Ліпкан В.А.*

СУЧАСНИЙ ЗМІСТ ІНФОРМАЦІЙНИХ ОПЕРАЦІЙ ПРОТИ УКРАЇНИ

В статье исследуется информационная безопасность страны как органическая составляющая национальной безопасности и определяется, что главным стратегическим национальным ресурсом современного государства становятся информация и информационные технологии, которые являются действенным инструментом в информационном противоборстве между странами.

Ключевые слова: информационная безопасность, информация, информационные технологии, информационные операции

В статті досліджується інформаційна безпека країни як органічна складова національної безпеки та визначається, що головним стратегічним національним ресурсом сучасної держави є інформація та інформаційні технології, що стають дієвим інструментом в інформаційному протиборстві країн.

Ключові слова: інформаційна безпека, інформація, інформаційні технології, інформаційні операції

The author studies the state information security as an organic component of national security and determines that information and information technologies are the main strategic national resources of a state effectively used in the information fight.

Key words: information security, information, information technologies, information operations

Одержати сотні перемог у бою –
це не межа мистецтва.
Підкорити супротивника без бою —
ось це венець мистецтва.
Сунь Цзи

Інформаційна безпека України є органічною складовою національної, відтак її розгляд є необхідним для формування базових знань та уявлень про феномен національної безпеки. Інформаційна складова є іманентної будь–якої якої складової національної безпеки, а відтак можна упевнено твердити про її значущість для теоретичного осмислення

* професор кафедри управління в органах внутрішніх справ Національної академії внутрішніх справ, доктор юридичних наук, доцент; експерт Міжнародної громадської організації «Міжнародна антитерористична єдність»

і відпрацювання реальних механізмів формування не тільки позитивного іміджу, а й безпечного інформаційного середовища функціонування та розвитку держави Україна.

Актуальність розгляду даної теми обумовлена низкою чинників, серед яких я хотів би зосередити увагу на наступних:

- нині головним стратегічним національним ресурсом, основою економічної та оборонної могутності держави, а також основою взагалі існування держави стає інформація та інформаційні технології;
- інформація у сучасному світі виступає атрибутом, від якого у визначальному плані залежить ефективність життєдіяльності сучасного суспільства, його можливі трансформації від конструктивних до деструктивних;
- інформаційні технології принципово змінили обсяг і важливість інформації, яка обертається в технічних засобах її збереження, обробки і передачі;
- загальна комп'ютеризація основних сфер діяльності призвела до появи широкого спектру внутрішніх та зовнішніх загроз, нетрадиційних каналів втрати інформації і несанкціонованого доступу до неї і як наслідок використання почасти на шкоду невизначеної кількості осіб;
- масове оснащення державних установ, підприємств, організацій і приватних осіб засобами комп'ютерної техніки і включення їх у світовий інформаційних простір містить у собі реальну загрозу створення розгалужених систем регулярного несанкціонованого контролю за інформаційними процесами і ресурсами, навмисного втручання в них, встановлення керованих алгоритмів управління і впливу на формування свідомості;
- реальністю сьогодення стало застосування інформаційної зброї і ведення інформаційно–психологічних війн, які включають різні форми прояву і відповідно є різними за своїми наслідками;
- недосконаліть правового регулювання суспільних відносин в інформаційній сфері і у сфері інформаційної безпеки (передусім неврегульованість інтернет відносин, несформованість правового поля ефективного функціонування інформаційного суспільства) призводить до серйозних негативних наслідків, які знаходять свій вираз в ускладненні підтримання необхідного балансу інтересів особи, суспільства і держави, формування конкурентоспроможних місцевих інформаційних агентств і засобів масової інформації, як наслідок може відбуватися не тільки втрата галузей економіки, а й втрата державності (Єгипет, Туніс, Марокко, Йємен, Бахрейн, Лівія, Сірія, Йорданія);
- недобросовісне використання інформаційного простору зсередини держави призводить до зниження рівня не тільки внутрішньої інформаційної безпеки України, прямим наслідком чого є дестабілізація соціально–політичної та економічної обстановки, проведення акцій опору прийняттю тих чи інших державних рішень (так звані акції опозиції), а й зовнішньої — як то дискредитація іміджу вищих посадових осіб (формування образу слабких і керованих, таких, що не відстоюють національні інтереси), формування уявлення про Україну, як державу одвічно приречену на блукання манівцями двокутника: Європа – Росія тощо;
- конституційні права громадян на недоторканність приватного життя, особистої та сімейної таємниці, таємниці листування не мають достатнього організаційно–правового і технічного забезпечення (заяви спецслужб про нагальність доступу до поштових служб Gmail, Skype свідчить про те, що до інших поштових служб є нелегальний простий доступ);
- погіршується ситуація із забезпеченням збереження державної таємниці, недостатньо розвинені механізми забезпечення службової та комерційної таємниці (події із

майором Мельниченко довели необхідність посилення контролю за збереженням державної таємниці);

• суттєва шкода завдана кадровому потенціалу колективів тих підприємств, які діють в сфері створення засобів інформатизації (передусім це стосується не прозорих схем у сфері закупівлі спеціальної техніки для органів державної влади, як наслідок витіснення національних виробників з даного сегмента ринку);

• відставання вітчизняних інформаційних технологій змушує при створенні інформаційних систем закуповувати імпортну техніку і залучати іноземні фірми, через що підвищується імовірність несанкціонованого доступу до інформації, що обробляється і зростає залежність від іноземних виробників комп'ютерної і телекомунікаційної техніки, а також програмного забезпечення.

Відтак процес інформатизації суспільства розвивається стрімко і почасти непередбачено. Інформатизація призводить до створення єдиного інформаційного простору, в межах якого відбувається накопичення, обробка, зберігання ін інформацією між суб'єктами цього простору — окремими особами, організаціями, державами.

Поява і активізації загроз в інформаційній сфері, передусім загроз від ведення інформаційно–психологічних війн, суттєво підвищує роль і значення інформаційної безпеки в системі національної безпеки України, і обумовлює розширення її змісту. Головна проблема для України — збереження контролю над ресурсами, у тому числі інформаційними. У свою чергу, втрата контролю над інформаційними ресурсами, національними інформаційними комунікаціями у XXI столітті може призвести до втрати національної незалежності і розчиненні у глобальному котлі квазіутворень. Майбутні війни — війни без застосування прямого насильства, засобами якого є непрямі дії, одним з методів яких інформаційні війни. Яскравим прикладом несилового втручання у внутрішні справи є інспіровані ззовні через інформаційні війни громадянські війни у більшості країн північної Африки.

Саме тому, лишаючи осторонь теоретичні дискусії щодо визначення поняття інформаційної безпеки, викладення власного погляду на концептуальні питання (адже це мною вже зроблено в непоодиноких публікаціях), у даній статті хотів би зосередити увагу на окремих питаннях ведення інформаційних війн проти моєї Батьківщини — України.

Загрози інформаційній безпеці з одного боку є організаційним компонентом системи управління національною безпекою, а з іншого — рівень їхньої активізації слугує індикатором ефективності її функціонування. Адже реалізація загроз і переростання їх у небезпеки свідчить про неефективність функціонування даної системи, і навпаки. На сьогодні розглядати будь–які загрози в інформаційній сфері необхідно з урахуванням того контексту, в якому вони виникають і знаходять свій вияв. Найбільш небезпечною на даному етапі розвитку українського суспільства є інформаційні війни.

Поняття інформаційної війни

Намагання у повній мірі усвідомити усі грані поняття інформаційної війни нагадують здебільшого намагання сліпих, які прагнуть зрозуміти природу слона: той, хто дотикає ногу, кличе її деревом; хто дотикає хвоста — називає його канатом. Відверто скажемо, що питання формування понятійного апарату в сфері інформаційної безпеки ще остаточно не вирішені, адже навіть і зараз, коли факт необхідності теорії національної безпеки у світі вже є усвідомленим (це власне моє твердження, що ґрунтується на неодноразовому навчанні за кордоном), більшість українських «метрів» продовжують тупцювати на місці, заперечуючи даний очевидний факт, продовжуючи хизуватися лише власним надбанням, не звертаючи увагу на кращі зарубіжні та вітчизняні зразки. Причини такої наукової слі-

поти я не буду аналізувати в рамках даної статті, адже вони стануть предметом мого окремого розгляду. Натомість, хотів би ще раз підкреслити: несформованість категорійно–понятійного апарату теорії інформаційної безпеки передусім пов'язано із несформованістю загальної теорії національної безпеки — націобезпекознавства та її понятійного апарату.

Слід зазначити, що як інформаційні війна, так і інформаційне протиборство і інформаційна боротьба є проявами одного більш широкого поняття — загрози національним інтересам та національній безпеці в інформаційній сфері. Для більш комфортного розуміння як синонім до вище наведеного поняття будемо вважати вираз інформаційна безпека.

Найбільш широко загрози інформаційним ресурсам можна розглядати як потенційно можливі випадки природного, технічного або антропогенного характеру, які можуть спричинити небажаний вплив на інформаційну систему, а також на інформацію, яка зберігається в ній. Виникнення загрози, тобто віднаходження джерела актуалізації певних подій у загрози характеризується таким елементом як уразливість. Саме за наявності вразливості як певної характеристики системи і відбувається активізація загроз. Безперечно, що самі загрози за своєю суттю відповідно до теорії множин є невичерпними, а отже і не можуть бути піддані повному описові у будь–якому дослідженні.

Хотів би навести перелік даних загроз відповідно до Закону України «Про основи національної безпеки України»:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Думається, що таке знущання над реальністю, яке продемонстровано авторами даного закону, наносить пряму шкоду державі, адже в даному переліку по суті не зазначено жодної загрози для держави, а деякі з них носять характер на самих загроз, а методів інформаційного впливу на об'єкт управління.

Саме тому, хочу запропонувати власний варіант розуміння даної проблеми. Ключовим виступає родове поняття: інформаційне протиборство.

Інформаційне протиборство — суперництво соціальних систем (країн, блоків країн) в інформаційній сфері з приводу впливу на ті або інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, в результаті якого одна група учасників суперництва отримує переваги, необхідні їм для подальшого розвитку, з одночасної втратою таких іншими.

За інтенсивністю, масштабами та засобами, які використовуються, виділяють наступні рівні інформаційного протиборства: інформаційна експансія, інформаційна агресія і інформаційна війна.

Інформаційна експансія — вид інформаційного протиборства, що полягає у досягненні національних інтересів методом безконфліктного проникнення в інформаційну сферу і розширення власних можливостей із використанням інформаційних ресурсів з метою:

- поступової, плавної, непомітної для суспільства зміни системи соціальних відносин за зразком системи джерела експансії;

• витіснення положень національної ідеології і національної системи цінностей і заміщення їх власними цінностями і ідеологічними установками;

• збільшення ступеня свого впливу і присутності, встановлення контролю над стратегічними інформаційними ресурсами, інформаційно–телекомунікаційною структурою і національними ЗМІ;

• нарощування присутності власних ЗМІ в інформаційній сфері об'єкту проникнення і т.п.

Інформаційна агресія — вид інформаційного протиборства, який полягає у вчиненні незаконний дій однієї зі сторін в інформаційній сфері, спрямованих на нанесення супротивнику конкретної, відчутної шкоди в окремих сферах його діяльності шляхом обмеженого і локального за своїми масштабами застосування інформаційного впливу.

Ознаки інформаційної агресії:

• виключення із засобів інформаційної дії самих небезпечних видів, що не дозволяють надійно контролювати розміри спричиненої шкоди — інформаційної зброї;

• обмеження розмірів простору, об'єктів інформаційної інфраструктури і соціальних груп, що піддаються ураженню інформаційною дією (агресія зачіпає не весь інформаційний простір держави–жертви, а тільки його частине);

• обмеження за метою (переслідує локальну, приватну мету) і часом (як правило, агресія припиняється після повного досягнення агресором усієї поставленої конкретної мети і рідко носить тривалий характер), а також за силами і засобами, що залучається.

Інформаційна війна — найвищий рівень інформаційного протиборства, спрямований на розв'язання суспільно–політичних, ідеологічних, а також національних, територіальних та інших конфліктних ситуацій між державами, народами, націями, класами й соціальними групами, транснаціональними корпораціями шляхом широкомасштабної реалізації способів і методів інформаційного насильства (інформаційної зброї). Інформаційна війна переслідує глобальну мету: повалення уряду, зміну політико–правового режиму, інспірування громадянської війни, як джерела перманентного хаосу і відповідно контрольованого суб'єктом управління даним хаосом. Інформаційна війна не є обмеженою у просторово–часовому форматі, адже її мета полягає у встановленні керованого примусового алгоритму управління через застування засобів інформаційної війни.

В інформаційній сфері агресія переростає у війну в тому випадку, якщо одна із сторін конфлікту починає широко застосовувати проти своїх супротивників інформаційну зброю. Цей критерій дозволяє виділити зі всього різноманіття процесів і явищ, що відбуваються в інформаційному суспільстві такі, які представляють для його нормального (мирного) розвитку найбільшу небезпеку.

На сьогодні відсутні міжнародні і національні правові норми, які дозволяють в мирний час (за відсутності офіційного оголошення війни з боку агресора) юридично кваліфікувати ворожі дії іноземної держави в інформаційній сфері, що супроводжуються нанесенням шкоди інформаційній або іншій безпеці країни, як акції інформаційної агресії або інформаційної війни. Крім того, відсутні чіткі, однозначні, юридично закріплені критерії оцінки отриманого в результаті інформаційної агресії або інформаційної війни матеріальної, моральної, економічної та інших видів шкоди. Це дозволяє в мирний час активно використовувати самий небезпечний і агресивний арсенал сил і засобів інформаційної війни – як основний засіб досягнення політичної мети.

Беззаперечним лідером на шляху впровадження в практику концепції інформаційного протиборства є США. Досить сказати, що витрати, в цій країні на реалізацію даної концепції до 2005 р., становили понад 17 млрд. доларів. Концепція інформаційного проти-

борства США на воєнному рівні була покладена в основу при розробці аналогічних концепцій провідних західних країн, а також керівних документів НАТО по цим питанням, хоча офіційні джерела твердять про рівність учасників НАТО і не використання даних документів. Це твердження, знову ж таки є власним досвідом автора, адже 18 березня 2011 року в Київському інституті міжнародних відносин під час проведення відеоконференції із проблем інформаційної безпеки країн–учасниць НАТО із представниками НАТО мною було поставлено низку конкретних запитань, але відповідей не тільки не було, але й доповідач спробував відверто відмежуватись від американських концепцій інформаційних війн. То виходить або даний «фахівець» з Брюсселю був абсолютно не обізнаний в темі, щодо якої робив доповідь, або свідомо уводив в оману представницьку публіку в Україні.

Розроблена в США концепція інформаційного протиборства передбачає його ведення на воєнному та державному рівнях. На державному рівні метою інформаційного протиборства є послаблення позицій конкуруючих держав, підрив їх національно–державних основ, порушення системи національного управління за рахунок інформаційного впливу на політичну, дипломатичну, економічну і соціальну сфери життєдіяльності країни, проведення психологічних операцій, підривних та інших деморалізуючих пропагандистських акцій. Воно спрямовано на забезпечення національних інтересів США, упередження міжнародних конфліктів, терористичних акцій, забезпечення інформаційної безпеки країни. Воно розглядається як вид стратегічного протиборства країн.

За висновками аналітиків американської корпорації «Ренд» воно передбачає вирішення наступних задач:

- створення в країні противника атмосфери бездуховності, негативного відношення до культурної спадщини (згадаємо, чим переповнені вітчизняні телеканали: бойовики, трілери, шоу);
- маніпулювання суспільною свідомістю і політичною орієнтацією груп населення держави з метою створення політичної напруги і хаосу (постійне протиставлення російськомовних – українськомовним, сходу і заходу, багатих і бідних, донецьких і київських);
- дестабілізація політичних відношень між партіями, об'єднаннями і рухами з метою провокації конфліктів, розпалення недовіри, підозрілості, загострення політичної боротьби, провокування репресій проти опозиції і навіть громадянської війни та інші (створення зі звичайних злочинців жертв репресій опозиції, розігрування політичної складової у суто кримінальних справах);
- зниження рівня інформаційного забезпечення органів влади і управління, ініціація помилкових управлінських рішень (впровадження в інститути державної влади принципів кумовстсва, родинних, а також територіальних, що створює основу для унеможливлення прийняття загальнодержавних виважених рішень);
- дезінформування населення про роботу державних органів, підрив їх авторитета, дискредитація органів управління (за даними Міністра закордонних справ України українські літаки були другі в світі, які евакуювали громадян більш ніж 20 країн з Японії, і першими евакуювали громадян 60 країн світу з Лівії, у тому числі і громадян США. Натомість ця інформація не є відомою широкому загалу, навпаки: більшість громадян України впевнена у безпорадності української влади, що насправді не відповідає дійсності);
- провокування соціальних, політичних, національних і релігійних зіткнень, ініціювання страйків, масових заворушень та інших акцій економічного протесту (за деякими даними за можливим провокаціями на релігійному і соціальному ґрунті стоять мільярдери з–за кордону, яких не влаштовує сучасна влада в Україні);
- ускладнення прийняття органами управління важливих рішень;

• підрив міжнародного авторитету держави, її співробітництва з іншими країнами (постійне обливання брудом за кордоном нашої країни і керівництва держави не сприяє формуванню не тільки позитивного іміджу, а й ускладнює налагодження співпраці з міжнародними інституціями).

• Основними формами інформаційного протиборства на державному рівні є:

• політичні, дипломатичні й економічні акції;

• інформаційні і психологічні операції;

• підривні і деморалізуючі пропагандистські дії;

• сприяння опозиційним і дисидентським рухам;

• надання усебічного впливу на політичне і культурне життя з метою розвалу національно–державних підвалин суспільства;

• проникнення в систему державного керування.

На воєнному рівні на наш погляд доцільно використовувати термін інформаційна боротьба за аналогією радіоелектронна боротьба, психологічна боротьба. Інформаційна боротьба визначається як комплекс заходів, які проводяться в масштабах ЗС для досягнення інформаційної переваги над противником шляхом впливу на інформацію, якою він володіє, процеси, що залежать від інформації, інформаційні системи, комп'ютерні мережі з одночасним захистом від аналогічних впливів з боку противника. Виділяються наступальна й оборонна складові інформаційної боротьби. Крім того, перед ЗС вперше поставлене завдання впливу на противника ще в загрозливий період з тим, щоб забезпечити вигідний для США напрямок процесів управління і прийняття рішень протилежною стороною.

Отже, основним завданням інформаційної боротьби є :

• отримання розвідувальної інформації шляхом перехвату та розшифровки інформаційних потоків, що передаються по каналам зв'язку, а також по побічним випромінюванням, а також за рахунок спеціального втілення технічних засобів перехвату інформації;

• отримання потрібної інформації шляхом перехвату і обробки відкритої інформації, що передається по незахищеним каналам зв'язку , циркулює в інформаційних системах, а також опублікованої у відкритих джерелах та ЗМІ;

• електромагнітний вплив на елементи інформаційних і телекомунікаційних систем;

• психологічний вплив, спрямований проти персоналу та осіб, що приймають рішення;

• формування і масоване розповсюдження по інформаційним каналам противника та глобальним мережам дезінформації та тенденційної інформації;

• вогневе придушення (у воєнний час) елементів інфраструктури державного і воєнного управління;

• здійснення несанкціонованого доступу до інформаційних ресурсів з подальшим їх викривленням, знищенням або викраденням, або порушенням нормального функціонування таких систем;

• захист від аналогічних впливів збоку противника.

• Отже основною метою інформаційних війн проти України є:

• ізоляція України на міжнародній арені;

• підрив морально–психологічного стану військовослужбовців і населення держави;

• посилення антивоєнних і антиурядових настроїв у країні противника;

• консолідація населення й особового складу своїх збройних сил і країн–союзників.

Однією з головних цілей інформаційної війни є подавлення в людині морального творчого початку.

Література

1. An Introduction to Computer Security: The Nist Handbook.Draft. – National Institute of Standart and Technology, Technology Administration U. S. Department of Comerce, 1994.
2. Актуальні проблеми інформаційної безпеки України. Аналітична доповідь УЦЕПД / /Національна безпека і оборона. –К.: 2001. –№1. –С. 2–59.
3. Актуальні проблеми інформаційної безпеки України: аналіт. доп. УЦЕПД) // «Нац. безпека і оборона». – 2001. – №1 (13). – С. 2–50.
4. Андреев В. Развитие информационного пространства Украины и цивилизованное вхождение в информационное общество XXI века // Техника спец. назначения. – 2002. – № 1–2. – С. 16–17.
5. Арістова І.В. Державна інформаційна політика: організаційно–правові аспекти / МВС України, Ун–т внут. справ, За заг. ред. О.М. Бандурки – Х., 2000. –366 с.
6. Аркуша Л.І. Проблеми взаємодії та інформаційного забезпечення правоохоронних органів у боротьбі з економічною організованою злочинною діяльністю // Информационное обеспечение противодействия организованной преступности: Сб.науч.ст. / Под ред. М. Ф. Орзиха, В. Н. Дремина. — О.: Фенікс, 2003. – С. 109–117. – Библиотека журнала «Юридический вестник».
7. Атаманчук Г.В. Новое государство: поиски, иллюзии, возможности. – М.: «Славян. диалог»,1996. – 223 с.
8. Афанасьев В. Г. Социальная информация / Под. ред. Л. Ф. Пирожкова. – М.: Гран, 1994. – 164 с.
9. Базанов Ю., Баранов О., Брижко В. Права человека и защита персональных данных. – К.: Госкомитет связи и информатизации Украины, 2000. – 84 с.
10. Бакуменко В.Д. Теоретико–методологічні засади формування державно–управлінських рішень: Автореф… док–ра. наук з держ.упр: 25.00.01 / Укр. акад. держ. упр. при Президентові України – К., 2001, –36 с.
11. Баранов А. Информационный суверенитет или информационная безопасность ? // Нац. безпека і оборона. – 2001. – № 1 (13). – С. 70–76.
12. Баранов А. Информационный суверенитет или информационная безопасность? // Національна безпека і оборона. –К.:2001. –С. 70–76.
13. Бачило И. Л. Правовое регулирование процессов информатизации // Государство и право. – 1994. – № 12. – С. 72.
14. Бачило И. Л., Лопатин В. Н., Федотов М. А. Информационное право / Под ред. Б. Н. Топорнина. – Санкт–Петербург: Юрид. центр «Пресс». – 2001. –328 с.
15. Без свободи слова немає демократії // Уряд. кур'єр. – 2001. – 17 січн. – С. 1–2.
16. Гавловський В. І. ін. Організаційно–правові питання формування державної інформаційної політики в Україні // Наук. вісн. зб. наук. пр. Акад. держ. податков. служби України. – 2002 – № 3. – С. 177–182.
17. Гавловський В., Гуцалюк М., Калюжний Р. ін. Питання концепції реформи інформаційного законодавства України. // Правов., нормат. та метрол. забезпечення системи захисту інформації в Україні. – 2000. – № 1 – С. 17–21.
18. Гавловський В., Гуцалюк М., Калюжний Р. Інформаційному суспільству України – інформаційне законодавство (щодо питань реформування законодавства у сфері суспільних інформаційних відносин) // Правов., нормат. та метрол. забезпечення системи захисту інформації в Україні. – 2001. № 2. – С. 7–11.
19. Гавловський В., Гуцалюк М., Цимбалюк В. Удосконалення інформаційного законодавства як засіб оптимізації протидії комп'ютерній злочинності // Наук. вісн. Нац. акад.внутр. справ України. – 2001. – № 3 – С. 20–24.

20. Гавловський В., Калюжний Р., Цимбалюк В. ін. Проблеми державної інформаційної політики: гармонізація міжнародного і національного інформаційного права // Прав., нормат. та метрол. забезпечення системи захисту інформації в Україні. – 2001. – № 4.
21. Гавловський В., Калюжний Р., Цимбалюк В.С. та ін. Інформаційне законодавство України: концептуальні основи формування // Право України. – 2001. – № 7. – С. 88–91.
22. Гавловський В.Д, Голубєв В.О., Цимбалюк В.С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій – Х.: Фоліо, 2002. – 284 с.
23. Гавловський В.Д., Гуцалюк М.В., Калюжний Р.А. та ін. Інформаційне забезпечення управлінської діяльності в умовах інформатизації: організаційно–правові питання теорії й практики. – Запоріжжя: Просвіта, 2002. – С. 38.
24. Герасименко В. А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994. – 400 с.
25. Голубєв В. О. Захист банківської інформації від несанкціонованого доступу // Правов., нормат. та метрол. забезпечення системи захисту інформації в Україні: Матеріали міжнар. наук.–практ. конф. – К., 1998. – С. 50–53.
26. Голубєв В. О. Правові аспекти захисту інформаційних технологій // Вісн. Запоріз. юрид. інст–ту МВС України. –1997. – № 2. – С. 35–40.
27. Голубєв В. О. Правові аспекти захисту інформації // Правов., нормат. та метрол. забезпечення системи захисту інформації в автоматизованих системах України. – К., 1998. – С. 44.
28. Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій / За заг. ред. Р.А. Калюжного, М.Я. Швеця . – Запоріжжя : Просвіта, 2001. – 252 с.
29. Литвиненко О. В. Спеціальні інформаційні операції та пропагандистські кампанії: Моногр. – К., – 2000. – 222 с.
30. Литвиненко О.В. Проблеми забезпечення інформаційної безпеки в пострадянських країнах (на прикладі України та Росії): Автореф. дис. ... канд. політ. наук . 23.00.04. – К., 1997. – 18 с.
31. Литвиненко О.В. Спеціальні інформаційні операції. — К.: Рада національної безпеки і оборони України; Національний ін–т стратегічних досліджень, 1999. — 163 с.
32. Ліпкан В.А., Максименко Ю.Є., В.М.Желіховський Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. — К.: КНТ, 2006. — 280 с. (Серія: Національна і міжнародна безпека)
33. Ліпкан В.А. Теоретичні основи та елементи національної безпеки України: Монографія. — К.: Текст, 2003. — С. 333 – 343.
34. Лопатин В. Н. Информационная безопасность России: Человек. Общество. Государство / Санкт–Петербургский университет МВД России. –СПб: Фонд «Университет, 2000. –С. 347–348. – 428 с.
35. Лопатин В.Н. Информационная безопасность: Человек. Общество. Государство: Санкт–Петербург ун–т МВД России. – СПб: Фонд «Университет», 2000. – 426 с.
36. Лопатин В.Н. Информационная безопасность в системе государственного управления: Теоретические и организационно–правовые проблемы: Дис. … канд. юрид. наук: 12.00.02. — СПб., 1997. — 193 с.
37. Мазур М. Качественная теория информации. – М.: Прогресс, 1982.– 249 с.
38. Матвеев М. М. Взаимодействие представительных и исполнительных органов в системе местного самоуправления: Автореф. дис. ... канд. юрид. наук. 12.00.02. – М., 1992. – 18 с.

39. Національна безпека України 1994–1996 рр. /Ред. О.Ф.Белов – К.: НІСД, 1997.– 200 с.
40. Нечипоренко В. П. Информационный капитал научно–технической деятельности // НТИ. – 1998. – Сер.1. – № 11. – С. 2– 8.
41. Нижник В. Н., Ситник Г.П., Білоус В. Т. Національна безпека України (методологічні аспекти, стан і тенденції розвитку): Навч. посіб. / За заг.ред. П.В. Мельника, Н.Р. Нижник. – Ірпінь, 2000. – 304 с.
42. Нижник Н. Р., Машков О.А. Системний підхід в організації державного управління: Посіб. / За ред. Н. Р. Нижник – К.: Вид–во УАДУ, 1998. – С. 85.
43. Общая теория национальной безопасности: Учебник, Под общ. ред. А.А.Прохожева. — М.: Изд–во РАГС, 2002. — 320 с.
44. Олійник О.В., Соснін О.В. Правові проблеми регулювання інформаційної діяльності // Стратег. панорама. – 2002. – № 4,– С. 166–174.
45. Оцінка Електронної готовності України /Стратегічні рекомендації/ Доповідь у рамках проекту Уряду України / ПРООН – «Інноваційний трамплін: ІКТ задля добробуту України». – К.: Держ. ком. зв'язку та інформатизації України, – 2002 . – 8 с.
46. Павлютенкова М. Информационная война — реальная угроза или современный миф? // Власть. — 2001. — № 12. — С. 19 – 23.
47. Почепцов Г. Г. Национальная безопасность Украины в контексте вопросов и парадоксов // Зеркало недели. – 1997. – 7–14 нояб.
48. Почепцов Г.Г. Национальная безопасность стран переходного периода: [Учеб.пособие для студентов спец. «Международная информация»] / Ин–т содерж.методов обучения. Ин–т междунар. отношений Киев. Нац.Ун–та им Т.Шевченко – К., 1996. –134 с.
49. Правовая информатика и кибернетика: Учебник // Под ред. Н.С.Полевого. — М.: Юрид. лит., 1993. — 528 с.
50. Расторгуев С.П. Философия информационной войны. — М.: Вузовская книга, 2001. — 468 с.
51. Рибак М. І., Атрохов А. В. До питання про інформаційні війни // Наука і оборона. – № 2.– 1998. – С. 65–68.