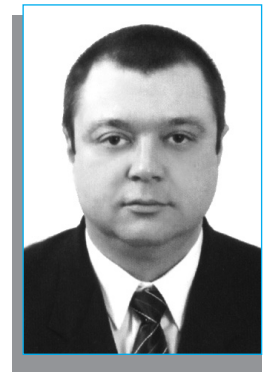
В. ПИЛИПЧУК
доктор юридичних наук, професор,
член-кореспондент НАПрН України,
заслужений діяч науки і техніки України,
директор Науково-дослідного інституту
інформатики і права НАПрН України

О. ДЗЬОБАНЬ
доктор філософських наук, професор,
головний науковий співробітник
Науково-дослідного інституту інформатики
і права НАПрН України



УДК 1:316.4

Глобальні виклики й загрози національній безпеці в інформаційній сфері

У статті розглянуто основні геополітичні зміни в інформаційній сфері, тенденції розвитку інформаційного простору на глобальному, регіональному і національному рівнях, ключові проблеми та сучасні виклики і загрози національній безпеці в інформаційній сфері.

Ключові слова: національна безпека, інформаційна сфера, інформаційна безпека, виклики і загрози, інформаційне протиборство.

Глобальний розвиток інформаційно-комунікаційних технологій породив нові інформаційні відносини та організаційні форми в економіці й виробництві, став новим джерелом продуктивності праці й активізував процеси формування глобальної економіки. Стає все більш очевидним, що інформація та інформаційні ресурси є найважливішими чинниками розвитку, стратегічним ресурсом, де первинною є не вартість праці та природних ресурсів, а вартість знань.

Інформація стала продуктивною силою і товаром, який продається й купується, одночасно будучи засобом захисту і нападу у відстоюванні державних, корпоративних і особистих інтересів суб'єктів владних відносин. Нормальна життєдіяльність людини, суспільства і держави стала цілком визначатися рівнем розвитку, якістю функціонування і безпекою інформаційної сфери, де вирішальними є якість і швидкість обробки інформації.

Слід зауважити, що розвиток інформаційної сфери не визнає національно-державних меж і веде до утворення глобальних інформаційних ресурсів, контрольованих міждержавними організаціями і корпораціями, що нав'язують свої стандарти поведінки і мислення. Тому вислів «хто володіє інформацією – той володіє світом» – сповна підтверджується політичною й економічною практикою.

Варто також звернути увагу на те, що в сучасній геополітичній ситуації змінюється політика практично всіх європейських країн, а також роль і місце військово-політичних механізмів забезпечення безпеки й оборони. На перший план висувається проблема будівництва нової системи європейської і національної безпеки, яка має включати всі наявні інститути безпеки та оборони за чіткого поділу їх функцій.

З геополітичної точки зору нова інформаційна ера змінює традиційні уявлення про символи могутності й способи досягнення світового панування. Споконвіку йшлося про наземний простір, потім – про повітряний і морський, а нині мова йде про актуалізацію ролі інформаційного простору та про нове поле геополітичного протиборства – інформаційну сферу. Як справедливо стверджує Д. Дубов, «поява нової інформаційної реальності (масштабної інформатизації, збільшення залежності воєнного сектору від сучасних інформаційних технологій, спрощення комунікацій та пришвидшення руху інформаційних потоків) суттєво трансформує глобальну реальність, а заразом і те, як саме використовуються ключові простори в інтересах геополітичних гравців» [1, с. 106]. Тому проблема сучасних викликів і загроз інформаційній безпеці України є вкрай актуальною.

Нині ще точаться суперечки про єдину глобальну інформаційну інфраструктуру, про універсальні способи доставки інформації, але позначилася цілком певна тенденція: панівної ролі набуває Інтернет, незаперечним лідером освоєння якого є США. Однак уже сьогодні існує думка про необхідність оптимізації шляхів глобальних інформаційних потоків. Тобто вже можна говорити про те, що світ стоїть на порозі нової сутички за контроль над інформаційним простором і «транспортуванням інформації».

Безумовно, в сучасних геополітичних умовах зростає значення інформаційного фактору. Чітко простежується тенденція підвищення ролі інформаційного ресурсу держав у загальній системі оборонного потенціалу. До найважливіших його елементів належать інформаційні системи і засоби стратегічного попередження, управління військами і зброєю, навігації, розвідки, радіоелектронної боротьби.

Досягнення інформаційної переваги (домінування) забезпечує можливість

випереджати суперника у прийнятті військово-політичних рішень і є основою й багато в чому запорукою успіху у воєнних діях. Як зазначають сучасні вітчизняні дослідники, науково-технічна революція створила глобальний інформаційний простір, у якому володіння інформаційними ресурсами стає головним фактором геополітичної конкуренції, тому інформаційна галузь належить до стратегічних інтересів будь-якої країни й потребує особливої уваги [2–4].

Технологічний відрив США, Японії та низки європейських країн, розгортання ними робіт зі створення на базі сучасних інформаційних технологій інформаційної зброї та військової техніки нового покоління ведуть до якісно нового етапу гонки озброєнь. Пріоритетний розвиток систем і засобів попередження про ракетно-ядерний напад, ППО і ПРО, зброї на нових фізичних принципах у сукупності призводить до критичного зниження ролі ядерного стримування.

Результати досліджень деяких вчених свідчать, що вплив на військово-інформаційний ресурс може стати одним із джерел небезпеки для національних інтересів. Останніми роками найбільш складною формою впливу вважається рефлексивне керування процесом прийняття військово-політичних рішень за допомогою цільового формування інформації чи дезінформації, що спонукає здійснювати бажані дії. Наприклад, цьому питанню приділяється велика увага в рамках прийнятої у США стратегічної концепції суперництва. Широке впровадження автоматизованих інформаційних систем відкриває нові можливості для несанкціонованого проникнення до закритої інформації і навіть її цільової зміни, як зазначає І. Лазарєв [5].

Таким чином, геополітичні трансформації зумовлюють характер відносин співробітництва і протиборства у XXI ст. Головна сфера протиборства – інформаційний простір глобального, регіонального і національного рівнів. Геополітичні умови визначають військово-інформаційну політику держави в найбільш важливих сферах геополітичного суперництва і протиборства.

Мета цієї статті – виокремити основні глобальні виклики й загрози інформаційній безпеці України в інформаційній сфері.

Результати проведених досліджень надають змогу виокремити такі основні геополітичні зміни в інформаційній сфері:

1) інформаційний простір західних держав стрімко перетворюється в єдиний глобальний інформаційний простір, де домінуючу роль у контролі над інформаційними потоками відіграють США і країни ЄС;

2) формується глобальна інформаційна інфраструктура на основі мережі Інтернет, що може розглядатися як посилення просторової взаємозалежності держав;

3) істотно розширився військово-інформаційний простір, контрольований країнами НАТО;

4) у сучасному інформаційному просторі підсилюються процеси, пов'язані з розвитком відносин партнерства та глобального інформаційного протистояння, розгорнутого РФ;

5) однією з основних сфер геополітичного протиборства стає інформаційний простір глобального, регіонального і національного рівнів. При цьому його пріоритет на вказаних рівнях залежить від конкретних цілей держави і може постійно змінюватися.

За довгостроковими прогнозами, перспективи світового розвитку визначатиме глобальне перегрупування сил у результаті інформаційного прогресу в США, ЄС, Японії, Китаї, Індії та Росії. Передбачається розвиток трьох потужних геостратегічних та інформаційних «центрів світу»: *американського* (США), *європейського* (Європейський Союз) й *азійського* (Китай, Індія, Японія). Подібним центром інформаційного впливу в сучасних умовах намагається стати і Російська Федерація. Україна в такій міжнародній конструкції посідає особливе місце завдяки геополітичному розташуванню.

За цих умов у різних країнах світу, зокрема в Росії, активно розробляються і застосовуються на практиці інформаційно-психологічні засоби ведення глобального інформаційного протиборства. Насамперед вони стосуються сфери використання інформації проти людського інтелекту.

Згідно з американською термінологією виділяють чотири основні категорії таких засобів:

– операції проти волі нації;

– операції проти командування супротивника;

– операції проти ворожих військ;

– операції на рівні національних культур.

Незважаючи на те, що засоби впливу (дезінформація, чутки, пропаганда, агітація, міфи тощо) залишилися колишніми, принципово новим елементом стали засоби одержання й доставки інформації. Це, зокрема, системи глобального та міжрегіонального телерадіомовлення, за допомогою яких реальні події з відповідними коментарями та спеціально підібрані факти й аргументи стають доступними аудиторії в багатьох країнах світу.

Украй важливою в контексті інформаційної безпеки людини, суспільства і держави є проблема протидії інформаційному насильству, інформаційним операціям та глобальному інформаційному протиборству (війнам) [6].

Для комплексного розгляду цих проблем у 2011–2014 рр. Національним інститутом стратегічних досліджень та Науково-дослідним інститутом інформатики і права НАПрН України спільно з іншими вітчизняними та іноземними партнерами проведено низку відповідних міжнародних, загальнодержавних і міжвідомчих наукових заходів. За їх результатами слід звернути увагу на деякі ключові проблеми інформаційної безпеки:

– в інформаційній сфері людства відбуваються революційні зміни і трансформації, які активізують нові глобальні виклики і загрози;

– більшість країн світу вже зіштовхнулася з проблемами кібертероризму, кіберзлочинності та іншими проблемами інформаційної безпеки;

– протягом останніх десятиліть спостерігається тенденція до поширення інформаційної агресії і насилля;

– набувають поширення спроби маніпуляції свідомістю людини, агресивна реклама, періодично проводяться інформаційно-психологічні операції;

– майже у 120 країнах світу (за оцінками американських експертів) ведуться розробки інформаційної зброї або її елементів (для порівняння – розробки зброї масового знищення здійснюються майже у 20 країнах);

– наслідки використання сучасної інформаційної зброї (згідно з висновками вчених та експертів європейських країн, України, РФ і США) можуть бути зіставними із застосуванням зброї масового ураження;

– новітні виклики і загрози в інформаційній сфері становлять реальну загрозу безпеці людства та міжнародному правопорядку.

За нашими оцінками, які знайшли підтримку в ході вказаних міжнародних заходів, жодна держава світу в умовах інформаційної глобалізації не здатна самостійно забезпечити власну інформаційну безпеку.

Узагальнюючи характер зовнішніх загроз інформаційній безпеці України, до їх основних джерел варто віднести:

1) діяльність іноземних політичних, економічних, військових, розвідувальних та інформаційних структур, спрямовану проти інтересів України в інформаційній сфері;

2) прагнення низки країн до домінування та обмеження інтересів України у світовому інформаційному просторі, витісненню її із зовнішнього і внутрішнього інформаційних ринків;

3) загострення міжнародної конкуренції за володіння інформаційними технологіями й ресурсами;

4) збільшення технологічного відриву провідних держав світу і нарощування їхніх можливостей з протидії створенню конкурентоздатних вітчизняних інформаційних технологій;

5) діяльність космічних, повітряних, морських, наземних технічних та інших засобів (видів) розвідки іноземних держав;

6) розробка низкою держав концепцій інформаційних воєн, що передбачають створення засобів небезпечного впливу на інформаційні сфери інших країн, порушення нормального функціонування інформаційних і телекомунікаційних систем, інформаційних ресурсів, одержання несанкціонованого доступу до них.

Крім цього, у контексті даного дослідження варто звернути увагу на основні види загроз інформаційній безпеці:

– витіснення вітчизняних інформаційних агентств, засобів масової інформації із внутрішнього інформаційного ринку та посилення залежності духовної, економічної і політичної сфер громадського життя України від закордонних інформаційних структур;

– маніпулювання інформацією (дезінформація, приховування чи перекручування інформації).

Із числа зовнішніх загроз інформаційній безпеці України у сфері зовнішньої політики найбільшу небезпеку становлять:

– інформаційний вплив іноземних політичних, економічних, військових та інформаційних структур на розробку і реалізацію зовнішньої політики держави;

– поширення за кордоном дезінформації про зовнішню політику України;

– порушення прав громадян і юридичних осіб в інформаційній сфері в Україні й за кордоном;

– спроби несанкціонованого доступу до інформації і впливу на інформаційні

ресурси, інформаційну інфраструктуру органів державної влади, що реалізують державну зовнішню політику, українських представництв і організацій за кордоном, представництв України при міжнародних організаціях.

Таким чином, останнім десятиліттям позначилися основні потенційні загрози інформаційній безпеці України. У світі відбулися певні позитивні зміни, що сприятливо позначилися на геополітичному становищі пострадянських країн, проте сучасний світ усе-таки не став більш стабільним і безпечним. На зміну колишньому ідеологічному протиборству прийшло геополітичне суперництво нових центрів сили. Інформаційне протистояння етносів, релігій і цивілізацій стало виходити на передній план у системі міждержавних відносин.

Специфіка періоду, що нині переживає Україна, характеризується пошуком вектора політичної орієнтації в міждержавному й геополітичному просторі. Позаяк, після здобуття незалежності якісно погіршилися її економічні, військові можливості, виникла безліч пов'язаних із агресивністю чинників, які загрожують національним інтересам або здатних при подальшому несприятливому розвитку подій трансформуватися в реальні загрози їх безпеці [7].

Загрози такого типу є постійними і притаманними як стабільним, так і транзитивним соціальним системам. Однак в умовах українського соціокультурного транзиту з'являється велика кількість нових загроз, які руйнують основи інформаційної безпеки людини, суспільства і держави.

Загалом, традиційний підхід до визначення загроз інформаційній безпеці дає змогу виокремити такі основні групи загроз.

Перша група пов'язана з бурхливим розвитком нового класу зброї – інформаційної, яка здатна ефективно впливати і на психіку, свідомість людей, і на інформаційно-технічну інфраструктуру суспільства й армії.

Друга група – інформаційно-технічні загрози для людини, суспільства і держави – це новий клас соціальних злочинів, що ґрунтується на використанні сучасної інформаційної технології (махінації з електронними грошима, комп'ютерне хуліганство тощо).

Третя група – електронний контроль за життям, настроями, планами громадян, політичних організацій.

Четверта група – використання нових інформаційних технологій з політичною метою.

Запропонований підхід до аналізу системи інформаційного забезпечення та інформаційної безпеки дає змогу виокремити такі головні групи загроз:

1) загрози, пов'язані з руйнуванням або деградацією базисної інформаційної підсистеми суспільства, що забезпечує збереження і розвиток його інформаційно-культурного ядра. Реальним носієм і зберігачем цього ядра є система освіти і виховання нових поколінь суспільства. Реальною загрозою для неї є, з одного боку, недостатня увага самого суспільства до захисту і розвитку свого інформаційно-культурного базису, а з другого – зайвий і не завжди позитивний інформаційний вплив на цю систему з боку інших держав, зацікавлених у її трансформації у прийнятному для них напрямі;

2) загрози, пов'язані з руйнуванням або деградацією динамічної продуктивної інформаційної підсистеми суспільства. Реальними виробниками у цій сфері є всі наукові, технічні, аналітичні, ідеологічні центри, що створюють або імпортують відповідну інформаційну продукцію та інформаційні технології.

В умовах динамічного формування й розвитку інформаційного суспільства та глобального інформаційного простору практично неможливо визначити виключний перелік загроз інформаційній безпеці. Водночас аналіз сучасних тенденцій розвитку інформаційної сфери на глобальному, регіональному і національному рівнях, наукових здобутків та нормативно-правових актів з цієї проблематики, у тому числі положень Доктрини інформаційної безпеки України [8], дає змогу виділити ключові реальні та потенційні виклики і загрози інформаційній безпеці України:

– наявність проблем формування і реалізації державної інформаційної політики, адекватної викликам і загрозам інформаційній безпеці України;

– відсутність ефективного інформаційно-аналітичного забезпечення діяльності керівництва держави та органів державної влади;

– спроби втручання у внутрішні справи України з боку іноземних держав, організацій, груп та осіб, задіяння засобів масової інформації іноземних держав та глобальних інформаційних мереж для підриву державного суверенітету, конституційного ладу, територіальної цілісності;

– використання інформаційного простору іноземними державами з метою інформаційної чи воєнної агресії; можливість втягування України у збройні конфлікти з іншими державами через використання національного сегменту кіберпростору;

– поширення негативних інформаційних та інформаційно-технологічних впливів на свідомість людини, здатних змінювати її психічні стани, психологічні та фізіологічні характеристики, здійснювати керований вплив на свободу вибору;

– створення іноземними державами кібервійськ, кіберпідрозділів у традиційних родах військ, розроблення нових видів інформаційної зброї та зброї кібернетичного характеру;

– критична залежність національної інформаційної інфраструктури від іноземних виробників високотехнологічної продукції; неналежний рівень інформатизації діяльності державних органів, органів місцевого самоврядування та інших напрямів інформаційної діяльності;

– відсутність ефективної державної стратегії та системи протидії зовнішній інформаційній експансії у національний інформаційний простір; обмеження свободи слова та поширення в засобах масової інформації культу насильства, жорстокості, зневажливого ставлення до людської і національної гідності, провокування протистояння в суспільстві;

– реалізація програмно-математичних засобів, що порушують функціонування інформаційних систем, радіоелектронне блокування засобів зв'язку та управління, включення у програмно-технічні засоби прихованих шкідливих функцій;

– використання неліцензованого і несертифікованого програмного забезпечення, засобів і комплексів обробки інформації, відсутність пріоритетного розвитку національного програмного забезпечення;

– недостатній рівень розвитку національної інформаційної інфраструктури, низька конкурентоздатність вітчизняних високотехнологічних виробництв інформаційних технологій, інформаційної продукції та послуг;

– недостатня надійність інформаційно-телекомунікаційних систем збирання, обробки та передачі інформації в умовах надзвичайних ситуацій, відсутність ефективних загальнодержавних та місцевих систем сповіщення, завчасного прогнозування і реагування на надзвичайні ситуації;

– прояви неправомірного доступу до персональних даних та інформаційних ресурсів органів державної влади і місцевого самоврядування; порушення встановленого порядку збирання, обробки, зберігання і передачі даних, а також розголошення інформації з обмеженим;

– незаконне перехоплення інформації в телекомунікаційних мережах, поширення правопорушень, терористичних, сепаратистських та інших злочинних проявів в інформаційній сфері; невідповідність юридичної відповідальності сучасним викликам і загрозам інформаційній безпеці;

– відсутність ефективного демократичного контролю за діяльністю суб'єктів забезпечення інформаційної безпеки, захищеності національної інформаційної інфраструктури та інформаційного простору України.

Зазвичай, переважна більшість указаних загроз притаманна як усталеним, так і транзитивним країнам, однак підкреслимо, що в умовах соціокультурного та економічного транзиту, який переживає Українська держава і суспільство, ці загрози актуалізуються й загострюються через неможливість ефективно протистояти їм наявної системи забезпечення національної безпеки.

Загалом можна зробити висновок, що внаслідок глобалізації, із розвитком глобального інформаційного простору інформаційне протиборство все більше утверджується як основний вид боротьби за сфери впливу, ресурси, владу та інші інтереси. Ця боротьба має своєю головною метою досягнення інформаційної переваги для контролю і керування свідомістю населення країн, переважно через засоби масової інформації та глобальні інформаційні мережі.

Сучасні виклики інформаційній безпеці України, як справедливо зазначають В. Конах та О. Лазоренко, зумовлені як внутрішніми, так і зовнішніми чинниками. Внутрішні – найбільшою мірою пов'язані з відсталістю інформаційних технологій в Україні від провідних країн світу, недостатньою дієвістю органів державної влади та законодавства в інформаційній сфері, а також байдужістю, низьким рівнем розуміння та професійної відповідальності як окремих груп, так і громадян, що нині провадять свою діяльність в інформаційному просторі України. Зовнішні – з намаганнями іноземних суб'єктів впливати на світовий та вітчизняний інформаційний простір з метою забезпечення власних інтересів» [9, с. 77].

У цій ситуації на перший план висуваються проблеми інформаційної безпеки, насамперед її інформаційно-психологічної складової. Нині очевидним постає і той факт, що чим більшими інформаційними можливостями володіє держава, тим імовірніше (за інших рівних умов), що вона досягне стратегічних переваг в інформаційному просторі. Це є особливо актуальним для визначення ролі й місця України в сучасних умовах інформаційної глобалізації.

Поширення й використання інформаційних технологій, ресурсів, продукції і послуг торкається інтересів усієї міжнародної спільноти і лише широке міжнародне співробітництво та міжнародно-правове регулювання здатне забезпечити їхнє безпечне застосування в інтересах кожної держави. Міжнародне співробітництво України в галузі інформаційної безпеки має будуватися на основі поєднання національних інтересів в інформаційній сфері, чітких уявлень про реальні та потенційні виклики і загрози, методи й засоби їх запобігання, виявлення і припинення, а також належного правового забезпечення.

Список використаних джерел

1. Дубов Д. В. Зрушення сфер геополітичного протиборства: від географічної експансії – до конструювання інформаційно-кібернетичних просторів / Д. В. Дубов // Стратегічні пріоритети. – 2014. – №1 (30). – С. 106–115.
2. Бондар Ю. В. Поле битви – інформаційний простір / Ю. В. Бондар. – К. : МАУП, 2006. – 152 с.
3. Виговська О. С. Державна інформаційна політика: концептуальні засади формування та розвитку / О. С. Виговська // Гілея: науковий вісник. – Вип. 82 (3) : зб. наук. пр. / голов. ред. В. М. Вашкевич. – К. : ПП «Вид-во "Гілея"», 2014. – С. 371–373.
4. Степанов В. Ю. Сучасний інформаційний простір: особливості та тенденції розвитку : монографія / В. Ю. Степанов. – Х. : [С. А. М.], 2010. – 280 с.
5. Лазарев И. А. США строят новую систему информационной безопасности / И. А. Лазарев // Эксперт. – 1999. – № 3. – С. 12–17.
6. Дзьобань О. П. Інформаційне насильство та безпека: світоглядно-правові аспекти : монографія / О. П. Дзьобань, В. Г. Пилипчук ; за заг. ред. проф. В. Г. Пилипчука. – Х. : Майдан, 2011. – 244 с.
7. Дзьобань О. П. Національна безпека України: концептуальні засади та світоглядний сенс : монографія / О. П. Дзьобань. – Х. : Майдан, 2007. – 284 с.
8. Про Доктрину інформаційної безпеки України [Електронний ресурс] : Указ Президента України від 08.07.2009 р. № 514/2009. – Режим доступу: http://www.president.gov.ua/documents/9570.html.
9. Конах В. К. Загрози та виклики національним інтересам України в інформаційній сфері в умовах глобалізації / В. К. Конах, О. А. Лазоренко // Стратегічні пріоритети. – 2014. – №2 (31). – С. 73–78.

Стаття надійшла до редколегії 10.09.2014

Пилипчук В., Дзебань А. Глобальные вызовы и угрозы национальной безопасности в информационной сфере

В статье рассмотрены основные геополитические изменения в информационной сфере, тенденции развития информационного пространства на глобальном, региональном и национаном уровнях, ключевые проблемы и современные вызовы и угрозы национальной безопасности в информационной сфере.

Ключевые слова: национальная безопасность, информационная сфера, информационная безопасность, вызовы и угрозы, информационное противоборство.

Pilipchuk V., Dzeban O. The Global Calls and Threats of National Safety in an Informative Sphere

The article reviews the main geopolitical changes in the information sector, development trends information space at global, regional and national levels, key issues and emerging challenges and threats to national security in the information sector.

The research is based on the complex application of research philosophy, general and applied levels of interconnection and complementarity.

Pointed out in major geopolitical changes in the information sector, including the rapid transformation of the information space western states into a single global information space with a dominant role in the control of information streams of United States and the EU; enhance spatial interdependence of states due to the global information infrastructure based on the Internet; significant expansion of military information space; reinforcement processes associated with the development of partnerships and global information counter, expanded the Russian Federation; converting the information space of global, regional and national levels on one of the main areas of geopolitical confrontation.

Substantiated the importance of information security in the context of human society and the state information counter problems of violence, information operations and global information confrontation (war).

The main sources of external information security threats Ukraine, including the activities of foreign political, economic, military, intelligence and information structures; desire of some countries to limit domination and interests of Ukraine in the global information space; aggravation of international competition for the possession of information technology and resources; increasing technological gap between the leading nations of the world and increase their ability to counter create competitive domestic information technology; activity space, air, sea, land and other technical means (types of) intelligence of foreign countries; development of a number of states concepts of information warfare.

The grounded key actual and potential challenges and threats to information security of Ukraine, including the existence of problems of formation and implementation of adequate public information policy; lack of effective information-analytical support of the leadership of the state and public authorities; attempts to interfere in the internal affairs of Ukraine from foreign countries by means of media and communication; Use of the information space by foreign States to information or military aggression; spread negative information and information technology's impact on the human mind; development of new types of foreign powers information weapons and weapons of cyber character; dependence of critical national information infrastructure from foreign manufacturers of high-tech products; lack of priority of the national software; low competitiveness of domestic high-tech industries of information technology; manifestations of unauthorized access to personal data and information resources of state and local governments; spread offenses, terrorist, separatist and other criminal offenses in the area of information; discrepancy legal liability modern challenges and threats to information security; lack of effective democratic control over the activities of information security, protection of the national information infrastructure and information space Ukraine.

It is concluded that international cooperation Ukraine in the field of information security should be based on a combination of national interests in the area of information, clear understanding of the real and potential threats and challenges, methods and means of prevention, detection and suppression, as well as the proper legal support.

Keywords: national safety, informative sphere, informative safety, calls and threats, informative opposing.