: Truman Telley books, 1989. – P. 32.

262. Hurrell A. Explaining the Resurgence of Regionalism in World Politics // Review of International Studies. 1995. October. Vol. 21, Herd G. Russia»s Baltic Policy After the Meltdown Security // Dialogue. – 1999. – № 30. – P.58-67.

263. Toffler A. War and Anti-War. - N.Y., 1994.