В. Іванов

Інформаційна безпека України: аспект діяльності ЗМК

Розгляд проблем інформаційної безпеки проводиться у складний для українських ЗМК період. Преса, радіо і телебачення України переживають глибоку кризу. Сьогодні в країні фактично немає газет і журналів, телекомпаній і радіостанцій, які б отримали справжню економічну незалежність. Економічний успіх видання, теле- радіопрограми України – в силу діючого законодавства, існуючих правових, адміністративних і економічних регламентів ринку ЗМК – майже зовсім не залежить від чисельності аудиторії.

Основна частина населення країни близька до того, що скоро буде позбавлена доступу до друкованого слова, а виходить, і до аналітичної інформації про соціально-економічне, політичне і духовне життя України, про події за рубежем. Ми змушені констатувати, що наша країна давно перестала бути "найбільш читаючою". За рівнем насиченості періодичними виданнями на тисячу чол. населення вона значно (в 5–20 разів) відстає від інших країни світу. У порівнянні з початком 90-х років, коли кожна українська сім'я передплачувала в середньому 3–4 видання, зараз на сім'ю, за минулорічними даними, в середньому припадає 0,71 передплачених видання, а в Луганській області – 0,32. Контраст особливо помітний, якщо порівняти ці дані з показниками інших країн світу. За даними Всесвітньої газетної асоціації, і лідером тут є Латвія, де газети читають 96 % дорослих. Потім йдуть Фінляндія (91 %), Швеція (89 %), Норвегія (81 %), Німеччина (79 %), Австрія (76 %), Великобританія (74 %), Литва (73 %), Нідерланди, Люксембург, Естонія (70 %), США (61 %).

Як на мій погляд, сама ця ситуація є найбільшою загрозою інформаційній безпеці держави.

У нас якось звикли з великою недовірою ставитися до всього, що містить слово "безпека". Багато хто в цьому відчуває якусь загрозу правам особи, демократичним свободам. Треба вже позбутися цього постсоціалістичного синдрому. В усьому світі інформаційна безпека визнана необхідною складовою нормального розвитку суспільства. У тих же Сполучених Штатах постійно діє Комітет з політики інформаційної безпеки, який очолюють заступник міністра оборони і директор ЦРУ. Зараз згідно з директивою Президента США № 63 (1998 р.) розгортається загальноамериканська система інформаційної безпеки. У грудні 1999 р. резолюцію з питань інформаційної безпеки прийняла Генеральна Асамблея ООН. Метою є вироблення міжнародних принципів, що спрямовані "на посилення безпеки глобальних інформаційних та телекомунікаційних систем" і сприяють "боротьбі з інформаційним тероризмом і криміналом". У червні того ж року була прийнята Концепція інформаційної безпеки держав-учасниць СНД.

У сусідній Росії в вересні минулого року була прийнята Доктрина інформаційної безпеки РФ. У лютому 2000 р. закон "Про інформаційну безпеку" був прийнятий у Білорусі. Причому в Росії системи інформаційної безпеки будуються вже на регіональному рівні. В Новгородській області створено Раду з інформаційної безпеки, у Хабаровському краї прийнято Концепцію інформаційної безпеки краю, аналогічні кроки зроблені в Свердловській та Воронезькій областях.

Тому дуже добре, що РНБО продовжує свої зусилля по забезпеченню належного рівня інформаційної безпеки в Україні. До речі, важливість цього питання чітко усвідомлюють представники інформаційного бізнесу. В липні 2000 р. компанія "Анна" запустила портал "Український центр інформаційної безпеки", що об'єднує близько 10000 тисяч ресурсів, присвячених цій проблемі.

Особлива увага саме до цієї складової загальної безпеки в Україні і світі обумовлена входженням суспільства у нову, інформаційну стадію розвитку. Зараз завдяки вільним інформаційним потокам світ перетворюється у своєрідне глобальне село, якщо говорити за Г.Маклюеном. Інформаційна революція, яка була викликана широким застосуванням комп'ютерної техніки та інформаційних технологій, призвела до необхідності переглянути ряд ключових положень розвитку сучасного суспільства, в тому числі у сфері безпеки.

Ми звикли розуміти під захистом інфор-

маційної безпеки перш за все якісь обмежувальні дії. Але це неправильно. Взагалі, під інформаційною безпекою прийнято розуміти стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави. На жаль, законодавча база в цій галузі відстає від потреб практики. Ті закони та нормативні акти, які існують в цій сфері, носять, переважно, обмежувальний чи заборонювальний характер. Тобто безпека розуміється як захищеність інформації та інфраструктури, що її підтримує, від випадкових чи спеціальних втручань штучного або природного характеру, які можуть завдати шкоди власникам чи користувачам інформації. Цей підхід явно застарілий. В наш час від держави потрібна не стільки заборона чи обмеження, скільки підтримка, організація та координація робіт. До речі, саме такий підхід превалює у цивілізованих країнах. У США вже 12 років діє Закон про комп'ютерну безпеку. Так от, наголос у цьому законі зроблений не на заборони, а на комплекс заходів з навчання користувачів, що мають справу з критичною інформацією, на підготовку роз'яснювальної документації тощо. Тобто це заходи для свідомого підтримання режиму безпеки.

До основних об'єктів інформаційної безпеки відносяться:

- особистість, її права та свободи;
- суспільство, його матеріальні та духовні цінності;
- держава, її конституційний лад, суверенітет та територіальна цілісність.

Які ж можуть бути загрози? Як зовнішні (недружня політика іноземних держав в області глобального інформаційного моніторингу, поширення інформації та нових інформаційних технологій), так і внутрішні (протизаконна діяльність різних структур в області збору, обробки та передачі інформації, яка призводить до порушення прав громадян і організацій).

Для того, щоб побачити, які ж пріоритети мають інші держави у цій сфері, можна проаналізувати Доктрину інформаційної безпеки РФ. Першою з 4-х складових національних інтересів Росії в інформаційній сфері виділене дотримання конституційних прав і свобод людини, друге – це інформаційне забезпечення державної політики РФ, третє – розвиток сучасних інформаційних технологій і тільки четверте – захист інформаційних ресурсів. Як бачимо, наголос явно не на обмежувальні дії, а на розвиток.

Таким чином, інформаційна безпека держави буде забезпечена тільки у випадку ефективного та безперешкодного функціонування ЗМК. На жаль, якраз для цього у нас умови ще не створені. Українські газети абсолютно правильно у листопаді 2000 р. віднесли до найактуальнішої на той час загрози інформаційній безпеці дефіцит газетного паперу. А "Урядовий кур'єр" навіть виніс таке формулювання у заголовок.

Хоча й інших загроз вистачає. До них можна віднести ті значні фінансові труднощі, яких зазнають регіональні газети, теле- й радіокомпанії, різке скорочення вітчизняного кіновідеовиробництва, погіршення матеріального стану журналістів, особливо, знов-таки, в регіонах. Щорічно після закриття газет і журналів сотні журналістів залишаються без роботи. Одночасно посилюється тиск на журналістів політичними, економічними і адміністративними методами. Особливо часто переслідування журналістів ведуться у судовому порядку.

І одними законами чи іншими правовими актами тут нічого не вирішиш, бо треба відзначити, що в законодавстві України вже приділяється визначена увага цій проблемі. Взагалі, Україна посідає одне з перших місць у СНД за кількістю законів, присвячених діяльності мас медіа. Але толку від цього мало. Жоден із законів в інформаційній сфері не виконується у повному обсязі. Таким чином, річ не в законах, а в рівні їх виконання.

Тепер я хотів би конкретизувати загрози, які виникають в інформаційній сфері. Не секрет, що у ряді держав розробляються чи вже розроблені концепції інформаційних воєн. Так, війну у Перській затоці чи в Югославії було виграно не тільки внаслідок бойових дій, але й спеціальних інформаційних операцій. Причому починалися вони задовго до початку бойових дій. Згадаємо, перед початком бомбардування Югославії міністр закордонних справ Великобританії Кук стверджував, що серби страчують по 2 тис. албанців на день. А коли Косово було захоплено, спеціальна комісія знайшла трохи більше 2 тисяч трупів, причому ідентифікувати їх виявилося дуже важко. А у Перській затоці відразу після початку "Бурі у пустелі" на екранах американських телевізорів виникла заплакана арабська дівчина, нібито медсестра з кувейтського пологового будинку, яка розповіла жахливі речі про те, як іракські солдати викидали немовлят з барокамер і вбивали їх. Війна в Затоці була повністю морально виправдана в очах пересічних американців. А потім виявилося що та дівчина – донька кувейтського посла у Вашинг-

тоні, а її слова – вигадка. Американці дуже пильно слідкують за тим, щоб журналісти висвітлювали події у вигідному для армії напрямку. Так, під час тієї ж війни з Іраком всі журналісти були зібрані у так звані пули і пересувалися тільки по затверджених американськими військовими коридорах. Тих же, хто випадав із загальної картини, відразу намагалися дискредитувати. Так, кореспондент ВВС Д. Сімпсон був звинувачений в тому, що піддався сербській пропаганді за те, що він показав у репортажі сербів, які говорили про свої антинатівські настрої.

Складовою частиною інформаційних воєн є кібервійни. У листопаді минулого року президент США У. Клінтон та міністр оборони В. Коен підписали наказ про підготовку до кібервоєн. Уже зараз при цьому можуть використовуватися DdoS-атаки, комп'ютерні віруси, виведення з ладу комп'ютерів за допомогою електро- і радіоперешкод. Причому американське командування ставить ведення інформаційних воєн в один ряд із застосуванням балістичних ракет і контролем за космосом. До інформаційних воєн також активно готується і китайська армія.

Не можна оминати і такої загрози інформаційній безпеці особистості, як психотронна зброя. Ми звикли ставитися до повідомлень про неї з недовірою, бо параноїків у нас і без всякої зброї вистачає. Але я дозволю собі навести одну цитату: "В останній час активно ведуться розробки методів і засобів комп'ютерного проникнення у підсвідомість людини і здійснення на неї глибокого впливу. Враховуючи безконтрольність розповсюдження комп'ютерних технологій, вплив яких на психіку має необмежені можливості, слід говорити про появу нової інформаційної зброї масового знищення". Це сказав не якийсь парапсихолог, а декан факультету інформаційної безпеки Московського інженерно-фізичного інституту А. Маланюк під час свого виступу у Державній Думі Росії на парламентських слуханнях, що були присвячені інформаційній безпеці.

Треба відзначити, що спецслужби розвинених країн світу активно використовують мережу Інтернет моніторингу інформаційних потоків чи, простіше кажучи, відстежування змісту веб-сайтів, електронної пошти, інформаційних запитів тощо. У нас широко критикувалося введення в Росії, а потім в Україні системи оперативно-розшукових заходів (російською – СОРМ-2), яка була спрямована на це. Але на Заході вже кілька десятиліть діє система "Ешелон", яка перехоплює повідомлення та аналізує їх зміст на предмет присутності підозрілих слів та висловів. За допомогою 120 супутників перехоплювалася інформація, що проходила телефонними лініями, радіо, супутниковим зв'язком. Існування цієї системи, яка була створена спецслужбами США, Великобританії, Канади, Австралії та Нової Зеландії, приховувалося навіть від союзників по військових блоках. Тільки після того, як 21 жовтня 1999 р. рух "Хактивісти" провів "День боротьби з "Ешелоном" (вони пересилали якмога більше листів із словами "революція", "плутоній", "Північна Корея", "ЦРУ" тощо), Австралія визнала його існування. Євросоюз уже кілька разів розглядав питання діяльності "Ешелону". З'ясувалося, що перехоплювалося навіть листування французьких та італійських дипломатів. Дані "Ешелону" активно використовувалися в економічному шпигунстві та допомозі вітчизняним фірмам. Так, в Європарламенті стверджувалося, що у 1994 р. в результаті того, що Агентство національної безпеки США прослухало та передало конкурентам зміст переговорів французької компанії "Томпсон" з бразильцями, був зірваний контракт на суму 40 млрд. франків. У 1995 р. Європейський консорціум Airbus Industry втратив контракт на поставку літаків у Саудівську Аравію після того, як його комерційна пропозиція була перехоплена і передана корпорації Boeing.

Але навіть масштаби "Ешелону" повністю не задовольняють потреб спецслужб. У Великобританії у липні минулого року був прийнятий закон, згідно з яким уряд отримав право відстежувати електронну пошту громадян та декодувати криптовані повідомлення. Створена нова установа – Урядовий Центр технічної підтримки, яка буде діяти за схемою СОРМ-2. Тобто провайдери будуть зобов'язані протягнути виділену лінію в офіс цього центру. Різниця в тому, що уряд готовий відшкодувати провайдерам витрати на встановлення нового обладнання (на це виділено 30 млн. доларів). Крім того, за поправкою Палати лордів, на перехоплення e-mail буде потрібна санкція на прослуховування. Але, якщо спецслужби самі не зможуть розшифрувати якесь повідомлення, новий закон зобов'язує користувачів надавати поліції паролі для розшифрування своїх листів.

Звичайно, Інтернет посилює загрозу до державних таємниць та конфіденційної інформації громадян (це з особливою гостротою ставить на порядок денний питання криптографічного захисту інформації). Неабияку, хоча і приховану, небезпеку являють собою обмін науковою інформацією через Інтернет. З одного боку, це прогре-

сивний спосіб обміну думками про новітні досягнення науки, але, з іншого, таким чином через численні запити, анкети тощо можуть збиратися відомості, що становлять державну таємницю. Взагалі, йдучи за світовою практикою, таємна інформація має бути недоступна через Інтернет, тобто вона має циркулювати тільки у закритих локальних комп'ютерних мережах.

Часто права користувачів Інтернету порушуються з комерційною метою. Наприклад, багато компаній передають користувачам, коли ті відвідують їх сайти, так звані "cookies". Це невеликі приховані програми, які відслідковують інтереси користувача (до яких сайтів він звертається) і пересилають ці дані до своєї компанії, яка використовує їх для прямої реклами (тобто реклами певних товарів тільки тим людям, яких ці товари можуть зацікавити). У лютому 1999 р. офіційні національні представники від 15 країн Європейського Союзу прийняли рекомендацію щодо суворої секретності даних, що передаються. Згідно з нею користувач має точно знати, які саме персональні дані про нього передаються у мережу. З 1 листопада 2000 р. США погодилося виконати вимогу Євросоюзу, і тепер американським компаніям заборонено розсилати "cookies".

З іншого боку, доцільно, щоб органи влади виставляли на своїх домашніх сторінках в Інтернеті інформацію про свою діяльність, організовували обговорення найважливіших документів, двосторонній зв'язок з рядовими громадянами. Крім того, держава має створити сприятливі умови для інвестицій у розвиток комп'ютерних мереж, виникненню нових компаній і конкуренції у цій сфері, бо це буде сприяти наближенню до рівня розвинених країн і переходу суспільства до інформаційної стадії розвитку. На це, зокрема, спрямований проект країн великої "сімки" "Держава онлайн". У Данії всі рішення уряду мають бути доступні через Інтернет одночасно з їх публікацією в пресі. У Норвегії уряд пропонує через глобальну комп'ютерну мережу єдиний пакет інформації по найважливіших життєвих проблемах. У Великобританії навіть створена книга "Електронне представлення державних послуг". Аналогічні кроки роблять інші розвинені країни.

В Україні у рекомендаціях парламентських слухань "Свобода слова в Україні: стан, проблеми, перспективи" (квітень 1997 р.) зокрема говориться: "Інтернет може посилити загрозу для державних таємниць, особистої конфіденційної інформації громадян та збільшити залежність національного інформаційного простору від закордонної продукції, чужої інформаційної політики". Вже в жовтні того ж 1997 р. Кабінет Міністрів України затвердив Концепцію технічного захисту інформації, тобто діяльності, яка спрямована на забезпечення інженерно-технічними засобами порядку доступу, цілісності та доступності (неможливості блокування) інформації, котра становить державну та іншу таємницю, що передбачена законом, конфіденційної інформації, а також цілісності та доступності відкритої інформації, яка має важливе значення для особи, суспільства і держави. Для цього передбачена "обов'язковість захисту інженерно-технічними засобами інформації, котра складає державну та іншу таємницю, що передбачена законом, конфіденційної інформації, яка є власністю держави, відкритої інформації, що важлива для держави, незалежно від того, де ця інформація циркулює, а також відкрита інформація, яка важлива для суспільства і держави, якщо ця інформація циркулює в органах державної влади і органах місцевого самоврядування, Національній академії наук, Збройних Силах, інших військових формуваннях, органах внутрішніх справ, на державних підприємствах, в державних установах і організаціях". Звичайно, реалізація цих планів може суттєво зменшити доступ до офіційної інформації, бо всі види інформації, крім державної таємниці, законом не передбачені і будуть визначатися, мабуть, через якісь галузеві інструкції. У лютому 1998 р. в Україні був прийнятий Закон "Про Національну програму інформатизації". Причому однією з цілей цієї програми є забезпечення інформаційної безпеки України.

Ще одна проблема, яка виникає у зв'язку з розвитком глобальних комп'ютерних мереж – це проблема дотримання авторського права.

Взагалі, за кордоном все частіше постають питання, пов'язані зі зловживанням можливостями Інтернету. У Німеччині наприкінці 1995 р. баварський прокурор визначив, що більш ніж 200 телеконференцій порушують німецьке законодавство по боротьбі з порнографією. Але вдіяти нічого не зміг, бо сервери, де були розміщені ці матеріали, розташовані далеко за межами країни. У Канаді та Японії були заарештовані особи, які розміщували порнографічні картинки на своїх домашніх сторінках в Інтернеті. У Сингапурі влада зобов'язала провайдерів послуг Інтернету контролювати зміст домашніх сторінок, звертаючи увагу на матеріали про секс, політику та релігію. Причому політичні партії для того, щоб відкрити свою домашню сторінку в Інтернет, мають отримати урядову ліцензію. Франція через небезпеку тероризму

у 1996 р. навіть звернулася до уряду США, з тим, щоб було притягнуто до відповідальності ісламське угрупування, яке діяло в Каліфорнії і розповсюджувало через Інтернет інструкції по створенню саморобних бомб на зразок тих, що вибухнули у паризькому метро. До найрадикальніших засобів звернулися у Китаї. Там усі користувачі Інтернету мають бути обов'язково зареєстровані у кантонах та префектурах і повинніповідомляти владу про всі зміни у своїй діяльності.

Деякі країни приймають спеціальні законодавчі акти щодо розповсюдження порнографії в Інтернет. Так, у жовтні 1998 р. в Ірландії був прийнятий закон, який забороняє використання дитячих образів при виготовленні аудіовізуальних матеріалів сексуального характеру, а також розповсюдження дитячої порнографії. Дітьми тут вважаються особи, що не досягли 17 років. Порушники будуть штрафуватися у розмірі до 25 тис. фунтів або засуджуватися до 14 років позбавлення волі.

Необхідність дотримання балансу між вільним інформаційним потоком і захистом громадських та особистих інтересів розуміють і в Європейській Комісії. Наприкінці 1996 р. Рада з телекомунікацій Європейської Комісії прийняла рішення, яке спрямоване на запобігання розповсюдження в Інтернеті порнографії, особливо дитячої. Треба відзначити, і це підкреслювалося неодноразово, Інтернет дуже специфічний засіб комунікації і через свій транскордонний характер важко піддається правовому регулюванню. Всі учасники Інтернет підлягають законам своїх країн. Але незаконний зміст може бути виявлений не на території тієї країни, де він зберігається на сервері. Тому для врегулювання правових відносин в Інтернет необхідні міжнародні угоди щодо нього. А це в свою чергу ускладнюється різним підходам законодавства країн до тих чи інших порушень, наприклад, різний зміст вкладається у поняття "порнографія". Зараз загальний напрямок законодавчих ініціатив у галузі Інтернет спрямований на встановлення відповідальності провайдерів хостових послуг за зміст інформації, що міститься на їхніх комп'ютерах. Звичайно, це дуже складно з технічної точки зору і тому в деяких законодавствах відповідальність провайдерів обумовлюється тим, що вони знали про зміст незаконної інформації. Мережеві оператори, як правило, не притягуються до відповідальності, але у них вимагають припиняти доступ до клієнтів, що розповсюджують незаконну інформацію. Цікаво, що у Великобританії вже працюють системи саморегулювання в роботі провайдерів Інтернет. Там прийнятий "Кодекс поведінки" і створений фонд "Безпечна мережа", який допомагає провайдерам визначитися чи є та чи інша інформація незаконною. Канадська асоціація провайдерів послуг Інтернету також розробила Кодекс поведінки в Інтернеті. Його мета – допомогти членам Асоціації у дотриманні правових стандартів у роботі. У Франції існує Хартія Інтернет, у якій визначаються добровільні обов'язки користувачів і провайдерів в Інтернеті. У Німеччині провайдери Інтернет зорганізувалися у Freiwillige Selbstcontrolle Multimedia Dienstleanbieter (FSM) – Спілку добровільного самоврегулювання служб мультимедіа. Ця організація створена з метою вживати заходи по скаргах на зміст он-лайн потоків, але скарги мають стосуватися виключно інформації, що є пропагандою насильства чи іншим чином може зашкодити молодим людям. Кроки по створенню подібних організацій самоврегулювання зроблені і в інших країнах. Деякі неурядові організації у Великобританії навіть організують тиск на членів парламенту з вимогою забезпечити законодавчу підтримку приватності спілкування у WWW. Члени цього руху "Візьми шефство над депутатом" створили свою веб-сторінку, на якій всі бажаючі можуть взяти шефство над одним із депутатів парламенту і проводити з ним через Інтернет чи пошту роз'яснювальну роботу з цього питання. У Бельгії в травні 1999 р. був заключений протокол між Асоціацією провайдерів інтернет-послуг, Міністерством юстиції та Міністерством у справах телекомунікації. Мета цього протоколу – попередження злочинів за допомогою Інтернету: дитячої порнографії, пропаганди расизму, порушення законодавства про гральний бізнес. У протоколі закріплений обов'язок провайдера інформувати виконавчу владу про порушення, які він помітив. Корисно те, що провайдери не зобов'язані перевіряти інтернет-ресурси та шукати порушення.

Але інколи спроби самоврегулювання Інтернету набувають незаконних форм. У 1996 р. у Німеччині група хакеров "Організація рятування Європи" за чотири місяці знищила більш, ніж 50 сайтів, на яких містилася інформація, що стосувалася нацизму. У 1997 р. у Франції відбулася ціла "війна хакерів". Хакери – прибічники нацизму до чергової річниці Гітлера намагалися наводнити Інтернет екстремістською інформацією, а антинацистськи налаштовані хакери її активно знищували. Боротьба тривала десь тиждень, а потім припинилася сама собою. Один з представників французької провайдерської компанії сказав: "Таке враження, що дітям набридло грати в одну гру і вони вирішили вигадати нову. У березні 1999 р.

російською хакерською групою "Антифашистський фронт Росії" була проведена акція блокування серверу "Руспатріот", на якому були розміщені веб-сторінки таких націоналістичних об'єднань, як "Чорна сотня", "Пам'ять" тощо. Хакери викрали у власників серверу доменне ім'я ruspatriot.com, внаслідок чого всі відвідувачі серверу потрапляли на сторінку, де була розміщена карикатура Кукриніксів "Фашизм не пройде" і звернення "Антифашистський фронт Росії" до "нешановних та презирливих фашистів". У зверненні говориться, зокрема, про те, що члени фронту не будуть чекати на рішення судових органів, а самі зроблять все для зменшення присутності наці в Інтернеті. Після цієї акції подібні проводили вже деякі провайдери. Так, компанія "BizLink" вилучила з свого серверу електронні версії газет "Завтра" і "Дуель". Американський провайдер "Hyper Mart" закрив три сайти письменника О. Дугіна, через те, що "його агітація не відповідає цілям та завданням діяльності серверу". За російськими законами діяльність "Антифашистського фронту Росії" є незаконною, бо порушує ч. 2 ст. 272 Кримінального кодексу РФ "Неправомірний доступ до комп'ютерної інформації, здійснений групою осіб за попередньою угодою, чи організований групою", згідно з якою карається "неправомірний доступ ... до інформації на машинному носії, що охороняється законом, в ЕОМ, системі ЕОМ чи їх мережі..., якщо ця дія привела до знищення, блокування, модифікації чи копіювання інформації, порушення системи ЕОМ чи їх мережі". Покаранням може бути штраф від 500 до 800 розмірів мінімальної заробітної плати чи до позбавлення волі терміном до п'яти років. Звичайно, за законодавством усіх перелічених країн заборонено розповсюдження інформації екстремістського характеру, як воно, до речі, заборонено і Європейською конвенцією з прав людини, однак встановлювати законність чи незаконність інформації – це справа суду. Так, у 1997 р. за рішенням судів Великобританії було закрито два сайти за те, що там містилася інформація расистського характеру, бо було вирішено, що ця інформація "не відповідає інтересам людства".

Іноді війни у кіберпросторі набувають міждержавного характеру. Так, на початку 2000 р. близько місяця тривала війна між хакерськими групами з Азербайджану та Вірменії. Спочатку дві азербайджанські групи (Green Revenge і HijaK Team 187) зламали майже 25 вірменських сайтів, у відповідь вірменська група Liazor захопила майже всі найпопулярніші азербайджанські сайти, навіть сайти газет, телебачення та інтернет-провайдера. Після того, як вірменські хакери поміняли зміст цих сайтів, вони заявили, що не будуть опиратися поверненню їх законним власникам.

21 грудня 1998 р. Рада Європейського Союзу затвердила план дій по безпечному використанню Інтернету, який був запропонований Європейським парламентом за місяць до цього. План діє чотири роки (з 1 січня 1999 р. по 31 грудня 2002 р.), його бюджет складає 25 млн. євро. План передбачає створення різних "рівнів якості" Інтернету. Формуватися вони мають відповідно до "знаків Інтернет-якості" продукції. Ці положення мають бути найближчим часом закріплені як у національних законодавствах, так і в кодексах самоврегулювання інтернет-провайдерів. У березні 1999 р. Європейська Комісія прийняла звіт про результати обговорення положень Доповіді про конвергенцію телекомунікацій, ЗМІ та інформаційних технологій ("Зелена книга"). Основний висновок такий: правове регулювання в Інтернеті має носити прозорий, ясний і пропорційний характер, а також бути різним по відношенню до передачі даних і до змісту повідомлень. Подібні заклики до обережності під час спроб регулювання Інтернету лунають часто. Так, у Франції Вища Рада з аудіовізуальної політики організувала у 1999 р. міжнародну дискусію на тему регулювання інтернет-послуг. Сама Рада дотримується думки, що окремих спеціальних законів не потрібно, а надання радіо- чи телепослуг за допомогою Інтернету має регулюватися за вже існуючими законами щодо функціонування телерадіопростору.

Постають правові питання й у зв'язку з появою так званих електронних грошей. Ці гроші є еквівалентом банківського депозиту, які пересуваються по електронних мережах у вигляді зашифрованої серії цифр чи записані на картку з вбудованим мікропроцесором. З цими грішми можуть виникнути певні проблеми. Якщо поламається картка, то вони взагалі будуть втрачені, бо майже неможливо відстежити, скільки їх уже було витрачено з цієї картки. Створюються також широкі можливості для відмивання "брудних" грошей, приховування від податків та інших фінансових зловживань. Набагато важчим стає контроль над друкуванням національної валюти. Але, мабуть, найбільшою небезпекою є те, що хтось може довідатися про систему шифрування, яка використовується при випуску електронних грошей. Це може потягти найбільші збитки. Небезпечним є шахрайство в Інтернеті з грішми інвесторів. Як правило, шахрай у себе вдома робить домашню сторінку, причому таку, яка виглядає краще, ніж

сторінки солідних компаній. Там розміщується інформація про нібито молоду і дуже перспективну компанію. Тече потік інвестицій, а потім виявляється, що гроші зникли, а компанія була створена тільки для того, щоб їх витягти. Такі шахраї-спамери влізають у телеконференції інвесторів і подають інформацію про нібито дуже вигідні проекти. Крім того, були випадки, коли шахраї перехоплювали листи офіційних осіб, адресовані відкритим акціонерним компаніям, додавали до них брехливу інформацію і в такому перекрученому вигляді розповсюджували. Це робилося для маніпулювання курсом акцій.

Для захисту даних у глобальних комп'ютерних мережах широко застосовується шифрування, тобто криптографічні засоби. У різних країн є свої правила їх застосування. В Росії згідно з Законом "Про державну таємницю" та Указом Президента РФ № 334 від 3.04.96 забороняється діяльність фізичних та юридичних осіб, яка пов'язана з розробкою, виробництвом, реалізацією і експлуатацією шифрувальних засобів, а також захищених технічних засобів збереження, обробки і передачі інформації, наданням послуг в області шифрування інформації, без ліцензії, виданої Федеральним агентством урядового зв'язку та інформації при Президенті РФ. Таким чином введена фактична державна монополія на розвиток шифрувальних систем. У США навпаки спеціальний комітет Національної ради з досліджень Національної академії наук США прийняв рішення, що переваги широкого розповсюдження криптографії дають суспільству більше гарантій, ніж заборона та обмеження шифрувальних засобів. Комітет закликав змінити офіційну політику США, щоб криптографія була доступна для всіх правомочних суб'єктів американського суспільства. Особлива увага надається розробці засобів криптографічного захисту інформації від перекручення, для підтвердження особи користувача і для захисту інформації в мережах зв'язку. У Франції 19 січня 1999 р., через рік після прийняття державної програми з розвитку інформаційного суспільства, прем'єр-міністр запропонував нові заходи з розвитку Інтернет. І найпершим були пропозиції щодо зміни механізму регулювання шифрування даних. Якщо раніше з міркувань державної безпеки всі були зобов'язані повідомляти у державні органи шифр будь-якого коду передачі транскордонних повідомлень, що перевищували 40 біт, то тепер верхня планка складає 128 біт. Відповідні поправки з питань розвитку технологій та введення електронного підпису запропоновані у цивільний кодекс Франції.

З'явився і такий новий вид правопорушень, пов'язаний з Інтернет, як запуск сфальсифікованих повідомлень нібито від інформаційних агентств. Наприклад, у розпалі президентської компанії в Росії 1996 р. у західні країни прийшло повідомлення від імені агентства ІМА-ПРЕС про смерть президента Б.М.Єльцина. Агентство мусило офіційно спростовувати це повідомлення і розцінило його як провокацію. Від імені цього ж агентства по московських ЗМК і банківських структурах було розіслано сфальсифіковане повідомлення про "наїзд" на один з банків. А за наступне втручання хакерів у мережу ІМА–ПРЕС довелося відповідати волгоградській газеті "Молодежный курьер". Річ у тому, що у сфальсифікованій інформаційній стрічці, яка надійшла до газети електронною поштою нібито від ІМА-ПРЕС, містилися наклепницькі відомості про астраханського губернатора А. П. Гужвіна. Газета вимушена була виплатити губернатору 10 млн. карбованців і надрукувати спростування. Інший нашумілий скандал був пов'язаний з сайтом "Коготь-2". На цьому сайті була розміщена інформація щодо "корупційних" зв'язків алюмінієвого магната А. Бикова. При цьому ніяких доказів подібних зв'язків не наводилося. незважаючи на це, скандал широко обговорювався громадськістю Красноярського краю і мав неабиякі наслідки. А. Биков втратив значну частку довіри населення на користь свого опонента, губернатора краю О. Лебедя. З одного боку, це може викликати подив. Адже кількість користувачів Інтернету залишається невеликою. Але з іншого, згідно з теорією багатосходинкового потоку комунікації саме "лідери думок" в основному формують громадські настрої. Таким чином, роль порівняно дешевих кампаній по пропаганді (часто дезінформації) в Інтернеті важко переоцінити.

Взагалі, в Україні має бути вироблена чітка інформаційна політика, яка б відповідала національним цілям, цінностям та інтересам. Саме це, а не проведення якихось дискримінаційних кампаній принесло б реальну користь інформаційній безпеці держави. Самообмеження інформаційного простору країни – цього можуть жадати або вороги України, або люди, які повністю не розуміють тенденцій і механізмів світового розвитку. В сучасних умовах це може означати тільки одне: усунення України з числа більш-менш розвинених країн без всякої перспективи до її повернення у цей табір. Тільки інформаційна відкритість, активна власна інформаційна політика, спрямована на створення якнайгільговіших умов для виробників власного інформаційного продукту (в широкому сенсі цього слова) можуть зробити Україну незалежною могутньою державою.