УДК 340.13 + 007.51 + 165.12

ФУРАШЕВ В.М., *кандидат технічних наук, старший науковий співробітник, доцент, професор РАЕ*

ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Анотація. *Обґрунтування необхідності розробки та впровадження ситемоутворюючого законодавчого акта у сфері забезпечення інформаційної безпеки України та окреслення основних його положень.*

Ключові слова: *закон, інформаційна безпека, національна безпека, захист інформації, кіберпростір, кібербезпека, кібернетична безпека.*

Аннотация. *Обоснование необходимости разработки и внедрения системообразующего законодательного акта в сфере обеспечения информационной безопасности Украины и обозначение основных его положений.*

Ключевые слова: *закон, информационная безопасность, национальная безопасность, защита информации, киберпространство, кибербезопасность, кибернетическая безопасность.*

Summary. *Justification of the need to develop and implement a systemically important legislative act in the sphere of ensuring the information security of Ukraine and designation of its basic provisions.*

Keywords: *law, information security, national security, information protection, cyberspace, cyber security, cybernetic security.*

Постановка проблеми. У світлі подій, які розгорнулися в Україні та у світі, в цілому, вирішення питань законодавчого забезпечення інформаційної безпеки України набули невідкладного характеру.

Може виникнути два основних питання: що, наявної правової бази у цій сфері не достатньо? та чому саме інформаційної, а не кібербезпеки (кібернетичної безпеки)?

Й дійсно, по першому питанню, проблеми інформаційної безпеки країни не залишилися без уваги законодавців та керівників держави. На даний час в Україні наявна досить солідна нормативно-правова база у цій сфері [1 – 31].

Але проблема полягає у певній розпорошеності питань забезпечення інформаційної безпеки вказаної нормативно-правової бази, що суттєво знижує ефективність правового регулювання у цій сфері. Крім того, у даній нормативно-правовій базі часто застосовуються терміни без надання їх визначення, що надає змогу вільного їх трактування, а і відповідно, прийняття рішень, в тому числі і судових, на основі цих трактувань.

Що стосується другого питання, то дослідження [32] досить переконливо показали, що кіберпростір є невід’ємною складовою інформаційного простору, а і відповідно, поняття “інформаційна безпека” є ширшим поняттям від поняття “кібернетична безпека”. Тому поняття “кібербезпека (кібернетична безпека)” та “інформаційна безпека”, у визначеній сфері застосування, є тотожними за своєю сутністю. Застосування будь-якого з цих понять не змінює сутності процесу або явища. Тому, з огляду на це, і пропонується розглянути питання законодавчого забезпечення саме інформаційної безпеки України.

Метою статті є окреслення основних положень системостворюючого проекту Закону України “Про інформаційну безпеку України”.

Виклад основних положень. Найголовніше, на думку автора, у будь-якому законодавчому, іншому нормативно-правовому акті, з самого початку чітко означити предмет регулювання, тобто, надати чітке трактування того чи іншого терміна, який застосовується у даному акті. Це є основою для чіткого розуміння предмета регулювання та подальших дій щодо його застосування у практичній діяльності, в тому числі і розробка Стратегії інформаційної безпеки України, а також доктрини, концепції і відповідних програм, якими визначаються цільові настанови, принципи і напрями діяльності державних органів, військових формувань, органів місцевої влади та місцевого самоврядування, інститутів громадського суспільства та інших суб’єктів забезпечення інформаційної безпеки України та прийняття рішень щодо дій, спрямованих на порушення або не порушення складових інформаційної безпеки.

Необхідно також додати, що питання вирішення проблем інформаційної безпеки найголовнішою з яких є дилема між гарантованістю прав і свобод суспільства збирати, зберігати, використовувати і поширювати інформацію та об’єктивного вимушеного правового обмеження, неможливе без чіткого визначення об’єктів та суб’єктів права у всій його сукупності, виходячи із сутності явища, процесу, процедур тощо [33].

Саме тому, під час розробки системостворюючого законодавчого акта у сфері забезпечення інформаційної безпеки України, пропонується надання наступних термінів та їх визначень:

вірогідність інформації – віддзеркалення дійсності (істинного стану справ); достовірність (міра наближеності інформації до першоджерела або точність передачі інформації);

вчасність інформації – ознака того, що вона є саме тією, яка потрібна на даний момент; важливість, істотність у певний момент часу;

доступність інформації – здатність забезпечення, при необхідності, своєчасного безперешкодного доступу до інформації, що цікавить;

інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдання шкоди через: негативний інформаційний вплив за допомогою, в першу чергу, несанкціонованого створення, розповсюдження, використання свідомо спрямованої із визначеною метою неповної, невчасної, невірогідної та упередженої інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням;

інформаційна небезпека – стан життєво важливих інтересів людини, суспільства і держави, при якому можливо, зі значним ступенем вірогідності, нанесення їм шкоди через негативний інформаційний вплив за допомогою, в першу чергу, несанкціонованого створення, розповсюдження, використання свідомо спрямованої із визначеною метою неповної, невчасної, невірогідної та упередженої інформації; негативні наслідки застосування інформаційних технологій; несанкціоноване порушення режиму доступу до інформації з подальшим її розповсюдженням та використанням;

інформаційний простір – форма співіснування сукупності матеріальних та нематеріальних об’єктів і процесів, спрямованих на задоволення інформаційних потреб всіх живих істот на Землі;

інформаційна інфраструктура – сукупність організаційних структур та систем, які забезпечують функціонування та розвиток інформаційного простору, а також засобів інформаційної взаємодії до доступу користувачів (громадян та організацій) до інформаційних ресурсів. Включає в себе сукупність інформаційних центрів, підсистем,

банків даних і знань, систем зв’язку, центрів управління, апаратно-програмних засобів і технологій забезпечення збору, збереження, обробки та передання інформації;

кібербезпека (кібернетична безпека) – стан спроможності людини, суспільства і держави запобігання та уникнення спрямованого, в першу чергу – несвідомого, негативного впливу (управління) інформації;

кіберпростір (кібернетичний простір) – це форма співіснування сукупності матеріальних та нематеріальних об’єктів і процесів, спрямованих на породження, сприйняття, запам`ятовування, переробку та обмін інформацією. Кіберпростір – це віртуальний світ, який базується на реальному матеріальному фундаменті та з реальними наслідками свого “існування та розвитку”. Кіберпростір є невід’ємною складовою інформаційного простору;

комп`ютерний тероризм – різновид технологічного тероризму;

комп`ютерна злочинність – правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; за навмисне перехоплення технічними засобами, без права на це передач комп’ютерних даних; за навмисне пошкодження, знищення, погіршення, зміну або приховування комп’ютерної інформації без права на це; навмисне серйозне перешкоджання функціонуванню комп’ютерної системи;

конфіденційність інформації – властивість захищеності інформації від несанкціонованого доступу та спроб її розкриття користувачем, що не має відповідних повноважень;

народна дипломатія – союзи народів, а не держав, невід’ємною часткою яких є громадські організації, діяльність яких спрямована на вирішення більшості тих питань, якими займається офіційна дипломатія, але на неофіційному, суто людському, рівні (*зовнішній аспект*); діяльність громадських організацій, окремих громадян, яка спрямована на запобігання та уникнення або врегулювання внутрішніх конфліктів та непорозумінь, які можуть негативно впливати на національні інтереси та національну безпеку, а також пошуку шляхів та інструментаріїв посилення здійснення офіційної дипломатії (*внутрішній аспект*);

національний сегмент кіберпростору – це форма співіснування сукупності матеріальних та нематеріальних об`єктів і процесів, спрямованих на породження, сприйняття, запам`ятовування, переробку та обмін інформацією, розміщених на території України;

об’єкти інформаційного простору – суб’єкти природного середовища, природні та штучні інформаційні відносини між ними, процеси і процедури їх формування і використання, матеріальні та нематеріальні об’єкти і процеси, спрямовані на задоволення інформаційних потреб для забезпечення збереження життя та життєдіяльності живої істоти, угруповання живих істот;

об’єкти кіберпростору – живі істоти та їх угруповання, які спроможні сприймати, запам’ятовувати та переробляти інформацію, а також обмінюватися нею, серед яких, в першу чергу, людина, визначені верстви суспільства та суспільство в цілому, держава, природні та штучні інформаційні відносини між ними, процеси і процедури їх формування і використання, а також матеріальні та нематеріальні об`єкти і процеси, спрямовані на породження, сприйняття, запам’ятовування, збереження, переробку та обмін інформацією;

повнота інформації – віддзеркалення вичерпного характеру відповідності одержаних відомостей цілям збору; достатність для розуміння ситуації та прийняття рішення; характеристика, яка визначає кількість інформації, необхідної та достатньої для прийняття вірного рішення;

публічна дипломатія – це відображена та доведена до суспільства інформація по здійсненню цілей і завдань зовнішньої політики держави суб’єктами офіційної дипломатії;

санкціонованість поширення інформації – процес надання інформації споживачам, в рамках обумовлених повноважень;

цілісність інформації – показник того, що дані повні, умови того, що дані не були змінені при виконанні будь-якої операції над ними, будь то передача, зберігання або представлення.

Цілком розуміючи, що законотворча практика не передбачає концентрування такої кількості термінів та визначень у одному законопроекті, автор не очікує повної реалізації даної пропозиції. Головна мета полягає у привертанні уваги до цієї проблематики, яку, за бажанням, можливо вирішити шляхом внесення відповідних змін до чинних законів України у даній сфері.

Питання реальних та потенційних загроз інформаційній безпеці України досить повно розкрито у Законі України “Про основи національної безпеки України” [3] та Доктрині інформаційної безпеки України [22].

Серед принципів забезпечення інформаційної безпеки України, зокрема таких, як верховенство права, пріоритетність захисту прав і свобод людини і громадянина в інформаційній сфері, свобода збирання, зберігання, використання та поширення інформації, достовірність, повнота та неупередженість інформації, запобігання правопорушенням в інформаційній сфері та ін., доцільно зазначити:

- розмежування повноважень та взаємодія державних і недержавних суб’єктів забезпечення інформаційної безпеки з максимальним застосуванням механізмів публічної та народної дипломатії;
- особистої відповідальності громадян за власну безпеку, неухильного дотримання ними правил безпечної поведінки у сфері інформаційної безпеки, визначеної законодавством України;
- своєчасність і адекватність заходів захисту національних інтересів реальним і потенційним загрозам у сфері інформаційної безпеки;
- використання в інтересах України міждержавних систем та механізмів міжнародної колективної безпеки у сфері інформаційної безпеки.

До об’єктів інформаційної безпеки, поряд з людиною і громадянином, тобто, їхніми конституційними правами і свободою, фізичним та психологічним здоров’ям, захищеністю від негативного впливу інформаційних технологій та інформації, а також інформаційними ресурсами та інформаційною інфраструктурою (їх цілісністю, доступністю та захищеністю) та суспільством і державою (захищеністю їх законних інтересів в інформаційній сфері) слід також додати складові інформаційної інфраструктури.

Дуже важливим є визначення суб’єктів забезпечення інформаційної безпеки країни.

Виходячи з того, що інформаційна безпека є, з одного боку, невід’ємною складовою національної безпеки [22], а, з іншого – самостійною сферою в системі безпеки країни, то досить логічним буде визначення суб’єктами забезпечення інформаційної безпеки суб’єктів забезпечення національної безпеки країни [3].

Але при цьому необхідно враховувати, що, як було вище зазначено, функції та конкретні завдання по забезпеченню інформаційної безпеки, “розпорошені” по різних функціонально-тематичних нормативно-правових документах, які, переважною більшістю, знайшли відповідне відображення у функціональних обов`язках та повноваженнях органів центральної виконавчої влади. Але це не дозволяє з повною впевненістю стверджувати, що дані функціональні обов’язки та повноваження

“перекривають” увесь спектр завдань та злагодженість дій по забезпеченню інформаційної безпеки.

Аналогічна ситуація була і у питаннях забезпечення національної безпеки України, вихід було знайдено на законодавчому рівні шляхом утворення Ради національної безпеки та оборони України [1 – 2, ст. 107] та віднесення її до суб`єктів забезпечення національної безпеки [3, ст. 4].

Враховуючи значимість, причому постійно зростаючу, у системі забезпечення національної безпеки, без сумніву необхідний спеціально уповноважений орган, який би був координуючим та контролюючим органом у сфері забезпечення інформаційної безпеки та одним із суб’єктів забезпечення національної безпеки країни.

Що це за орган, самостійний або при якомусь іншому суб’єкті забезпечення інформаційної безпеки країни, з якими функціональними обов’язками та повноваженнями та ін.? Це дуже непрості питання, за вирішення яких не слід допустити помилок.

Під час вирішення поставлених вище питань, незалежно від форми державного управління – президентсько-парламентської або парламентсько-президентської, необхідно враховувати, що:

- Президент України “***забезпечує*** *державну незалежність, національну безпеку і правонаступництво держави*” та “***здійснює керівництво*** *у сферах національної безпеки та оборони держави*” [1 – 2, ст. 107] (*виділено Авт.*);

- Кабінет Міністрів України “***забезпечує*** *державний суверенітет і економічну самостійність України,* ***здійснення*** *внутрішньої і зовнішньої політики держави, виконання Конституції і законів України, актів Президента України*”, “***здійснює*** *заходи щодо забезпечення обороноздатності і національної безпеки України, громадського порядку, боротьби зі злочинністю*” та “***спрямовує і координує*** *роботу міністерств, інших органів виконавчої влади*” [1 – 2, ст. 116] (*виділено Авт.*).

З наведеного можна зробити висновок, що з одного боку, саме Президент України визначає стратегічні напрями у сфері національної безпеки та її складової – інформаційної безпеки, а з іншого боку – всі тактичні рішення та ресурсне забезпечення і координацію зусиль по їх реалізації здійснює Кабінет Міністрів України.

У даній ситуації виникає, можливо й некоректне питання, але принципове – що, з точки зору забезпечення інформаційної безпеки, важливіше: певна стабільна діяльність по розробці та супроводженню стратегічних напрямів забезпечення інформаційної безпеки або повсякденна, рутинна робота по розробці та практичній реалізації тактичних рішень втілення у життя цих стратегічних рішень, які потребують визначених, причому немаленьких, ресурсів та постійної координації всіх учасників цього процесу?

Для вирішення питань стратегічного характеру у сфері інформаційної безпеки є конституційний орган – Рада національної безпеки і оборони, рішення якої вводяться у дію указами Президента України, що є обов’язковими до виконання на території України та у яких є відповідні доручення Кабінету Міністрів України і, за необхідності, визначеним органам виконавчої влади та місцевого самоврядування.

Логічним було би утворення спеціально уповноваженого органу, який би був координуючим та контролюючим органом у сфері забезпечення інформаційної безпеки, тим більше, що є позитивний досвід організації та діяльності подібного органу – Державної комісії з питань запобігання та усунення можливих наслідків комп’ютерної кризи 2000 року [34].

Необов’язково даний уповноважений орган має бути у формі Державної, Національної або Урядової комісії. Може бути утворена інша координаційна інформаційно-аналітична структура при Кабінеті Міністрів України. Головне – у розробці та прийнятті рішень даного уповноваженого органу мають брати участь або безпосередньо керівники суб’єктів забезпечення інформаційної безпеки, або їх перші заступники, а дані рішення – обов’язкові до виконання на всій території України всіма органами виконавчої влади та органами місцевого самоврядування. Крім того, даний орган повинен бути постійно-діючим з широко розгалуженою мережею регіональних комісій.

Що стосується повноважень уповноваженого органу у сфері забезпечення інформаційної безпеки, то за “базу” можна взяти Положення про Державну комісію з питань запобігання та усунення можливих негативних наслідків комп’ютерної кризи 2000 року [34].

Що стосується повноважень інших суб’єктів забезпечення інформаційної безпеки України, то вони повинні бути кореспондовані з повноваженнями суб’єктів забезпечення національної безпеки. але з урахуванням особливостей цієї сфери безпеки.

У якості основних напрямів державної політики у сфері забезпечення інформаційної безпеки України вважається доцільним відображення:

- неухильного дотримання конституційного права громадян на свободу слова, доступу до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації, дискримінації в інформаційній сфері і переслідування журналістів за політичні позиції;

- формування та реалізація державної політики національного духовного та культурного відродження, яка відповідає інтересам Українського народу і визначає чіткі критерії і пріоритети формування національної інформаційної політики;

- інформаційно-психологічний аспект, зокрема щодо забезпечення конституційних прав і свобод людини і громадянина, створення сприятливого психологічного клімату в національному інформаційному просторі задля утвердження загальнолюдських та національних моральних цінностей.

З метою реалізації зазначених основних напрямів державної політики необхідно законодавчо закріпити здійснення наступних заходів:

гармонізацію законодавства України з питань інформаційної безпеки в сферах забезпечення національної безпеки з міжнародними нормами і стандартами;

створення дієвої та прозорої системи громадського контролю за діяльністю органів державної влади і органів місцевого самоврядування, громадсько-політичних структур та посилення взаємодії органів державної влади з громадськими організаціями у сфері боротьби з проявами обмеження конституційних прав і свобод людини і громадянина та маніпулювання масовою свідомістю;

запобігання монополізації національного інформаційного простору шляхом вдосконалення законодавчого регулювання процесів придбання, управління і використання засобів масової інформації, в тому числі й електронних інформаційних ресурсів, та забезпечення підтримки діяльності, спрямованої на формування оптимістичної морально-психологічної атмосфери в суспільстві, популяризації національних культурних цінностей, сприяння соціальній стабільності і злагоді, а також державної підтримки вітчизняного виробника інформаційної продукції;

залучення засобів масової інформації до неухильного додержання конституційних прав і свобод людини і громадянина, захисту конституційного устрою, вдосконалення

системи політичної влади з метою зміцнення демократії, духовних та моральних засад суспільства; підвищення ефективності функціонування органів державної влади;

посилення державного контролю за додержанням вимог інформаційної безпеки в системах збирання, обробки, зберігання і передачі інформації відповідно до положень національних нормативно-правових актів та міжнародних документів, ратифікованих Верховною Радою України;

захист інформації, зокрема щодо забезпечення конфіденційності, цілісності та доступності інформації, в тому числі технічного захисту інформації в національних інформаційних ресурсах від кібернетичних атак;

забезпечення своєчасного виявлення зовнішніх загроз національному інформаційному суверенітету та їх нейтралізації шляхом постійного удосконалення форм і способів протидії інформаційно-психологічним операціям, спрямованих на послаблення національної безпеки держави, підготовка спеціалістів з питань інформаційної безпеки;

посилення інформаційно-просвітницької діяльності серед населення щодо забезпечення інформаційної безпеки України;

формування вітчизняної індустрії високотехнологічної продукції, насамперед комп'ютерно-телекомунікаційних засобів і технологій, інформаційних послуг із забезпеченням їх конкурентоспроможності, підвищення ефективності використання державних, корпоративних і приватних інформаційних ресурсів;

розвиток національної інформаційної інфраструктури на засадах стимулювання вітчизняних виробників і користувачів новітніми інформаційно-телекомунікаційними засобами і технологіями, комп’ютерними системами і мережами національного походження;

технологічного розвитку, зокрема щодо розбудови та інноваційного оновлення національних інформаційних ресурсів, впровадження новітніх технологій створення, обробки та поширення інформації, в першу чергу, вітчизняного виробництва;

науково-технологічного супроводу формування і розвитку в Україні інформаційного суспільства з урахуванням вимог забезпечення інформаційної безпеки України на засадах підвищення технологічної конкурентоспроможності України у сфері інформатизації та зв’язку, удосконалення системи охорони та захисту права інтелектуальної власності, розширення можливостей доступу громадян до світового інформаційного простору, зокрема до наукової та науково-технічної інформації, інтеграції в міжнародні інформаційно-телекомунікаційні системи та організації на засадах рівноправності, економічної доцільності та збереження інформаційного суверенітету та розвитку міжнародного науково-технічного співробітництва в сфері забезпечення захисту інформації у міжнародних телекомунікаційних системах;

організаційно-технічне, інформаційне та ресурсне сприяння держави реалізації заходів по забезпеченню інформаційної безпеки.

Висновки.

1. Питання розробки та впровадження системоутворюючого законодавчого акта по забезпеченню інформаційної безпеки стало вже не просто актуальним, воно вже стало нагальним.

2. У даному дослідженні запропоновано основні підходи та конкретні положення системоутворюючого законодавчого акта по забезпеченню інформаційної безпеки.

Використана література

1. Конституція України : Закон України від 28.06.96 р. № 254к/96-ВР // Відомості Верховної Ради України (ВВР). – 1996. – № 30. – Ст. 141.

2. Про внесення змін до Конституції України : Закон України від 08.12.04 р. № 2222- IV // Відомості Верховної Ради України (ВВР). – 2005. – № 2. – С. 65. – Ст. 44.

3. Про основи національної безпеки України: Закон України від 19.06.03 р. № 964-IV // Відомості Верховної Ради України (ВВР). – 2003. – № 39. – Ст. 351.

4. Про Національну програму інформатизації : Закон України від 04.02.98 р. № 74/98-ВР // Відомості Верховної Ради України (ВВР). – 1998. – № 27-28. – Ст.181.

5. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.94 р. №80/94-ВР // Відомості Верховної Ради України (ВВР). – 1994. – № 31. – Ст. 286.

6. Про внесення змін до Закону України “Про інформацію” : Закон України від 13.01.11 р. № 2938-VI // Офіційний вісник України. – 2011. – № 10.

7. Про захист персональних даних : Закон України від 01.06.10 р. № 2297-VI : за станом на 16.01.12 р. // Відомості Верховної Ради України (ВВР). – 2010. – № 34. – С. 1188. – Ст. 481.

8. Про доступ до публічної інформації : Закон України від 13.01.11 р. № 2939-VI // Відомості Верховної Ради України. – 2011. – № 32. – С. 1491. – Ст. 314.

9. Про боротьбу з тероризмом : Закон України від 20.03.03 р. № 638-IV // Відомості Верховної Ради України (ВВР). – 2003. – № 25. – Ст.180.

10. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.05 р. № 2824- IV // Відомості Верховної Ради України (ВВР). – 2006. – № 5-6. – С. 128. – Ст.71.

11. Про електронні документи та електронний документообіг : Закон України від 22.05.03 р. № 851-IV : за станом на 16.01.12 р. // Відомості Верховної Ради України (ВВР). – 2003. – № 36. – Ст. 275.

12. Про електронний цифровий підпис : Закон України від 22.05.03 р. № 852-IV // Відомості Верховної Ради України (ВВР). – 2003. – № 36. – Ст. 276.

13. Про науково-технічну інформацію : Закон України від 25.06.93 р. № 3322-XII // Відомості Верховної Ради України (ВВР). – 1993. – № 33. – Ст. 345.

14. Про телекомунікації : Закон України від 18.11.03 р. № 1280-IV : за станом на 16.01.12 р. // Відомості Верховної Ради України (ВВР). – 2004. – № 12. – Ст. 155.

15. Кримінальний кодекс України : Закон України від 05.04.01 р. № 2341-III // Відомості Верховної Ради України. – 2001. – № 25. – Ст. 131.

16. Кримінальн-процесуальний кодекс України : Закон України від 13.04.12 р. № 4651-VI // Відомості Верховної Ради України (ВВР). – 2013. – № 9-10. – С. 474. – Ст. 88.

17. Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки : Закон України від 09.01.07 р. № 537-V // Відомості Верховної Ради України(ВВР). – 2007. – № 12. – С. 511. – Ст. 102.

18. Про кіберзлочинність : Конвенція Ради Європи від 23.11.01 р. № 994-575. – Режим доступу: http://zakon2.rada.gov.ua.

19. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобського характеру, вчинених через комп’ютерні системи від 28.01.03 р. // Офіційний вісник України. – 2010. – № 56.

20. Про підсумки парламентських слухань “Інформаційна політика України : стан і перспективи” : Постанова Верховної Ради України від 02.06.99 р. № 705-XIV // Голос України від 12.06.1999.

21. Про Рекомендації парламентських слухань з питань розвитку інформаційного суспільства в Україні : Постанова Верховної Ради України від 01.12.05 р. № 3175-XIV // Відомості Верховної Ради України(ВВР). – 2006. – № 15. – Стор. 604, – Ст. 131.

22. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 514/2009 // Офіційний вісник Президента України. – 2009. – № 20. – С. 18. – Ст. 677.

23. Про рішення Ради національної безпеки і оборони України від 17 червня 1997 року “Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин” : Указ Президента України від 21.07.97 р. № 663/97 // Урядовий кур’єр від 24.07.1997 р.

24. Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року “Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України” : Указ Президента України від 06.12.01 р. № 1193/2001 // Офіційний вісник України. – 2001. – № 50. – С. 28. – Ст. 2228.

25. Про рішення Ради національної безпеки і оборони України від 21 березня 2008 року “Про невідкладні заходи щодо забезпечення інформаційної безпеки України” : Указ Президента України від 23.04.08 р. № 377/2008 // Офіційний вісник Президента України. – 2008 р. – № 18. – С. 24. – Ст. 570.

26. Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року “Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України” : Указ Президента України від 06.12.01 р. № 1193/2001 // Офіційний вісник України. – 2001 р. – № 50. – С. 28. – Ст. 2228.

27. Про рішення Ради національної безпеки і оборони України від 21 березня 2008 року “Про невідкладні заходи щодо забезпечення інформаційної безпеки України” : Указ Президента України від 23.04.08 р. № 377/2008 // Офіційний вісник Президента України. – 2008 р. – № 18. – С. 24. – Ст. 570.

28. Про Доктрину інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 514/2009 // Офіційний вісник Президента України. – 2009. – № 20. – С. 18. – Ст. 677.

29. Про затвердження Концепції технічного захисту інформації в Україні : Постанова Кабінету Міністрів України від 08.10.97 р. №1126 : зі змінами станом на 16.01.12 р. – Режим доступу : http://zakon2.rada.gov.ua

30. Про затвердження Порядку взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах : Постанова Кабінету Міністрів України від 16.11.02 р. № 1772 // Офіційний вісник України. – 2002. – № 47. – С. 182. – Ст. 2155.

31. Про затвердження Державної цільової науково-технічної програми використання в органах державної влади програмного забезпечення з відкритим кодом на 2012 – 2015 роки : Постанова Кабінету Міністрів України від 30.11.11 р. № 1269 // Офіційний вісник України. – 2011. – № 96. – С. 32. – Ст. 3503.

32. В. Фурашев. Основні стримуючі фактори правового забезпечення інформаційної безпеки // Інформація і право. – № 2(5)/2012. – С. 163-170.

33. Фурашев В.М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності // Інформація і право. – № 2(8)/2013. – С. 113-119.

34. Про Державну комісію з питань запобігання та усунення можливих негативних наслідків комп’ютерної кризи 2000 року : Постанова Кабінету Міністрів України від 16.02.99 р. № 218 // Офіційний вісник України. – 1999 р. – № 7. – С. 146.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~