Тема XII

ПРАВОВІ ЗАСАДИ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

§ 1 Поняття на напрями безпеки інформаційної інфраструктури

Основні дії щодо збирання, зберігання, передачі та розповсюдження суспільно значущої інформації, як відомо, здійснюються за допомогою спеціальних технічних засобів та технологій. З розвитком науки та техніки ці інформаційні засоби і технології перетворюються на один із найважливіших компонентів інформаційних процесів, поряд із самою інформацією та суб'єктами інформаційних відносин. А це, у свою чергу, ставить відповідні вимоги щодо рівня безпеки інформаційних засобів і технологій та правового регулювання їх функціонування.

Слід зазначити, що на практиці існують значні розбіжності навіть щодо визначення обсягів відповідної сфери. Найбільш обґрунтованим виглядає підхід, згідно з яким до об'єктів цієї сфери відносять, зокрема, «інформаційні системи й інформаційні технології, засоби їх забезпечення», де під інформаційною системою розуміють «організаційно впорядковану сукупність документів (масивів документів) та інформаційних технологій, в тому числі з використанням засобів обчислювальної техніки і зв'язку, які реалізують інформаційні процеси».[1] Цілком логічним виглядає застереження «в тому числі» стосовно комп'ютерних технологій. Адже автоматизовані засоби обробки інформації з'явилися за історичними мірками зовсім недавно. І навпаки, протягом кількох тисячоліть існують традиційні способи обробки та передачі інформації – поштовий зв'язок, кур'єрська доставка тощо. Вже з по-

[1] Копылов В.А. Информационное право. – 2-е изд., перераб. и доп. – М.: Юристъ, 2002. – С.63.

чатком XX століття до них поступово додалися телеграфні, телефонні, радіо-, телевізійні і, нарешті, комп'ютерні мережі передачі інформації.

Дуже часто інформаційні системи розглядають тільки крізь призму інформаційно-обчислювальної техніки, визначаючи, наприклад, інформаційно-телекомунікаційна систему як «організаційно-технічну сукупність, що складається з автоматизованої системи та мережі передачі даних».[1]

Але звуження технологічного аспекту інформаційної безпеки тільки до інформаційних систем є, на нашу думку, невиправданим. Інформаційна безпека є комплексною категорією, що обумовлюється багатьма факторами. Інформаційні системи працюють не самі по собі. Будь-яка інформаційна система, особливо автоматизована, «поділяється на функціональну частину та частину забезпечення, кожна з яких поділяється на складові елементи мінімально можливої розмірності».[2] Функціональна частина інформаційної системи спрямована на виконання функцій і завдань, що підлягають реалізації за допомогою цієї системи. Частина забезпечення являє собою «наповнення» функціональної частини, за допомогою якого фактично реалізуються функції і завдання системи. Узагальнюючи такий підхід, ми можемо говорити, що інформаційна система функціонує за тими ж самими правилами і законами, що і будь-який інший вид систематизованої діяльності з розподілом ролей і функцій. Створення будь-якої системи обробки чи передачі інформації, починаючи від поштової служби і закінчуючи комп'ютерними мережами, включає величезну кількість етапів та елементів. До цього переліку входить: створення фізичних об'єктів, на яких ця система розміщується, створення технічного і програмного забезпечення, підготовка кадрів, забезпечення фінансовими та енергетичними ресурсами тощо. І загроза інформаційній безпеці може виникати на будь-якому етапі створення та експлуатації інформаційної системи.

Це означає, що існує певна сукупність об'єктів, суб'єктів та відносин між ними, що забезпечує здійснення інформаційних процесів у державі в цілому. Тому важливим для вивчення технологічного аспекту інформаційної безпеки є створення чіткого визначення і окреслення меж відповідної сфери.

---

[1] Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБУ «Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах» від 24 грудня 2001 р. № 76.

[2] Копылов В.А. Информационное право. – М.: Юристъ, 1997. – С. 152.

Цікавий комплексний підхід до проблеми запропоновано у Концепції Національної програми інформатизації, згідно з якою передбачається формування національної інфраструктури інформатизації (НІІ), яка включає:

- міжнародні та міжміські телекомунікаційні і комп'ютерні мережі;
- систему інформаційно-аналітичних центрів різного рівня;
- інформаційні ресурси;
- інформаційні технології;
- систему науково-дослідних установ з проблем інформатизації;
- виробництво та обслуговування технічних засобів інформатизації;
- системи підготовки висококваліфікованих фахівців у сфері інформатизації.[1]

Можна побачити, що під терміном «інфраструктура» поєднуються як технічні засоби та технології, так і установи й організації, що забезпечують процес інформатизації, починаючи з виробництва і обслуговування технічних засобів і закінчуючи підготовкою відповідних кадрів. Подібна інфраструктура повинна забезпечувати процеси інформатизації суспільства.

Але якщо мати на увазі саме інформаційні процеси, що відбуваються в державі, то ми можемо говорити і про відповідну *інформаційну інфраструктуру*, що ці процеси забезпечує. На відміну від визначеної законом інфраструктури інформатизації, інформаційна інфраструктура не включатиме безпосередньо інформаційні ресурси, адже вони є не компонентом, а предметом, що обробляється за допомогою цієї інфраструктури.

На нашу думку, саме термін «інформаційна інфраструктура», компонентами якого є технічні засоби, програмне забезпечення, різного роду установи й організації, найбільш чітко відображає сутність їхнього загального призначення. А це призначення полягає в тому, що ці компоненти є тим, за допомогою чого реалізуються інформаційні процеси. **Інформаційну інфраструктуру України можна визначити як сукупність технічних засобів і технологій, підприємств, установ і організацій, які реалізують інформаційні процеси і на які поширюється юрисдикція держави.** Інформація або інформаційні ресурси незалежно від форми власності є наповненням цієї інфраструктури, продуктом її діяльності. На

[1] Закон України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 року № 75/98-ВР // Відомості Верховної Ради України, 1998. – № 27-28. – Ст. 182.

нашу думку, існує нагальна потреба закріплення такого визначення на законодавчому рівні, що дасть можливість більш ефективної реалізації державою своїх владно-розпорядчих повноважень щодо регулювання розвитку і використання об'єктів інформаційної інфраструктури для захисту національних інтересів і безпеки.

Ще однією дуже важливою проблемою є визначення конкретних факторів, які потрібно враховувати, щоб охарактеризувати безпеку як конкретного інформаційного засобу або технології, так і всієї інформаційної інфраструктури, що заходиться на території України. Для цього потрібно виходити з функціонального призначення систем та об'єктів інформаційної інфраструктури. Головне їх завдання полягає у реалізації інформаційних процесів. А звідси головною цінністю є та інформація, яка обробляється в цих системах. Таким чином, інформаційна інфраструктура повинна забезпечувати інформацію або інформаційні ресурси, які обробляються від «потенційно або реально можливих дій, що приводять до неправомірного заволодіння відомостями, що охороняються».[1]

Видами таких неправомірних дій можуть бути:

- ознайомлення з конфіденційною інформацією різними шляхами і способами без порушення її цілісності;
- модифікація інформації в протиправних цілях як часткова або значна зміна складу і змісту відомостей;
- руйнування (знищення) інформації як акт вандалізму або з метою заподіяння прямої матеріальної шкоди.

Наслідком неправомірних дій з інформацією є «порушення її конфіденційності, повноти, достовірності та доступності, що, у свою чергу, призводить до *порушення як режиму управління, так і його якості* (підкреслено нами – Б.К.) в умовах спотвореної або неповної інформації»[2].

Таким чином, ми можемо говорити про те, що головним об'єктом загрози для інформаційної інфраструктури є суспільні відносини, які складаються з приводу управління і користування об'єктами цієї інфраструктури. А безпосереднім предметом загрози – інформаційні ресурси та інформація, що обробляється. Таким чином в аспекті безпеки інформаційна інфраструктура являє собою певну оболонку, яка захи-

---

[1] Ярочкин В.И. Информационная безопасность. – М.: Международные отношения, 2000. – С. 17.

[2] Там само.

щає інформацію, що знаходиться всередині її, від негативного впливу зовнішніх факторів.

Ці негативні фактори впливу можна класифікувати, залежно від його джерела, на три групи[1]:

Антропогенні фактори (безпосередньо створені людьми), які складають:

- ненавмисні або навмисні діяння обслуговуючого і управлінського персоналу, програмістів, користувачів, служби безпеки інформаційної системи;
- дії несанкціонованих користувачів (діяльність іноземних розвідувальних і спеціальних служб, кримінальних структур, недобросовісних партнерів та конкурентів, а також протиправна діяльність інших окремих осіб).

Техногенні фактори (викликані випадковим впливом технічних об'єктів):

- внутрішні (неякісні технічні і програмні засоби обробки інформації; засоби зв'язку, охорони, сигналізації; інші технічні засоби, що застосовуються в установі);
- глобальні техногенні загрози (небезпечні виробництва, мережі енерго-, водопостачання, каналізації, транспорт тощо), які призводять до зникнення або коливання електропостачання та інших засобів забезпечення і функціонування, відмов та збоїв апаратно-програмних засобів;
- електромагнітні випромінювання і наводки, витік через канали зв'язку (оптичні, електричні, звукові) тощо.

Природні фактори (вплив негативних природних чинників) – стихійні лиха, магнітні бурі, радіоактивний вплив.

Звідси для інформаційної структури взагалі і для кожного об'єкта її зокрема важливим є забезпечити незмінність внутрішніх умов обробки інформації при зміні (в тому числі і негативній) зовнішніх умов. Таким чином, **безпеку інформаційних систем та інформаційної інфраструктури держави взагалі можна охарактеризувати як стан забезпеченості необхідних умов і параметрів інформаційних процесів, що реалізуються за їх допомогою, від негативного впливу ззовні.**

В даному випадку під рівнем безпеки слід розуміти певні характеристики застосування будь-якої інформаційної технології, які гарантують конфіденційність, повноту, достовірність та доступність інфор-

[1] Див., напр.: Бачило И.Л., Лопатин В.Н., Федотов М.А. Информационное право / Под. ред. акад. РАН Б.Н. Топорнина. – СПб.: Юридический центр Пресс», 2001. – С. 643.

мації. Адже дотримання правових режимів інформації безпосередньо залежить від умов і параметрів усіх процесів, що відбуваються з нею, в тому числі від технічних характеристик носіїв інформації та засобів її зберігання.

Неважко зрозуміти, що контроль над інформаційною інфраструктурою одночасно означає і контроль над параметрами і умовами інформаційних процесів, що здійснюються за її допомогою, а безпека інформаційної інфраструктури багато в чому визначає і безпеку інформації, що обробляється за її допомогою. Цей контроль за інформаційною інфраструктурою може здійснюватися двома способами, які застосовуються паралельно. Перший забезпечується державною власністю на найбільш важливі (стратегічні) елементи інформаційної інфраструктури і полягає в безпосередньому державному управлінні відповідними об'єктами. Другий забезпечується юрисдикцією держави на власній території і полягає в запровадженні єдиних, обов'язкових стандартів інформаційних процесів, яких повинні дотримуватися власники або оператори об'єктів інформаційної інфраструктури.

Інформаційна інфраструктура держави взагалі може розглядатися як цілісна сукупність різного роду інформаційних систем та засобів їх забезпечення і мати певний середній показник рівня безпеки. У той же час кожен з елементів інформаційної структури має свої власні характеристики, правила, що регулюють його діяльність і звідси – різні показники рівня безпеки.

§ 2 Інформаційна безпека та мережа Інтернет

Розглядаючи проблему безпеки інформаційної інфраструктури, не можна не відзначити, що на сьогоднішній день найбільш складною є проблема правового регулювання відповідних аспектів функціонування глобальної світової мережі Інтернет. Труднощі починаються навіть з відсутності однозначного визначення суті цього явища, що для права взагалі є критичним фактором. Адже відсутність чітко окресленого предмета регулювання робить неефективним або взагалі унеможливлює саме це регулювання. Ця невизначеність стосується навіть технічних аспектів функціонування Інтернет. Право ж повинне розглядати Інтернет не лише з технічної точки зору, а й з соціальної, оскільки стосовно цієї мережі та всередині неї виникає новий тип суспільних відносин, що, можливо, повинен бути врегульований правом. Ми робимо

наголос на слові «можливо» тому, що саме питання необхідності та обсягів правового регулювання суспільних відносин, пов'язаних з мережею Інтернет, на сьогоднішній день також залишається об'єктом дискусій.

Таким чином, через цілий ряд обставин спроби дати формулювання або визначити зв'язок окремих ознак Інтернету як об'єкт права великого успіху не принесли. На сьогодні лише можна визначити Інтернет як універсальну систему об'єднаних мереж, які дають змогу забезпечити включення будь-яких масивів інформації для надання її користувачам, надання довідникових послуг та інших інформаційних послуг, а також здійснення різних цивільно-правових угод на основі комбінації інформаційно-комунікаційних технологій.[1]

На нашу думку, попри складність питання, слід виділити ключове стосовно до Інтернету слово – комунікація, або комунікаційна система. А це означає, що в принципі Інтернет може розглядатися як один із засобів масової комунікації, що має специфічні властивості. Це відкриває шлях до розуміння напрямів правового регулювання пов'язаних з ним суспільних відносин. По-перше, як і для будь-якої іншої комунікаційної системи (телефонної мережі, пошти), це правове регулювання правил її роботи, які адресовані особам, що забезпечують її функціонування, та правил користування нею, які адресовані споживачам її послуг. А обіг її наповнення – інформації – повинен регулюватися на загальних засадах, що прийняті у державі. Звісно, існує цілий ряд проблем юрисдикції, але, на нашу думку, не слід їх абсолютизувати. Адже юрисдикційні проблеми не вважаються дуже гострими, наприклад, при здійсненні міжнародних телефонних дзвінків або транслювання програм телебачення через супутники.

На нашу думку, спроби визначити Інтернет як якесь специфічне середовище, тобто певну віртуальну субстанцію, може стати спробою вивести цей засіб комунікації з правового поля, що гарантує свободу слова. Подібні спроби вже робилися в ряді держав і були припинені лише внаслідок ефективної роботи правозахисних механізмів. Так, у червні 1997 р. Верховний суд США відкинув положення закону «Про пристойність у засобах зв'язку», згідно з яким розповсюдження матеріалів непристойного змісту, до яких може отримати доступ неповнолітня особа, кваліфікується як злочин, оскільки це було б порушенням

[1] Бачило И.Л. Информационное право. Основы практической информатики. – М., 2001. – С. 209 – 210.

захищеного Конституцією права свободи слова[1].

Для знаходження компромісу між правами людини і питаннями безпеки в Інтернет у більшості розвинутих держав пропонується йти шляхом саморегуляції та тісної співпраці з недержавним сектором, що надає мережені послуги. Так, ще у 1997 р. Європейським парламентом було схвалено резолюцію, присвячену доповіді Комісії по протиправному та шкідливому змісту в Інтернет.[2]

Цією резолюцією було запропоновано класифікацію, згідно з якою матеріали протиправного змісту слід відрізняти від матеріалів шкідливого змісту. Матеріали протиправного змісту становить інформація, що прямо порушує вимоги національних чи міжнародних правових актів, в той же час під шкідливим змістом розуміється інформація, яка не є протиправною, але розповсюдження якої обмежене (лише для дорослих, наприклад), а також інформація, яка може образити деяких користувачів, хоча її публікація не обмежена з огляду на принцип свободи самовираження. І стосовно до цих двох категорій потрібно застосовувати зовсім різні заходи.

Згідно з цією резолюцією, матеріалами протиправного змісту повинні займатися за місцем їх створення правоохоронні органи, дії яких регулюються національним законодавством і угодами про судове співробітництво. Але й сама мережа Інтернет може сприяти через добре функціонуючі системи саморегуляції (кодекси поведінки і «гарячі лінії») відповідно до існуючого законодавства і за підтримки споживачів зниженню поширення матеріалів протиправного змісту (особливо дитячої порнографії і матеріалів расистського та антисемітського змісту).

А що стосується матеріалів шкідливого змісту, то пропонується насамперед надати користувачам можливості самим вирішувати проблему виключно технічними засобами (за допомогою систем фільтрації і рейтингової оцінки змісту), підвищуючи обізнаність батьків і розвиваючи саморегулювання, яке здатне створити необхідні рамки, зокрема щодо захисту неповнолітніх.

Такий підхід виглядає найбільш розумним і виваженим, адже він ґрунтується на повазі до права на свободу інформації та основоположному демократичному принципі відносин між людиною і державою «можливо все, що не заборонено законом». Адже обмеження видів

---

[1] Див.: http://www.aclu.org/court/renovacludec.html

[2] European Parliament Resolution of 24 April 1997 on the Commission communication on illegal and harmful content on the Internet (COM (96) 483).

інформації, що розповсюджується каналами Інтернет, яка є насамперед системою комунікації, тобто зв'язку, було б практично тим самим, що визначити, які теми можуть бути предметом приватних телефонних розмов, а які ні. Водночас гарантується можливість кожної людини свідомо обирати, яку інформацію вона хоче отримувати.

Враховуючи те, що національне законодавство України щодо обігу інформації в мережі Інтернет перебуває у стадії розвитку, було б доцільно покласти в основу їх розробки саме ці загальновизнані принципи.

Така позиція стала ще актуальнішою після прийняття Радою Європи, членом якої є й Україна, Декларації про свободу спілкування в Інтернет[1]. Приймаючи цю Декларацію, Рада Європи виявила послідовність у слідуванні проголошеним нею раніше принципам. Як зазначається, метою даної декларації є гарантування права на свободу інформації, встановленого ст. 10 Європейської конвенції щодо захисту прав і основних свобод людини. Для цього в декларації сформульовано сім основних принципів, які сприяють реалізації права на свободу слова у мережі Інтернет.

Згідно з цими принципами, держави-члени Ради Європи зобов'язуються:

- не встановлювати обмежень на зміст інформації в Інтернет більших, ніж ті, що існують щодо інших засобів доставки інформації;
- заохочувати саморегуляцію змісту інформації в Інтернет;
- виключити попередній державний контроль, зокрема утриматися від використання блокувань та фільтрів, які перешкоджають доступу до інформації, крім фільтрів, що не допускають до інформації вразливі групи, наприклад, дітей, до певних сайтів;
- утриматися від використання реєстраційних схем, які обмежують надання послуг через Інтернет;
- зняти перешкоди, які заважають забезпечити доступ до Інтернет або створення і функціонування Інтернет-сайтів для окремих верств суспільства;
- не зобов'язувати провайдерів проводити моніторинг всієї інформації, що проходить через їх сервер, та обмежити їх відповідальність за зміст інформації, що передається з використанням їхніх послуг;

[1] Declaration on freedom of communication on the Internet. Adopted by the Committee of Ministers at the 840th meeting of the Ministers' Deputies. Strasbourg, 28.05.2003./ http://www.coe.int/portalT.asp

• гарантувати право на анонімність в Інтернет (крім випадків розслідування злочинів та розшуку злочинців).

До недавнього часу практично єдиним нормативно-правовим актом, який стосується питань Інтернет, є Указ Президента «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні»[1].

Цим указом визначається (п. 1), що розвиток національної складової глобальної інформаційної мережі, забезпечення широкого доступу до цієї мережі громадян та юридичних осіб усіх форм власності в Україні, належне представлення в ній національних інформаційних ресурсів є одним із пріоритетних напрямів державної політики в сфері інформатизації, задоволення конституційних прав громадян на інформацію, побудови відкритого демократичного суспільства, розвитку підприємництва.

Для досягнення вказаних цілей пропонуються такі заходи, як:

• створення у найкоротші строки належних економічних, правових, технічних та інших умов для забезпечення широкого доступу до Інтернет;

• розширення і вдосконалення подання у мережі Інтернет об'єктивної інформації органів державної влади, місцевого самоврядування, установ, підприємств, організацій;

• забезпечення конституційних прав людини і громадянина на вільне збирання, зберігання, використання та поширення інформації, свободу думки і слова, вільне вираження своїх поглядів і переконань;

• забезпечення державної підтримки розвитку інфраструктури надання інформаційних послуг через мережу Інтернет;

• розвиток та впровадження сучасних комп'ютерних інформаційних технологій;

• вирішення завдань щодо гарантування інформаційної безпеки держави, недопущення поширення інформації, розповсюдження якої заборонене відповідно до законодавства;

• вдосконалення правового регулювання діяльності суб'єктів інформаційних відносин виробництва, використання, поширення та зберігання електронної інформаційної продукції, захисту прав на інте-

[1] Указ Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31 липня 2000 р. № 928/2000.

лектуальну власність, посилення відповідальності за порушення встановленого порядку доступу до електронних інформаційних ресурсів усіх форм власності, за навмисне поширення комп'ютерних вірусів.

Слід зазначити, що в цитованому указі дуже чітко і логічно вирішені питання інформаційної безпеки в Інтернет. Так, держава покладає на себе функції гарантування власної інформаційної безпеки та інформаційних прав і свобод людини. Забезпечення ж безпосередньо інформаційної безпеки людини, суспільства, різного роду юридичних осіб ґрунтується на створенні дієвих правових механізмів, за допомогою яких перелічені суб'єкти мали б можливість визначити і забезпечити необхідний, на їхню думку, рівень власної безпеки.

Також в аспекті захисту прав фізичних та юридичних осіб варто згадати постанову Вищого арбітражного суду України, яка визнає, що розміщення творів у мережі Інтернет у вигляді, доступному для публічного споживання, є їх відтворенням у розумінні ст. 4 Закону України «Про авторське право і суміжні права», у зв'язку з чим на розміщення творів в Інтернеті поширюється дія цього закону.[1]

Важливим кроком у розширенні використання електронних засобів зв'язку, і зокрема мережі Інтернет, стало прийняття у травні 2003 р. Законів України «Про електронні документи та електронний документообіг»[2] та «Про електронний цифровий підпис»[3].

Так, Законом «Про електронні документи та електронний документообіг» запроваджено єдине визначення електронного документа (до цього воно регулювалося кількома галузевими актами, наприклад, у сфері банківської справи та електронних розрахунків), встановлені єдині вимоги щодо реквізитів електронного документа, йому надано юридичної сили.

Закон встановлює поняття електронного документообігу (ст. 9), який являє собою «сукупність процесів створення, оброблення, відправлення, передавання, одержання, зберігання, використання та знищення електронних документів, які виконуються із застосуванням перевірки цілісності та у разі необхідності з підтвердженням факту одержання таких документів».

---

[1] Постанова Вищого арбітражного суду України «Про питання захисту авторських прав в Інтернеті» від 5 червня 2000 р. № 04-1/5-7/82. // Вісник господарського судочинства, 2001. – № 2.

[2] Закон України «Про електронні документи та електронний документообіг» від 22 травня 2003 р. № 851-IV

[3] Закон України «Про електронний цифровий підпис» від 22 травня 2003 р. № 852-IV

Цілями державного регулювання у сфері електронного документообігу, відповідно до цього Закону (ст. 4), є:

- реалізація єдиної державної політики електронного документообігу;
- забезпечення прав і законних інтересів суб'єктів електронного документообігу;
- нормативно-правове забезпечення технології оброблення, створення, передавання, одержання, зберігання, використання та знищення електронних документів.

Одним з реквізитів електронного документа є електронний підпис. Його використання регулюється Законом «Про електронний цифровий підпис» (вступає в силу з 1 січня 2004 р.). Цей закон визначає цифровий підпис як «дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних» (ст. 1). Застосування цифрового підпису можна розглядати як один із засобів криптографічного захисту інформації.

Іншим напрямком діяльності держави у сфері Інтернет є створення засад так званого електронного уряду – *e-government*, тенденції, яка швидко розвивається в багатьох розвинутих країнах світу. Якщо головна її мета – забезпечення за допомогою Інтернет прямого інтерактивного контакту між громадянами та урядовими установами, є поки що перспективою, то перший її етап – інформативний – вже отримав практичне втілення. В Україні вже діють електронні сторінки більшості органів державної влади та цілого ряду органів місцевого самоврядування. Було також створено і правову базу, яка регулює порядок розміщення таких сторінок в Інтернеті та їх наповнення.

Так, розпорядженням Голови Верховної Ради було затверджено положення про веб-сайт Верховної Ради. Згідно з цим нормативно-правовим актом, веб-сайт Верховної Ради України є офіційним джерелом інформації Верховної Ради України, який утворюється для висвітлення діяльності Верховної Ради України, її органів та апарату, взаємного обміну інформацією з органами державної влади України та органами місцевого самоврядування з питань, пов'язаних з діяльністю Верховної Ради України, інформаційної взаємодії з урядовими і неурядовими організаціями країн світового співтовариства, громадськістю.[1]

[1] Розпорядження Голови Верховної Ради України «Про положення про веб-сайт Верховної Ради України у глобальній інформаційній мережі Інтернет» від 24 травня 2001 р. № 462.

Відразу треба зазначити, що вперше в Україні електронний документ було названо офіційним джерелом інформації. Тобто логічно було б припустити, що розміщення на офіційному веб-сайті будь-яких відомостей вважається офіційною публікацією. Правда, що стосується нормативно-правових актів, то такий спосіб офіційної публікації не передбачено ані Регламентом Верховної Ради[1], ані відповідним указом Президента[2].

Щодо веб-сайту Верховної Ради, то, згідно з нормами вищезазначеного положення, забороняється використовувати веб-сайт Верховної Ради України в цілях, не пов'язаних з діяльністю Верховної Ради України та її органів, з метою отримання прибутку, а також на порушення законодавства України. Також визначаються основні рубрики інформаційного наповнення сайту, які включають бази законодавства та законопроектів, інформацію про діяльність Верховної Ради, депутатський корпус, структуру та апарат Верховної Ради, посилання на сайти парламентів інших країн. Передбачена можливість розміщення за принципом рівності веб-сторінок депутатських груп і фракцій, структурних підрозділів Верховної Ради.

Також передбачено (п. 9 розпорядження), що за розпорядженням Голови Верховної Ради доступ до відповідної веб-сторінки на веб-сайті Верховної Ради України може бути обмежено:

- за поданням Комітету Верховної Ради України з питань Регламенту, депутатської етики та організації роботи Верховної Ради України – до веб-сторінки депутатської фракції (групи), комітету та тимчасової комісії Верховної Ради України;
- за поданням керівника апарату Верховної Ради України – до веб-сторінки структурного підрозділу апарату Верховної Ради України.

Правова основа розміщення в мережі Інтернет інформації органів виконавчої влади була створена з прийняттям на початку 2002 р. постанови Кабінету Міністрів «Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади»[3]. Головною метою оприлюднення інформації органів виконавчої влади в Інтернет (п. 1) є підвищення ефективності та прозорості діяльності цих

[1] Регламент Верховної Ради України від 27 липня 1994 р. № 129/94-ВР // Відомості Верховної Ради України, 1994. – № 35. – Ст. 338.

[2] Указ Президента України «Про порядок офіційного оприлюднення нормативно-правових актів та набрання ними чинності» від 10 червня 1997 р. № 503/97.

[3] Постанова Кабінету Міністрів України «Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади» від 4 січня 2002 р. № 3.

органів шляхом впровадження та використання сучасних інформаційних технологій для надання інформаційних та інших послуг громадськості, забезпечення її впливу на процеси, що відбуваються у державі.

Шляхами оприлюднення відповідної інформації є:

• розміщення і періодичне оновлення міністерствами, іншими центральними та місцевими органами виконавчої влади інформації відповідно до вимог цього Порядку на власних веб-сайтах;

• створення єдиного веб-порталу Кабінету Міністрів України, призначеного для інтеграції веб-сайтів органів виконавчої влади та розміщення інформаційних ресурсів відповідно до потреб громадян.

Треба відзначити також норми, якими визначається порядок захисту інформації, розміщеної в мережі Інтернет. Зокрема, передбачено, що інформація, яка розміщується на веб-сайтах органів виконавчої влади та веб-порталі, повинна мати захист від несанкціонованої модифікації. Інформаційне наповнення, захист інформації від несанкціонованої модифікації та технічне забезпечення функціонування вебсайтів міністерств, інших центральних та місцевих органів виконавчої влади як складових частин веб-порталу зазначені органи здійснюють самостійно. Контроль за дотриманням вимог щодо захисту інформації, доступної через веб-портал, здійснюється Департаментом спеціальних телекомунікаційних систем та захисту інформації СБУ.

Діяльність органів державної влади в мережі Інтернет має і більш глобальні цілі. Так, на основі викладених у цитованій постанові завдань Кабінет Міністрів пропробляє концепцію «електронного органу виконавчої влади», для чого і створюється веб-портал, на якому кожен громадянин України, який має доступ до Інтернет, знайде потрібну інформацію про діяльність центральних та місцевих органів влади в Україні або отримає необхідні довідки і поради з приводу оформлення документів. Також у майбутньому планується використовувати Інтернет для відкритого діалогу з населенням.[1]

§ 3 Захист інформації в інформаційних системах

Іншим аспектом інформаційної безпеки є захист інформації, яка передається, зберігається та обробляється за допомогою комунікацій-

[1] Див.: Консультировать граждан, как общаться с чиновниками, доверят... электронному правительству // Факты. – 5 сентября 2002 г. – № 161. – С. 4.

них систем різних типів. В цьому напрямку в Україні вже створено цілу низку нормативно-правових актів.

Так, певні правові засади захисту інформаційної інфраструктури в Україні встановлюються нормами Закону «Про зв'язок»[1]. Зокрема, ст. 11 цього закону визначає порядок захисту інтересів держави у сфері зв'язку.

Норми ч. 2 ст. 11 Закону «Про зв'язок» визначають, що право власності, а також право на технічне обслуговування і експлуатацію мереж телекомунікацій загального користування може належати будь-якій юридичній особі – резиденту України. Таким чином, створюється правова гарантія того, що контроль за системами комунікації в Україні не буде здійснюватися іншими державами або суб'єктами-нерезидентами.

Передбачено також, що розвиток первинних мереж зв'язку проводять суб'єкти права власності на первинні мережі. На сьогоднішній день право власності на первинні мережі зв'язку загального користування в Україні належить ВАТ «Укртелеком», яке, згідно з вказаними правовими нормами, не може передавати їх у власність або управління іншим особам.

У разі визнання ВАТ «Укртелеком» банкрутом переважне право на придбання первинних мереж зв'язку, що перебувають на балансі відкритого акціонерного товариства «Укртелеком», належить державі.

Законом «Про зв'язок» передбачено (ст. 27) охорону таємниці інформації, що передається засобами зв'язку, в тому числі і з застосуванням організаційно-технічних заходів.

Крім того, передбачено і охорону безпосередньо об'єктів зв'язку. Так, згідно із ст. 28 Закону «Про зв'язок» підприємства, об'єднання, установи, організації та об'єкти зв'язку охороняються відомчою воєнізованою охороною, а в окремих підрозділах підприємств, об'єднань, установ та організацій зв'язку може встановлюватись особливий режим допуску. Охороні, згідно з чинним законодавством, підлягають всі об'єкти і споруди зв'язку, а винні в їх пошкодженні несуть дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність.

Важливим інструментом захисту інтересів і безпеки держави у сфері зв'язку є ліцензування підприємницької діяльності і сертифікація товарів і послуг у цій сфері.

---

[1] Закон України «Про зв'язок» від 16 травня 1995 року № 160/95-ВР // Відомості Верховної Ради України, 1995. – № 20. – Ст.143. (В редакції Закону № 1869-III від 13.07.2000)

Згідно з Законом «Про підприємництво» ліцензуванню, зокрема, підлягають:

• пересилання грошових переказів, листів до 20 (двадцяти) грамів, поштових карток;

• використання радіочастот;

• надання послуг телефонного зв'язку (крім відомчих об'єктів), технічне обслуговування мереж теле-, радіо- і проводового мовлення в межах промислової експлуатації;

• діяльність, пов'язана з розробкою, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів криптографічного та технічного захисту інформації, а також з наданням послуг із криптографічного та технічного захисту інформації.[1]

Видача ліцензій (документів державного зразка, які засвідчують право ліцензіата на провадження зазначеного в ньому виду господарської діяльності протягом визначеного строку за умови виконання ліцензійних умов) здійснюється уповноваженими Кабінетом Міністрів органами, передусім Міністерством зв'язку, у порядку, визначеному Законом «Про ліцензування певних видів господарської діяльності»[2].

Нормами ст. 24 Закону «Про зв'язок» визначено, що ліцензування видів діяльності в галузі зв'язку запроваджується з метою:

• здійснення єдиної державної політики в галузі зв'язку та захисту прав споживачів, координації діяльності різних підприємств в галузі створення і розвитку мереж, систем і служб зв'язку для забезпечення їх взаємодії між собою та з мережами зв'язку загального користування;

• сприяння демонополізації діяльності в галузі зв'язку, розвитку підприємництва і конкуренції; залучення коштів підприємств усіх форм власності до розвитку галузі;

• забезпечення високого рівня якості послуг зв'язку.[3]

Додатковими умовами видачі ліцензій є:

• додержання загальновстановлених правил і нормативних документів, які регламентують створення єдиної національної системи зв'язку України;

---

[1] Закон України «Про підприємництво» від 7 лютого 1991 р. // Відомості Верховної Ради України, 1991. – № 14. – Ст. 168.

[2] Закон України «Про ліцензування певних видів господарської діяльності» від 1 червня 2000 р. // Урядовий кур'єр. – 2000. – 2 серпня. – № 139.

[3] Закон України «Про зв'язок» від 16 травня 1995 року № 160/95-ВР // Відомості Верховної Ради України, 1995. – № 20. – Ст.143.

• використання для здійснення даного виду діяльності перспективних технічних засобів і технологій, що передбачаються в єдиній національній системі зв'язку України;

• необхідність розвитку в першу чергу соціально значущих послуг зв'язку, зниження тарифів на ці послуги, для чого допускається часткова реінвестиція на розвиток цих послуг від інших високорентабельних послуг зв'язку.

Видача ліцензій на використання каналів мовлення і діяльність у галузі телебачення та радіомовлення здійснюється згідно з Законом «Про телебачення і радіомовлення».[1]

Важливим напрямом захисту інформаційної безпеки є встановлення правових засад захисту інформації, що передається або обробляється за допомогою комунікаційних та автоматизованих систем. Основним нормативно-правовим актом у цій галузі вважається Закон «Про захист інформації в автоматизованих системах»[2] .

Згідно з цим законом (ст. 1) автоматизована система (далі – АС) визначається як система, що здійснює автоматизовану обробку даних і до складу якої входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення.

Визначено п'ять типів неправомірних дій щодо інформації в автоматизованих системах та самих автоматизованих систем (ст. 1), до яких належать:

1) витік інформації – результат дій порушника, внаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;

2) втрата інформації – дія, внаслідок якої інформація в АС перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі;

3) підробка інформації – навмисні дії, що призводять до перекручення інформації, яка повинна оброблятися або зберігатися в АС;

4) блокування інформації – дії, наслідком яких є припинення доступу до інформації;

5) порушення роботи АС – дії або обставини, які призводять до спотворення процесу обробки інформації.

---

[1] Закон України «Про телебачення і радіомовлення» від 21 грудня 1993 року № 3759-XII // Відомості Верховної Ради України, 1994. – № 10. – Ст. 43. (В редакції Закону від 11.05.2000 № 1709-III)

[2] Закон України «Про захист інформації в автоматизованих системах» від 5 липня 1994 року № 80/94-ВР // Відомості Верховної Ради України, 1994. – № 31. – Ст. 286.

Об'єктами захисту від неправомірних зазіхань є інформація, що обробляється в АС, права власників цієї інформації та власників АС, права користувача. Захист інформації здійснюється шляхом застосування сукупності організаційно-технічних заходів і правових норм для запобігання заподіянню шкоди інтересам власника інформації чи АС та осіб, які користуються інформацією.

Також Законом «Про захист інформації в автоматизованих системах» визначаються відносини між суб'єктами в процесі обробки інформації в автоматизованих системах, загальні вимоги щодо захисту інформації в АС і порядок організації цього захисту, відповідальність за порушення норм цього закону та засади міжнародного співробітництва України в сфері автоматизованих систем.

Зокрема, передбачено (ст. 11), що вимоги і правила щодо захисту інформації, яка є власністю держави, або інформації, захист якої гарантується державою, визначаються відповідними нормативно-правовими актами. Ці вимоги є обов'язковими для власників АС, де така інформація обробляється, і мають рекомендаційний характер для інших суб'єктів права власності на інформацію. Тобто захист інформації в АС побудовано на тих самих засадах, що захист інформації взагалі, згідно з якими захист державної, службової таємниці, особистих даних побудовано на вимогах правових актів, що визначають режим доступу до цієї інформації, а захист комерційної таємниці – на основі права власності на цю інформацію.

Політика в галузі захисту інформації в АС визначається Верховною Радою України, а державне управління в цій сфері здійснюється Кабінетом Міністрів.

Державне управління в сфері захисту інформації в автоматизованих системах здійснюється шляхом:

- проведення єдиної технічної політики щодо захисту інформації;
- розроблення концепції, вимог, нормативно-технічних документів і науково-методичних рекомендацій щодо захисту інформації в АС;
- затвердження порядку організації, функціонування та контролю за виконанням заходів, спрямованих на захист оброблюваної в АС інформації, яка є власністю держави, а також рекомендацій щодо захисту інформації – власності юридичних та фізичних осіб;
- організації випробувань і сертифікації засобів захисту інформації в АС, в якій здійснюється обробка інформації, яка є власністю держави;
- створення відповідних структур для захисту інформації в АС;

• проведення атестації сертифікаційних (випробувальних) органів, центрів і лабораторій, видачі ліцензії на право проведення сервісних робіт в галузі захисту інформації в АС;

• здійснення контролю захищеності оброблюваної в АС інформації, яка є власністю держави;

• визначення порядку доступу осіб і організацій зарубіжних держав до інформації в АС, яка є власністю держави, або до інформації – власності фізичних та юридичних осіб, щодо поширення і використання якої державою встановлено обмеження.

Взагалі, коли мова йде про захист інформації, то більшість дослідників погоджується з тим, що цей захист може мати лише комплексний характер. Але в цій комплексній системі можна виділити цілий спектр напрямків діяльності суб'єктів захисту інформації, які характеризуються властивими специфічними методами і способами захисту інформації. Зазвичай виділяють:

правовий захист – спеціальні закони, інші нормативні акти, правила, процедури і заходи, що забезпечують захист інформації на правовій основі;

організаційний захист – це регламентація виробничої діяльності і взаємовідносин виконавців на нормативно-правовій основі, що виключає або послаблює заподіяння якої-небудь шкоди виконавцям;

інженерно-технічний захист – використання різних технічних засобів, що попереджають заподіяння шкоди інформації.[1]

Але слід зазначити, що в будь-якому разі в основі всіх перерахованих заходів лежать правові норми, якими регламентується діяльність у сфері захисту інформації. Крім того, правовий захист інформації, який було розглянуто в попередніх розділах, стосується, так би мовити, інформації в чистому вигляді, незалежно від її носія. А от наступні – організаційний і інженерно-технічний аспекти захисту інформації спрямовані не безпосередньо на інформацію, а на системи, об'єкти та носії, на яких ця інформація збирається, зберігається, обробляється та розповсюджується.

Так, наприклад, головні напрямки підвищення безпеки передачі інформації, що є власністю держави, визначено в Указі Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних»[2]. Зокрема, передбачається запро-

[1] Див.: Ярочкин В.И. Информационная безопасность. – М.: Международные отношения, 2000. – С. 32 – 33.

[2] Указ Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних» від 24 вересня 2001 р. № 891/2001.

вадити щодо органів виконавчої влади, інших державних органів, а також підприємств, установ та організацій, які одержують, обробляють, поширюють і зберігають інформацію, що є об'єктом державної власності та охороняється згідно із законодавством, спеціальний порядок підключення до іноземних і міжнародних мереж передачі даних, у тому числі до мережі Інтернет, спеціальний порядок придбання комп'ютерної та телекомунікаційної техніки, засобів програмного забезпечення, та здійснювати передачу даних глобальними мережами виключно через підприємства (операторів), що визначатимуться Державним комітетом зв'язку та інформатизації України. Органам місцевого самоврядування також рекомендується здійснювати передачу даних глобальними мережами в порядку, передбаченому вищезазначеним указом.

Комплексний характер захисту інформаційної інфраструктури реалізовано і в національному законодавстві. Так, зокрема, зазначається, що захист державних інформаційних ресурсів в автоматизованих системах, що входять до складу інформаційно-телекомунікаційних систем, здійснюється шляхом запровадження комплексної системи захисту інформації (КСЗІ). КСЗІ складається з комплексу технічних, криптографічних, організаційних та інших заходів і засобів, спрямованих на недопущення блокування інформації, несанкціонованого ознайомлення з нею та/або її модифікації.[1]

Основними елементами комплексної системи захисту інформації можна вважати заходи технічного та криптографічного захисту інформації, а також комплекс заходів організаційного характеру, який включає встановлення відповідних режимів діяльності об'єктів інформаційних систем, контроль за дотриманням правил і норм здійснення захисту інформації, контроль за діяльністю суб'єктів захисту інформації тощо.

§ 4 Технічний захист інформації

Згідно з положенням «Про технічний захист інформації в Україні», яке було затверджене Указом Президента, технічний захист інформації (ТЗІ) являє собою «діяльність, спрямовану на забезпечення інженер-

[1] Див.: Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України «Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах» від 24 грудня 2001 р. № 76.

но-технічними заходами конфіденційності, цілісності та доступності інформації»[1]. Комплекс заходів щодо технічного захисту інформації може здійснюватися лише в інформаційній системі або на іншому об'єкті інформаційної інфраструктури. Рівень безпеки інформації, яка обробляється в системах та на об'єктах інформаційної інфраструктури, визначається комплексом її властивостей, який включає три компоненти:

1) конфіденційність – властивість інформації бути захищеною від несанкціонованого ознайомлення;

2) цілісність – властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;

3) доступність – властивість інформації бути захищеною від несанкціонованого блокування.

Лише забезпечення всіх цих трьох характеристик інформації, що підлягає захисту, є умовою ефективного і безпечного використання суб'єктами інформаційних процесів необхідних об'єктів інформаційної інфраструктури.

Технічний захист інформації здійснюється за допомогою системи технічного захисту інформації, яка являє собою «сукупність суб'єктів, об'єднаних цілями та завданнями захисту інформації інженерно-технічними заходами, нормативно-правову та їхню матеріально-технічну базу»[2].

Суб'єктами цієї системи є:

- Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України;
- органи державної влади, органи місцевого самоврядування, органи управління Збройних сил України та інших військових формувань, утворених згідно із законодавством, відповідні підприємства, установи та організації (далі – органи, щодо яких здійснюється ТЗІ);
- державні наукові, науково-дослідні та науково-виробничі підприємства, установи та організації, що належать до системи Служби безпеки України і виконують завдання ТЗІ;
- військові частини, підприємства, установи та організації всіх форм власності й громадяни-підприємці, які провадять діяльність з ТЗІ за відповідними дозволами або ліцензіями;

[1] Указ Президента України «Про Положення про технічний захист інформації в Україні» від 27 вересня 1999 р. № 1229.

[2] Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України «Про Положення про контроль за функціонуванням системи технічного захисту інформації» від 22 грудня 1999 р. № 61.

• навчальні заклади з підготовки, перепідготовки та підвищення кваліфікації фахівців з ТЗІ.

Організація технічного захисту інформації в органах, щодо яких здійснюється ТЗІ, покладається на їхніх керівників. Основними завданнями суб'єктів системи ТЗІ є:

• забезпечення технічного захисту інформації згідно з вимогами нормативно-правових актів з питань технічного захисту інформації;

• видання у межах своїх повноважень нормативно-правових актів із питань технічного захисту інформації;

• здійснення контролю за станом технічного захисту інформації.

Безпосередні організаційно-технічні принципи, порядок здійснення заходів із технічного захисту інформації, характеристики загроз для інформації, норми та вимоги з технічного захисту інформації визначаються окремими нормативно-правовими актами, які в основному мають конфіденційний характер.

Неодмінно слід відзначити існування диференціації щодо вимог та стандартів технічного захисту інформації. Ця диференціація залежить від суб'єкта власності інформації, що захищається, та її правового режиму. Так, щодо захисту конфіденційної інформації, яка перебуває у приватній власності і режим якої визначається її власником, положення більшості нормативно-правових актів з ТЗІ мають рекомендаційний характер. Водночас ці нормативно-правові акти обов'язкові для органів державної влади та органів місцевого самоврядування, які здійснюють технічний захист інформації, необхідність охорони якої визначена законодавством.

Роботи з ТЗІ проводяться організаціями, які мають ліцензії на право провадження господарської діяльності у галузі ТЗІ. Також передбачена можливість здійснення робіт з ТЗІ для власних потреб органами державної влади та місцевого самоврядування у дозвільному порядку. Ліцензування господарської діяльності з ТЗІ, а також надання дозволів на проведення робіт з ТЗІ для власних потреб здійснюється Департаментом спеціальних телекомунікаційних систем та захисту інформації СБУ.

Також встановлено класифікацію основних видів робот з ТЗІ, які виконуються за дозволами департаменту. Ця класифікація побудована з урахуванням основних можливих шляхів витоку інформації, що охороняється, яким кореспондують відповідні заходи захисту і включає:

• розроблення, впровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є акустичні поля;

• розроблення, впровадження, дослідження ефективності, обслуговування на об'єктах інформаційної діяльності комплексів (систем) технічного захисту інформації, носіями якої є електромагнітні поля та електричні сигнали;

• розроблення, виробництво, впровадження, дослідження ефективності, супроводження засобів та комплексів технічного захисту інформації в інформаційних системах, інформаційних технологій із захистом інформації від несанкціонованого доступу;

• виявлення та блокування витоку мовної та видової інформації через закладні пристрої на об'єктах інформаційної діяльності.[1]

Велика увага також приділяється експертно-контрольній діяльності у сфері технічного захисту інформації, здійснення якої входить до функцій Інспекції з питань захисту інформації Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України.

Згідно з «Положенням про контроль за функціонуванням системи технічного захисту інформації»[2], ця діяльність здійснюється у формі контрольно-інспекційної роботи з питань ТЗІ та атестації виділених приміщень.

Контрольно-інспекційна робота з питань ТЗІ являє собою діяльність, спрямовану на визначення та вдосконалення стану ТЗІ органів, щодо яких здійснюється ТЗІ, та на проведення контролю за виконанням суб'єктами системи ТЗІ завдань або проведенням діяльності в галузі ТЗІ за відповідними дозволами і ліцензіями.

Контрольно-інспекційна робота з питань ТЗІ включає планування та проведення перевірок стану ТЗІ в органах, щодо яких здійснюється ТЗІ, проведення аналізу та надання рекомендацій щодо вдосконалення заходів з ТЗІ в зазначених органах та перевірок з ТЗІ інших суб'єктів системи ТЗІ щодо виконання ними завдань або провадження діяльності в цій галузі за відповідними дозволами та ліцензіями.

Самі перевірки бувають трьох видів: комплексні, цільові (тематичні) та контрольні. Під час перевірок контролю підлягають органі-

[1] Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України «Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб» від 23 лютого 2002 р. № 9.

[2] Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України «Про Положення про контроль за функціонуванням системи технічного захисту інформації» від 22 грудня 1999 р. № 61.

заційні, організаційно-технічні, технічні заходи з ТЗІ у виділених приміщеннях, інформаційних системах і об'єктах, повнота та достатність робіт з атестації виділених приміщень.

Ще одним напрямком контрольної діяльності є атестація виділених приміщень, у рамках якої здійснюється комплекс спрямованих на реалізацію заходів з ТЗІ робіт, метою яких є приведення виділених приміщень у відповідність до вимог нормативних документів з ТЗІ та визначення відповідності захищеності виділеного приміщення встановленій категорії.

Також в Україні діє Державна експертиза в сфері технічного захисту інформації, яка проводиться з метою оцінки захищеності інформації, яка обробляється або циркулює в автоматизованих системах, комп'ютерних мережах, системах зв'язку, приміщеннях, інженерно-технічних спорудах тощо (далі – об'єкти інформаційної діяльності), та підготовки обґрунтованих висновків для прийняття відповідних рішень.[1]

Важливим інструментом державного управління технічним захистом інформаційних систем є також стандартизація і сертифікація їхньої діяльності. Для цих цілей, зокрема, встановлено, що Державний комітет стандартизації, метрології та сертифікації затверджує проекти державних стандартів технічного захисту інформації та проводить реєстрацію нормативних документів, відповідно до яких виготовляються засоби забезпечення технічного захисту інформації, виключно за погодженням з Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки.[2]

§ 5 Криптографічний захист інформації

Іншим напрямком підвищення безпеки інформаційних систем є криптографічний захист інформації, що обробляється за їх допомогою. Взагалі цей вид захисту інформації можна назвати найдавнішим, оскільки його корені сягають ще IV тисячоліття до н.е., коли в стародавніх Єгипті, Шумері, Китаї, Індії та Ассирії виникли перші шифри. Але

[1] Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України «Про Положення про державну експертизу в сфері технічного захисту інформації» від 29 грудня 1999 р. № 62.

[2] Постанова Кабінету Міністрів «Про деякі питання захисту інформації, охорона якої забезпечується державою» від 13.03.2002 р. № 281

основоположником криптографічної науки вважається К. Шенон, який в 1946 р. видав роботу під назвою «Теорія зв'язку в секретних системах», у якій були викладені головні теоретичні основи сучасної криптографії. Саме з того часу застосування криптографічного захисту інформації стало швидко поширюватися не лише у військово-політичній сфері, а й у промисловості, банківській діяльності, приватній кореспонденції тощо.

Криптографія стала не лише справою спецслужб, як би вони того не хотіли. 70 – 80-ті рр. XX ст. відзначаються посиленням суспільного інтересу до криптографії. Виявилось, що криптографічні засоби можуть бути добрим інструментом захисту прав громадян на конфіденційність листування і переговорів. Цьому сприяло відкриття односторонніх функцій і криптографії з відкритими ключами, так званих хеш-функцій (спеціальних ознак повідомлень, за якими легко ідентифікувати повідомлення і виявити його модифікації); механізмів цифрового підпису (аналога звичайного рукописного підпису, який надає електронним документам юридичної сили) тощо.[1]

В Україні нормативно-правове регулювання питань криптографічного захисту інформації розвивається досить швидко. Безпосередньою основою цього виду діяльності є затверджене Указом Президента «Положення про порядок здійснення криптографічного захисту інформації», згідно з яким криптографічний захист інформації являє собою «вид захисту, що реалізується за допомогою перетворень інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо»[2] .

Цим же указом визначені основні терміни, що використовуються у криптографічному захисті інформації:

засіб криптографічного захисту інформації – програмний, апаратно-програмний, апаратний або інший засіб, призначений для криптографічного захисту інформації;

криптографічна система (криптосистема) – сукупність засобів криптографічного захисту інформації, необхідної ключової, нормативної, експлуатаційної, а також іншої документації (у тому числі такої, що визначає заходи безпеки), використання яких забезпечує належ-

[1] Див.: Потий О. Криптография, прошлое и настоящее // Служба безопасности, 2001. – № 2 – 3. – С. 28 – 30.

[2] Указ Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» від 22 травня 1998 р. № 505/98.

ний рівень захищеності інформації, що обробляється, зберігається та (або) передається.

Сам же криптографічний захист інформації реалізується за допомогою відповідної системи криптографічного захисту інформації, яку складають сукупність органів, підрозділів, груп, діяльність яких спрямована на забезпечення криптографічного захисту інформації, та підприємств, установ і організацій, що розробляють, виробляють, експлуатують та (або) розповсюджують криптосистеми і засоби криптографічного захисту інформації.

Конкретні вимоги до засобів криптографічного захисту інформації залежать від правового режиму останньої і її суспільного та державного значення. Так, для криптографічного захисту інформації, що становить державну таємницю, та службової інформації, створеної на замовлення державних органів або яка є власністю держави, використовуються криптосистеми і засоби криптографічного захисту, допущені до експлуатації Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. Такі криптосистеми і засоби перебувають виключно у державній власності.

В той же час засоби криптографічного захисту службової інформації та криптосистеми з відповідного дозволу можуть перебувати і в недержавній власності.

І, нарешті, щодо криптосистем і засобів криптографічного захисту конфіденційної інформації встановлено лише вимогу наявності сертифікату відповідності.

Законодавством також встановлено вимоги щодо ліцензування діяльності, пов'язаної з розробкою, виготовленням, ввезенням, вивезенням, реалізацією та використанням засобів криптографічного захисту інформації, а також з наданням послуг із криптографічного захисту інформації.

Важливим аспектом, що забезпечує надійність криптографічного захисту інформації, є не лише якість та характеристики самих криптосистем, а й організаційні заходи, які унеможливлюють витік інформації, що може допомогти у зламі криптографічного захисту. З цією метою встановлено особливий порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації та постачання і використання ключів до цих засобів.

Заходи щодо організаційного забезпечення криптографічного захисту інформації (КЗІ) реалізуються шляхом встановлення:

• режиму безпеки, який являє собою реалізовану систему правових норм, організаційних та організаційно-технічних заходів, яка

створюється на підприємствах під час розроблення, дослідження, виробництва та експлуатації засобів КЗІ з метою обмеження доступу до конфіденційної інформації;

• спеціальних вимог до КЗІ, тобто вимог до принципів побудови засобів КЗІ та технічної реалізації криптографічних алгоритмів у засобах КЗІ, вимоги до криптографічних якостей, а також вимоги і норми щодо захисту від можливих каналів витоку небезпечних сигналів засобів КЗІ.[1]

Серед головних вимог до інформаційної безпеки засобів КЗІ слід назвати такі:

• Особи, які допущені до розробки, виготовлення і експлуатації КЗІ, повинні мати допуск, відповідний рівню таємної або конфіденційної інформації, яку передбачається захищати такими засобами КЗІ.

• У засобах КЗІ повинні використовуватися криптоалгоритми та криптопротоколи, які є державними стандартами України або рекомендовані Департаментом спеціальних телекомунікаційних систем та захисту інформації СБУ.

• Засоби КЗІ без уведених діючих ключових даних мають гриф обмеження доступу, який відповідає грифу опису криптосхеми.

• Гриф обмеження доступу засобів КЗІ із завантаженими ключовими даними визначається грифом обмеження доступу ключових документів.

• Гриф обмеження доступу ключових документів, що використовуються засобами КЗІ, повинен відповідати максимальному грифу обмеження доступу інформації, яка захищається.

Безпосередньо порядок постачання і використання ключів до засобів КЗІ і відповідні організаційні та технічні заходи безпеки регулюються спеціальною інструкцією, затвердженою спільним наказом Держстандарту та СБУ, якою запроваджено «єдині вимоги, обов'язкові для виконання юридичними особами будь-яких форм власності, що передбачені чинним законодавством».[2]

---

[1] Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України «Про затвердження Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації» від 30 листопада 1999 р. № 53.

[2] Наказ Держстандарту України та Служби безпеки України «Про затвердження Тимчасової інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації» від 28 листопада 1997 р. № 708/156.

Новий напрямок застосування засобів КЗІ відкривається із набуттям чинності Закону «Про електронний цифровий підпис»[1]. Електронний цифровий підпис (ст. 1 закону) – вид електронного підпису, отриманого за результатом криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується і дає змогу підтвердити його цілісність та ідентифікувати підписувача. Електронний цифровий підпис накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Електронний цифровий підпис після необхідної перевірки за правовим статусом прирівнюється до власноручного підпису (печатки).

Запровадження в Україні електронного документообігу і відповідно використання електронного цифрового підпису викликає необхідність здійснення цілого ряду організаційних заходів. Так, зокрема, Законом «Про електронний цифровий підпис» передбачається створення центрів сертифікації ключів, акредитованих центрів сертифікації ключів, засвідчувального центру, центрального засвідчувального органу та контролюючого органу. До функцій даних установ буде входити вирішення цілого комплексу питань, пов'язаних з наданням особистих ключів для електронного цифрового підпису, їх сертифікатів, засвідчення їх чинності, блокування, скасування, а також надання необхідної акредитації, ведення відповідних реєстрів тощо.

§ 6 Система захисту інформаційної інфраструктури

Підбиваючи деякі підсумки аналізу основних нормативно-правових актів із захисту інформаційної інфраструктури, ми можемо говорити про те, що цей аспект інформаційної безпеки є найбільш розробленим в українському законодавстві. Пояснюється це тим, що означеним питанням захисту інформаційних ресурсів приділялася значна увага ще за часів СРСР, і таким чином існувала можливість запозичення відповідного досвіду. Однак разом з тим високі темпи інформатизації суспільства привели Україну до того рубежу, за яким використання виключно внутрішнього досвіду і старих напрацювань вже неможливе (особливо враховуючи наше хронічне відставання в інформаційній сфері). Розрив же між розвинутими країнами і рештою світу невпинно збільшується. Нові реалії ставлять і нові вимоги в правовому регулю-

[1] Закон України «Про електронний цифровий підпис» від 22 травня 2003 р. № 852-IV.

ванні захисту інформації, який повинен стати каталізатором запровадження нових технічних та організаційних засобів.

По-перше, існує нагальна потреба більш послідовно слідувати задекларованому комплексному підходові у галузі захисту інформаційної інфраструктури України, включаючи законодавче закріплення самого її визначення. Визначення інформаційної інфраструктури та основ компетенції держави по її захисту повинно бути включене до Закону «Про інформацію», а також деталізоване в комплексному нормативно-правовому акті «Про захист інформації та інформаційної інфраструктури».

Такий комплексний підхід до захисту інформаційної інфраструктури країни характеризується, зокрема, поширеними нині думками про те, що «якщо інформаційну систему розглядати як ціле, то інформаційну безпеку можна представити як її частину, хоча і концентровано виражену», адже, «комплекс механізмів захисту (організаційних, правових, технічних, економічних тощо) інформаційної системи формує головні якості її стану – цілісність і стійкість. Без них інформаційна сфера як система існувати не може».[1]

Законодавчим актом про захист інформації та інформаційної інфраструктури повинні бути визначені єдині засади системи захисту єдиної інформаційної інфраструктури України. Така система повинна включати в себе цілий комплекс заходів, до якого входять:

1) правові – правові норми, що регулюють відносини, що виникають з приводу створення та використання інформаційної інфраструктури, та відповідальність суб'єктів цих відносин;

2) організаційні – дотримання встановленого порядку створення та використання об'єктів інформаційної інфраструктури, включаючи фізичний захист цих об'єктів;

3) технічні – застосування інженерно-технічних заходів, що роблять інформацію недосяжною для протиправних дій;

4) криптографічні – надання інформації такого вигляду, що унеможливлює протиправне або неавторизоване її використання;

5) економічні – фінансове забезпечення заходів щодо захисту інформаційної інфраструктури та створення фінансових гарантій і стимулів необхідного розвитку цієї інфраструктури.

Окрім цього, існує цілий ряд окремих аспектів функціонування інформаційної інфраструктури України, встановлення правового ре-

[1] Кузнецов П.У. Системные проблемы правового обеспечения информационной сферы. // Право и политика, 2001. – № 6. – С. 43.

гулювання яких є нагальною потребою підвищення рівня інформаційної безпеки.

Ще одним аспектом функціонування інформаційної інфраструктури є необхідність на законодавчому рівні визначити правовий статус і порядок формування та розпорядження електронних баз даних. На сьогоднішній день в Україні не існує єдиного нормативно-правового акта. Бази даних за власною ініціативою створюються різними міністерствами та відомствами, органами місцевого самоврядування, підприємствами, установами й організаціями, і відповідно їхній правовий статус визначається кількома десятками підзаконних актів. Не існує навіть єдиного визначення бази даних. На нашу думку, така ситуація є неприпустимою. Деякі елементи правового статусу баз даних повинні визначатися тільки на законодавчому рівні. Зокрема, потрібно визначити:

1) правові засади створення і використання цих баз їх власником, щоб виключити можливість порушення прав та законних інтересів фізичних і юридичних осіб (в першу чергу це стосується персональних даних);

2) компетенцію та обов'язки органів державної влади, місцевого самоврядування, підприємств, установ і організацій щодо ведення баз даних та надання інформації з цих баз. Насамперед необхідно визначити конкретні органи, яким доручено ведення баз даних з тих чи інших питань (це дасть можливість зацікавленим особам звернутися до цих органів за необхідною інформацією), та правовий режим і умови надання відповідної інформації третім особам (що виключить як необґрунтовані відмови у наданні інформації, так і протиправне поширення цієї інформації);

3) спеціальні права, які надаються укладачам баз даних, згідно з якими база даних в цілому розглядається як об'єкт інтелектуальної власності, а її власнику надається право перешкоджати витягу або повторному використанню всього або суттєвої частини змісту бази даних.

Звісно, вищесказане є далеко не повним переліком проблем, які потребують свого нормативно-правового регулювання в цілях захисту безпеки інформаційної інфраструктури. Але вкрай потрібно створити головні засади та принципи, на основі яких можна здійснювати подальший розвиток системи безпеки інформаційної інфраструктури. Причому, на нашу думку, в цьому процесі не слід займатися «винайденням велосипеда», оскільки в світі існує досить багато країн з більш розвинутою інформаційною інфраструктурою, які вже встигли раніше зіткну-

тися з тими проблемами, які постають перед Україною сьогодні. І їхній досвід є дуже цінним.

ПРОГРАМА КУРСУ «ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ»

Тема І. Поняття та категорії національної безпеки

Основні підходи до визначення поняття «національна безпека». Історія формування категорії «національна безпека». Основи нормативно-правового регулювання питань національної безпеки в Україні. Характеристика основних положень Закону України «Про основи національної безпеки України. Сутність категорії «національні інтереси», її співвідношення з категорією «національна безпека».

Тема ІІ. Правова та соціальна характеристика інформації

Основні підходи до визначення терміна «інформація» в сучасних гуманітарних та природничих науках. Значення інформації в державному та суспільному житті. Інформатизація та розвиток інформаційних технологій в сучасному світі. Основні характеристики інформації. Правила, якими регулюється обіг інформації. Види інформації, визначені в українському законодавстві. Поняття інформаційних відносин. Види інформаційних відносин, які є об'єктом інформаційної безпеки.

Тема ІІІ. Захист інформаційної безпеки як функція держави

Основні підходи до визначення поняття «інформаційна безпека». Головні характеристики, що визначають юрисдикцію держави в інформаційній сфері. Функції, які виконує сучасна держава в інформаційній сфері. Характеристика понять «інформаційний суверенітет», «інформаційній простір», «інформаційний ринок». Функції держави щодо захисту інформаційної безпеки. Нормативно-правові акти, що визначають функції держави із захисту інформаційної безпеки.

Тема ІV. Основні напрямки політики інформаційної безпеки України

Напрямки інформаційної безпеки, визначені національним законодавством. Види загроз інформаційній безпеці України та їх класи-

фікація. Особливості забезпечення інформаційної безпеки держави. Особливості забезпечення інформаційної безпеки людини та суспільства. Поняття державно-правового механізму інформаційної безпеки.

Тема V. Правова база політики інформаційної безпеки

Поняття, предмет та метод інформаційного права. Причини та особливості формування нової галузі інформаційного права. Створення правової бази як засіб реалізації політики інформаційної безпеки. Інформаційне право та правова база політики інформаційної безпеки, їх співвідношення. Структура правової бази політики інформаційної безпеки.

Тема VI. Інституціональний механізм політики інформаційної безпеки

Поняття, структура інституціонального механізму політики інформаційної безпеки. Державні та недержавні суб'єкти, що впливають на процес формування і реалізації політики інформаційної безпеки. Компетенція та розподіл функцій центральних органів державної влади – Верховної Ради України, Президента України, Кабінету Міністрів України в галузі інформаційної безпеки. Структура та компетенція Ради національної безпеки та оборони України. Інші органи державної влади, що виконують у рамках своєї діяльності окремі завдання щодо захисту інформаційної безпеки України: а) Служба безпеки України, б) Міністерство внутрішніх справ, в) Міністерство освіти і науки України, г) Міністерство культури і мистецтв України, д) Державний комітет інформаційної політики, телебачення і радіомовлення, є) Державний комітет зв'язку та інформатизації, е) Національна рада з телебачення і радіомовлення тощо.

Тема VII. Організаційно-правові форми та методи політики інформаційної безпеки

Базові принципи захисту інформаційної безпеки, визначені в національному законодавстві. Фактори, що впливають на формування політики інформаційної безпеки. Основні форми проведення в життя політики інформаційної безпеки. Специфіка застосування методів державного управління у сфері інформаційних відносин. Відповідність заходів із захисту інформаційної безпеки характеру та актуальності загроз. Проблема узгодження заходів щодо захисту інформаційної безпеки з принципами демократії та гарантіями прав людини.

Тема VIII. Додержання інформаційних прав і свобод людини як основа інформаційної безпеки

Права і свободи людини в галузі інформації, які гарантовані Конституцією України. Основні міжнародно-правові акти, якими визначаються права людини в інформаційній сфері. Класифікація прав і свобод людини в галузі інформації. Існуючі проблеми та загрози щодо реалізації конституційних прав людини в сфері інформації, їхні причини. Визначені законодавством випадки і підстави обмеження прав людини в галузі інформації, необхідні при цьому гарантії.

Тема IX. Основні напрямки захисту інформаційної безпеки людини та суспільства

Поняття «персональні дані» і правові основи їх захисту. Право людини на доступ до правової інформації. Право людини на доступ до екологічної інформації. Поняття, види і способи негативного інформаційного впливу на свідомість людини, правові засади його попередження. Гарантії інформаційної безпеки громадян як суб'єктів політичного процесу.

Тема X. Безпека інформаційного розвитку

Розвиток інформаційних технологій та обумовлені ним проблеми інформаційної безпеки. Національна програма інформатизації України та передбачені нею заходи в галузі інформаційної безпеки. Правові засади захисту національного інформаційного ринку України. Правові проблеми, пов'язані з обмеженням застосування інформаційної зброї та попередженням інформаційного тероризму, міжнародно-правова регламентація цих питань. Хартія глобального інформаційного суспільства.

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації в цілях інформаційної безпеки

Правове регулювання суспільного обігу інформації. Поняття, ознаки та види режимів доступу до інформації. Правове регулювання обігу інформації, що становить державну таємницю. Поняття та види конфіденційної інформації. Обмеження доступу до інформації в інтересах слідства та судочинства. Правове регулювання обігу інформації, що становить службову таємницю. Види та особливості правового регулювання обігу інформації, що становить комерційну таємницю. Інформація, що становить професійну таємницю: а) адвокатська таємниця,

б) лікарська таємниця, в) таємниця вчинення нотаріальних дій, г) таємниця страхування, д) банківська таємниця. Обмеження, які застосовуються щодо виробництва та ввезення в Україну інформаційної продукції.

Тема XII. Правові засади безпеки інформаційної інфраструктури

Поняття «інформаційна інфраструктура» та основні напрямки її захисту. Принципи правового регулювання функціонування мережі Інтернет і пов'язані з цим проблеми інформаційної безпеки. Правові засади захисту інформації в інформаційних системах. Правові засади технічного захисту інформації. Правові засади криптографічного захисту інформації.

КОНТРОЛЬНІ ЗАПИТАННЯ

Тема І. Поняття та категорії національної безпеки

1. Які основні визначення поняття «національна безпека» ви знаєте?
2. Як відбувалося формування категорії «національна безпека»?
3. Якими основними нормативно-правовими актами регулюються питання національної безпеки в Україні?
4. Розкрийте основні положення Закону України "Про основи національної безпеки України.»
5. Розкрийте сутність категорії «національні інтереси» і як вона співвідноситься з поняттям «національна безпека».

Тема ІІ. Правова та соціальна характеристика інформації

1. Які основні підходи до визначення поняття «інформація» ви знаєте?
2. Яке значення має інформація в державному та суспільному житті, що таке «інформатизація»?
3. Які основні характеристики має інформація? Якими правилами регулюється обіг інформації?
4. Які види інформації визначені в українському законодавстві?
5. Що таке інформаційні відносини, які з них є об'єктом інформаційної безпеки?

Тема ІІІ. Захист інформаційної безпеки як функція держави

1. Які основні визначення поняття «інформаційна безпека» ви знаєте?
2. Назвіть головні характеристики, що визначають юрисдикцію держави в інформаційній сфері.
3. Які основні функції виконує сучасна держава в інформаційній сфері?

4. Дайте визначення понять «інформаційний суверенітет», «інформаційній простір», «інформаційний ринок».

5. У чому полягають функції держави щодо захисту інформаційної безпеки, якими нормативно-правовими актами вони визначаються?

Тема IV. Основні напрямки політики інформаційної безпеки України

1. Які основні напрямки інформаційної безпеки визначені національним законодавством?

2. Які види загроз інформаційній безпеці України ви можете назвати?

3. В чому полягають особливості забезпечення інформаційної безпеки держави?

4. В чому полягають особливості забезпечення інформаційної безпеки людини та суспільства?

5. Сформулюйте визначення поняття державно-правового механізму інформаційної безпеки.

Тема V. Правова база політики інформаційної безпеки

1. Що являє собою інформаційне право, назвіть його предмет та метод.

2. Якими чинниками обумовлено формування галузі інформаційного права?

3. Як співвідносяться поняття “інформаційне право» та “правова база політики інформаційної безпеки»?

4. Дайте характеристику правової бази як засобу реалізації політики інформаційної безпеки.

5. Назвіть складові правової бази політики інформаційної безпеки.

Тема VI. Інституціональний механізм політики інформаційної безпеки

1. Що таке інституціональний механізм політики інформаційної безпеки?

2. Назвіть основних суб’єктів формування і проведення в життя політики інформаційної безпеки.

3. В чому полягає компетенція центральних органів державної влади в галузі інформаційної безпеки: а) Верховної Ради України, б) Президента України, в) Кабінету Міністрів України?

4. Охарактеризуйте структуру та компетенцію Ради національної безпеки та оборони України.

5. Назвіть основні завдання щодо захисту інформаційної безпеки України, які в рамках своєї діяльності виконують: а) Служба безпеки України, б) Міністерство внутрішніх справ, в) Міністерство освіти і науки України, г) Міністерство культури і мистецтв України, д) Державний комітет інформаційної політики, телебачення і радіомовлення, є) Державний комітет зв'язку та інформатизації, е) Національна рада з телебачення і радіомовлення.

Тема VII. Організаційно-правові форми та методи політики інформаційної безпеки

1. Які основні принципи захисту інформаційної безпеки визначені в національному законодавстві?
2. Які фактори впливають на формування політики інформаційної безпеки?
3. Назвіть основні форми проведення в життя політики інформаційної безпеки.
4. Охарактеризуйте специфіку застосування методів державного управління в сфері інформаційних відносин.
5. Як співвідноситься діяльність держави щодо захисту інформаційної безпеки з принципами демократії та гарантіями прав людини?

Тема VIII. Додержання інформаційних прав і свобод людини як основа інформаційної безпеки

1. Назвіть основні права людини в галузі інформації, які гарантовані Конституцією України.
2. Назвіть основні міжнародно-правові акти, якими визначаються права людини в інформаційній сфері.
3. Як можна класифікувати права людини в галузі інформації?
4. Які проблеми, на вашу думку, існують щодо реалізації конституційних прав людини в сфері інформації, в чому їх причини?
5. В яких випадках і на яких підставах можливе обмеження прав людини в галузі інформації?

Тема IX. Основні напрямки захисту інформаційної безпеки людини та суспільства

1. Що таке персональні дані і яким чином здійснюється їх захист?
2. Охарактеризуйте право людини на доступ до правової інформації.
3. Охарактеризуйте право людини на доступ до екологічної інформації.

4. Якими нормативно-правовими актами регламентується захист людини від негативного інформаційного впливу?

5. Які гарантії інформаційної безпеки громадян як суб'єктів політичного процесу ви можете назвати?

Тема X. Безпека інформаційного розвитку

1. Які нові завдання в галузі інформаційної безпеки обумовлені розвитком інформаційних технологій?

2. Які основні завдання в галузі інформаційної безпеки визначені Національною програмою інформатизації України?

3. Охарактеризуйте правові засади захисту національного інформаційного ринку України.

4. Які правові проблеми пов'язані з обмеженням застосування інформаційної зброї та попередженням інформаційного тероризму?

5. В чому полягають основні положення Хартії глобального інформаційного суспільства?

Тема XI. Організаційно-правові основи захисту та обмеження обігу інформації в цілях інформаційної безпеки

1. Охарактеризуйте особливості правового регулювання суспільного обігу інформації.

2. Що таке режим доступу до інформації?

3. Охарактеризуйте правове регулювання обігу інформації, що становить державну таємницю.

4. Які види конфіденційної інформації ви знаєте?

5. Що таке таємниця приватного життя?

6. Охарактеризуйте правове регулювання обмеження доступу до інформації в інтересах слідства та судочинства.

7. Охарактеризуйте правове регулювання обігу інформації, що становить службову таємницю.

8. Охарактеризуйте правове регулювання обігу інформації, що становить комерційну таємницю.

9. Охарактеризуйте правове регулювання обігу окремих видів інформації, що становить професійну таємницю: а) адвокатська таємниця, б) лікарська таємниця, в) таємниця вчинення нотаріальних дій, г) таємниця страхування, д) банківська таємниця

10. Які обмеження застосовуються щодо виробництва та ввезення в Україну інформаційної продукції?

Тема XII. Правові засади безпеки інформаційної інфраструктури

1. Що таке інформаційна інфраструктура і яким чином здійснюється її захист?

2. Охарактеризуйте правове регулювання забезпечення інформаційної безпеки в функціонуванні мережі Інтернет.

3. Охарактеризуйте правові засади захисту інформації в інформаційних системах.

4. Охарактеризуйте правові засади технічного захисту інформації.

5. Охарактеризуйте правові засади криптографічного захисту інформації.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. *Аверьянов В.Б.* Аппарат государственного управления: содержание деятельности и организационные структуры. – К.: Наукова думка, 1990.

2. Адміністративне право України / За загальною редакцією академіка Є.В. Ківалова. – Одеса: Юридична література, 2003.

3. Административное право России. Особенная часть. / Отв. редактор Д.Н. Бахрах. – М.: БЕК, 1997.

4. *Атаманчук Г.В.* Теория государственного управления: курс лекций. – М.: Юридическая литература, 1997.

5. *Бандурка О.М.* Основи управління в органах внутрішніх справ України: теорія, досвід, шляхи вдосконалення. – Харків: Основа, 1996.

6. *Бахрах Д. Н.* Административное право. - Москва: БЕК, 1999.

7. *Бачило И.Л.* Информационное право. Основы практической информатики. – М., 2001.

8. *Бачило И.Л., Лопатин В.Н., Федотов М.А.* Информационное право. / Под. ред. акад. РАН Б.Н. Топорнина. – СПб.: Юридический центр Пресс, 2001.

9. Безпека комп'ютерних систем. Злочинність у сфері комп'ютерної інформації і її попередження. / Ред. О.П. Снігірьов. – Запоріжжя: Павел, 1998 р.

10. *Венгеров А.Б.* Право и информация в условиях автоматизации управления. – М., 1978.

11. *Венгеров А.Б.* Теория государства и права. – М., 1999.

12. *Винер Н.* Кибернетика и управление, их связь в животном и машине. – М.: Иностранная литература, 1958.

13. *Возженков А.В.* Национальная безопасность: теория, политика, стратегия. – М.: НПО «Модуль», 2000.

14. *Гаврилов О.А.* Курс правовой информатики. – М.: Издательство НОРМА, 2000.

15. Державне управління в Україні. / За загальною ред. В.Б. Авер'янова. – К., 1999.

16. *Заєць А.П.* Правова держава в контексті новітнього українського досвіду. – К., 1999.

17. Інформація, аналіз, прогноз – стратегічні важелі ефективного державного управління. Всеукраїнська науково-практична конференція. – К.: УкрІнтеі, 2000.

18. Інформація, зв'язок і телекомунікації в Україні: економіка, право, управління. / Ред. Довгий С.О., Холод Б.І. – К.: Укртелеком, 2001.

19. Информация. Дипломатия. Психология. – М.: Известия, 2002.

20. Информационные технологии и информационная политика. – М., 1994.

21. *Кастельс М.* Информационная эпоха: экономика, общество, культура: Пер. с англ. под науч. ред. Шкаратана О.И. – М.: ГУ ВШЭ, 2000.

22. *Колпаков В. К.* Адміністративне право України. - Київ: Юрінком Інтер, 1999.

23. Коментар до Конституції України. – К.: Інститут законодавства Верховної Ради, 1996.

24. Компьютерные технологии в криминалистике и информационная безопасность. – М. : Акад. упр. МВД РФ, 1997.

25. Компьютерные террористы: Новейшие технологии на службе преступного мира. / Ред.- сост. Ревяко Т.И. – Мн.: Литература, 1997.

26. Конституційно-правові форми безпосередньої демократії в Україні: проблеми теорії і практики. До 10-ї річниці незалежності України. – К.: Інститут держави і права ім. В.М. Корецького НАН України, 2001.

27. Конституція незалежної України: У 3-х кн. / Ред. С.П. Головатий. – К.: Українська правнича фундація, 1995. Конституції нових держав Європи та Азії / Упоряд. С. Головатий. – К.: Українська правнича фундація. Видавництво «Право», 1996.

28. Концепція реформування політичної системи України (проект) – К., 2001.

29. *Копылов В.А.* Информационное право. – 2-е изд., перераб. и доп. – М.: Юристъ, 2002.

30. *Кормич Б.А.* Організаційно-правові засади політики інформаційної безпеки України. – Одеса: Юридична література, 2003.

31. *Кормич Л.І. Багацький В.В.* Культурологія (історія і теорія світової культури XX століття). – Харків: Одіссей, 2002.

32. *Косевцов В.О., Бінько І.Ф.* Національна безпека України: проблеми і шляхи реалізації пріоритетних національних інтересів. / Рада національної безпеки України, НІСД. – К., 1996.

33. *Кремень В.Г., Бінько І.Ф. Головащенко С.І.* Політична безпека України: концептуальні засади та система забезпечення. – К.: МАУП, 1998.

34. *Курушин В.Д., Минаев В.А.* Компьютерные преступления и информационная безопасность: Справочник. – М.: Новый юрист, 1998.

35. *Литвиненко О.В.* Інформаційна безпека Європи. – К., 1999.

36. *Михальченко М. Самчук З.* Україна доби межичасся. Блиск і убозтво куртизанів. – Дрогобич: Видавнича фірма «Відродження», 1998.

37. Національна безпека України, 1994 – 1997 рр.. Наукова доповідь НІСД. / Редкол.: О.Ф. Бєлов (голова) та ін.. – К.: НІСД, 1997.

38. *Почепцов Г.Г.* Национальная безопасность стран переходного периода. – К., 1996.

39. Права людини та інформація: Зб. наук. праць. – К., 2001.

40. *Рабинович П.М., Панкевич І.М.* Здійснення прав людини: проблеми обмежування (загальнотеоретичні аспекти). – Львів, 2001.

41. *Рассолов М.М.* Информационное право. – М., Юристъ, 1999.

42. *Северин В.А.* Правовое обеспечение информационной безопасности предприятия. – М., 2000.

43. *Сіган Бернард Г.* Створення конституції для народу чи республіки, що здобули свободу. – Київ: Інститут демократії ім. П. Орлика, 1993.

44. *Слісаренко І.Ю.* Практичне втілення «свободи слова» на пострадянському просторі. – Національний демократичний інститут міжнародних відносин. – К., 2002.

45. Стратегія національної безпеки України в контексті досвіду світової спільноти: Зб. ст. за матер. міжнар. конф. – К.: Сатсанга, 2001.

46. Україна: утвердження незалежної держави 1991 – 2001 /під. ред. В.М. Литвина. – К.: Видавничий дім «Альтернативи», 2001.

47. *Шиллер Г.* Манипуляторы сознанием: пер. с англ. / предисл. Я. Засурского. – М.: Мысль, 1980.

48. *Ярочкин В.И.* Информационная безопасность. – М.: Международные отношения, 2000.

49. *Cleveland H.* The knowledge executive. Leadership in an information society. – New York: Truman Talley books, 1989.

50. *Toffler A.* Powershift. Knowledge, wealth, and the violence at the edge of the 21-century. New York: Bantam books, 1990.

НОРМАТИВНО-ПРАВОВІ АКТИ

1. Акт проголошення незалежності України // Відомості Верховної Ради України, 1991. - № 38. – Ст. 502.

2. Декларація про державний суверенітет України від 16 липня 1990 р. – Відомості Верховної Ради України. – 1990 - № 31. – Ст. 429.

3. Декларация руководящих принципов по использованию вещания через спутники для свободного распространения информации, развития образования и расширения культурных обменов от 15 ноября 1972 года.

4. Загальна декларація прав людини. Прийнята Генеральною Асамблеєю ООН 10 грудня 1948 р. Док.ООН/PES/217 A

5. Загальний кодекс правил для адвокатів країн Європейського Співтовариства. Прийнято делегацією дванадцяти країн-учасниць на пленарному засіданні у Страсбурзі в жовтні 1988 р. // Бюлетень законодавства і юридичної практики України «Адвокатура в Україні» – Київ: «Юрінком», 2000. – № 1.

6. Закон України «Основи законодавства України про культуру» від 14 лютого 1992 р. № 2117-XII // Відомості Верховної Ради України, 1992. – № 21. – Ст. 294.

7. Закон України «Про адвокатуру» від 19 грудня 1992 р. № 2887-XII // Голос України. – 1993. – 29 січня.

8. Закон України «Про банки і банківську діяльність» від 7 грудня 2000 року № 2121-III // Відомості Верховної Ради України, 2001. – № 5- 6. – Ст. 30.

9. Закон України «Про видавничу справу» від 5 червня 1997 р. № 318/97-ВР. // Відомості Верховної Ради України, 1997. – № 32. – Ст. 206.

10. Закон України «Про внесення змін до Кодексу України про адміністративні правопорушення щодо встановлення відповідальності за порушення законодавства про державну таємницю» від 21 вересня 1999 р. № 1080-XIV. // Відомості Верховної Ради України, 1999. – № 49. – Ст. 429.

11. Закон України «Про державну підтримку засобів масової інформації та соціальний захист журналістів» від 23 вересня 1997 р. № 540/97-ВР // Відомості Верховної Ради України, 1997. – № 50. – Ст. 302.

12. Закон України «Про державну статистику» від 17 вересня 1992 р. // Відомості Верховної Ради України, 1992. – № 43. – ст.608 (В редакції Закону № 1922-III від 13.07.2000).

13. Закон України „Про державну таємницю» від 21 січня 1994 року № 3855-XII // Відомості Верховної Ради України, 1994. – № 16. – Ст. 93. (В редакції Закону N 1079-XIV від 21.09.99)

14. Закон України „Про електронні документи та електронний документтообіг» від 22 травня 2003 р. № 851-IV.

15. Закон України „Про електронний цифровий підпис» від 22 травня 2003 р. № 852-IV.

16. Закон України «Про захист інформації в автоматизованих системах» від 5 липня 1994 року № 80/94-ВР. // Відомості Верховної Ради України, 1994. – № 31. – Ст. 286.

17. Закон України «Про звернення громадян» від 2 жовтня 1996 р. № 393/96-ВР // Відомості Верховної Ради України, 1996. – № 47. – Ст. 256.

18. Закон України «Про зв'язок» від 16 травня 1995 року № 160/95-ВР // Відомості Верховної Ради України, 1995. – № 20. – Ст.143.

19. Закон України «Про інформацію» від 2 жовтня 1992 р. // Відомості Верховної Ради України, 1992. – № 48. – Ст. 650.

20. Закон України «Про кінематографію» від 13 січня 1998 р. № 9/98-ВР// Відомості Верховної Ради України, 1998. – № 22. – Ст. 114.

21. Закон України «Про Концепцію Національної програми інформатизації» від 4 лютого 1998 року № 75/98-ВР // Відомості Верховної Ради України, 1998. – № 27-28. – Ст. 182.

22. Закон України «Про ліцензування певних видів господарської діяльності» від 1 червня 2000 р. // Урядовий кур'єр. – 2000. – 2 серпня. – № 139.

23. Закон України «Про науково-технічну інформацію» від 25 червня 1993 року № 3322-XII // Відомості Верховної Ради України, 1993. – № 33. – Ст. 345.

24. Закон України «Про Національну програму інформатизації» від 4 лютого 1998 р. №74/98-ВР. // Відомості Верховної Ради України, 1998. – № 27-28. – Ст. 181.

25. Закон України «Про Національну раду України з питань телебачення і радіомовлення» від 23 вересня 1997 р № 538/97-ВР // Відомості Верховної Ради України, 1997. – № 48. – Ст. 296.

26. Закон України «Про оперативно-розшукову діяльність» від 18 лютого 1992 року № 2135-XII. – Відомості Верховної Ради України, 1992. – № 22. – ст. 303.

27. Закон України «Про основи національної безпеки України» від 19 червня 2003 р. //Голос України. – 22 липня 2003 р. – № 134.

28. Закон України «Про підприємництво» від 7 лютого 1991 р. // Відомості Верховної Ради України, 1991. – № 14. – Ст. 168.

29. Закон України «Про основи національної безпеки України» від 19 червня 2003 р. // Голос України. – 22 липня 2003 р. - № 134.

30. Закон України «Про підприємства в Україні» від 27 березня 1991 року № 887-XII // Відомості Верховної Ради України, 1991. – № 24. – Ст. 272.

31. Закон України «Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації» від 23 вересня 1997 року // Відомості Верховної Ради України, 1997. – № 49. – ст. 299.

32. Закон України «Про Раду національної безпеки і оборони України» від 5 березня 1998 року № 183/98-ВР // Відомості Верховної Ради. – 1998. – № 35. – Ст. 237.

33. Закон України „Про особливості державного регулювання діяльності суб'єктів господарювання, пов'язаної з виробництвом, експортом, імпортом дисків для лазерних систем зчитування» від 17 січня 2002 р. № 2953-III // Відомості Верховної Ради України, 2002 – № 17. – Ст. 121.

34. Закон України «Про рекламу» від 3 липня 1996 року // Відомості Верховної Ради України, 1996. – № 39. – Ст. 181.

35. Закон України «Про Службу безпеки України» від 25 березня 1992 р. № 2229-XII // Відомості Верховної Ради України, 1992. – № 27. – Ст. 382.

36. Закон України «Про телебачення і радіомовлення» 21 грудня 1993 року № 3759-XII // Відомості Верховної Ради України, 1994. – № 10. – Ст. 43. (В редакції Закону від 11.05.2000 № 1709-III).

37. Закон України «Про Уповноваженого Верховної Ради України з прав людини» // Відомості Верховної Ради України, 1998. – № 20. – Ст. 99.

38. Звернення Верховної Ради України до Ради Європи, Організації по безпеці та співробітництву в Європі, міжнародних парламентських організацій, парламентів і урядів європейських країн з приводу тривожної ситуації в інформаційному просторі України. Звернення Верховної Ради від 15 червня 1999 р.

39. Конвенція про доступ до інформації, участь громадськості в процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля від 28 червня 1998 р. (Ратифіковано 16 липня 1999 р.) / / Відомості Верховної Ради України, 1999. – № 34. – Ст. 296.

40. Конвенція про захист прав і основних свобод людини 1950 року, Перший протокол та протоколи № 1, 4, 6, 7, 9, 10 та 11 до Конвенції (Рим, 4.XI.1950) / «European Treaty Series» - № 5.

41. Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру від 28 січня 1981 року. /Збірка договорів Ради Європи. Українська версія. – К.: Парламентське видавництво, 2000. – С. 427 – 439.

42. Конституція України. Прийнята Верховною Радою України 28 червня 1996 року // Відомості Верховної Ради України, 1996. – №30 – Ст. 141.

43. Кримінальний кодекс України. Прийнятий сьомою сесією Верховної Ради України 5 квітня 2001 р. – Київ: Юрінком-Інтер, 2001.

44. Кримінально-процесуальний кодекс України (зі змінами і доповненнями станом на 15 вересня 2001 р.) – Харків, 2001.

45. Лист Міністерства культури і мистецтв «Щодо фільмів, які заборонені для розповсюдження і демонстрування в Україні» № 9 – 3216/17 від 1 липня 1999 р.

46. Меморандум про взаєморозуміння щодо співробітництва в сфері телекомунікацій і розвитку Всесвітньої інформаційної інфраструктури між Урядом України та Урядом Сполучених Штатів Америки від 22 листопада 1994 р., м. Вашингтон.

47. Міжнародний пакт про громадянські і політичні права. Прийнято 16 грудня 1966 року Генеральною Асамблеєю ООН. Док. ООН A/RES/2200 A (XXI)

48. Міжнародний пакт про економічні, соціальні і культурні права. Прийнято 16 грудня 1966 року Генеральною Асамблеєю ООН. Док. ООН A/RES/2200 A (XXI)

49. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України «Про затвердження Положення про дозвільний порядок проведення робіт з технічного захисту інформації для власних потреб» від 23 лютого 2002 р. № 9.

50. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України «Про затвердження Положення про порядок розроблення, виготовлення та експлуатації засобів криптографічного захисту конфіденційної інформації» 30 листопада 1999 р. № 53.

51. Наказ Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України «Про затвердження Порядку захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах» від 24 грудня 2001 № 76.

52. Постанова Вищого арбітражного суду України «Про питання захисту авторських прав в Інтернеті» від 5 червня 2000 р. № 04-1/5-7/82. // Вісник господарського судочинства. – 2001. – № 2.

53. Постанова Верховної Ради України «Про Воєнну доктрину України» від 19 жовтня 1993 р. № 3529-XII // Відомості Верховної Ради України, 1993. – № 43. – Ст. 409.

54. Постанова Верховної Ради України «Про діяльність Кабінету Міністрів України, інших органів державної влади щодо забезпечення свободи слова, задоволення інформаційних потреб суспільства та розвитку інформаційної сфери в Україні» від 16 лютого 1999 р. № 430-XIV.

55. Постанова Верховної Ради України «Про концепцію (основи державної політики) національної безпеки України» від 16 січня 1997 р. № 3/97-ВР // Голос України, 1997. – 4 лютого. – С. 5.

56. Постанова Верховної Ради України «Про підсумки парламентських слухань «Інформаційна політика України: стан і перспективи» від 2 червня 1999 р. № 705-XIV.

57. Постанова Верховної Ради України «Про проголошення незалежності України» від 24 серпня 1991 р. //Відомості Верховної Ради України, 1991. – № 38. – ст. 502.

58. Постанова Верховної Ради України «Про рекомендації учасників парламентських слухань «Свобода слова в Україні: стан, проблеми, перспективи» від 25 квітня 1997 р. № 236/97-ВР. / Відомості Верховної Ради України, 1997. – № 22. – Ст. 162.

59. Постанова Верховної Ради України «Про проект закону України про інформаційний суверенітет і інформаційну безпеку України» від 21 вересня 1999 року № 1072 – XIV.

60. Постанова Кабінету Міністрів «Про деякі питання захисту інформації, охорона якої забезпечується державою» від 13 березня 2002 р. № 281.

61. Постанова Кабінету Міністрів України «Про затвердження Інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави» від 27 листопада 1998 р. № 1893.

62. Постанова Кабінету Міністрів України «Про затвердження Положення про Державний департамент інтелектуальної власності» від 20 червня 2000 р. № 997.

63. Постанова Кабінету Міністрів України «Про затвердження Положення про Державну комісію з питань зв'язку і радіочастот» від 26 липня 1994 р. № 506.

64. Постанова Кабінету Міністрів України «Про перелік відомостей, що не становлять комерційної таємниці» від 9 серпня 1993 р. № 611.

65. Постанова Кабінету Міністрів України «Про положення про державне посвідчення на право розповсюдження і демонстрування фільмів» від 17 серпня 1998 р. № 1315.

66. Постанова Кабінету Міністрів України «Про Порядок оприлюднення у мережі Інтернет інформації про діяльність органів виконавчої влади» від 4 січня 2002 р. № 3.

67. Постанова Кабінету Міністрів України «Про Урядову комісію з питань інформаційно-аналітичного забезпечення діяльності органів виконавчої влади» від 7 травня 2000 р. № 777.

68. Постанова Центральної виборчої комісії «Про Положення про порядок поширення інформації Центральної виборчої комісії» від 12 грудня 2000 № 113.

69. Рішення Конституційного суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К.Г.Устименка) від 30 жовтня 1997 року № 5-зп. – Справа № 18/203-97.

70. Рішення Національної ради з питань телебачення і радіомовлення «Про затвердження Положення про порядок ліцензування каналів мовлення» від 28 вересня 2000 р. № 12.

71. Указ Президента України «Питання Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України» від 6 жовтня 2000 р. № 1120/2000.

72. Указ Президента України «Про державну економічну підтримку вітчизняних друкованих засобів масової інформації» від 16 квітня 1997 р № 332/97.

73. Указ Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних» від 24 вересня 2001 р. № 891/2001.

74. Указ Президента України «Про Державний комітет інформаційної політики, телебачення і радіомовлення України» від 25 липня 2000 р. № 919/2000.

75. Указ Президента України «Про додаткові заходи щодо забезпечення відкритості у діяльності органів державної влади» від 1 серпня 2002 р. № 683/2002.

76. Указ Президента України «Про заходи щодо впровадження Концепції адміністративної реформи в Україні» від 22 липня 1998 року № 810/98.

77. Указ Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31 липня 2000 р. № 928/2000.

78. Указ Президента України «Про невідкладні додаткові заходи щодо зміцнення моральності у суспільстві та утвердження здорового способу життя» від 15 березня 2002 р. № 258/2002.

79. Указ Президента України «Про Міністерство освіти і науки України» від 7 червня 2000 року № 773/2000.

80. Указ Президента України «Про Положення про Державний комітет зв'язку та інформатизації України» від 3 червня 1999 р. № 601/99.

81. Указ Президента України «Про Положення про Міністерство культури і мистецтв України» від 31 серпня 2000 року № 1038/2000.

82. Указ Президента України «Про Положення про порядок здійснення криптографічного захисту інформації в Україні» від 22 травня 1998 р. № 505/98.

83. Указ Президента України «Про Положення про технічний захист інформації в Україні» від 27 вересня 1999 р. № 1229.

84. Указ Президента України «Про Статут та організаційну структуру Національного інституту стратегічних досліджень» від 2 серпня 1993 року № 296/93.

85. Хартия Глобального информационного общества. Принята 22 июля 2000 г., Окинава. / Информация. Дипломатия. Психология. – М.: Известия, 2002. – С. 602 – 610.

86. Developments in the field of information and telecommunications in the context of international security / Fifty-six session. Report of the First Committee. 14 November 2000. United Nations. A/56/533.

87. United Nations. A/RES/56/19 «Developments in the field of information and telecommunications in the context of international security» Resolution Adopted By The General Assembly. 7 January 2002.

Навчальне видання

Кормич Борис Анатолійович

**ІНФОРМАЦІЙНА БЕЗПЕКА:
ОРГАНІЗАЦІЙНО-ПРАВОВІ ОСНОВИ**

Навчальний посібник

Редактор *Вдовиченко Валентина Миколаївна*
Коректор *Асташева Марія Василівна*
Комп'ютерна верстка *Полончук Микола Андрійович*
Дизайн обкладинки *Вакуленко Микола Миколайович*

Підписано до друку 16.02.2004.
Формат 60 x 84 1/16. Папір офсетний. Друк офсетний. Гарнітура Newton.
Умовн. друк. аркушів – 24. Обл.-вид. аркушів — 23,04.
Наклад 1000 примірників.
Замовлення № _____

Видавництво «Кондор»
Свідоцтво ДК № 1157 від 17.12.2002 р.
03057, м. Київ, пров. Польовий, 6,
тел./факс (044) 456-60-82, 241-83-47

Книги видавництва «Кондор» завжди можна придбати у наших регіональних партнерів:

- м. Київ, «Наукова думка», вул. Грушевського, 4, тел. (044) 228-06-96;
- м. Київ, «Знання», вул. Хрещатик, 44,тел. (044) 229-10-45;
- м. Київ, маг. «Буква» Будинку книги, вул. Л. Толстого, 11/61, тел. (044) 230-25-74;
- м. Київ, ДчП Книгарня №52, вул. Ю. Гагаріна, 13, тел. (044) 552-22-41;
- м. Київ, «Академкнига» № 7, вул. Стрітенська, 17, тел. (044) 212-34-72;
- м. Київ, ТОВ «Книгарня «Слово», вул. Васильківська, 6, тел. (044) 235-43-66
- м. Вінниця, «Кобзар», вул. Привокзальна, 2/1, тел. (0432) 21-67-44;
- м. Дніпропетровськ, «Бібколектор», пр. Кірова, 22, тел. (0567) 78-38-39;
- м. Донецьк, «Будинок книги», вул. Артема, 147а, тел. (0622) 55-44-76, 90-58-88;
- м. Житомир, «ЦНТЕІ», вул. Велика Бердичівська, 31, тел. (0412) 37-22-56;
- м. Житомир, ТОВ «Житомиркнига», вул. Черняхіського, 12а, тел. (0412) 37-27-74, 37-41-45;
- м. Запоріжжя, ТОВ «Сучасник ЛТД», просп. Леніна, 151, тел. (0612) 33-12-27;
- м. Запоріжжя, фірма «Константа-», пр. Леніна, 142, (0612) 62-50-70, 13-75-05
- м. Івано-Франківськ, «Сучасна українська книга», Вічовий майдан, 3, тел. (03422) 3-04-60;
- м. Івано-Франківськ, КП «Букініст», Незалежності, 19, (03422) 2-38-28;
- м. Кіровоград, ОКП «Бібколектор», вул. Гайдара, 44, тел. (0522) 27-74-78
- м. Кіровоград, «Книжковий світ», вул. Набережна, 13, тел. (0522) 24-94-64;
- м. Кривий Ріг, «Букініст», пл. Визволення, 1, тел. (0564) 92-37-32;
- м. Львів, Бібколектор, вул. Лисенка, 21, тел. (0322) 75-79-86;
- м. Львів, ТОВ «Ноти», просп. Шевченка, 16, тел. (0322) 72-67-96;
- м. Львів, «Еней», вул. Тургенєва, 52/7, тел. (0322) 35-12-93К
- м. Луганськ, «Глобус-книга», вул. Радянська, 58, (0642) 53-62-30;
- м. Луцьк, «Освіта», просп. Волі, 8, тел. (0332) 72-46-14;
- м. Одеса, «Епос», вул. Троїцька, 28, тел. (0482) 25-85-69;
- м. Полтава, «Планета», вул. Жовтнева, 60а, тел. (05322) 7-20-19;
- м. Рівне, «Іскра», вул. Бандери, 36а, тел. (0362) 23-63-16;
- м. Рівне, «ДККП Рівнекнига», вул. Островського, 16, тел. (0362) 22-41-05;
- м. Тернопіль, ТОВ «Дар», вул. Б. Хмельницького, 17, тел. (0352) 22-24-33;
- м. Ужгород, «Кобзар», площа Корятовича, 1, тел. (03122) 3-35-16;
- м. Харків, «Авіоніка», вул. Сумська, 51, тел. (0572) 14-04-70;
- м. Харків, «Вища школа», вул. Петровського, 6/8, тел. (0572), 47-80-20;
- м. Херсон, ЗАТ «Херсонкнига», просп. 40-річчя Жовтня, 31а, тел. (0552) 22-57-76;
- м. Хмельницький, ТОВ «Проскурівкнига», вул. Володимирська, 63, тел. (0382) 76-29-36;
- м. Черкаси, «Будинок книги», вул. Хрещатик, 200, тел. (0472) 45-99-20;
- м. Черкаси, ТОВ «Фірма «Світоч», вул. Б. Вишневецького, тел. (0472) 47-92-20;
- м. Чернівці, ДКТП «Наука», вул. Заньковецької, 4, тел. (03722) 2-59-35;
- м. Чернівці, ОРТП «Чернівцікнига», вул. Шептицького, 23, тел. (03722) 2-23-13.

Книготорговельним організаціям та оптовим покупцям звертатися за тел./факсом: (044) 241-66-07, 241-83-47.
E-mail: condor@kiev.ldc.net, condor@public.ua.net.
http://www.condor-books.com