УДК 342.951:004

ЗОЛОТАР О.О., *кандидат юридичних наук, старший науковий співробітник,*
Науково-дослідний інститут інформатики і права НАПрН України
ТРУБІН І.О., *кандидат юридичних наук,*
Науково-дослідний інститут фінансового права

КЛАСИФІКАЦІЯ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ

Анотація. *Стаття присвячена аналізу наукових поглядів та стану нормативно-правового регулювання класифікації загроз інформаційній безпеці.*
Ключові слова*: інформаційна безпека, класифікація, загроза інформаційній безпеці.*

Аннотация*. Статья посвящена анализу научных взглядов и состояния нормативно-правового регулирования классификации угроз информационной безопасности.*
Ключевые слова: *информационная безопасность, классификация, угроза информационной безопасности.*

Summary*. The article is concerned with analysis of scientific views and the legal regulation of the classification of information security threats.*
Keywords*: information security, classification, information security threat.*

Постановка проблеми. В сучасних умовах розвиток більшості країн світу відбувається під впливом інтеграційних процесів. Якщо в окремих випадках (на рівні окремих країн) спостерігається добровільне об’єднання, то в інших заінтересовані у відповідному процесі держави спонукають до об’єднання шляхом використання спеціальних засобів та проведення відповідних заходів, зокрема і в інформаційній сфері, спрямованих на завдання шкоди для досягнення власних цілей.

Саме інформаційна сфера є однією з найбільш важливих, і її захист визначається серед пріоритетів державної політики. Необхідність підтримання безпеки схвалена на державному рівні, що пояснює активну діяльність уповноважених органів влади спрямовану на забезпечення інформаційної безпеки відносин, пов’язаних із збиранням, накопиченням, обробкою та передачею інформації.

Осторонь від цих перетворень не залишається й наука. Вчені досить активно беруть участь у розробці теоретичних положень, що стосуються інформаційної безпеки та можуть бути враховані у процесі прийняття політичних рішень. Предметом наукових дискусій є, як загальні організаційно-правові аспекти інформаційної безпеки, так і спеціальні, до яких можна віднести визначення загроз інформаційній безпеці, їх класифікацію тощо.

Варто зазначити, що питання пов’язані з темою дослідження, зустрічаються в працях: Берко А., Бодрука О., Бойченко О., Гуцу С., Живко З., Євдоченко Л., Кормича Б., Кузьменко Б., Євдоченко Л., Ліпкана В., Литвиненка О., Логінова А., Макарової М., Марущака А., Максименка Ю., Пилипчука В., Погребняка А. та інших.

Незважаючи на значний рівень наукового осмислення проблем інформаційної безпеки, питання загроз, зокрема їх класифікації, мають дискусійний характер, що й обумовлює актуальність статті. Водночас, теоретичні розробки досліджуваного питання необхідні для формування дієвої системи моніторингу та управління у сфері інформаційної безпеки, а також вдосконалення відповідної нормативно-правової бази.

Метою статті є узагальнення наукових поглядів щодо класифікації загроз інформаційній безпеці та оцінка положень відповідних нормативно-правових актів.

Задля досягнення поставленої мети визначені *завдання*:

– дослідження та узагальнення сучасних наукових підходів до класифікації загроз інформаційній безпеці;

– аналіз положень національного законодавства, що визначає загрози національній безпеці;

– формулювання авторського концептуального підходу до класифікації загроз інформаційній безпеці.

Виклад основного матеріалу. Розвиток інформаційного суспільства і, як результат, перетворення в різних сферах суспільних відносин, включаючи й економічні, призвели до появи ряду позитивних і негативних наслідків. До позитивних наслідків відносять такі: пришвидшення передачі інформації значного обсягу, прискорення її обробки та впровадження [16, с. 3], своєрідну трансформацію інформації, яка в наш час ототожнюється з цифровим або віртуальним простором.

Б. Кормич зазначає, що основні дії щодо збирання, зберігання, передачі та розповсюдження інформації здійснюються за допомогою спеціальних технічних засобів і технологій. Відповідно з розвитком науки та техніки ці інформаційні засоби і технології перетворилися на один із найважливіших компонентів інформаційних процесів, одночасно із самою інформацією та суб’єктами інформаційних відносин [9, с. 322]. Значною мірою розвиток вищезгаданих інформаційних засобів й технологій має одночасні негативні прояви – як то збільшення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків і баз даних, порушення технологій обробки інформації, запуску програм-вірусів, знищення та модифікація даних в інформаційних системах, перехоплення інформації в технічних каналах її витоку [16, с. 3].

У зв’язку з цим окремим предметом наукових дискусій є питання щодо безпеки та захищеності відносин, пов’язаних зі збором, обробкою, зберіганням й використанням інформації. У співвідношенні з поняттями “безпека” та “захищеність” “загрозою” можна вважати можливу небезпеку, тобто будь-які дії чи події, які можуть настати за різних обставин у навколишньому середовищі та стати передумовою порушення безпеки і завдання збитків.

Узагалі в інформаційних відносинах протягом останніх років сформувався та закріпився термін “інформаційна безпека”, під яким розуміють стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається завдано шкоди через: неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [16]. Тобто вже в цьому визначенні закладено певні підстави для класифікації, однак про це згодом.

На думку В. Ліпкана, загрози національним інтересам та національній безпеці в інформаційній сфері є синонімом поняття “інформаційна безпека” [13].

Інформаційна безпека є невід’ємним напрямом розбудови інформаційного суспільства, розвиток якого повинен відбуватись не тільки через нарощування технологічних можливостей здійснення інформаційного обміну, а й шляхом глибокого усвідомлення усіма суб’єктами інформаційних відносин – власниками інформації та її користувачами, виробниками інформаційних технологій і засобів, постачальниками послуг, державою – необхідності здійснення всіх заходів щодо інформаційних ресурсів та забезпечення інформаційної безпеки держави [3, с. 51].

Щодо правової науки, то, на думку А. Марущака, поглиблення досліджень з проблем інформаційної безпеки потрібно віднести до пріоритетів розвитку інформаційного права України. Загрози національній безпеці України, що виникають у сфері національних інформаційних ресурсів, зумовлюють актуальність наукових пошуків з проблем правомірного використання телекомунікацій у сучасному інформаційному суспільстві, юридичних механізмів протидії кібернетичним загрозам [17, с. 22].

Рівень сучасних викликів і загроз в інформаційній сфері наочно підтверджує справедливість і виключну значущість положень статті 17 Конституції України про те, що захист державного суверенітету і забезпечення інформаційної безпеки є однією з основних функцій держави і всього українського народу [20, с. 20].

Інформаційна безпека як складова національної безпеки відповідно до сучасного розвитку її теорії в узагальненому вигляді ґрунтується на таких базових елементах: національні інтереси – загроза – захист [18, с. 8]. Саме загрози стану захищеності суспільних відносин є важливим елементом процесу забезпечення інформаційної безпеки.

На нашу думку, це пояснюється тим, що інформаційну небезпеку створюють інформаційні загрози, які поширюються в інформаційному просторі. При цьому, інформаційні загрози – це сукупність умов і факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства, держави в інформаційній сфері [19, с. 59].

Враховуючи те, що інформаційна безпека є невід’ємною складовою національної безпеки, її регулювання потребує дієвих механізмів у формі політичних рішень або прийнятих нормативно-правових актів. Функціонування відповідного механізму, на нашу думку, можливе лише за умови належного рівня наукового осмислення теоретичних положень щодо інформаційної безпеки взагалі та сутності загроз зокрема. Чинники, що зумовлюють ескалацію загроз інформаційній безпеці, мають комплексний характер – вони охоплюють усі сфери життєдіяльності людини, суспільства і держави, а відповідно мають міжвідомчий характер. Таким чином, на практиці аналіз загроз – це завжди суб’єктивний процес сприйняття певною особою чи соціальною групою певних факторів через призму власних інтересів і фахового рівня. Разом із тим, об’єктивне визначення загроз передбачає чітке усвідомлення параметрів, поза межами яких певне явище втрачає можливості саморегуляції та потребує зовнішнього втручання для збереження стабільності соціальної системи, а також певних умов, що перетворюють ті ж самі фактори або на реальну, або на потенційну загрозу [2].

Досліджуючи відносини у сфері забезпечення інформаційної безпеки, науковці звертають свою увагу на таке поняття, як “загрози інформаційній безпеці”. Подальше заглиблення в процес наукового пізнання згаданого питання дало змогу виявити відсутність єдності у поглядах, що стосуються класифікації відповідних загроз як на нормативно-правовому, так і на науковому рівнях.

Відповідно до Закону України “Про основи національної безпеки України” до загроз національним інтересам і національній безпеці в інформаційній сфері відносять наступні: 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 [23].

Доктрина інформаційної безпеки України визначає основні реальні та потенційні загрози інформаційній безпеці України, класифікуючи їх за сферами життєдіяльності особи, суспільства і держави, зокрема: у зовнішньополітичній сфері, сфері державної безпеки, воєнній, внутрішньополітичній, економічній, соціальній та гуманітарній, науково-технологічній, в екологічній сферах [5].

У Законі України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 − 2015 роки” загрозами інформаційній безпеці визначено: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [24].

У Державному стандарті України “Захист інформації. Технічний захист інформації. Основні положення” – ДСТУ 3396.0-96 безпосереднє формулювання класифікації загроз відсутнє, проте в ньому передбачено можливі шляхи реалізації загроз. Саме вони дають можливість уявити або визначити ймовірні загрози інформаційним відносинам (відносинам щодо збору, обробки й накопичення інформації). У частині 4.1.3 підпункту 4.1 пункту 4 визначено, що загрози можуть здійснюватися:

– технічними каналами, що включають канали побічних електромагнітних випромінювань і наводок, акустичні, оптичні, радіо-, радіотехнічні, хімічні та інші канали;

– каналами спеціального впливу шляхом формування полів і сигналів з метою руйнування системи захисту або порушення цілісності інформації;

– несанкціонованим доступом шляхом підключення до апаратури та ліній зв’язку, маскування під зареєстрованого користувача, подолання заходів захисту для використання інформації або нав’язування хибної інформації, застосування закладних пристроїв чи програм та вкорінення комп’ютерних вірусів [7].

Як критерій можна використати: спосіб впливу на інформацію або шляхи реалізації загроз.

Постанова Кабінету Міністрів України “Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах” містить пункт 16 Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, який визначає, що для забезпечення захисту інформації в системі створюється комплексна система захисту інформації (далі – система захисту), яка призначається для захисту інформації від:

– витоку технічними каналами, до яких належать канали побічних електромагнітних випромінювань і наведень, акустично-електричні та інші канали, що утворюються під впливом фізичних процесів під час функціонування засобів обробки інформації, інших технічних засобів і комунікацій;

– несанкціонованих дій з інформацією, у тому числі з використанням комп’ютерних вірусів;

– спеціального впливу на засоби обробки інформації, який здійснюється шляхом формування фізичних полів і сигналів та може призвести до порушення її цілісності та несанкціонованого блокування [22].

Як критерій можна використати: спосіб впливу на інформацію або шляхи реалізації загроз.

Державний стандарт України “Захист інформації. Технічний захист інформації. Терміни та визначення” – ДСТУ 3396.2-97 містить ряд термінів, пов’язаних з інформаційною безпекою, які мають пряме відношення до класифікації загроз [8].

Так, пункт 5 “Загроза для інформації” містить наступні визначення:

5.1. Витік інформації – неконтрольоване поширення інформації, яке призводить до її несанкціонованого одержання.

5.2. Порушення цілісності інформації – спотворення інформації, її руйнування або знищення.

5.3. Блокування інформації – унеможливлення санкціонованого доступу до інформації.

Класифікація загроз відповідно має наступний вигляд: загрози витоку інформації; загрози порушення цілісності інформації; загрози блокування інформації. Загальний критерій не визначено.

Така різноманітність класифікацій в чинному законодавстві обумовлена не лише різноманітними підходами до вибору класифікаційних ознак та цілями класифікації, а й відсутність належного теоретичного обґрунтування сутності загроз інформаційній безпеці. З метою узагальнення існуючих наукових поглядів щодо класифікації загроз інформаційній безпеці та визначення концептуального підходу до формулювання цього елементу правовідносин пропонуємо розглянути окремі з них.

Згадуваний вище професор В. Ліпкан пропонує класифікувати загрози інформаційній безпеці відповідно до загальної класифікації загроз національній безпеці: за джерелами походження: природного походження, техногенного походження, антропогенного походження; за ступенем гіпотетичної шкоди: загроза та небезпека; за повторюваністю вчинення: повторювані та продовжувані; за сферами походження: екзогенні та ендогенні; за ймовірністю реалізації: вірогідні, неможливі, випадкові; за рівнем детермінізму: закономірні та випадкові; за значенням: допустимі та неприпустимі; за структурою впливу: системні, структурні та елементні; за характером реалізації: реальні, потенційні, здійснені, уявні; за ставленням до них: об’єктивні та суб’єктивні; за об’єктом впливу – особа; суспільство; держава [13].

В іншій праці, інтегруючи різноманітні підходи, а також пропозиції щодо розв’язання даного питання, запропоновано такі види загроз інформаційній безпеці: розкриття інформаційних ресурсів; порушення їх цілісності; збій в роботі самого обладнання [12].

Схожі погляди на перелік загроз інформаційній безпеці висловлює: А. Логінов у власному дисертаційному дослідженні. Зокрема, вчений визначає загрози як:

- розкриття інформаційних ресурсів;
- порушення цілісності інформаційних ресурсів;
- збій у роботі обладнання [14].

Б. Кузьменко та О. Чайковська пропонують класифікацію загроз, яка ґрунтується на визначенні властивостей інформації:

- загрози порушення конфіденційності інформації, в результаті реалізації яких інформація стає доступною суб’єкту, що не володіє повноваженнями для ознайомлення з нею;
- загрози порушення цілісності інформації, до яких відноситься будь-яке зловмисне спотворення інформації, оброблюваної з використанням автоматизованих систем;
- загрози порушення доступності інформації, що виникають в тих випадках, коли доступ до деякого ресурсу автоматизованих систем для легальних користувачів блокується [10, с. 6-7].

У свою чергу С. Гуцу [4] та О. Литвиненко [11] сходяться на тому, що основні загрози інформаційній безпеці можна представити у такому вигляді:

– загрози впливу неякісної інформації (недостовірної, фальшивої, дезінформації) на особистість, суспільство, державу;

– загрози несанкціонованого й неправомірного впливу сторонніх осіб на інформацію і інформаційні ресурси (їх виробництво, системи формування й використання);

– загрози інформаційним правам і свободам особистості (праву на виробництво інформації, її поширення, пошук, одержання, передавання та використання; праву на інтелектуальну власність на інформацію, в тому числі й речову).

Л. Євдоченко, формуючи власний підхід до класифікації інформаційних загроз та з метою вироблення рекомендацій щодо організації державою дієвих форм і методів забезпечення інформаційної безпеки, визначає і класифікує загрози за кількома критеріями: за способом впливу на об’єкти інформаційної безпеки (інформаційні, фізичні й програмно-математичні, організаційно-правові); за джерелами надходження (внутрішні та зовнішні); за характером вияву (політичні, економічні, організаційно-технічні) [6, с. 8].

Визначальною для процесу наукового пізнання є теза, що:

– трактування проблем, пов’язаних з інформаційною безпекою, для різних категорій суб’єктів може істотно відрізнятися, наприклад, безпека для закритих державних організацій та комерційних структур;

– інформаційна безпека не полягає винятково у захисті інформації. Це принципово ширше поняття. Суб’єкт інформаційних відносин може постраждати (отримати матеріальні і/або моральні збитки) не тільки від несанкціонованого доступу до інформації, а й від пошкодження системи, що зумовить перерву в роботі [1, с. 20].

Тому цілком логічними та вартими на увагу є класифікації загроз які мають більш вузький або, іншими словами, спеціальний характер, зокрема загрози інформаційній безпеці мережевих ресурсів.

Наприклад, М. Макарова виділяє такі ймовірні загрози в мережі:

– дані навмисно перехоплюються, читаються або змінюються;

– користувачі ідентифікують себе неправильно (з шахрайською метою);

– користувач отримує несанкціонований доступ з однієї мережі до іншої [15, с. 188].

У цьому ж контексті ширшу класифікацію пропонує А. Погребняк, який зазначає, що загрози можуть бути як випадковими, так і навмисними.

До випадкових загроз відносяться: а) помилки обслуговуючого персоналу і користувачів; б) втрата інформації внаслідок неправильного її збереження; в) випадкове знищення або заміна; г) збій у роботі устаткування, електроживлення, дискових систем, комплектуючих елементів мережі; ґ) некоректна робота програмного забезпечення, зокрема внаслідок зараження комп’ютерними вірусами тощо [21, с. 46-47].

До навмисних загроз відносяться: а) несанкціонований доступ до інформації і мережевих ресурсів; б) розкриття і модифікація даних і програм, їх копіювання; в) розкриття, модифікація або підміна трафіка обчислювальної мережі; г) розробка і поширення комп’ютерних вірусів, введення в програмне забезпечення логічних бомб; ґ) крадіжка магнітних носіїв і розрахункових документів; д) руйнування архівної інформації або навмисне її знищення; е) фальсифікація повідомлень, відмова від факту одержання інформації або зміна часу його прийому; є) перехоплення та ознайомлення з інформацією, яка передана по каналах зв’язку [21, с. 50].

Висновки.

Будь-яка з наведених класифікацій до певної міри є умовною, оскільки:

1) залежно від мети та методів наукового пізнання може здійснюватись за різними підставами;

2) має суб’єктивний характер, тобто залежно від суб’єкта, що її здійснює, та його здатності розрізняти ознаки об’єкта класифікації.

У підсумку також варто відзначити теоретико-прикладне значення класифікації інформаційній безпеці. Вона обумовлена потребою внутрішньо-логічної впорядкованості цієї системи і, на нашу думку, виконує дві важливі функції – евристичну и аналітичну. Евристична функція забезпечує пошук, виявлення існуючих загроз, орієнтацію в них, вивчення сукупності певних груп, що стосуються окремих об’єктів та суб’єктів безпеки, умов часу і простору. Аналітична функція полягає у розробці методів аналізу цих загроз, перевірки її достовірності, виявлення шляхів їх нейтралізації.

Так, на теоретичному рівні вироблення єдиного підходу до критеріїв класифікації не є самоціллю, оскільки залежить від конкретних потреб теорії та практики. Водночас, це є одним із шляхів упорядкування понятійно-категоріального апарату такої науки та галузі, як інформаційне право. З практичної точки зору питання, що досліджується, безпосередньо пов’язане з реалізацією цілей розвитку інформаційного суспільства та напрямів відповідної національної політики, що визначаються в Основних засадах розвитку інформаційного суспільства в Україні на 2007 – 2015 роки.

Використана література

1. Берко А.Ю. Методи та засоби оцінювання ризиків безпеки інформації в системах електронної комерції / А.Ю Берко, В.А. Висоцька, І.В. Рішняк // Вісник Національного університету “Львівська політехніка”. – 2008. – № 610. – С. 20-33.

2. Бодрук О. Структури воєнної безпеки : національний та міжнародний аспекти : монографія / О. Бодрук. – К. : НІПМБ, 2001. – 300 с. – С. 37

3. Бойченко О. В. Політика інформаційної безпеки в системі інформаційного забезпечення органів внутрішніх справ // Форум права. – 2009. – № 1. – С.50-55.

4. Гуцу С.Ф. Правові основи інформаційної діяльності. – Режим доступу : http://studrada.com.ua

5. Доктрина інформаційної безпеки України : Указ Президента України від 08.07.09 р. № 14/2009. – Режим доступу : // www.president.gov.ua

6. Євдоченко Л.О. Удосконалення системи державного забезпечення інформаційної безпеки України в умовах глобалізації : автореф. дис. на здобуття наук. ступеня канд. наук з держ. упр. : 25.00.01 / Л.О. Євдоченко. – Л., 2011. – 24 с.

7. Захист інформації. Технічний захист інформації. Основні положення : ДСТУ 3396.0-96. – [Чинний від 1997.01.01]. – Режим доступу : //www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=5D34EDB7C9C9D4491C0171ACCAD297E1?art_id=38883&cat_id=38836

8. Захист інформації. Технічний захист інформації. Терміни та визначення : ДСТУ 3396.2-97. – [Чинний від 1998.01.01]. – Режим доступу : //www.dstszi.gov.ua/dstszi/control/uk/publish/article;jsessionid=5D34EDB7C9C9D4491C0171ACCAD297E1?art_id=38934&cat_id= 38836

9. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : дис. на здобуття наукового ступеня д-ра юрид. наук. : 12.00.07 / Б.А. Кормич. – Х., 2004.

10. Кузьменко Б.В. Захист інформації : навч. посіб. – Ч. 2 / Б.В. Кузьменко, О.А. Чайковська. – К. : Видавничий відділ КНУКіМ, 2009. – 69 с.

11. Литвиненко О. Проблема інформаційної безпеки в контексті міграційних процесів. – Режим доступу : //www.nbuv.gov.ua/portal/soc_gum/Ukralm/2012_7/lytvynenko.pdf

12. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції. – Режим доступу : //www.pidruchniki.ws/12800528/politologiya/ponyattya_zagroz_informatsiyniy_bezpetsi

13. Ліпкан В.А. Національна безпека України. – Режим доступу : //www.pidruchniki.ws/15341220/politologiya/ponyattya_vidi_zagroz_natsionalnim_interesam_natsionalniy_bezpetsi_informatsiyniy_sferi

14. Логінов А.В. Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади : дис. на здобуття наукового ступеня кандидата юридичних наук : 12.00.07 / А.В. Логінов. – Національна академія внутрішніх справ України. – К., 2005.

15. Макарова М.В. Електронна комерція : посібник для студентів вищ. навч. закладів / М.В. Макарова. – К. : Видавничий центр “Академия”, 2002. – 272 с.

16. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук. : 12.00.01 / Ю.Є. Максименко – К., 2007. – 22 с.

17. Марущак А.І. Пріоритети розвитку інформаційного права України // Інформація і право. – 2011. – № 1. – С. 20-24.

18. Олійник О.В. Організаційно-правові засади захисту інформаційних ресурсів України : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : 12.00.07 / О.В. Олійник. – К., 2006. – 20 с.

19. Соціально-правові основи інформаційної безпеки : навч. посібник / [В.М. Петрик, А.М. Кузьменко , В.В. Остроухов та ін.] ; за ред. В.В. Остроухова. – К. : Росава, 2007. – 496 с.

20. Пилипчук В.Г. Системні проблеми розвитку правової науки в інформаційній сфері // Вісник Академії правових наук України. – 2011. – № 3. – С. 16-27.

21. Погребняк А.В. Технології комп’ютерної безпеки : монографія / А.В. Погребняк. – Рівне : МЕГУ, 2011. –117 с.

22. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах : Постанова Кабінету Міністрів України від 29.03.06 р. № 373 // Офіційний вісник України. – 2006. – № 13.

23. Про основи національної безпеки України : Закон України : від 19.06.03 р. № 964-IV // Відомості Верховної Ради України. − 2003. – № 39.

24. 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. − 2007. – № 12. – Ст. 102.

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