

УДК 027.021:004.65

ДОВГАНЬ О.Д., кандидат юридичних наук, старший науковий співробітник

ОРГАНІЗАЦІЯ РОБОТИ ПО ПІДВИЩЕННЮ ЕФЕКТИВНОСТІ ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ РЕСУРСІВ: АСПЕКТ БЕЗПЕКИ

***Анотація.** У статті розглянуто питання організації роботи по використанню інформаційних ресурсів та запропоновано шляхи по підвищенню її ефективності.*

***Ключові слова:** інформаційні ресурси, інформаційна безпека, інформаційне забезпечення, бібліотечні установи.*

***Аннотация.** В статье рассмотрен вопрос организации работы по использованию информационных ресурсов и предложены пути по повышению ее эффективности.*

***Ключевые слова:** информационные ресурсы, информационная безопасность, информационное обеспечение, библиотечные учреждения.*

***Summary.** The article considers the issue of organization of work on the use of information resources and offers the ways to increase its efficiency.*

***Keywords:** information resources, information safety, dataware, library establishments.*

Постановка проблеми. Аналіз теоретичних узагальнень і розвитку практичної діяльності в сфері інформаційної безпеки України свідчить, що навіть при розвитку демократичних процесів в суспільстві, при зростаючих впливах процесів глобалізації збереження національної специфіки розвитку потребує організуючого начала, в якості якого виступає сучасна держава. У відповідності із своєю прямою функцією вона має бути центром організації безпеки суверенних інформаційних ресурсів, а також координувати безпекову діяльність соціальних структур суспільства з точки зору відстоювання національних інтересів, оскільки у нинішніх умовах ці структури мають змогу брати участь у прямих інформаційних обмінах в глобальному інформаційному просторі через систему інформаційних комунікацій, слабо контрольовану або ж і зовсім не контрольовану державою. Специфіка розвитку інформаційного суспільства, таким чином, обумовлює необхідність в організації системи безпеки, в тому числі й інформаційної, пов'язаної із захистом і розвитком національних інформаційних ресурсів, одного із найважливіших продуктів нового суспільства.

Інформаційна безпека держави реалізується в процесі діяльності як органів державної влади, так і недержавних інститутів, як через діяльність державних спеціальних органів регулювання інформаційних правовідносин і процесів, так і через структуру інших органів державної влади та громадські організації. У зв'язку із розвитком процесів інформатизації, що обумовлюють забезпечення доступу до інформаційних ресурсів всім членам суспільства, в якості паралельного процесу з'являються якісно нові проблеми організації військової та державної безпеки, економіки, культури, внутрішньої та зовнішньої політики тощо.

З огляду на розвиток глобальних інформаційних процесів і безальтернативне включення в їх розвиток всіх націй і держав, проблеми організації інформаційної безпеки України виходять далеко за межі території нашої держави. Тому інституціональний механізм формування політики інформаційної безпеки включає не лише внутрішньодержавний масштаб, але й співробітництво з міжнародними інститутами, що покликані регламентувати процеси глобального інформаційного простору.

Інформаційна безпека в національному законодавстві розглядається як системне явище. Законом України “Про основи національної безпеки України” визначається, що всі напрямки цієї безпеки побудовано на основі базових елементів [1]. Даний закон розкриває шляхи формування ефективної правової бази розвитку сучасної інформаційної безпеки (ст. 2). Зважаючи на складність, багатоаспектність прояву інформаційних загроз сучасності, законом передбачається відповідна жанрова різноманітність документів для забезпечення ефективної практики організації безпеки: законів, концепцій та доктрин. У контексті розвитку сучасних інформаційних процесів ст. 3 цього Закону передбачає процес створення системи, що відповідає перебігу подій і ситуацій в вітчизняній інформаційній сфері. На основі аналізу суспільної практики в сфері розвитку сучасної інформаційної сфери, закон визначає найбільш дієві напрями розвитку правових норм, засобів і форм державного впливу на інформаційну сферу.

Відповідний державно-правовий механізм інформаційної безпеки Б.А. Кормиш визначає як “впорядковану сукупність інститутів держави, задіяних у процесі формування і впровадження політики інформаційної безпеки, внутрішні та зовнішні ролі і відносини якої регулюються системою правових норм та принципів” [2]. Цей державно-правовий механізм, у відповідності з означеними нами напрямками реалізації політики інформаційної безпеки, складається з трьох взаємопов’язаних елементів.

По-перше, це сукупність державних інституцій, задіяних у процесі формування і впровадження політики інформаційної безпеки, тобто інституціональний механізм інформаційної безпеки.

По-друге, це сукупність ролей та відносин, яка включає правові відносини, що виникають при проведенні політики інформаційної безпеки, та специфічні ролі, форми і методи діяльності суб’єктів проведення політики інформаційної безпеки.

По-третє, це ієрархічна сукупність правових норм та принципів, що регулюють зміст та процес проведення політики інформаційної безпеки, тобто правовий механізм інформаційної безпеки [2].

Мета статті. З точки зору організації інформаційної безпеки сьогодні відчувається необхідність розробки правових актів, пов’язаних із регламентуванням, визначенням принципів збереження, правилами використання суверенних інформаційних ресурсів. Сучасні дослідження інформаційних процесів свідчать про те, що в наш час особливо назріла потреба в забезпеченні функціональної визначеності інформаційних систем, їх сумісності між собою та з діяльністю державного апарату управління.

Виклад основного матеріалу. Захист інформаційного суверенітету держави тісно пов’язаний із поняттям інформаційної безпеки, що може бути розглянута, як захищеність внутрішньої інформації як такої, тобто захищеність якості інформації, її надійність, захищеність різних галузей інформації від розголошення, а також захищеність інформаційних ресурсів. З іншого боку, інформаційна безпека означає контроль над інформаційними потоками, обмеження використання провокаційної, ворожої суспільної інформації, включаючи контроль над рекламою; захист національного інформаційного простору від зовнішньої інформаційної експансії.

Серед головних складових інформаційної безпеки держави виділяють: обсяг інформаційного продукту, що виробляється в державі і державою; здатність мереж витримувати зростаюче інформаційне навантаження; можливість держави керувати розвитком вироблення та розповсюдження інформації; можливість доступу народонаселення до усіх можливих інформаційних джерел, а також відкритість більшості з них.

Аналізуючи дослідження вітчизняних фахівців, головні цілі політики інформаційної безпеки України можна сформулювати таким чином: реалізація конституційних прав громадян, суспільства та держави на інформацію; захист інформаційного суверенітету України, зокрема, національного інформаційного ресурсу та систем формування суспільної свідомості; забезпечення рівня інформаційної достатності для прийняття рішень державним установам, підприємствам та громадянам; належна присутність країни у світовому інформаційному просторі. Крім того, розглядаючи актуальність формування, функціонування та безпеки національного інформаційного простору, експерти виділяють наступні цілі: зміцнення інформаційної безпеки України, загалом її національної безпеки за рахунок більш ефективного використання національного потенціалу; підняття рівня і значення вітчизняного інформаційного продукту та технологій, національних інформаційних ресурсів, розвитку інформаційної інфраструктури України у відповідності до її національних інтересів на засадах державного суверенітету України; упорядкування інформаційних відносин у національному інформаційному просторі України, особливо зміна співвідношення розповсюдження в країні вітчизняної та зарубіжної інформаційної продукції та інформаційних технологій на користь вітчизняних; державна підтримка вітчизняних суб'єктів національного інформаційного простору, забезпечення інформаційної та духовної, культурної ідентифікації України в міжнародних інформаційних відносинах, піднесення міжнародного авторитету вітчизняного інформаційного продукту та технологій, його виробників [3].

Найзагальніші принципи організації інформаційної діяльності в інтересах державного управління пов'язані із необхідністю врахування глибини управлінського впливу на соціальні структури суспільства, тобто місця і ролі держави в житті кожного окремого члена суспільства, функціонування соціальних структур на всіх рівнях, до яких він належить. Інформаційні потреби владних структур пов'язані також із необхідністю забезпечення реалізації існуючої ієрархії суспільно значимих цілей, над досягненням яких працює влада, врахування співвідносності діючої правової бази з реальними практичними її діями. Ці інформаційні потреби мають також бути конкретно пов'язані з урахуванням специфіки керованих соціальних структур, характерних особливостей їх розвитку в контексті загальносуспільних інтересів.

Структурна організація системи управління інформаційною безпекою має бути адекватною загальній системі державного управління. Тобто вона повинна бути багаторівневою і територіально розподіленою з чіткою координацією дій складових елементів. Ефективне функціонування цієї системи передбачає централізоване управління з конкретними відомчо-розпорядчими функціями, які мають забезпечувати системний моніторинг і регулювання всіх компонентів національного інформаційного простору. Вона повинна у будь-яких ситуаціях зовнішнього чи внутрішнього інформаційного протистояння (експансії, агресії, тероризму або війни) зберігати життєво важливі параметри функціонування.

В практиці діяльності державних органів про це часто забувають і вводять в управлінську інформацію багато політики, ідеології, пропаганди та обіцянок, не співвіднесених із реальною практикою, її потребами. Вимоги безпеки у сфері інформаційних ресурсів мають узгоджуватись із принципами, за якими розвивається система надання адміністративних послуг в Україні [4]. Серед них особливої уваги на сьогодні набувають принципи доступності послуг для всіх фізичних та юридичних осіб та пов'язаний з ним принцип відкритості.

Однією із основних її складових має бути інформація, що стосується власне управлінської діяльності, а також ресурси, що відносяться до категорії національного надбання і відображають національну традицію в сфері державного управління, в тому числі розвиток інституту президентства в Україні.

При формуванні сучасної правової бази організації безпеки суверенних інформаційних ресурсів у зв'язку із швидкоплинним перебігом подій у інформаційному просторі постійно виникають проблеми, пов'язані з відставанням розроблених правових актів з реальними інформаційними процесами.

Прикладом такого відставання може бути правове регламентування такої важливої складової суверенних інформаційних ресурсів як національне надбання. До даного реєстру, згідно з постановою Кабінету Міністрів України [5] з метою обліку було внесено об'єкти матеріальної та духовної культури виняткової історичної, художньої, наукової чи іншої культурної цінності, що мають важливе значення для формування національної самосвідомості українського народу і визначають його вклад у всесвітню культурну спадщину. Постанова визначала порядок занесення та виключення об'єктів реєстру, координацію дій суспільних інституцій щодо управління та охорони національного надбання. Пізніше список пам'яток отримав назву “Державного реєстру нерухомих пам'яток України” [6]. У 2002 році згідно з Розпорядженням Кабінету Міністрів України [7] наукові об'єкти: фонд рукописів, стародруків, рідкісних видань віднесено до таких, що становлять національне надбання.

Однак, інформаційні ресурси як такі, інформація, що складає культурне надбання багатьох поколінь українського народу, інформація, що є основою його самоідентифікації, що сьогодні слугує орієнтиром для формування сучасних суспільно значимих масивів інформації, статусу національного надбання донині не одержала.

Відставання у нормотворчості є однією з причин розвитку протиправної діяльності в інтернет-мережах, його успішно використовують “продвинуті” хакери від спортивно-розважальних цілей в соціальних мережах до кібертероризму з серйозними суспільними наслідками.

Для подолання наявного відставання, прогнозування ситуації правники мають уважно відстежувати особливості розвитку сучасних інформаційних процесів і продукувати правові розробки, виходячи із цієї ситуації. Очевидно, що спостереження за даними процесами найбільш успішним може бути при аналізі інформаційно-аналітичного забезпечення управлінської сфери. На користь цього свідчить та обставина, що інформаційно-управлінські процеси виникають скрізь, де відбувається структуризація суспільства, а ця структуризація, у свою чергу, обумовлює відповідну структуризацію всередині інформаційних баз і ускладнення їх ієрархії.

Оскільки процес постійного проникнення в неосвоєну навколишню дійсність є необхідною умовою розвитку суспільства, його інфраструктури, умовою розвитку всяких інформаційних баз, глибина цього проникнення визначається двома основними факторами: суспільною потребою і наявним інформаційним ресурсом, необхідним запасом узагальненої інформації.

Сучасні дослідники справедливо зауважують, що “управлінська інформація – це частина соціальної інформації, що виділена із її загального масиву згідно з критеріями придатності до обслуговування державно-правових процесів формування і реалізації управлінських впливів. Вона своїми “коренями” проникає в соціальну інформацію, однак вибирає звідти тільки те, що відображає управлінські потреби, інтереси і цілі людей, їх керівну сукупну волю, конкретні механізми і способи організації та регулювання їх свідомості, поведінки і діяльності” [8].

Система безпеки при визначенні правової регламентації управлінської діяльності має передбачати відповідні вимоги впливів, пов'язані із специфікою ієрархічної структури процесу інформаційного забезпечення.

Комплектування суверенних інформаційних баз ресурсами управлінської інформації має враховувати специфіку вимог чотирьох основних рівнів інформаційно-аналітичного забезпечення органів влади, що створюють повну інформаційну картину про ситуацію в керованому регіоні. “Сюди слід віднести рівні забезпечення вирішення політичних, стратегічних, тактичних і оперативних задач. Всі вони взаємопов'язані.

При виділенні управлінських рівнів у відповідності із вказаним вище розподілом управлінських задач необхідно також брати до уваги специфіку інформаційно-аналітичної роботи на кожному із рівнів. У даному випадку необхідно говорити про формування ієрархії знання. При цьому ієрархія інформаційно-аналітичних підрозділів передбачає перехід на новий рівень абстракції стосовно підрозділів, що знаходяться в ієрархії нижче” [9]. В сучасних умовах набуває першочергової актуальності специфіка вимог до інформаційного забезпечення управлінської праці, пов'язана з постійною необхідністю прийняття рішень в умовах дефіциту часу.

Сучасні дослідження інформаційних процесів свідчать про те, що в наш час особливо назріла потреба в забезпеченні функціональної визначеності інформаційних систем, їх сумісності між собою та з діяльністю державного апарату управління.

Питанням інформаційної безпеки має бути регламентування сучасного інформаційного обслуговуванні всіх груп користувачів і насамперед – управлінських структур з огляду на ряд вимог, реалізація яких забезпечує ефективність даного процесу. Інформація має бути мінімальною, достатньою й необхідною, вірогідною й надійною, сучасною й оперативною, придатною до використання для машинної обробки [10].

Мінімальність передбачає використання лише таких інформаційних обсягів, без яких не можливий процес управління об'єктом і вдосконалення цього процесу. Достатність означає такий обсяг інформації, який дає вичерпне, повне уявлення про функціонування об'єкта та можливості його розвитку. При визначенні потреб в окремих видах інформації необхідно враховувати оптимальну періодичність забезпечування користувачів, кореляцію сформованих інформаційних потоків з іншими в загальній системі суспільного інформування.

Враховуючи характерну особливість сучасності, пов'язану зі стрімко зростаючими обсягами інформаційних ресурсів і великими обсягами в них низькоякісної, а то і просто шкідливої, спамової інформації, до числа безпекових проблем має відноситись таке комплектування суверенних інформаційних ресурсів, яке б гарантувало високу достовірність та вірогідність їх використання. Без вірогідної інформації про об'єкт управління не можливо організувати роботу, спрямовану на формування перспектив його розвитку і передбачуваності.

Як свідчить практика, з упровадженням електронних інформаційних технологій в управлінську діяльність на регіональному рівні, до інформаційних структур, що виконують запити регіонів, формуються певні специфічні вимоги.

Одна із них пов'язана з реалізацією в оптимальному режимі діалектичного процесу, що виражається, з одного боку в формуванні спільного для регіону інформаційно-телекомунікаційного простору з тенденцією до уніфікації технологій і вимог при забезпеченні інтеграції державних та інших інформаційних ресурсів, а з іншого – забезпечення такого змістовного насичення інформаційної діяльності, яке б, задовольняючи управлінські потреби, не допускала б шкідливих впливів на розвиток місцевої своєрідності [11].

Важливим питанням активного включення регіонів до єдиної загальнодержавної інформаційної системи є спільна з ними діяльність по організації безпеки національних інформаційних ресурсів, регламентація доступу до всієї системи суспільно значимих інформаційних ресурсів в умовах зростаючих глобальних впливів.

На думку В.Б. Авер'янової сьогодні “назріла потреба створити Державну автоматизовану систему виконавчої влади України. Прототипом її може стати досвід і результати роботи щодо створення колишньої Республіканської автоматизованої системи України (РАС), галузевих автоматизованих систем (ГАС) і автоматизованих систем управління підприємством (АСУП). Водночас потребує детальної розробки механізм підготовки, перепідготовки та розстановки кадрів служб інформаційного забезпечення системи виконавчої влади, механізм забезпечення інформаційної системи сучасними технологіями збирання та обробки інформації, матеріально-технічними засобами, механізм здійснення профілактики й ремонту засобів обчислювальної техніки, підтримки інформаційної системи у робочому стані. Крім того, необхідно розробити ефективний механізм захисту інформації у системі виконавчої влади від несанкціонованого до неї доступу” [12].

Новим питанням інформаційної безпеки, що потребує ґрунтовного вивчення є також процес, пов'язаний із реалізацією в суспільній практиці концепції електронного уряду. Сутність її полягає у можливості використання інформаційних технологій, зокрема Інтернет, для надання владних послуг безпосередньо тому, хто їх потребує 24 години на добу 7 днів на тиждень, а також у вдосконаленні громадського контролю, акумуляції творчого потенціалу громадян у вдосконаленні управлінської діяльності. Очікується, що впровадження електронного уряду сприятиме встановленню тісних зв'язків між органами державної влади та громадянами.

При цьому важливим для зміцнення національних традицій в розвитку наукової діяльності, виробництва сучасної наукової інформації є також забезпечення доступу в системі суверенних інформаційних ресурсів до знань, акумульованих в наявних інформаційних базах і нинішнім, і минулими поколіннями. Тобто пов'язана із використанням інформації неоперативної, але необхідної в творчому пошуку. Лише з використанням цієї інформаційно-цільової “основи”, що виражає закономірності пізнавальної діяльності нашого суспільства, воно зможе організувати творчу роботу, діяти зважено, цілеспрямовано, ефективно, відстоюючи власні інтереси і самобутність.

При використанні традиційної (такої, що не несе ознаки оперативності) інформації, введенні її в суспільний обіг, сьогодні однією із основних проблем є проблема переведення інформації в доступну для користувача з використанням сучасних технологій форму, в електронну форму. Проблема ця дуже трудомістка, затратна, натикається на серйозні правові бар'єри і не приносить її учасникам негайних дивідендів. Але про її актуальність свідчать поки що скромні спроби крупних бібліотечних закладів, зокрема Національної бібліотеки України імені В.І. Вернадського, інших бібліотечних закладів і створення електронних бібліотек і популярність цих новоутворень в середовищі користувачів [13].

Сучасна підготовка використання інформації, що відбирається в базах, потребує врахування ще однієї специфічної особливості: точності, якомога більшої відповідності кінцевій меті пошуку інформаційного матеріалу. Цього вимагають комп'ютерні технології роботи з інформацією як при постановці задач, в процесі супроводу їх виконання, так і при аналізі одержаних результатів.

Використання інформаційних ресурсів у творчому процесі пов'язане із необхідністю вирішення цілого ряду нових проблем, що виникли в сфері збереження

інтелектуальної власності. Багато неврегульованих питань на сьогодні існує у зв'язку з впровадженням інтернет-технологій, переведенням в електронний вигляд авторських творів, документів, що знаходились на інших носіях (папір, кіно-та фотопродукція, а також ін.) Взагалі, слабо контрольована діяльність в Інтернеті з усіма плюсами і мінусами цього явища ще потребує ґрунтовного осмислення для вироблення продуктивних принципів, законів загальносуспільних інформаційних обмінів в умовах нового, постіндустріального суспільства [14], належний правовий захист прав інтелектуальної власності залежить від стану законодавства України, приведення його у відповідність до міжнародно-правових стандартів, вирішення проблеми їх практичної реалізації, узгодженості між нормативно-правовими актами, недосконалості механізму захисту, ефективної боротьби з правопорушеннями [15].

Проведені українськими дослідниками пошуки свідчать про те, що головними причинами недостатнього рівня ефективності системи охорони інтелектуальної власності фахівці найчастіше називають такі: відсутність у держави засобів на патентування і здійснення реєстраційних процедур за кордоном (54,8 %); низький рівень правової культури в країні (46,6 %); відсутність належних знань та інформації про порядок захисту інтелектуальної власності за межами України (45,2 %); законодавчу неврегульованість в Україні питань трансферу технологій, у тому числі у випадках виїзду українських фахівців на роботу за кордон (43,8 %).

Дане коло проблемних питань вимагає глибокої і послідовної правотворчої роботи з визначенням відносин, що підлягають першочерговому правовому регулюванню, та підготовкою ефективних управлінських і правових рішень. Ознайомлення з роботами вчених у цьому напрямі засвідчує, що їх авторами виявлені, в основному, процесуально-правові проблеми з'ясування і доведення фактів порушення авторських прав при розміщенні інформації в Інтернеті [16].

Як свідчить аналіз, не забезпеченим на належному рівні залишається механізм захисту особистих немайнових прав інтелектуальної власності; відсутність дієвих механізмів захисту авторського права, належного рівня відповідальності правопорушників функціонування інформаційного обігу в Україні. Нормативна база не встигає за розвитком відносин у сфері комп'ютерного програмування, технологій; відсутня єдина система захисту прав суб'єктів промислової власності; існують проблеми забезпечення доказів при поданні позову про порушення прав інтелектуальної власності.

Одним із найважливіших напрямів розвитку нормативної бази в сучасних умовах є пов'язаний із системою матеріалізації технічної, технологічної та іншої інформації, що має значення для промислового прогресу. Мається на увазі розвиток спеціального законодавства, яке покликане регламентувати суспільні відносини щодо технічних, технологічних та інших нововведень. Це спеціальне законодавство отримало назву патентного, а сукупність норм, що його утворюють, відома під назвою патентного права.

Дослідники відзначають, що патентне право стає одним з ефективних механізмів регулювання соціальної, економічної, науково-технічної, інноваційної та ринкової політики світової спільноти. Патентне право є одним з важливих та найскладніших інститутів права інтелектуальної власності. Об'єктами відносин, що регулюються нормами патентного права, виступають результати науково-технічної та художньо-конструкторської творчості, тобто нематеріальні блага, що є продуктами творчої праці. Охорона об'єктів патентного права передбачає формалізацію у законі їх ознак, дотримання спеціального порядку визначення пріоритету, перевірку новизни та встановлення особливого режиму їх використання. В основу правової охорони вказаних об'єктів покладено те, що виникнення права інтелектуальної власності на них

пов’язується з одержанням охоронного документа, яким засвідчуються права на винаходи, корисні моделі та промислові зразки – патенту [17].

Законодавства про промислову власність Україна не мала ніколи. Тільки після проголошення незалежності в Україні почалися активні кодифікаційні роботи, в тому числі і в галузі законодавства про промислову власність. Очевидно, першою ластівкою в цьому напрямку варто вважати Закон України “Про власність”, який у ст. ст. 13 і 41 визначає, що результати інтелектуальної діяльності є об’єктами права власності, і дав приблизний перелік результатів інтелектуальної діяльності, яким надається правова охорона передусім цим Законом.

Певний вклад у вирішення проблеми було зроблено Законом “Про науково-технічну інформацію” від 25 червня 1993 р. Потім було прийнято пакет законів про промислову власність, серед яких: закони України “Про охорону прав на винаходи і корисні моделі”, “Про охорону прав на промислові зразки” та ін. Вони склали правову основу захисту прав на об’єкти промислової власності.

Поряд із цим були прийняті Закон України “Про державну таємницю” від 21 січня 1994 р., “Про захист інформації в автоматизованих системах” від 5 липня 1994 р., “Про наукову і науково-технічну експертизу” від 10 лютого 1995 р.. У зв’язку з прийняттям пакету законів про промислову власність внесені відповідні зміни до Цивільного кодексу України, в Кодекс законів про працю України, до Митного кодексу та інші. Відповідні зміни внесені також і до раніше прийнятих законів України [18]. Цим самим питання інтелектуальної власності, особливостей сучасної інформаційної діяльності були пов’язані з інтересами держави і нації в цій дуже перспективній сфері людської діяльності.

Паралельно дослідники зауважують, що в Україні існують злочини у сфері використання електронно-обчислювальних машин, систем та комп’ютерних мереж і мереж електрозв’язку і чинним законодавством встановлена відповідальність за них. Для придушення цих злочинів система кримінальної відповідальності повинна застосовувати практику кримінального законодавства органами юстиції, встановити більш жорсткі покарання, розширити кількість норм, які б встановлювали відповідальність, і основою державної політики в цій сфері повинні стояти дослідження вітчизняних дослідників-юристів, тим паче під час внесення змін до законодавства в цій галузі. Слід пам’ятати, що організована злочинність давно прийняла на озброєння обчислювальну техніку, тому не слід залишати дану галузь без огляду. Адже зі швидкими темпами інформатизації злочини в цій сфері стають дедалі частішими та суттєво впливають на стан злочинності в державі та її розвиток. Тому для недопущення виникнення таких злочинів, окрім інших заходів, необхідно грамотно та правильно будувати КСЗІ [19].

Дана точка зору є справедливою і для унормування практики сучасних інформаційних обмінів, і для комплектування новою інформацією національних інформаційних ресурсів.

Використана література

1. Про основи національної безпеки України : Закон України від 19.06.03 р. № 964-IV // Офіційний вісник України. – 2003. – № 29. – С. 38. – Ст. 1433.
2. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : дис. на здобуття наук. ступеня док-ра. ю. н. – К., 2004 р. – С. 135.

3. Степко О.М. Аналіз головних складових інформаційної безпеки держави / О.М. Степко // Науковий вісник Інституту міжнародних відносин НАУ. – Сер. : Економіка, право, політологія, туризм. – К. : Вид-во Нац. авіац. ун-ту “НАУ-друк”, 2011. – Вип. 1(3). – С. 83-92.
4. Концепція розвитку надання адміністративних послуг органами виконавчої влади. – Режим доступу : [//www.zakon.rada.gov.ua/cqj-bin/laws/mein.cgi?meg=90-27](http://www.zakon.rada.gov.ua/cqj-bin/laws/mein.cgi?meg=90-27)
5. Про затвердження Положення про Державний реєстр національного культурного надбання : Постанова Кабінету Міністрів України від 12.08.92 р. № 466.
6. Про охорону культурної спадщини : Закон України // Відомості Верховної Ради України. – 2000. – № 39. – Ст. 333.
7. Розпорядження Кабінету Міністрів України від 19.09.02 р. № 472-р.
8. – Режим доступу : [//www.refi.su/teotiya_upravleniya10.html](http://www.refi.su/teotiya_upravleniya10.html)
9. “Северный регион” № 2(8)/2003. – С. 159-164.
10. – Режим доступу : [//www.osvita.ua/vnz/reports/gov_reg/18353](http://www.osvita.ua/vnz/reports/gov_reg/18353)
11. Інформаційна складова соціокультурної трансформації українського суспільства. – К. : Нац. б-ка України ім. В.І. Вернадського.– 2012 . – С. 38.
12. – Режим доступу : [//www.ukrkniga.org.ua/ukrkniga-text/692/33](http://www.ukrkniga.org.ua/ukrkniga-text/692/33)
13. Костенко Л.И. Электронная научная библиотека НБУВ / Л.И. Костенко, А.А. Чекмарев // Библиотеки национальных академий наук : проблемы функционирования, тенденции развития. Научно-практический и теоретический сборник. – Вып. 1. – К. : НБУВ, 2000. – С. 147- 154.
14. Корнеєва Т.М. Права людини в інформаційному суспільстві. Комунікаційні права : четверте покоління прав людини / Т.М. Корнеєва // Інформаційне суспільство. Шлях України. – С. 120-126.
15. Рудник Т.В. Захист права інтелектуальної власності як один із основних напрямів державної політики України / Т.В. Рудник : матеріали міжнародної науково-практичної Інтернет-конференції [“Тенденції розвитку юридичної науки: проблеми та досягнення”]. – Тернопіль, 2011. – С. 108.
16. Шашенков Я.О. Правове регулювання відносин, пов’язаних із використанням Інтернет-технологій / Я.О. Шашенков // Науковий вісник Національного університету державної податкової служби України. – Сер. : Економіка, право. – 2011. – № 2(53). – С. 183-187.
17. Еннан Р.Є. Патентне право як інститут права інтелектуальної власності / Р.Є. Еннан // Правове життя сучасної України. – Т. 2. – Одеса : Фенікс, 2011. – С. 345.
18. Гапотій В.Д. Захист права інтелектуальної власності в Україні / В.Д. Гапотій, А.М. Солоненко. – Мелітополь : ТОВ “Видавничий будинок ММД”, 2011. – С. 83.
19. Хавіков І.В. Протидія злочинам у сфері використання електронно-обчислювальних машин, систем та комп’ютерних мереж і мереж електрозв’язку шляхом створення КСЗІ // Протидія злочинності : теорія та практика. – Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2011. – С. 195-198.

~~~~~ \* \* \* ~~~~~