Л.І. Северин, С.Л. Северин, А.В. Дудатьєв

П Р А В О В Е
ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ІНФОРМАЦІЇ

Міністерство освіти і науки України
Вінницький національний технічний університет

Л. І. Северин, С. Л. Северин, А. В. Дудатьєв

Правове забезпечення захисту інформації

Затверджено Вченою радою Вінницького національного технічного університету як навчальний посібник для студентів напряму підготовки 1601 – "Інформаційна безпека". Протокол № 10 від 27 травня 2004 р.

Вінниця ВНТУ 2004

УДК 34 : 681.3
С 28

Р е ц е н з е н т и :

О.Д. Азаров, доктор технічних наук, професор
А.М. Пєтух, доктор технічних наук, професор
О.Ф. Мельничук, кандидат юридичних наук, доцент

Рекомендовано до видання Вченою радою Вінницького національного технічного університету Міністерства освіти і науки України

Северин Л.І., Северин С.Л. Дудатьєв А.В.
С 28 **Правове забезпечення захисту інформації.** Навчальний посібник. - Вінниця: ВНТУ, 2004. – 145 с.

У посібнику розглянуті основні поняття, об'єкти, суб'єкти та принципи інформаційного права. В ньому розкриваються особливості правового регулювання суспільних відносин у сфері захисту інформації, наводиться характеристика засад інформаційного законодавства України у сфері боротьби з комп'ютерною злочинністю.

Посібник розрахований на студентів закладів освіти, що спеціалізуються за фахом "Інформаційна безпека. Захист інформації в комп'ютерних системах і мережах." Може бути корисним для працівників підприємств, організацій та громадян, які користуються комп'ютерною технікою.

УДК 34 : 681.3

Зміст

Передмова

Інформацію без перебільшення можна віднести до одного з вирішальних ресурсів розвитку. Вона в сучасному світі активно впливає на всі сфери життєдіяльності не тільки окремих держав, а і всього світового співтовариства. Особливе місце відводиться інформаційним ресурсам в умовах ринкової економіки, важливим фактором якої є конкуренція. Перемагає той, хто краще, якісніше, дешевше і оперативніше (час – гроші!) виробляє і продає. По сутті це універсальне правило ринку, в умовах якого виступає правило: хто володіє інформацією, той володіє світом.

У конкурентній боротьбі широко розповсюджені різні дії, направлені на отримання конфіденційної інформації різними способами, аж до прямого промислового шпигування з використанням сучасних технічних засобів розвідки.

В цих умовах захисту інформації від несанкціонованого користування нею відводиться значне місце. При цьому завданнями захисту інформації є:

- захист конституційних прав громадян і збереження особистої таємниці та конфіденційності персональних даних, що є в інформаційних системах;
- збереження державної таємниці, конфіденційності документованої інформації згідно з законодавством;
- забезпечення прав суб'єктів у інформаційних процесах та при розробці, виробництві, застосуванні інформаційних систем, технологій та засобів забезпечення;
- запобігання розголошенню, витоку і несанкціонованого доступу до інформації, яка охороняється;
- запобігання протиправних дій щодо знищення, модифікації, перекручення, копіювання, блокування інформації;
- запобігання інших форм незаконного втручання в інформаційні ресурси та інформаційні системи.

Як видно з перерахованих завдань інформаційна безпека – доволі об'ємна і багатогранна проблема, що охоплює не тільки визначення необхідності захисту інформації, але й те, як її треба захищати, від чого захищати, коли захищати і яким повинен бути цей захист. Тобто структура системи захисту інформації в інформаційних системах доволі складна. Провідна роль у цій структурі належить підсистемі правового захисту, яку автори розкривають у даному посібнику.

Автори висловлюють подяку доктору технічних наук, проф. Азарову О. Д., доктору технічних наук, проф. Пєтуху А. М., кандидату юридичних наук, доц. Мельничук О.Д. за цінні зауваження і рекомендації та студентам Головеньку О., Каменєвій Т. і Бринзак Ю. за надання допомоги у підготовці посібника до видання.

Глава 1. Загальні положення

В епоху інформаційної революції розвиток держави визначає насамперед рівень її досягнень у сфері обробки інформації.

Сьогодні Україна вибрала стратегічний шлях свого розвитку, що полягає в інтеграції в Європейське співтовариство. Як відомо, однією з особливостей цього співтовариства є побудова інформаційного суспільства, яке широко використовує досягнення інформаційних технологій і, зокрема, глобальної комп'ютерної мережі *Internet.*

Однак, розвиток інформаційних технологій, розширення виробництва технічних засобів і сфери застосування комп'ютерної техніки породили новий вид суспільно небезпечних діянь, коли комп'ютерна інформація неправомірно використовується або стає об'єктом зазіхання. Об'єктивно це пояснюється зниженням рівня захищеності інформаційних систем, зростанням кількості антисоціальних проявів внаслідок поширення користувачів глобальних комп'ютерних мереж, використання наукових та технічних досягнень криміналітетом. Інтереси організованих злочинних груп і окремих правопорушників спрямовані на відмивання "брудних коштів", поширення неправдивої інформації, фінансові махінації, і в першу чергу, порушення у банківсько-кредитній сфері, де активно використовуються автоматизовані системи.

Особливої актуальності проблема кіберзлочинності набула в наш час. Жодна держава сьогодні не здатна протистояти цьому злу самостійно. Тому паралельно з розвитком національного законодавства, спрямованого на боротьбу з комп'ютерними злочинами, є нагальною потребою активізація міжнародного співробітництва, налагодження міжнародно-правового механізму регулювання.

1.1. Визначення термінів

Інформація – відомості про суб'єкти, об'єкти, явища та процеси.

Інформація з обмеженим доступом – інформація, право доступу до якої обмежено встановленими правовими нормами і (чи) правилами.

Таємна інформація – інформація з обмеженим доступом, яка містить відомості, що становлять державну або іншу передбачену законом таємницю.

Конфіденційна інформація – інформація з обмеженим доступом, якою володіють, користуються чи розпоряджаються окремі фізичні чи юридичні особи або держава і порядок доступу до якої встановлюється ними.

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

Порушення цілісності інформації – спотворення інформації, її

руйнування або знищення.

Блокування інформації – унеможливлення санкціонованого доступу до інформації.

Загроза для інформації – витік, можливість блокування або порушення цілісності інформації.

Доступ до інформації – можливість одержання, оброблення інформації та (чи) порушення її цілісності.

Несанкціонований доступ до інформації – доступ до інформації, за якого порушується порядок його здійснення і встановлені правові норми.

Інформаційне суспільство – суспільство, в якому діяльність людей здійснюється на основі використання послуг, що надаються за допомогою електронних інформаційних технологій зв'язку.

Інформаційна безпека – вид інформаційних правовідносин щодо створення, підтримки, охорони та захисту бажаних для людини, суспільства і держави безпечних умов їх життєдіяльності; суспільні процеси, пов'язані зі створенням безпечних (нормальних) умов поширення, розповсюдження, зберігання та використання інформації; стан правовідносин, пов'язаний з нормальним (безпечним) створенням, розповсюдженням, обробкою, зберіганням та використанням інформації у певному просторі, часі та колі осіб.

Комп'ютерний злочин (кіберзлочин) – суспільно небезпечна дія, яка класифікується кримінальним законодавством України як злочин, що вчинений з використанням комп'ютерних продуктів або у якому комп'ютерні продукти є предметом чи засобом злочинного посягання; злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж.

Протидія комп'ютерній злочинності (боротьба з кіберзлочинністю) – діяльність суб'єктів суспільних відносин відповідно законодавству України щодо:

- виявлення, упередження (профілактика), розкриття, розслідування комп'ютерних злочинів та притягнення винних до відповідальності;
- виявлення та усунення технічних загроз інформаційній безпеці людини, суспільству, державі, які можуть використовуватися для вчинення правопорушень;
- виявлення причин і умов вчинення злочинів та мінімізація їх наслідків.

Організація протидії комп'ютерним правопорушенням здійснюється відповідно до положень адміністративного, цивільного, трудового та кримінального законодавства, а також інформаційної та інших підгалузей законодавства.

Суспільні інформаційні відносини (інформаційні правовідносини – це:

- суспільні відносини щодо інформації;
- суспільні відносини, об'єктом яких є інформація;

- суспільні відносини щодо одержання, використання, поширення та зберігання інформації (відомостей, даних, знань) у всіх сферах життя і діяльності особи, суспільства і держави;

- суспільні відносини, які виникають, здійснюються та припиняються в процесі інформаційної діяльності.

1.2. Основи систем захисту інформації

Існують різні уявлення про системи захисту інформації (СЗІ) з точки зору їх призначення, складу і виконуваних функцій. Для формування повного уявлення про СЗІ розглянемо їх основні складові, а саме:

- законодавча, нормативно-методична і наукова база;
- структура і задачі органів (підрозділів), що здійснюють комплексний захист інформації;
- організаційно-технічні та режимні заходи;
- програмно-технічні методи і засоби захисту інформації.

Основи систем захисту інформації представлені на рис. 1.

Рис. 1. Основи систем захисту інформації

Однією з основних складових СЗІ є нормативно-методологічна база, у змісті документів якої доцільно розкрити такі групи питань:

а) основи:

- структура і задачі органів (підрозділів), що забезпечують захист інформації;
- організаційно-технічні та режимні заходи і методи (політика інформаційної безпеки);
- програмно-технічні способи і засоби.

б) напрями:

- захист об'єктів корпоративних систем;
- захист процесів, процедур і програм оброблення інформації;
- захист каналів зв'язку;

- заглушення побічних електронних випромінювань;
- управління системою захисту.

в) етапи:

- визначення інформаційних і технічних ресурсів, що підлягають захисту;
- виявлення потенційно можливих загроз і каналів витоку інформації;
- проведення оцінювання уразливості та ризиків інформації при наявних загрозах і каналах витоку;
- визначення вимог до системи захисту;
- здійснення вибору засобів захисту інформації та їх характеристики;
- впровадження і організація використання обраних заходів, способів і засобів захисту;
- здійснення контролю цілісності та управління системою захисту.

На жаль, законодавча база ще відстає від потреб практики. Діючі закони, укази і постанови носять в основному заборонний характер. Ряд нормативних положень захисту інформації в інформаційних системах, розроблених раніше, не відповідають рівню розвитку сучасних інформаційних технологій. Роботи у цьому напрямку постійно відстають від потреб і носять односторонній характер (в основному зведені до захисту інформації від витоку технічними каналами).

У літературі справедливо приділяють увагу *правовим аспектам захисту інформації,* які можуть виникнути при недостатньо продуманому чи зловмисному використанні інформаційних систем. До них відносяться:

- правові питання захисту інформації і встановлення юридичної відповідальності за забезпечення її збереження;
- юридичні та технічні питання захисту інформації від несанкціонованого доступу, які б виключали можливість її використання;
- установлення юридично закріплених норм і методів захисту авторських прав і пріоритетних розробників програмного продукту;
- розробка заходів для надання юридичної сили електронним документам і формування юридичних норм, які визначають відповідальність за якість таких документів;
- правовий захист інтересів експертів, які передають свої знання у фонди банків даних;
- встановлення правових норм і юридичної відповідальності за використання інформаційних систем в особистих інтересах, які суперечать інтересам інших осіб чи суспільству.

Сьогодні поки що відсутня повна нормативно-правова і методична база для побудови інформаційних і обчислювальних систем в захищеному виконанні, придатних для оброблення секретної інформації у державних закладах і комерційних структурах.

При розробці засобів захисту виникає ряд *проблем правового*

характеру.

1. Ліцензування діяльності з розробки захисту інформації (система ліцензування направлена на створення умов, при яких право займатися захистом інформації надано тільки організаціям, що мають на цей вид діяльності відповідний дозвіл).

2. Сертифікація засобів захисту (система сертифікації направлена на захист споживача від несумлінного виконавця).

3. Відповідність розроблюваних засобів захисту концептуальним вимогам до захисту, стандартам та іншим нормативним документам.

4. Відсутність нормативно-правового забезпечення для вирішення спірних ситуацій з використанням цифрового підпису в арбітражному суді.

5. Оцінювання інформації у вартісному вираженні надто проблематичне і часто не може бути вирішене, наприклад, при виникненні загроз інформаційним системам, що обробляють секретну інформацію. У цьому випадку відповідальність встановлюється за аналогією з діючими нормами кримінального права.

Аналіз показує, що в цілому можна виділити такі *критерії складу зловживань* у сфері оброблення інформації:

- порушення права реєстрації інформаційних систем і переліку інформації, що обробляється;
- порушення правил збирання інформації, а саме: отримання інформації без дозволу і збирання понад дозволеного переліку;
- зберігання персональної інформації понад установлений строк;
- порушення правил зберігання інформації;
- передача третім особам відомостей, що складають комерційну таємницю, чи персональних відомостей;
- невчасне інформування про події, явища і факти, які можуть заподіяти шкоду здоров'ю чи нанести матеріальні збитки;
- перевищення меж компетенції облікової діяльності, допущення неповних облікових записів і фальсифікації даних;
- надання зацікавленим особам явно неточної інформації;
- порушення встановленого порядку забезпечення безпеки інформації;
- порушення правил технології оброблення інформації;
- порушення норм захищеності інформації, встановлених законом;
- порушення правил доступу до інформації чи до технічних засобів;
- порушення механізму захисту інформації та проникнення у систему;
- обхід засобів захисту і проникнення у систему;
- викрадання інформації;
- несанкціоноване знищення даних в інформаційних системах;
- перекручення (модифікація) програмного забезпечення;
- несанкціонована модифікація даних в інформаційних системах;
- перехоплення електромагнітних, акустичних чи оптичних

випромінювань;

- перехоплення інформації, що передається лініями зв'язку;
- виготовлення і розповсюдження явно непридатного програмного забезпечення;
- розголошення парольно-ключової інформації;
- несанкціоноване ознайомлення (спроба) з захищуваними даними;
- розповсюдження комп'ютерних вірусів;
- несанкціоноване копіювання;
- внесення у програмне забезпечення змін, в тому числі і вірусного характеру.

1.3. Підсистема організаційно-правового захисту

Така підсистема призначена для регламентації діяльності користувачів інформаційних систем і є упорядкованою сукупністю організаційних рішень, нормативів, законів і правил, які визначають загальну організацію робіт з захисту інформації.

Організаційно-правовий захист має таку структуру (рис.2):

а) *організаційно-правові питання*
- органи, підрозділи і особи, відповідальні за захист інформації;
- нормативно-правові, методичні та інші матеріали;
- міри відповідальності за порушення норм захисту інформації;
- порядок вирішення спірних ситуацій;

б) *реєстраційні аспекти*
- фіксація підпису під документом;
- фіксація фактів ознайомлення з інформацією;
- фіксація фактів зміни даних;
- фіксація фактів копіювання змісту;

в) *юридичні аспекти* (затвердження в якості законів)
- правил захисту інформації;
- мір відповідальності за порушення правил захисту інформації;
- реєстраційних рішень;
- процесуальних норм і правил;

г) *морально-психологічні аспекти*
- підбір і розміщення кадрів;
- навчання персоналу;
- система моральних і матеріальних стимулів;
- контроль за дотримуванням правил.

1.4. Інформаційне право. Об'єкти та суб'єкти інформаційного права

Інформаційне право – сукупність юридичних норм і інститутів, які регулюють інформаційні відносини в інформаційній сфері.

Об'єктами інформаційних відносин є документована або публічно

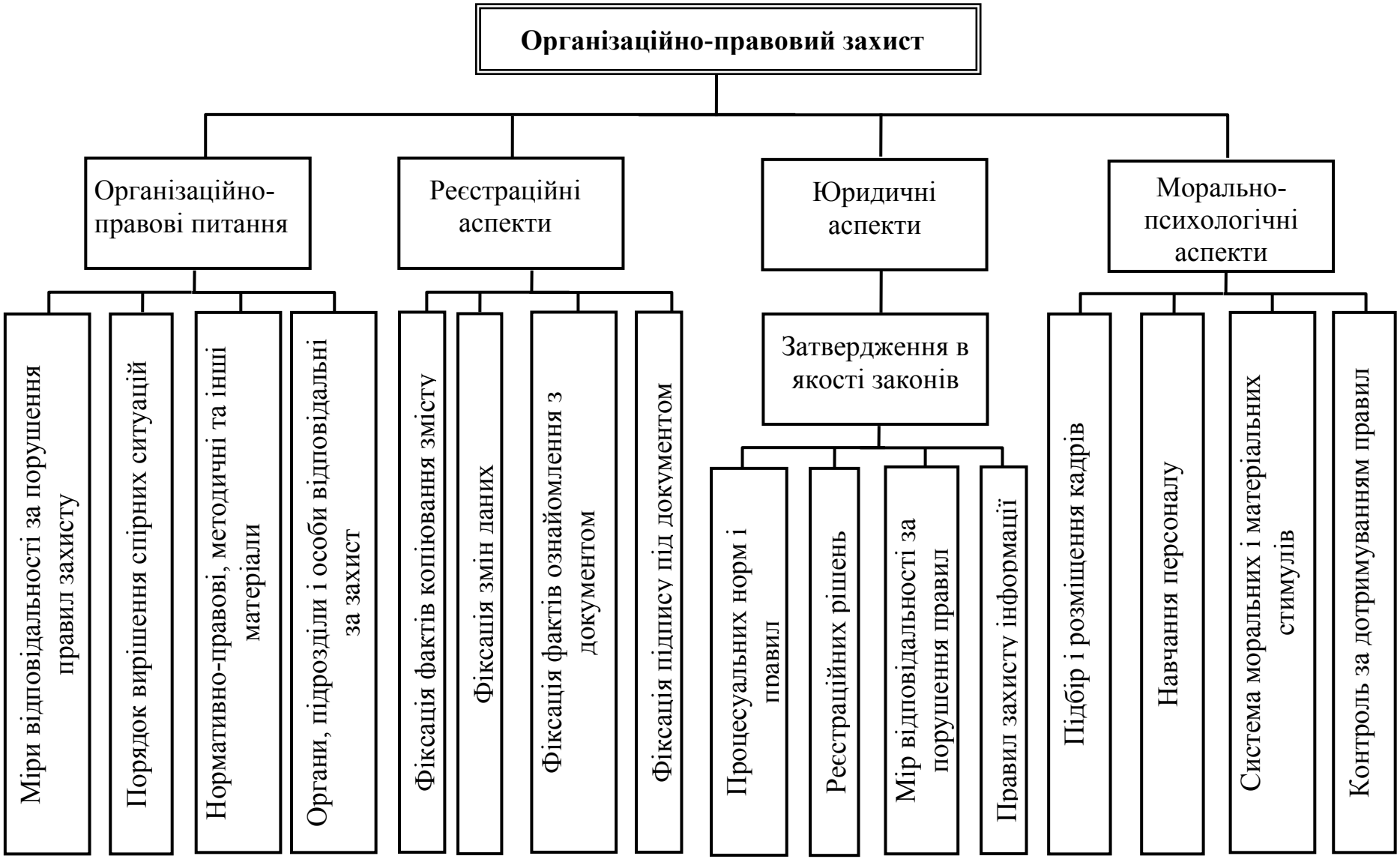

Рис.2. Структурна схема організаційно-правового захисту

оголошувана інформація про події та явища в галузі політики, економіки, культури, а також у соціальній, економічній, міжнародній та інших сферах.

До *основних суб'єктів інформаційних відносин* (рис.3) відносяться особи, які приймають участь у створенні, передаванні та розповсюдженні, отриманні та споживанні інформації. Це перш за все творці чи виробники інформації, власники та споживачі інформації.

Творці чи виробники інформації – це особи, внаслідок інтелектуальної діяльності яких з'являється інформація. До них відносяться і автори, які створили продукцію, і особи (в тому числі і органи державної влади, місцевого самоврядування, юридичні особи), які не претендують на авторство з приводу створеної ними інформації.

Власники інформації – це посередники між творцями і споживачами інформації; особи, що набувають виключне право на передавання і розповсюдження інформації і забезпечують доведення утвореної інформації до споживача.

Рис. 3. Основні суб'єкти інформаційних відносин

Споживачі інформації – це особи, що потребують інформації, виконують пошук і отримують її для задоволення своїх потреб (підвищення знань, освіта, прийняття рішень тощо).

До суб'єктів інформаційних відносин відносяться також і ті особи, які приймають участь у створенні та застосуванні засобів і механізмів програмно-технічного забезпечення інформаційних процесів – інформаційних систем, мереж, інформаційних технологій та засобів їх забезпечення (інформаційних, лінгвістичних, технічних, програмних тощо).

Таким чином, інформаційне право можна визначити як комплексну

галузь права, представлену системою соціальних норм і відносин, що виникають в інформаційній сфері (виробництво, перетворення, зберігання і споживання інформації) та охороняються державою.

1.5. Інформація як об'єкт інформаційного права

Під інформацією як об'єктом права розуміють створювані у процесі інтелектуальної діяльності відомості (дані) про навколишній світ і процеси, які в ньому протікають, чи повідомлення, що інформують про стан справ.

Інформація об'єкт багатофункціональний, вона створюється, передається і застосовується у всіх сферах діяльності та забезпечує виконання чисельних функцій і задач, що стоять перед різними суб'єктами – органами державної влади, місцевого самоврядування, фізичними та юридичними особами.

При *передаванні інформації* у державі та суспільстві *вона може виступати* як:

- товар у процесах її створення, зберігання і використання, передавання і розповсюдження;
- засіб для здійснення правової координації і керування поведінкою суб'єктів (через офіційні документи і судові рішення);
- джерело для прийняття рішень;
- джерело знань при навчанні і вихованні в процесах здійснення конституційного права на освіту;
- засіб оповіщення суспільства про події і явища (через ЗМІ), що відбуваються, в порядку здійснення конституційного права на інформацію;
- засіб звітності про діяльність юридичних і фізичних осіб (податкова, бухгалтерська, статистична звітність тощо);
- засіб реалізації прав і свобод особистості через надання відомостей про особистість різним структурам (право на життя, право на житло, право на освіту, право на виховання, право на працю тощо).

Слід звернути увагу на те, що інформація одночасно може виступати і в якості джерела, що несе певне функціональне навантаження, і як товар. Наприклад, нормативні правові акти, виконуючи основну функцію – розповсюдження правових норм і доведення їх до кожного, одночасно виступають і в якості товару при продажі інформаційних продуктів і наданні інформаційних послуг, укладених на їх основі.

Те ж саме можна сказати і про персональні дані, які за рубежем продаються і здаються в оренду для реалізації певного маркетингу. Продаються також різні інформаційні ресурси, які вміщують відомості про корисні копалини, про науковий і технічний розвиток суспільства, про його творчий потенціал тощо.

1.6. Особливості та юридичні властивості інформації

На відміну від відомих, традиційних для права об'єктів, інформація володіє специфічними особливостями і юридичними властивостями, які часто визначають і відносини, що виникають при її передаванні між суб'єктами і характер їх поведінки.

До таких особливостей і властивостей можна віднести.

1. Інформація при включенні в оборот відособлюється від її творця чи власника і стає річчю у вигляді символів чи знаків. Внаслідок цього вона існує окремо і не залежить від творця і володільника. Звідси виникає юридична властивість інформації – *можливість виступати в якості об'єкта,* що передається від одного суб'єкта до іншого і вимагає юридичного закріплення факту її належності суб'єктам, які беруть участь у її передаванні.

2. Інформація, що передається від одного суб'єкта до іншого, одночасно належить двом учасникам інформаційних відносин. Це основна відмінність інформації від речі. Юридична властивість інформації у зв'язку з цим – її *фізична невідчужуваність від творця,* власника і споживача. Така можливість вимагає розробки і застосування до інформації при її передаванні особливих правових механізмів, що заміняють механізм відчуження речі.

3. Інформація при включенні в оборот документується і відображається на матеріальному носії. Існують дві групи носіїв:

а) *жорсткі,* до яких інформація прив'язана жорстко (папір, лазерні диски тощо);

б) *віртуальні,* до яких інформацію не можна прив'язати жорстко, по яких вона ніби ковзається (дискети з перезаписом, оперативна пам'ять персональних комп'ютерів тощо). Юридична властивість, що витікає з цієї особливості, полягає у *двоєдності інформації і матеріального носія, на якому ця інформація закріплюється.*

4. Інформація представляється у визначених організаційних формах – окремі дані (відомості), документ, масив (база) даних (документів), бібліотек, фонд документів, архів тощо. Звідси юридична властивість – *можливість відносити до інформаційних даних як окремі вихідні документи, так і складні організаційні структури,* що вміщують інформацію. Це інформаційні системи, бази даних, інформаційні мережі, бібліотеки, архіви тощо.

1.7. Основні принципи інформаційного права

Під принципами інформаційного права розуміють основні вихідні положення, що юридичне закріплюють об'єктивні закономірності господарського життя, які проявляються в інформаційній сфері. Принципи

інформаційного права дозволяють формувати це право як самостійну галузь, внаслідок чого вони є системоутворювальними.

Основними принципами інформаційного права є (рис. 4):

- *принцип інформаційних відносин* як відносин, які утворюють галузь інформаційного права, значить, що інформаційні відносини, які виникають, виходячи з особливостей і юридичних властивостей інформації та її багатофункціональності як основного об'єкта інформаційного права, володіють на цій основі специфікою, що відрізняє їх від інших суспільних відносин, і складають основу суспільних відносин в інформаційній сфері;

- *принцип інформаційної власності* значить, що при передачі та розповсюдженні інформації як основного об'єкта інформаційного права (творці, власники і споживачі інформації) і їх поведінка реалізується на основі інформаційних правомочностей – права знати, володіти і застосовувати інформацію;

- *принцип невідчужуваності інформації* від її творця, власника і споживача (неможливо позбавити суб'єкта отриманих знань) значить, що механізм відчуження інформації повинен замінятись механізмом добровільної відмови від певних інформаційних правомочностей через установлення за договором прав, обов'язків і відповідальності за використання цієї інформації після її передачі вказаним суб'єктам;

- *принцип комплексного регулювання* відносин інформаційної власності (тобто визначення інформації своєю власністю) значить, що такі відносини можуть регулюватися і авторським правом, і правом майнової власності в залежності від конкретних умов;

- *принцип інвестиційної власності* означає, що механізм авторського права може бути розповсюджений на створення будь-якої відкритої інформації, яка представляє для її творця інтерес, у тому числі і той, що не відноситься до результатів творчості. При цьому захищаються тільки особисті майнові права творця інформації;

- *принцип інформаційної речі,* заснований на двоєдності матеріального носія та інформації, відображеної в ньому, значить, що при передаванні інформаційних речей об'єктивно існують особливі категорії власників інформаційних речей (власники-творці, власники-володільники і власники-споживачі інформаційних речей), які реалізують традиційні правомочності власників, але при обов'язковому дотриманні інформаційних правомочностей;

- *принцип типових інформаційно-правових норм* значить, що такі норми, незалежно від галузі правового регулювання, володіють певною специфікою, заснованою на особливостях і юридичних властивостях інформації. Ця специфіка виявляється в тому, що будь-яка інформаційно-правова норма забезпечує регулювання відносин з приводу створення, володіння, передавання, розповсюдження і застосування інформації через інформаційні правомочності суб'єктів, виходячи з особливостей і функціонального призначення конкретної

інформації.

Рис. 4. Основні принципи інформаційного права

Багатофункціональність інформації приводить до необхідності застосування в інформаційному праві різні методи правового регулювання інформаційних відносин у залежності від виду інформації та її призначення в інформаційних процесах: збирання, накопичення і зберігання інформації, пошуку, передавання, розповсюдження і використання інформації.

Зокрема, при регулюванні відносин з приводу відповідальності за допущені правопорушення в інформаційній сфері повинні використовуватися методи законодавства про адміністративні порушення і кримінального права.

1.8. Законодавство і промисловий шпіонаж

Багато спеціалістів відзначають слабкість юриспруденції розвинутих країн у відношенні захисту підприємств від промислового шпіонажу. Американський спеціаліст з цього приводу висловився так: "Немає ще законів, які б забезпечували надійний захист від викрадачів секретних знань і даних. Ті, хто краде цю цінну інформацію, знаходяться у вигіднішому положенні порівняно *з* тими, хто краде матеріальне майно, тому що перші не попадають під дію закону про крадіжку майна. Окрім

того, промисловий шпигун, як правило, ризикує отримати шість місяців тюрми за те, за що воєнний шпигун був би розстріляний, а винагорода промислового шпигуна у випадку удачі була б у декілька разів більша винагороди воєнного шпигуна".

Викрадення промислового секрету важкодоказове. Неадекватні закони, за словами американського юриста, обмежують суди і дають їм мало шансів у переслідуванні злочинців, які займаються промисловим шпигунством. Так, у США для того, щоб вимагати законодавчого захисту у *ви-випадку розголошення торгового секрету* необхідно довести:

- що предмет, який розглядається як торговий секрет, є таким фактично;
- право власності на нього;
- що дії особи, яка розкриває торговий секрет, відносяться до однієї з таких категорій:

1) торговий секрет, отриманий нечесним шляхом;

2) розголошення чи використання торгового секрету являє собою порушення довірчих відносин між особами;

3) особа узнала секрет (в тому числі і від третьої особи) і знала про те, що це секрет.

Краще захищена запатентована інформація, хоча і тут багато слабких місць. Так, закон США передбачає заборону на публікацію відомостей у пресі протягом року до подання заявки на патентування. В інших країнах (окрім Франції і Голландії), простої заборони на розголошення інформації вистачає для того, щоб довести, що вона секретна. Про те і тут законодавство недосконале.

Але ні в яке порівняння з законами розвинутих країн не можуть йти закони (а точніше, відсутність у них легальної чіткої, ієрархічної єдності, що викликає суперечливе тлумачення та застосування їх норм у практиці) на території країн СНД. Таке положення шокує західних бізнесменів і викликає в них побоювання інвестування нових технологій у спільні підприємства, що діють на території СНД.

Комерційною таємницею не є такі документи і відомості:

- установчі документи, документи, що дозволяють займатися підприємницькою діяльністю чи господарською діяльністю, або її окремими видами;
- інформація за всіма встановленими формами державної звітності;
- дані, необхідні для перевірки нарахування і виплати податків та інших обов'язкових платежів, відомості про чисельність і склад працівників, їх заробітну плату в цілому, за професіями і посадами, а також про наявність вакансій;
- документи про виплату податків і обов'язкових платежів;
- інформація про забруднення навколишнього природного середовища, незабезпечення безпеки та умов праці, реалізації продукції, яка наносить шкоду здоров'ю, а також про інші порушення

законодавства і розміри нанесеної при цьому шкоди;

- документи про платоспроможність;

- відомості про участь посадових осіб підприємства у кооперативних, малих підприємствах, об'єднаннях та інших організаціях, які займаються підприємницькою діяльністю;

- відомості, які згідно з діючим законодавством, підлягають оголошенню.

Зазначені відомості підприємства зобов'язані надавати контролювальним органам державної влади і правоохоронним органам, а також іншим юридичним особам за їх вимогою, згідно з діючим законодавством.

Кажуть, що успішно проведені акції промислового шпигунства ведуть до отримання незаконних переваг над конкурентами. Проте чи слід вважати промисловий шпіонаж таким серйозним злочином у світі ринкових відносин, де править конкуренція і де кожний неминуче стає переможцем чи переможеним.

"Проколи" безпеки фірм на Заході нерідкі, проте керівництво звичайно намагається швидко закрити справу, щоб уникнути розголосу і не ставити під удар свою репутацію. Звичайна позиція керівника фірми: "Зі мною це ніколи не трапиться", часто підводить його самого, його співробітників, клієнтів і акціонерів. На фірмах рідко проявляють серйозне відношення до загрози зі сторони спецслужб інших держав, причому спецслужб навіть дружніх країн.

Керівництво фірм ігнорує можливість шпигунства зі сторони конкурентів, не цікавиться методом негласного збирання інформації, а безпека до цього часу вважається об'єктом накладних витрат і не розглядається в якості об'єкта інвестицій на захист цінностей і ресурсів. Коли проблема все ж виникає, від неї стараються збутися одним ударом.

Політична філософія 80-х років внесла великий вклад у руйнування лояльності, гордості та самодисципліни працівників фірм. Колись сильний "корпоративний дух" сьогодні згорає в котлі індивідуалізму ринкових відносин. Співробітник, що затаїв злобу на свого керівника, являє собою найбільшу загрозу інформаційній безпеці, про те це найменше усвідомлюється керівництвом компанії.

У наші дні розміри "інформаційної біржі", де люди займаються купівлею-продажем інформації, значно розширилися, причому продаж нелегально добутих відомостей не є чимось зовсім незвичайним. Про діяльність брокерів на такій біржі за зрозумілими причинами мало що відомо, і це дуже характерно для даної діяльності.

Оцінюючи правовий аспект промислового шпигунства, журнал "International Security Review" відзначає, що у всіх країнах Європейського Союзу не має законів, які прямо трактують промислове шпигунство в якості протиправної дії. Так, у Великобританії парламенту ще тільки передбачається визнати промислове шпигунство злочином, хоча в цій

країні існує біля десяти законодавчих актів, що регулюють ті чи інші сторони інформаційної безпеки. Проте спроби прийняти закон "Про промислову інформацію" у 1968 р. і "Про зловживання довірою" у 1981р., в яких були дані означення понять "промислове шпигунство", і "загроза вивідування шляхом інсценованого інтерв'ю", успіхами не увінчалися. У той же час у ряді штатів США промислове шпигунство законодавчо вважалося злочином.

Основною силою, що рухає промислове шпигунство у ринковому суспільстві, завжди була конкуренція. Всі конкуруючі фірми мають відомості, які звичайно легко отримати з галузевих періодичних видань, під час звичайних ділових контактів. Проте деякі дані фірми завжди стараються зберегти у таємниці. Це відомості, за якими полюють конкуренти: технологічні процеси, стратегії маркетингу, результати науково-дослідних і дослідно-конструкторських робіт – звичайні цілі промислового шпигунства. Саме ці відомості повинні бути чітко визначені і надійно захищені від крадіжок і несанкціонованого доступу. Чим більше такої інформації, тим частіше стоїть проблема забезпечення безпеки.

Контрольні питання

1. Розкажіть про позитивні та негативні наслідки інформаційних технологій.
2. Охарактеризуйте основи систем захисту інформації.
3. Опишіть суть правових аспектів захисту інформації.
4. Розкрийте суть проблем правового характеру, що виникають при розробці засобів захисту інформації.
5. Наведіть критерії складу зловживань у сфері оброблення інформації.
6. Охарактеризуйте підсистему організаційно-правового захисту інформації.
7. Дайте означення інформаційного права, об'єктів та суб'єктів інформаційного права.
8. Розкажіть про особливості інформації як об'єкта інформаційного права.
9. Охарактеризуйте особливості та юридичні властивості інформації.
10. Наведіть класифікацію основних принципів інформаційного права.
11. Розкрийте причини росту комп'ютерної злочинності.

Глава 2. Система правового регулювання суспільних інформаційних відносин

2.1. Види правового регулювання

Система правового регулювання суспільних інформаційних відносин в умовах інформатизації (інформаційного суспільства) України базується на доктрині поділу права на публічне (державне) і приватне.

Публічне (державне) регулювання суспільних відносин знаходить вираження у системі законодавства та підзаконних нормативних актах, виданих відповідно до компетенції Президентом України, Кабінетом Міністрів України, органами державної виконавчої і судової влади та органами місцевого самоврядування.

Провідними принципами публічного права у сфері діяльності органів державної влади щодо суспільних відносин, в основі яких є інформація, такі (рис.5):

Рис. 5. Провідні принципи публічного права у сфері діяльності органів державної влади

- юридичне закріплення прав, обов'язків, зобов'язань, гарантій та відповідальності державних органів влади перед особами і суспільством;
- визначення та забезпечення співвідношення інтересів людини, суспільства, держави у сфері суспільних інформаційних відносин;
- законність.

У державному (публічному) праві, згідно з доктриною поділу його на провідні комплексні галузі, виділяють такі механізми захисту від правопорушення: конституційно-правовий, цивільно-правовий,

адміністративно-правовий, захист засобами трудового права та кримінально-правовий захист.

Приватне правове регулювання суспільних інформаційних відносин в Україні здійснюється приватними особами (фізичними і недержавними юридичними особами, громадськими формуваннями) на засадах (рис.6):

Рис. 6. Засади приватного правового регулювання інформаційних відносин

- норм публічного правового регулювання з урахуванням законних прав та інтересів інших осіб і суспільства;

- конституційного принципу дозволеності діянь, на заборонених законодавством (“дозволено все, що не заборонено законом”);

- автономії волі приватних осіб щодо виконання, здійснення та припинення правовідносин (через правочини, угоди (статути), добрі звичаї, норми суспільної моралі, корпоративної (ділової) етики тощо).

Галузева ознака сутності приватно-правового регулювання захисту прав виражається в діях публічного органу влади (суду, державного органу) щодо порушення справи (кримінальної, адміністративної, цивільної чи дисциплінарної) тільки за заявою відповідної форми щодо порушення. Тобто, для державного органу влади функція захисту від *делікту* (правопорушення, що тягне за собою відповідальність особи, яка допустила його) виникає переважно тоді, коли є відповідна заява потерпілого. Нема заяви – нема й делікту. Цю аксіому слід пам’ятати всім.

Незнання, невміння або небажання громадян та інших суб’єктів інформаційних відносин захищати свої права, зокрема щодо захисту інформації в автоматизованих системах, негативно впливає не тільки на їх приватні інтереси, але й на стан правопорядку у цілому в Україні, правову культуру та правову ментальність суспільства.

2.2. Правовий захист інформації

Як відомо, ***право*** *– це система або сукупність норм – правил поведінки і діяльності особи та інших суб'єктів правовідносин, що відображають найбільш важливі економічні, політичні, моральні, громадянські та інші соціальні відносини у формі правових звичаїв, державних законів і інших нормативно-правових актів, правових прецедентів, правових договорів, які:*

- встановлені державною владою, всім населенням (референдумом, віче тощо) або загальновизнані суспільством;
- виражають суб'єктивні права і обов'язки громадян, юридичних осіб, держави та інших суб'єктів, а також форм та засобів їх захисту;
- виражають принципи рівності та рівноправ'я всіх суб'єктів, міру справедливості, принцип юридичної (правової) свободи і відповідальності за нанесені шкоди і суспільної небезпеки, принцип істини і правди;
- є загальнообов'зковими для всіх суб'єктів суспільних відносин, охороняються державною владою і суспільством від порушень і направлені на охорону соціальних (матеріальних і духовних) цінностей з позицій потреб і інтересів всього суспільства і народу;
- направлені на розвиток і зміцнення демократії, особистості, громадянського суспільства, загального блага, правопорядку і правової держави.

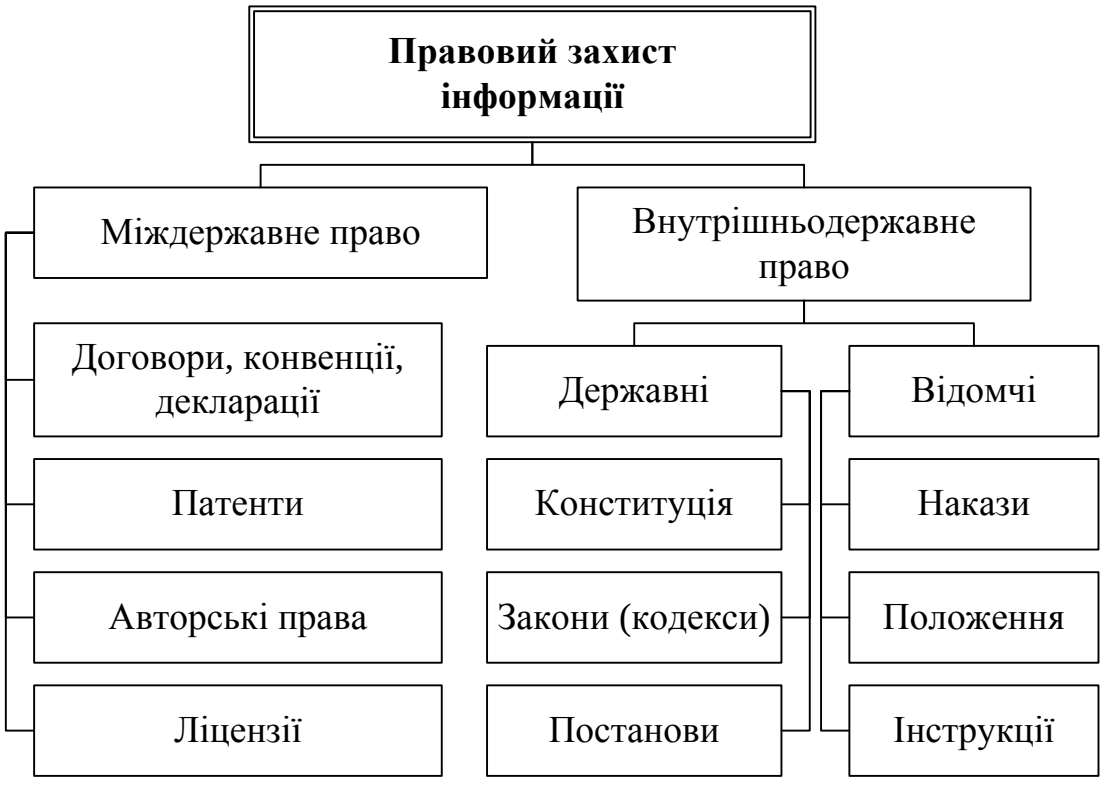

Рис. 7. Структура правового захисту інформації

Правовий захист інформації – це спеціальні закони, інші нормативні акти, правила, засоби і заходи, що забезпечують захист інформації на правовій основі.

Правовий захист інформації як ресурс визнаний на міжнародному, державному рівні і визначається міждержавними договорами, конвенціями, деклараціями та реалізується патентами, авторським правом і ліцензіями на їх захист. На державному рівні правовий захист регулюється державними і відомчими актами (рис.7).

В нашій країні такими правилами (актами, нормами) є Конституція України, закони України, цивільне, адміністративне, кримінальне право, викладені у відповідних кодексах. Щодо відомчих нормативних актів, то вони визначаються наказами, положеннями та інструкціями, що видаються відомствами, організаціями і підприємствами і діють у рамках певних структур.

2.3. Законодавство у сфері боротьби з комп'ютерною злочинністю

Правове регулювання протидії кіберзлочинам та кіберзлочинності базується на засадах інформаційного законодавства, яке є комплексною галуззю законодавства України (рис.8).

Основу публічно-правового регулювання суспільних інформаційних відносин становить Конституція України, прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року.

Розвиток положень Конституції України щодо регулювання суспільних інформаційних відносин відображений в конкретних нормах кодифікованих провідних галузей законодавства:

- Кримінальний Кодекс України від 5.04.2001р. №2341-III;
- Кримінально-процесуальний кодекс України станом на 20.09.2001р.;
- Кримінально-виконавчий кодекс України від 11.07.2001р. № 1129-IV;
- Цивільний кодекс України від 16.01.2003р. №435-IV;
- Господарський процесуальний кодекс України від 6.11.1991р. №1798-XII;
- Кодекс України про адміністративні правопорушення станом на 20.06.2000р.;
- Кодекс законів про працю України станом на 1.12.2000р.;
- Господарський кодекс України від 16.01.2003р. №436-IV;

Окремі норми суспільних інформаційних відносин містяться в:

- Митному кодексі України від 11.07.2002р. №32-IV;
- Арбітражно-процесуальному кодексі України від 6.11.1991р. №1798-XII;
- інших кодексах України;

- основах законодавства України щодо окремих галузей суспільних відносин.

Рис. 8. Засади публічно-правового регулювання суспільних інформаційних відносин

Спеціальне законодавство щодо боротьби з комп'ютерною злочинністю ґрунтується на законодавстві провідних галузей права, у тому числі у сфері правоохоронної діяльності, і складається з законів, що визначають компетенції та функції окремих державних органів влади: прокуратури, міліції, служби безпеки, державної податкової служби. Також окремі положення боротьби з комп'ютерною злочинністю визначені у законодавстві України про оперативно-розшукову діяльність, про організаційні правові основи боротьби з організованою злочинністю, про боротьбу з корупцією, про оборону, про обмеження монополізму та недопущення недобросовісної конкуренції у підприємницькій діяльності, про захист від недобросовісної конкуренції, інших законодавчих актах, в яких визначається компетенція, функції об'єктів інформаційних відносин.

2.4. Спеціальне законодавство у сфері суспільних інформаційних відносин в Україні

Протидія кіберзлочинам та кіберзлочинності в Україні ґрунтується на нормах спеціального інформаційного законодавства, основу якого становить Закон України "Про інформацію" (2.10.1992р., №2657-XII).

Положення цього закону знаходить свій розвиток у законодавчих нормах, які є системоутворювальними щодо публічно-правового (державного) регулювання окремих сфер суспільних інформаційних відносин, у тому числі Законах України про:

- мови (28.10.1989р.№8312-XI);
- державну таємницю (21.01.1994р.№3855-XII);
- авторське право і суміжні права (23.12.1993р. №3792-XII);
- науково-технічну інформацію (25.06.1993р. №3322-XII);
- бібліотеки і бібліотечну справу (21.01.1995р. №3322-XII);
- національний архівний фонд і архівні установи (24.12.1993р. №3814-XII);
- обов'язковий примірник документів (9.04.1999р. №595-XIV);
- розповсюдження примірників аудіовізуальних творів та фонограм, про електронні документи та електронний документообіг (22.05.2003р. № 851-IV);
- про електронний цифровий підпис (22.05.2003р.№852-IV) тощо.

Умовно-автономний субінститут інформаційного законодавства утворює законодавство у сфері зв'язку та інформатизації, яке складається з системоутворювальних законів України про:

- зв'язок (16.05.1995р. №160/95-ВР);
- захист інформації в автоматизованих системах (5.07.1994р. №80/94-ВР);
- концепцію національної програми інформатизації (4.02.1998р. №75/98-ВР);
- національну програму інформатизації (4.02.1998р. №75/98-ВР);
- охорону прав на типографії інтегральних мікросхем (5.11.1997р.№621/97-ВР).

Автономні субінститути інформаційного законодавства утворюють закони України у сфері масової інформації про:

- інформаційні агентства (28.02.1995р. №74/95-ВР);
- видавничу справу (5.06.1997р. №318/97-ВР);
- порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні засобами масової інформації (23.09.1997р. №539/97-ВР);
- систему суспільного телебачення і радіомовлення (18.07.1997р. №485/97-ВР);
- національну раду України з питань телебачення і радіомовлення

(23.09.1997р. №538/97-ВР);

- радіочастотний ресурс України (1.06.2000р. №1770-III);
- кінематографію, інші законодавчі акти.

2.5. Міжгалузевий зв'язок інформаційного законодавства

Як опосередкований об'єкт, інформація виступає з'єднувальною ланкою з іншими міжгалузевими інститутами законодавства.

До провідних системоутворювальних законодавчих актів, які містять норми суспільних відносин, виражені через інформацію, належать Закони України про власність, про рекламу, державну статистику, бухгалтерський облік та фінансову звітність в Україні, охорону культурної спадщини, освіту, загальну середню освіту, професійно-технічну освіту, наукову і науково-технічну діяльність, наукову і науково-технічну експертизу, метрологію та метрологічну діяльність, топографо-геодезичну і картографічну діяльність, гідрометеорологічну діяльність, застосування електронних контрольно-касових апаратів і товарно-касових книг при розрахунках із споживачами у сфері торгівлі, громадського харчування та послуг. Державний реєстр фізичних осіб – платників податків та інших обов'язкових платежів, Національну депозитарну систему та особливості електронного обігу цінних паперів в Україні, інші законодавчі акти.

Інформація, як один з важливих чинників, виступає у сфері економічних правовідносин (банківських, господарських, комерційних, підприємницьких, інвестиційних, інноваційних тощо), і знаходить своє відображення у системоутворювальному законодавстві – Законах України про банки і банківську діяльність, про економічну самостійність України; про зовнішньоекономічну діяльність; про підприємництво; про цінні папери і фондову біржу; про інвестиційну діяльність; про товарну біржу; про аудиторську діяльність; про регулювання товарообмінних (бартерних) операцій у галузі зовнішньоекономічної діяльності; про захист національного товаровиробника від демпінгового імпорту; про захист національного товаровиробника від субсидованого імпорту; про застосування спеціальних заходів щодо імпорту в Україну тощо.

Окремі положення щодо регулювання інформаційних правовідносин в умовах становлення в Україні інформаційного суспільства знайшли закріплення і відображення **в Постановах Верховної Ради України** про:

- затвердження концепції (основ державної політики) національної безпеки України;
- організацію роботи з формування єдиної системи правової інформації в Україні;
- консультативну раду з питань інформатизації при Верховній Раді України та положення про консультативну раду з питань інформатизації

при Верховній Раді України, в інших нормативно-правових актах Верховної Ради України.

Суспільні інформаційні відносини як опосередкований об'єкт регулюються також **Декретами Кабінету Міністрів України** про державний нагляд за додержанням стандартів, норм і правил та відповідальності за їх порушення; про стандартизацію і сертифікацію тощо.

2.6. Система підзаконних нормативно-правових актів щодо боротьби з комп'ютерною злочинністю в Україні

Державна політика України щодо боротьби з комп'ютерною злочинністю та комп'ютерними злочинами знаходить вираз у системі підзаконних нормативно-правових актів органів державної влади щодо їх компетенції. Її складають Укази Президента України, нормативно-правові акти Уряду України, нормативні акти міністерств і відомств щодо їх компетенції, функцій, прав і обов'язків.

Розвиток положень чинного законодавства знаходить відображення у конкретних підзаконних нормативно-правових актах, як:

Укази Президента України про:

- рішення Ради національної безпеки і оборони від 17 червня 1997 року "Невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин";
- комісію з питань інформаційної безпеки;
- деякі заходи щодо захисту інтересів держави в інформаційній сфері;
- єдину комп'ютерну інформаційну мережу державних органів приватизації;
- електронний обіг цінних паперів і національний депозитарій;
- міжвідомчу комісію з питань приєднання України до Генеральної угоди з тарифів і торгівлі та вступу до Світової організації торгівлі;
- положення про державний центр страхового фонду документації України;
- заходи щодо впровадження концепції адміністративної реформи в Україні;
- державну реєстрацію нормативних актів міністерств та інших органів державної виконавчої влади;
- положення про державних експертів з питань таємниць;
- положення про технічний захист інформації в Україні;
- заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї

мережі в Україні;

- заходи щодо захисту інформаційних ресурсів держави;
- заходи щодо вдосконалення криптографічного захисту інформації в телекомунікаційних та інформаційних системах;
- вдосконалення порядку здійснення організаційно-структурних змін у сфері забезпечення інформаційної безпеки;
- положення про порядок здійснення криптографічного захисту інформації в Україні;
- єдиний державний реєстр нормативних актів;
- рішення Ради національної безпеки і оборони України від 21 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України".

Постанови Кабінету Міністрів України про:

- першочергові заходи інформатизації;
- затвердження переліку обов'язкових етапів робіт під час проектування, впровадження та експлуатації систем і засобів автоматизованої обробки та передачі даних;
- затвердження плану заходів щодо формування інформаційно-аналітичної системи органів державної влади;
- заходи щодо посилення контролю за обґрунтованістю проектів інформатизації діяльності центральних органів виконавчої влади;
- затвердження положення про забезпечення режиму секретності під час обробки інформації, що становить державну таємницю, в автоматизованих системах;
- уточнення термінів впровадження засобів контролю;
- перелік відомостей, що не становлять комерційної таємниці;
- положення про порядок видачі суб'єктам підприємницької діяльності спеціальних дозволів (ліцензій) на здійснення окремих видів діяльності;
- порядок надання Кабінетом Міністрів України дозволу на використання запатентованого винаходу (корисної моделі) чи запатентованого зразка без дозволу власника патенту, але з виплатою йому відповідної компенсації;
- положення про технічний захист інформації в Україні;
- створення єдиного державного реєстру підприємств і організацій України;
- єдиний ліцензійний реєстр;
- впровадження штрихового кодування товарів;
- затвердження інструкції про порядок обліку, зберігання і використання документів, справ, видань та інших матеріальних носіїв інформації, які містять конфіденційну інформацію, що є власністю держави;
- утворення міжвідомчого комітету з проблем захисту прав на об'єкти інтелектуальної власності;
- перелік платних послуг, які можуть надавати інформаційні підрозділи органів внутрішніх справ;
- деякі питання реалізації державної інформаційної політики;

- підписання угоди між Кабінетом Міністрів України і Урядом Киргизької Республіки про співробітництво в галузі інформації;
- створення єдиної комп'ютерної мережі арбітражних судів;
- затвердження положення про державну реєстрацію нормативних актів міністерств та інших органів державної влади;
- затвердження єдиного державного реєстру нормативних актів та здійснення правової інформатизації України;
- державне підприємство "Інформаційний центр" Міністерства юстиції;
- затвердження генерального державного замовника національної програми інформатизації;
- керівника національної програми інформатизації;
- затвердження положення про формування та виконання національної програми інформатизації;
- утворення експертно-консультативної ради з питань інформатизації при Кабінеті Міністрів України;
- затвердження порядку локалізації програмних продуктів (програмних засобів) для виконання національної програми інформатизації;
- програму створення урядової інформаційно-аналітичної системи з питань надзвичайних ситуацій;
- заходи щодо створення єдиної бази статистичних даних та статистичної звітності про зовнішньоторговельні операції;
- деякі питання захисту інформації, охорона якої забезпечується державою;
- інші нормативні акти Уряду України.

Контрольні питання

1. Розкажіть про особливості правового регулювання суспільних інформаційних відносин.
2. Дайте характеристику публічного (державного) регулювання суспільних відносин.
3. Дайте визначення та характеристику права.
4. Наведіть структуру правового захисту інформації.
5. Поясніть суть приватно-правового регулювання суспільних інформаційних відносин.
6. Перерахуйте основні джерела публічно-правового регулювання суспільних інформаційних відносин.
7. Наведіть класифікацію законодавчих актів міжгалузевого зв’язку.
8. Охарактеризуйте систему підзаконних нормативно-правових актів щодо боротьби з комп’ютерною злочинністю.

Глава 3. Державна інформаційна політика

3.1. Напрями і способи державної інформаційної політики

Державна інформаційна політика – це сукупність основних напрямів і способів діяльності держави щодо одержання, використання, поширення та зберігання інформації.

Головними напрямами і способами державної інформаційної політики є (рис. 9):

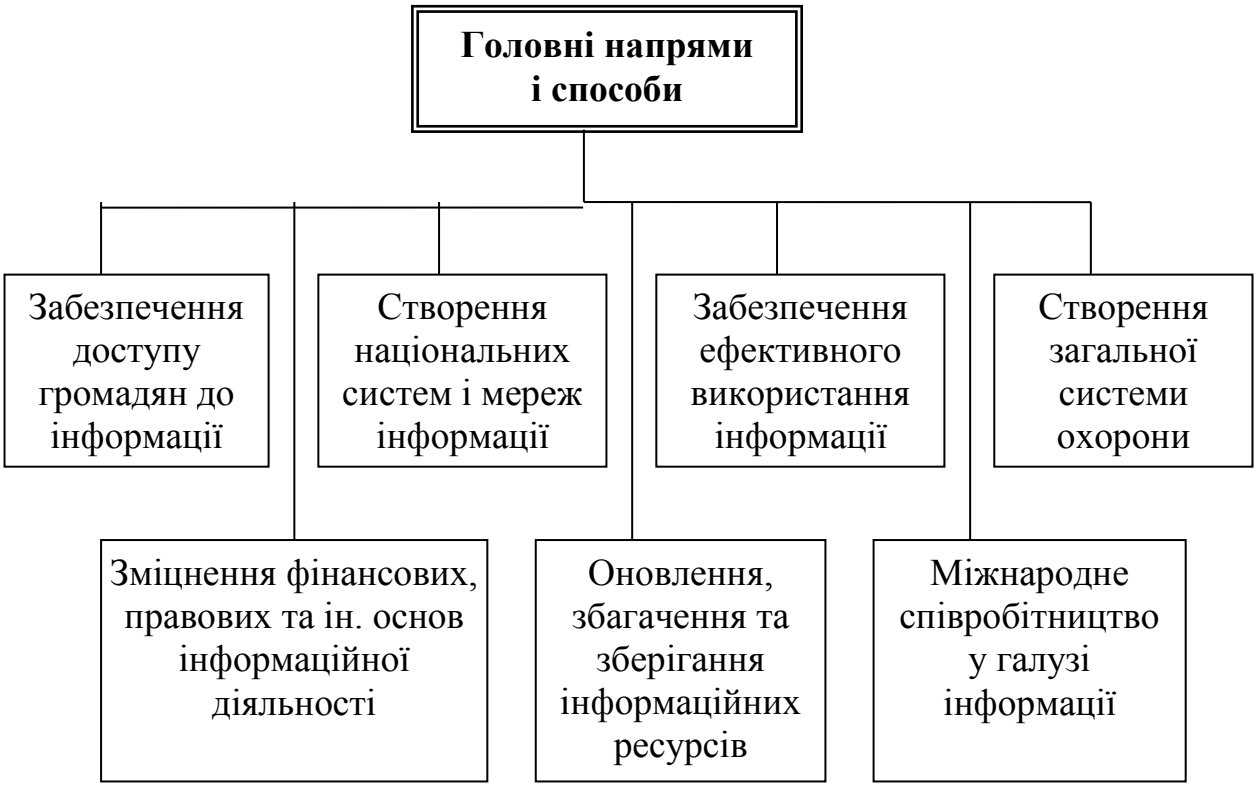

Рис. 9. Головні напрями і способи державної інформаційної політики

- забезпечення доступу громадян до інформації;
- створення національних систем і мереж інформації;
- сприяння постійному оновленню, збагаченню та зберіганню національних інформаційних ресурсів;
- зміцнення матеріально-технічних, фінансових організацій, правових і наукових основ інформаційної діяльності;
- забезпечення ефективного використання інформації;
- створення загальної системи охорони інформації;
- сприяння міжнародному співробітництву в галузі інформації і гарантування інформаційного суверенітету України.

Державну інформаційну політику розробляють і здійснюють органи державної влади загальної компетенції, а також відповідні органи спеціальної компетенції.

4.2. Принципи державної інформаційної політики України

Сутність державної інформаційної політики України визначається рядом положень Конституції України на рівні таких принципів (рис 10).

Рис.10. Основні принципи державної інформаційної політики України

1. Державна інформаційна політика у контексті верховенства прав людини:

- людина, її безпека визначаються в Україні найвищою соціальною цінністю (стаття 3);
- утвердження і забезпечення прав і свобод людини є головним обов'язком держави (стаття 3);
- ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України (стаття 32);
- громадянам гарантується свобода творчості, моральних і

матеріальних інтересів, що виникають у зв'язку з різними видами інтелектуальної діяльності (стаття 54).

2. Державна інформаційна політика щодо мовного суверенітету:

- державною мовою в Україні є українська мова (стаття 10);

- держава забезпечує всебічний розвиток і функціонування української мови у сфері суспільного життя на всій території України (стаття 10).

3. Державна інформаційна політика у сфері рівності інших мов – в Україні гарантується розвиток, використання і захист російської, інших мов національних меншин (стаття 10).

4. Геополітичні чинники державної інформаційної політики випливають з Конституції таким чином: зовнішньополітична діяльність України спрямована на забезпечення її національних інтересів і безпеки шляхом підтримання мирного і взаємовигідного співробітництва з членами міжнародного співтовариства за загальновизнаними принципами і нормами міжнародного права (стаття 18).

5. Державна інформаційна політика щодо забезпечення потреб та інтересів особи, суспільства, держави у контексті відносин права власності:

- власність не повинна використовуватися на шкоду людині і суспільству (стаття 13);

- кожен має право володіти, користуватися і розпоряджатися своєю власністю, результатами своєї інтелектуальної, творчої діяльності (стаття 41);

- право приватної власності є непорушним (стаття 41).

6. Державна інформаційна політика щодо інформаційної безпеки людини, суспільства, держави:

- захист суверенітету, забезпечення інформаційної безпеки є найважливішими функціями держави, справою всього українського народу (стаття 17);

- кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції (стаття 31);

- винятки можуть бути встановлені лише судом у випадках, передбачених законодавством, з метою запобігання злочинові чи з'ясування істини під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо (стаття 31).

7. Державна інформаційна політика щодо співвідношення потреб, інтересів особи та суспільства, захисту їх від свавілля державних чиновників:

- примусове відчуження об'єктів права приватної власності може бути застосоване лише як виняток з мотивів суспільної необхідності, на підставі та у порядку, встановлених законом, і за умов попереднього й повного відшкодування їх вартості (стаття 41);

- примусове відчуження таких об'єктів з наступним повним відшкодуванням їх вартості допускається лише в умовах воєнного та надзвичайного стану (стаття 41);

- кожен має право на відшкодування за рахунок держави чи органів місцевого самоврядування матеріальної та моральної шкоди, завданої незаконними рішеннями, діями чи бездіяльністю органів державної влади, органів місцевого самоврядування, їх посадових осіб при здійсненні ними своїх повноважень (стаття 56);

- кожен має право будь-якими не забороненими законом засобами захистити свої права і свободи від порушень і протиправних посягань (стаття 55).

8. Державна інформаційна політика у міжнародних відносинах ґрунтується на положеннях статті 9 Конституції України:

- чинні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, є частиною національного законодавства;

- укладання міжнародних договорів, які суперечать Конституції України, можливе лише після внесення відповідних змін до Конституції України.

Зазначений перелік юридично визначених принципів – норм державної інформаційної політики, визначених у Конституції України, можна продовжувати.

Окремі положення щодо розвитку конституційних норм та деякі інші чинники державної інформаційної політики визначені й в інших (понад 260 законів) законах України.

За підрахунками вітчизняних дослідників кількісний склад підзаконних нормативно-правових актів органів державної влади щодо реалізації державної інформаційної політики характеризується такими показниками: 300 постанов Верховної Ради (нормативного змісту), біля 400 Указів Президента, біля 90 розпоряджень Президента, 1160 постанов Кабінету Міністрів, біля 210 розпоряджень Кабінету Міністрів, більш ніж 1100 нормативних актів міністерств і відомств.

3.3. Недоліки законотворчої діяльності

У сфері суспільних інформаційних відносин нормотворення в Україні здійснюється через вирішення окремих проблем в окремих законах та підзаконних нормативних актах фрагментарно. В той же час значний масив норм щодо інформації розміщено в кодифікованому законодавстві, зокрема в цивільному, адміністративному, трудовому, кримінальному. Таким чином, в Україні сформувалася національна специфічна змішана доктрина права, яка поєднує в особі елементи англо-американської та європейської континентальної юридичних систем.

За наявною доктриною серед недоліків законотворчої діяльності в

Україні визначаються такі.

1. Відсутність легальної чіткої ієрархічної єдності законів, що викликає суперечливе тлумачення при застосуванні норм на практиці.

2. У зв'язку з тим, що різні закони та підзаконні акти, що регулюють суспільні відносини, об'єктом яких є інформація, приймались у різні часи без узгодження понятійного апарату (особливо щодо рецепції, імплементації правового регулювання окремих суспільних інформаційних відносин, визначених у законодавстві інших країн та міжнародних угодах), вони мають ряд термінів, які недостатньо коректні, не викликають відповідну інформаційну рефлексію або взагалі не мають чіткого визначення свого змісту.

3. Термінологічні неточності, різне тлумачення однакових за назвою та формою понять і категорій призводить до їх неоднозначного розуміння і застосування на практиці. Наприклад, „інформація", „таємна інформація і таємниця", „документ" і „документована інформація", „майно" і „власність", „інтелектуальна власність", „володіння", „автоматизована система" тощо. Це, в свою чергу, порушує соціальні конфлікти (правопорушення) в інформаційних відносинах між їх учасниками та створює умови для уникнення від відповідальності правопорушників, що негативно впливає на формування високої культури правовідносин на рівні найкращих здобутків світової інформаційної цивілізації.

4. Велика кількість законів та підзаконних нормативних актів у сфері інформаційних відносин ускладнює їх пошук, аналіз та узгодження для практичного застосування.

5. Має місце розбіжність щодо розуміння структури і складу системи законодавства у сфері інформаційних відносин та підходів до їх формування. Нерідко в окремих законах (у тому числі тих, якими ратифікуються міжнародні угоди) в систему законодавства включають норми, що виражені в підзаконних нормативних актах. Це створює в практиці правозастосування деякими учасниками суспільних відносин колізію норм, ігнорування норм закону на користь норм підзаконного акту. Особливо це притаманно розробкам законопроектів та проектів двосторонніх міждержавних угод, правова культура яких сформована на старій доктрині, що суперечить діючій Конституції України (зокрема, п.п. 3, 5, 6, 11 статті 84).

6. Нові правові акти у сфері суспільних інформаційних відносин нерідко неузгоджені концептуально з раніше прийнятими, що призводить до правового хаосу. Зазначений аспект також є свідченням рівня інформаційно-правової культури як розробників актів, так і тих, хто їх легалізує (приймає).

Як свідчить аналіз, чинне законодавство України у сфері

суспільних відносин щодо інформації (у методологічному аспекті) сьогодні нагадує будинок, який будується громадою без визначеного єдиного плану. При цьому деякі будівельники державної інформаційної політики (ініціатори законопроекту чи підзаконного нормативного акту) проводять роботу на свій розсуд, не узгоджуючи її з іншими розробниками та чинним законодавством. Тобто спостерігається хаотичне нарощування публічного права, що може становити загрозу національній безпеці України. У зв'язку з цим деякими науковцями взагалі висловлюється думка про кризу у теорії та практиці права.

Існує думка, що в основу систематизації норм міжнародного та національного інформаційного права мають покладатись узгоджені, відпрацьовані юридичною наукою і перевірені практикою *основоположні наукові принципи:*

- поєднання традицій і новацій правотворення;
- інкорпорування норм чинного інформаційного законодавства України в нову систему через агрегацію інститутів права;
- формування міжгалузевих інститутів права на основі зв'язків з галузевими інститутами та нормами публічного і приватного міжнародного права.

У зв'язку з цим у правознавстві, теорії права, на базі емпіричного матеріалу, виникла потреба напрацювання методологічних засад нового напряму досліджень, предметом яких є процеси виникнення, зміни і припинення суспільних відносин щодо інформації (відомостей, даних, знань, сигналів тощо) та формування державної інформаційної політики.

Можна констатувати – сукупність правових норм у цій сфері досягла за кількістю такої критичної маси, що зумовлює можливість і необхідність виділення їх в окрему правову інституцію.

3.4. Кодифікація інформаційного законодавства України

Формування державної інформаційної політики та відображення її у національному інформаційному законодавстві України має стати на шлях систематизації через кодифікацію – створення системоутворювального кодексу – *Кодексу про інформацію.*

Цей кодекс має розвивати визначені в Конституції України положення інформаційних відносин, у тому числі щодо інформаційної безпеки людини, нації, суспільства, держави в контексті світової інформаційної безпеки. Він має:

- об'єднати, гармонізувати і розвивати норми і принципи суспільних відносин, визначені в законодавстві України:
- враховувати ратифіковані Україною нормативні акти (угоди, конвенції) міжнародного права;

- легалізувати позитивні звичаї у сфері інформаційних відносин та норми суспільної моралі, загальнолюдські цінності, визначені Організацією Об'єднаних Націй в її статуті, Декларації прав людини та інших загальноприйнятих міждержавних нормативних актах, які сьогодні виступають у ролі стандартів, за якими визначається цивілізованість не тільки окремої країни, але й світового співтовариства в цілому.

Кодекс України про інформацію покликаний об'єднати в одному законодавчому акті регулювання провідних суспільних відносин, об'єктом яких є інформація, незалежно від форми, способу, засобу чи технології її прояву у суспільних відносинах. У разі виникнення необхідності публічно-правового урегулювання нових суспільних відносин щодо інформації агрегувати їх юридичні формулювання у Кодекс через внесення в нього на рівні законів змін і доповнень без порушення нових системоутворювальних законодавчих актів, уникати помилок, характерних для фрагментарного законотворення.

Методологічною базою правотворення такого Кодексу має стати юридична доктрина щодо умовного поділу права України на галузі за такою принциповою моделлю: основа – Конституційне право; його положення знаходять паралельний розвиток (відповідно до методів правового регулювання і захисту прав) в адміністративному, цивільному, кримінальному праві та інших підсистемах національного права України, в яких інформація виступає як опосередкований (додатковий, факультативний) предмет регулювання суспільних відносин.

Пропонується розробку проекту Кодексу проводити методом агрегації: удосконалення окремих правових норм чи створення нових міжгалузевих правових інститутів не повинно порушувати цілісність та призначення законодавства, а покращувати, удосконалювати його дієвість в цілому, створювати нову системну якість, яка не притаманна окремим його складовим.

Мета Кодексу визначається згідно з теорією системи цілей. Метою Кодексу є правове регулювання співвідношення потреб та інтересів особи, суспільства, держави у сфері суспільних відносин щодо інформації у різних формах її об'єктивного вираження (творах, результатах інтелектуальної інформаційної діяльності тощо) та технології фіксації (літери, знаки, образи, цифри тощо).

Провідними підцілями, напрямами, завданнями визнається правове забезпечення:

- життєво важливих потреб та інтересів людини (громадянина);
- життєво важливих потреб та інтересів соціальних громад, суспільства;
- життєво важливих потреб та інтересів держави.

Провідними функціями Кодексу мають бути (рис. 11) :

регулятивна – визначення прав та обов'язків, зобов'язань суб'єктів;

нормативна – визначення норм, правил поведінки суб'єктів інформаційних відносин;

охоронна – визначення гарантій та меж правомірної поведінки, за якими діяння утворюють правопорушення (делікти) та відповідальність за них відповідно до норм цивільного, адміністративного, трудового, кримінального права;

захисна – юридичне закріплення способів, засобів, методів та меж самозахисту суб'єктів суспільних інформаційних відносин та публічно-правового захисту (через органи державної влади);

інтегративна – системне поєднання комплексу визначених юридичних норм, які регулюють інформаційні відносини в Україні, тобто Кодекс має стати поєднувальною ланкою між провідними традиційними галузями права щодо застосування їх методів у сфері інформаційних відносин;

комунікативна – зазначення в окремих статтях посилань на чинне законодавство або необхідність в якому може виникнути.

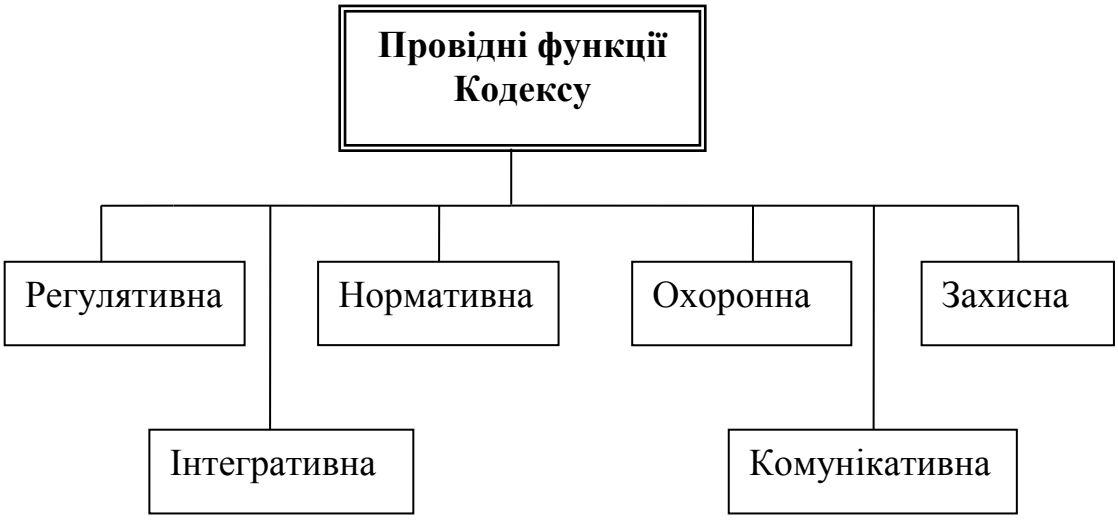

Рис. 11. Провідні функції проекту Кодексу про інформацію

Серед провідних завдань Кодексу у контексті державної інформаційної політики можна визначити такі:

- визначення консенсусу (згоди) в суспільних стосунках, узгодженості розуміння та застосування юридичних норм, правомірної поведінки учасників інформаційних відносин, відносин в інформаційній сфері;

- забезпечення інформаційного суверенітету, незалежності України

у міжнародних стосунках (у тому числі через електронні телекомунікації);

- забезпечення інформаційної безпеки громадян, їх окремих спільнот, суспільства та держави як складових національної безпеки України;
- визначення правомірної поведінки учасників інформаційних відносин в Україні;
- захист інформації від несанкціонованого доступу, правопорушень (знищення , модифікації, перекручення, порушення приватності, конфіденційності тощо).

Контрольні питання

1. Опишіть головні напрямки і способи державної інформаційної політики.
2. Наведіть класифікацію основних принципів державної інформаційної політики.
3. Розкажіть про принципи державної інформаційної політики у контексті верховенства прав людини.
4. Охарактеризуйте суть принципу державної інформаційної політики щодо інформаційної безпеки людини, суспільства, держави.
5. Назвіть недоліки законотворчої діяльності у сфері інформаційних відносин в Україні.
6. Опишіть задачі, що стоять перед правознавцями в зв'язку з необхідністю систематизації інформаційного права.
7. Охарактеризуйте положення інформаційних відносин, які необхідно розвинути у Кодексі про інформацію.
8. Наведіть класифікацію провідних функцій Кодексу про інформацію.
9. Розкажіть про провідні завдання Кодексу у контексті державної інформаційної політики.

Глава 4. Кримінальна характеристика комп'ютерних злочинів

4.1. Загальна частина

Згідно зі ст. 11 Кримінального кодексу України злочином є суспільно небезпечне винне діяння (дія або бездіяльність) вчинене *суб'єктом злочину.*

Злочинна дія – це активна форма поведінки особи.

Злочинна бездіяльність – це пасивна форма поведінки людини. Вона має місце тоді, коли на особу покладались законом, договором, випливали з професійних, посадових, сімейних відносин певні обов'язки і особа їх не виконала.

Злочин – це завжди винне діяння. Особа при вчиненні злочину має відповідне психічне відношення до вчинюваної дії чи бездіяльності, передбачених Особливою частиною Кримінального Кодексу (КК), та їх наслідків, виражене у формі умислу або необережності.

Жодне діяння, які б небезпечні наслідки не наступили, не може розглядатися як злочин, якщо воно вчинене невинно. Наприклад, застосування до винної особи фізичного примусу, внаслідок якого особа не може керувати своїми діями, дії непереборної сили тощо.

Не є злочином дія або бездіяльність, яка хоча формально і містить ознаки будь-якого діяння, передбаченого Кримінальним кодексом, але через малозначність не становить суспільної небезпеки, тобто особа не заподіяла і не могла заподіяти істотної шкоди фізичній чи юридичній особі, суспільству або державі.

За ст. 12 залежно від ступеня тяжкості злочини поділяються на злочини невеликої тяжкості, середньої тяжкості, тяжкі та особливо тяжкі.

При класифікації злочинів враховуються максимальні покарання, передбачені в статтях Особливої частини Кодексу, а не ті, які обираються для конкретної особи. Як передбачено в ст.12, для злочинів невеликої тяжкості – це позбавлення волі на строк не більше двох років або інше, більш м'яке покарання; для злочинів середньої тяжкості – позбавлення волі на строк не більше п'яти років; для тяжких злочинів – позбавлення волі на строк не більше десяти років. Особливо тяжким є злочин, за який передбачене покарання у вигляді позбавлення волі на строк понад десяти років або довічного позбавлення волі.

За своєю криміналістичною сутністю навмисні дії є злочином з чітко вираженими етапами розвитку злочинної діяльності. Вони відрізняються один від одного за характером дії і ступенем завершеності кримінального діяння. Визначення таких стадій необхідне для правильного правового оцінювання вчиненого злочину. Згідно зі статтями 14 і 15 та Особливої

частини Кримінального кодексу України можна виділити три таких стадії: готування до злочину, замах на злочин, закінчення злочину.

Готуванням до злочину є підшукування або пристосування засобів чи знарядь, підшукування співучасників або змова на вчинення злочину, усунення перешкод, а також інше умисне створення умов для вчинення злочину, написання спеціальної програми, що дозволяє подолати захист інформаційної мережі організації, збір інформації щодо клієнтів, системи захисту, підбір паролів, подолання системи захисту від несанкціонованого доступу.

Замахом на злочин – є вчинення особою з прямим умислом діяння (дії або бездіяльності) безпосередньо спрямованого на вчинення злочину. На цій стадії маніпуляцій даними, збереженими в пам'яті комп'ютерної системи, і її керувальними програмами організується несанкціонований рух коштів на користь зловмисника чи іншої особи, маскуються сліди вчинення злочину.

Замах на вчинення *злочину є закінченим*, якщо особа виконала всі дії, які вважала необхідними для доведення злочину до кінця. Це заключна стадія, коли довершені всі несанкціоновані транзакції і зловмисник має можливість скористатися результатами свого злочинного діяння.

У ст. 18 визначається, що *суб'єктом злочину є фізична осудна особа, яка вчинила злочин у віці, з якого відповідно до цього Кодексу може наставати кримінальна відповідальність.*

Згідно з законодавством (ст. 22) кримінальній відповідальності підлягають особи, яким до вчинення злочину виповнилося шістнадцять років.

4.2. Комп'ютерні злочини

Кримінальний Кодекс України містить розділ XVI, що передбачає відповідальність за вчинення *злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж,* а саме:

- незаконне втручання в роботу електронно-обчислювальних машин, комп'ютерів, систем та комп'ютерних мереж (ст. 361);
- викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем (ст. 362);
- порушення правил експлуатації автоматизованих електронно-обчислювальних систем (ст. 363).

Об'єктом перерахованих злочинів є: встановлений порядок використання автоматизованих систем (АС), суспільні відносини, що виникають з приводу порушення правил експлуатації автоматизованих ЕОМ , їх систем чи комп'ютерних мереж.

Предметом злочинного посягання є кілька елементів сфери

електронного інформаційного забезпечення життя суспільства:

- електронно-обчислювальні машини (ЕОМ);
- комп'ютерна інформація;
- програмні матеріали, що забезпечують нормальне функціонування ЕОМ;
- носії інформації;
- системи ЕОМ чи комп'ютерні мережі.

Електронно-обчислювальна машина визначається як фізична систе - ма (устаткування чи комплекс устаткувань), призначена для автоматизації алгоритмічної обробки інформації і обчислень.

Комп'ютерна інформація – інформація, що використовується за допомогою АЕОМ, яка містить відомості про певні факти, події, явища, процеси, окремих осіб, а також програми для автоматизованих електронн- обчислювальних машин і бази даних, має ідентифікаційні реквізити власника, який визначив режим (правила) їх використання.

Програмні матеріали – набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктивному кодах).

Носії інформації – це фізичні об'єкти, поля і сигнали, хімічні середовища, накопичування даних в інформаційних системах.

Автоматизована система (АС) – сукупність керованого об'єкта, вимірювальної, перетворювальної, передавальної та виконувальної апаратури, в якій одержання, перетворення і передавання інформації, формування команд управління та їх використання для впливу на процес управ - ління здійснюються частково автоматично, а частково за участю людей-операторів.

Об'єктивна сторона злочинів характеризується діями:

- втручання в роботу АС
- розповсюдження комп'ютерного вірусу;
- викрадення, тобто заволодіння комп'ютерною інформацією шляхом крадіжки, грабежу чи розбою, її привласнення або заволодіння шляхом шахрайства, чи зловживання службовою особою своїм службовим становищем, або у вимаганні такої інформації;
- порушення правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж особою, яка відповідає за їх експлуатацію, якщо це спричинило викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту, або незаконне копіювання комп'ютерної інформації, або істотне порушення роботи таких машин, їх систем чи мереж.

Втручання в роботу АС полягає в будь-яких діях зловмисника, які

впливають на всю сукупність операцій, що здійснюються за допомогою технічних і програмних засобів (зберігання, введення, записування, перетворення, передача, зчитування, знищення). Несанкціоноване втручання веде до порушення роботи АС, тим самим приводить до перекручування або знищення самої інформації чи її носіїв.

Втручанням в роботу АС буде і різного роду вплив на канали передачі інформації між засобами її обробки і зберігання в самій АС і між окремими АС та іншими електронними і електричними чи механічними системами, внаслідок чого інформація, що передається, знищується або перекручується.

Під *перекрученням інформації* розуміється зміна її змісту, порушення цілісності, в тому числі і вилучення (знищення) окремих фрагментів.

Знищення інформації означає втрату можливості використовувати її власниками (фізичними і юридичними особами). Одним із способів знищення інформації є її блокування, тобто припинення доступу до неї користувачам АС.

Закінченим даний злочин вважається коли втручання призвело до перекручення чи знищення комп'ютерної інформації (матеріальний склад злочину).

Розповсюдження комп'ютерного вірусу шляхом застосування спеціальних програм і технічних засобів охоплює:

- передачу будь-яким способом програм і технічних засобів іншим особам з метою використання для несанкціонованого доступу до машин, систем чи комп'ютерних мереж і спричинення таким чином перекручення або знищення комп'ютерної інформації чи її носіїв;
- введення таких засобів в АС на стадії її виготовлення, монтажу, розширення, ремонту, реалізації, користування;
- введення в АС таких засобів під час штатного (службового) чи санкціонованого користування;
- ознайомлення інших осіб з програмними і технічними засобами розповсюдження комп'ютерного вірусу та способами незаконного проникнення в машини, системи чи мережі.

Розповсюдження комп'ютерного вірусу як належне до формального складу злочину, вважається закінченим злочином зразу ж після того, як відбулася передача, закладка, введення програм і технічних засобів або ознайомлення інших осіб з програмними засобами які здатні спричинити перекручення або знищення комп'ютерної інформації.

Даний злочин вважається *вчиненим повторно*, якщо його скоїла особа, яка раніше вчиняла який-небудь із злочинів, передбачених ч.1 або 2 ст. 361 КК, незалежно від того, чи була раніше засуджена за вчинений злочин.

Суб'єктом цих злочинів може бути будь-яка фізична осудна особа, яка досягла 16-річного віку. У першу чергу це ті особи, яких власник або

уповноважена ним особа чи розпорядник АС призначили обслуговувати АС, а також і сторонні особи.

Що ж до розповсюдників комп'ютерного вірусу, то ними, перш за все, виступають розробники програмних і технічних засобів проникнення до АС (хакери), здатні спричинити перекручення або знищення комп'ютерної інформації чи її носіїв, виготовлювачі цих програм і засобів, а також інші особи.

Суб'єктивна сторона злочинів, передбачених ч.1 ст. 361-363 характеризується умислом щодо вчинюваних злочинцем дій, а психічне його ставлення до наслідків може характеризуватися прямим чи непрямим умислом або необережністю:

- прямий умисел про незаконному втручанні в роботу АС, яке призвело до перекручення чи знищення комп'ютерної інформації, є неявним, коли метою втручання було перекручення чи знищення комп'ютерної інформації;
- непрямий умисел щодо наслідків при незаконному втручанні в роботу АС матиме місце тоді, коли метою втручання було здійснення доступу до інформації для незаконного ознайомлення з нею (державна чи інша таємниця, комерційна таємниця, конфіденційні відомості, розголошення яких може заподіяти шкоду державі, фізичним і юридичним особам), в результаті чого відбулося спотворення чи знищення комп'ютерної інформації, про можливість чого зловмисник був прекрасно обізнаний, свідомо це допускав, хоча і не бажав;
- незаконне втручання в роботу автоматизованої системи за обставин, викладених в попередньому варіанті ситуації, але коли злочинець, маючи, на його думку, засоби і методи несанкціонованого зняття інформації, які не повинні були б призвести до перекручення чи знищення інформації, все ж спричиняє шкідливі наслідки, його психічне ставлення до них характеризується необережністю у одному з її видів;
- розповсюдження комп'ютерного вірусу характеризується лише прямим умислом, оскільки у цьому злочині суб'єктивну сторону визначає психічне ставлення суб'єкта лише до вчинюваних ним дій;
- прямий умисел щодо викрадення, привласнення чи вимагання комп'ютерної інформації;
- непрямий умисел чи необережність щодо наслідків істотного порушення експлуатації АС.

Незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж може бути способом вчинення інших злочинів, а саме: диверсії (ст. 113), шпигунства (ст. 114), шахрайства (ст. 190), виготовлення, збуту та використання підроблених недержавних паспортів (ст. 224) тощо. Дії винного в таких випадках кваліфікуються за сукупністю злочинів за однією з названих чи інших статей та ст. 361.

4.3. Види комп'ютерних злочинів у галузях економіки України

Для України найбільш відомими і характерними є комп’ютерні злочини у галузі економіки. Зафіксовано непоодинокі випадки вчинення правопорушень *у сфері кредитно-банківської системи,* коли зловмисники здійснювали спроби формування фіктивних електронних платежів з метою отримання незаконним шляхом коштів у регіональних відділеннях банків України.

Також зафіксовані спроби *несанкціонованого доступу до комп'ютерної мережі банків шляхом втручання в їх роботу і вчинення шахрайства, зловживання службовим становищем, службове підроблення документів.*

Нерідко, не маючи реальної наявності коштів на кореспондентських і субкореспондентських рахунках, при мінімальних кредитних залишках на кореспондентських рахунках, до проведення за дебетом подаються у електронному вигляді розрахунково-платіжні документи на значні загальні суми, чим допускається *несанкціонована емісія грошових коштів.*

Виявлено низку спроб *використання банківсько-кредитних технологій* та комп'ютерних інформаційних технологій для незаконного передавання через електронну систему платежів з використанням розрахунків у Національному банку України до комерційних банків в Україні та за кордон.

Встановлено факти втручання в електронну банківську систему з метою *крадіжки грошей із застосуванням електронних платежів, у тому числі за допомогою пластикових кредитних та дебіторських карток.*

За роки існування системи електронних платежів, яка розроблена Національним банком України, неодноразово робились *спроби зламу* її – несанкціонованого проникнення через подолання комп'ютерних систем технічного захисту за допомогою комп'ютерних програм. Правоохоронними органами спільно з управлінням захисту інформації Департаменту інформації Національного банку України та іншими його структурами виявлено та ліквідовано більше 30 організованих злочинних угруповань, які спеціалізувалися на крадіжках грошей у банківській сфері.

Правоохоронні органи України неодноразово припиняли діяльність груп, які займалися *незаконною конвертацією безготівкових коштів в готівку іноземною валютою, у тому числі з використанням офшорних компаній.*

До валютних операцій залучені українські та іноземні фірми, здебільшого офшорні компанії, зареєстровані на підставних осіб. За допомогою комп'ютерних технологій зловмисники перераховують безготівкові кошти через українські банки на рахунки підставних фірм. Після цього гроші переводяться у валюту-готівку. Частина цих коштів

повертаються в Україну, а частина залишається за кордоном. Як правило, злочинні організації такого виду досить розгалужені регіонально.

За допомогою *несанкціонованого отримання паролів доступу* та інших засобів ідентифікації законних користувачів до захищених технічними засобами комп'ютерних систем у мережі Інтернет робляться спроби отримати доступ до комп'ютерних інформаційних баз, переважно державних відомств з метою крадіжки інформації шляхом її копіювання або знищення.

Мають місце випадки, коли правопорушники проникають до приміщень обчислювальних центрів комерційних та державних установ з метою викрадення (зняття копії) інформації та технологій її обробки. Нерідко викрадають не всю комп'ютерну техніку у потерпілих організаціях, а вилучають з комп'ютерів вінчестери чи дискети, на яких міститься комп'ютерна інформація.

Дуже поширене *порушення авторських прав та права інтелектуальної власності* щодо володіння, розповсюдження та користування комп'ютерними продуктами ("комп'ютерне корсарство", "комп'ютерне піратство", "інтелектуальне електронне корсарство"). За даними Союзу боротьби з розкраданнями програмного продукту (Business Software Alliance (BSA)), Україна визнана неконтрольованою територією, де 95% комп'ютерних програм експлуатуються без дозволу законних власників.

За даними міжнародних організацій Україна в результаті "компютерного корсарства" щорічно несе збитки близько 30 мільйонів американських доларів через несплату податків.

Високий рівень "інтелектуального електронного корсарства" є серйозною перешкодою для вступу України до Світової організації торгівлі, європейських структур, міждержавних регіональних економічних організацій та двосторонніх міждержавних економічних відносин.

4.4. Організована комп'ютерна злочинність

Комп'ютерна злочинність тісно пов'язана з різними видами організованої злочинності та корупції. Зокрема, "відмивання" грошей зі злочинами у сфері застосування комп'ютерних технологій, що є частково непомітним виміром організованої злочинності.

За експертними оцінками на міжнародному рівні щорічно в світі "відмивається" 300-500 мільярдів доларів (з яких 30-40% походить від наркотиків, а решта як прибуток від фіксальних порушень, контрабанди зброєю, тероризму, шахрайства).

Організована кіберзлочинність посідає провідне місце поряд з наркобізнесом та торгівлею зброєю.

Комп’ютерну злочинність за територіальними ознаками умовно поділяють на (рис. 12):

Рис. 12. Види комп’ютерної злочинності за територіальними ознаками

- *національну* – в межах державних кордонів України;
- *транскордонну (транснаціональна, міжнародна);*
- *глобальну* – без обмежень у просторі і часі, у тому числі у всесвітніх мережах комп’ютерної телекомунікації;
- *континентальну* – у межах окремих континентів;
- *регіональну (локальну)* – між окремими країнами чи групами країн.

Розвиток глобальних систем телекомунікації сприяє розвитку такого економічного явища як електронної торгівлі (*е-комерція*). Не знаходиться поза цим процесом і Україна. Домінуюче місце в цьому явищі займає розвиток міжнародних валютних розрахунків за допомогою пластикових розрахункових карток, на зразок VISA. Організовані транскордонні злочинні формування також активно освоюють цей сегмент економічних відносин для організації злочинного бізнесу: підробки розрахункових пластикових карток, шахрайства з банкоматами тощо.

На міжнародному рівні Україна віднесена до країн, де найвищий рівень *порушення прав та права інтелектуальної власності на комп’ютерні програмні продукти (організоване “комп'ютерне піратство“).*

Нелегальна індустрія комп'ютерних програмних продуктів в Україні, за експертними оцінками, має рівень регіону Східної Європи з найвищим показником, зокрема щодо комп’ютерних програм (в середньому – майже 80%).

Організоване комп'ютерне піратство призводить до:

- руйнування національної індустрії комп'ютерних програмних

продуктів;

- знецінення престижу фахівців-виробників комп'ютерних програмних продуктів, зменшення їх рівня матеріального забезпечення;
- розвитку тіньової економіки у сфері виробництва комп'ютерних програмних продуктів;
- ухилення від сплати податків;
- відтік висококваліфікованих кадрів у сфері комп'ютерної індустрії за кордон.

4.5. Хакерський рух – база організованої злочинності

Значного поширення з розвитку глобалізації інформатизації суспільства набуває таке соціальне явище, як хакерський рух – формування корпорацій осіб, одержимих знаннями до комп'ютерних технологій. Зафіксовані непоодинокі випадки коли організовані злочинні формування використовують учасників цього руху для вчинення комп'ютерних злочинів. За експертними оцінками хакерський рух, окремі його представники є базою для комп'ютерної злочинності.

Хакери (одержимі комп'ютерні програмісти) проводять міжнародні, у тому числі всесвітні, зльоті, з'їзди (Ізраїль, Росія та інші країни). Мета хакерського руху – показати справжнє обличчя хакера: "Вони не ті люди, які зламують комп'ютери. Ті хто це робить – крекери... Хакери – це ті люди, які трудяться для того, щоб інші робили комп'ютерні програми краще". Як свідчать дослідження, межі між хакером незловмисником і крекером (хакером зловмисником) знайти майже неможливо. Нерідко "хакери-одиночки" чи їх спільноти, не розуміючи своєї ролі, виконують замовлення кримінальних угруповань.

Як правило, хакери – прекрасні знавці інформаційної техніки, які мають неординарні здібності, тому для них не є проблемою маніпулювання комп'ютерними системами на відстані; вони несанкціоновано перекачують тексти і протоколи з World Wide Web на сайті комп'ютера жертви, блокують обслуговування (DDOS-атака) тощо. Пошкодити кабель зв'язку і несанкціоновано приєднатися до комп'ютерної мережі, вгадати пароль входу до комп'ютера, змінити атрибути файлів у автоматизованій базі даних, стерти зашифрований файл, замінити числа у бухгалтерській звітності – все це досить просто для хакера, які б досконалі технічні та програмні замки не створювали винахідники. Девіз хакерів: "Що створено руками одних, з часом буде зламано руками інших, особливо якщо за це взятися громадою".

За оцінками експертів, загальна кількість атак хакерів на комп'ютерні робочі місця і загальні втрати від цих атак постійно зростають.

Слід зазначити, що в Україні зростання хакерського руху відповідає світовій тенденції. За останніми узагальненими неофіційними (оперативними) даними хакери в Україні, Росії та інших країнах

колишнього Радянського Союзу об’єднані в регіональні групи, мають свої електроні засоби інформації (газети, журнали, електронні дошки об'яв в Інтернеті). Вони проводять електронні конференції, мають свій словник жаргонів, який постійно поповнюється і поширюється за допомогою комп'ютерних бюлетенів, що містять всі необхідні відомості для “підвищення майстерності” початківців – методики проникнення в конкретні системи і способи зламу комп'ютерних програмних систем захисту.

Українські та російські хакери і крекери тісно контактують зі своїми колегами з інших країн, співпрацюють з ними, обмінюються досвідом, широко використовуючи для цього канали глобальних телекомунікаційних мереж (Інтернет).

Умовою формування і розвитку хакерського руху в Україні є високий рівень безробіття серед випускників вищих технічних закладів освіти, де викладають поглиблені знання з комп’ютерного програмування.

Однією з причин хакерського руху, а також витоку висококваліфікованих кадрів за кордон експерти визначають невідповідність орієнтації при масовій підготовці спеціалістів у вищих навчальних технічних закладах сучасним суспільним ринковим відносинам. При дослідженні української системи підготовки фахівців у сфері комп’ютерної індустрії з’ясовано, що здебільшого у вищих закладах освіти їх готують як виконавців, найманих працівників, а не підприємців. Тобто їх вчать продавати себе у найм, а не на ринкових засадах результати своєї інтелектуальної праці. Вітчизняна вища технічна школа мало приділяє уваги наданню знань підприємницькій діяльності та правовій підготовці. Вона готує фахівців-виконавців, які зорієнтовані на те, що їм держава, підприємці (у тому числі іноземні) повинні створити умови для праці.

4.6. Латентність комп’ютерної злочинності

За експертними оцінками, багато комп’ютерних злочинів не виявляють або про них не повідомляють потерпілі. Друга, зокрема, є одним із головних факторів, що зумовлюють високий рівень латентності цього виду злочинів. За оцінками фахівців, біля 90% комп'ютерних злочинів поки що залишається поза увагою правоохоронних органів держави.

Достовірні дані збитків від комп’ютерної злочинності визначити важко – ні зловмисники, ні потерпілі не намагаються надавати їм гласності за певних обставин. Одні – через можливу відповідальність за вчинене, а інші – через страх втрати іміджу, ділової репутації тощо. Це також пояснює високий рівень латентності правопорушень і брак про них відомостей у засобах масової інформації. На думку експертів, до широкої громадськості доходить лише 1% від всіх випадків виявлених порушень,

що звичайно мають кримінальний характер і приховати які стало неможливо.

Існує також професійний психологічний феномен, зокрема серед працівників технічного захисту інформації в автоматизованих системах. У цих службах штат працівників сформований переважно з асів, які мають технічну освіту, в тому числі програмістів-математиків. Нерідко ці фахівці не те, що не володіють відповідними навичками, але й теоретично не знають, як правильно документувати порушника та кваліфікувати його дії, в які правоохоронні органи слід звертатися в разі виявлення порушення. Це зумовлено тим, що в більшості технічних вузів, юридична підготовка, як правило, обмежується лише однією юридичною навчальною дисципліною – "Основи права".

З точки зору когнітології, через недостатню правову підготовку так звані "технарі" відчувають певний технократичний психологічний "комплекс", тобто переконані, що вирішити питання комп'ютерної злочинності можна тільки за допомогою технічних і програмно-математичних засобів. Більшість з них не беруть до уваги прописної істини, що всі інженерно-технічні засоби захисту АС, які створені одними людьми, з часом, при бажанні або потребі, обов'язково будуть зруйновані чи подолані іншими. Адже недарма в народі кажуть, що на одного умільця, який створить новий замок, знайдеться багато таких, котрі знайдуть декілька способів його відкрити чи зламати.

Проблема латентності також значною мірою пов'язана з об'єктивними і суб'єктивними можливостями правоохоронних органів. Незважена політика держави щодо скорочення штатів правоохоронних органів, переорієнтація їх на нові прояви злочинності, низький рівень матеріального забезпечення спричиняють відтік висококваліфікованих кадрів.

Причиною високого рівня латентності комп'ютерної злочинності в Україні також є те, що правоохоронні органи не можуть забезпечити відповідну реакцію на постійно зростаючий обсяг оперативної інформації про комп'ютерні злочини, яку вони мають у повному обсязі опрацювати. Чим більші ресурсні обмеження, тим більший обсяг сигналів про злочини система правоохоронних органів змушена від себе відштовхувати, залишаючи їх у "латентній тіні". Дослідження різних країн на рівні статистичної закономірності свідчать, що зростання злочинності на 2-3% в свою чергу , збільшує кількість ухилення порушників від відповідальності.

Характерною ознакою латентності комп'ютерної злочинності є таке явище. Нерідко, зафіксувавши спробу проникнення в базу даних державного відомства, при зверненні відповідних правоохоронних органів, провайдери, які обслуговують українських абонентів у мережі Інтернет, на прохання знайти і зафіксувати порушника, обмежуються відключенням абонента від мережі... Тим самим приховуються правопорушення від обліку та вжиття заходів щодо притягнення винних до відповідальності.

Як свідчить практика, нерозкриті вчасно злочини формують у порушників відчуття безкарності та можливості для вчинення повторних правопорушень. Зустрівши опір технічної системи захисту проти несанкціонованого проникнення, вони шукають нових знань і шляхів отримання інформацій, в тому числі щодо можливостей подолання технічного захисту і не втратять нагоди скористатися нею.

У законодавстві України передбачається покарання за приховування злочинів. У разі викриття прихованого правопорушення, особливо такого, коли досягнута протиправна мета, відповідальність має покладатися і на тих, хто приховав факт вчинення такого злочину. Зазначені положення особливо актуальні для захисту АС, які мають юридичний статус права держаної власності. Відповідальність за приховування та недонесення за окремі злочини передбачена Кримінальним кодексом України.

Слід ще раз наголосити, що професійні амбіції "технарів" мусять бути чітко узгоджені з суспільними потребами. Саме для цього існує державне (публічне) право: конституційне, адміністративне, цивільне, трудове і кримінальне.

Комп'ютерна злочинність – це соціальне явище, якому можна протистояти тільки спільними зусиллями – громадою, спільним розумом фахівців-науковців і практиків різних галузей знань.

4.7. Збитки від міжнародної комп'ютерної злочинності

Згідно з даними Комісії з попередження злочинності та кримінального права Організації Об'єднаних Націй щорічний економічний збиток від комп'ютерних злочинів, за оцінками експертів, обчислюється мільярдами доларів США.

У сфері електронної торгівлі із застосуванням пластикових карток, за даними міжнародних фінансових організацій, з 1998-1999 роки спостерігається зростання правопорушень приблизно на 54%. Тільки втрати VISA по Україні оцінюються у сумі 1459,842 мільйонів доларів США за 1999-2000 роки.

Дослідження свідчать, що тільки обсяг операцій у разі електронного передавання валюти вказує на те, що потенційні втрати значно вищі, ніж при тих же самих операціях з використанням паперових документів. Втрати ж окремо взятої держави в таких випадках за лічені хвилини можуть досягати дуже значних розмірів, якщо держави не будуть вживати упереджувальних заходів.

Збитки виробників комп'ютерних програмних продуктів внаслідок порушення авторського права та інших прав інтелектуальної власності щодо комп'ютерного програмного забезпечення щорічно становлять близько 11 млрд. доларів США.

Загальні об’єктивні збитки в Україні обрахувати неможливо через брак офіційних методик їх обчислень та таких показників державної статистики. Проте є підстави вважати, що невизначеність стосовно протидії економічній кіберзлочинності – одна із головних причин повільного економічного зростання національного багатства України.

Контрольні питання

1. Охарактеризуйте поняття злочину.
2. Наведіть класифікацію злочинів за ступенями тяжкості.
3. Розкажіть про етапи розвитку злочинної діяльності.
4. Дайте характеристику злочинів у сфері використання електронно-обчислювальних систем та комп’ютерних мереж.
5. Охарактеризуйте предмети злочинного посягання.
6. Поясніть суть об’єктивної сторони злочинів.
7. Розкрийте суть суб’єктивної сторони комп'ютерних злочинів.
8. Опишіть види комп’ютерних злочинів у галузях економіки України.
9. Наведіть класифікацію комп'ютерних злочинів за територіальними ознаками.
10. Охарактеризуйте види організованої комп’ютерної злочинності.
11. Опишіть суть міжнародного хакерського руху.
12. Розкрийте причини виникнення та розвитку хакерського руху в Україні.
13. Поясніть суть латентності комп’ютерної злочинності.
14. Опишіть причини зростання латентності кіберзлочинів.
15. Охарактеризуйте заходи боротьби з ростом латентності комп'ютерних злочинів.
16. Наведіть класифікацію збитків від міжнародної комп’ютерної злочинності.

Глава 5. Нормативно-правові аспекти захисту інформації

5.1. Загальні положення

На сьогоднішній день інформація відіграє ключову роль у функціонуванні суспільних і державних інститутів, а також у житті кожної людини. Ефект, який досягається за рахунок упровадження інформаційних технологій, зростає при збільшенні масштабів обробки інформації, включаючи обчислювальні машини та автоматизовані системи управління.

Дослідження українського законодавства в сфері інформаційних технологій, констатує, що нормативне забезпечення цієї галузі має невисокий загальний рівень розробленості.

Як позитивне, слід, насамперед, зазначити визнання державою права власності на інформацію. Тому відповідно до ст. 41 Конституції інформація є предметом державної охорони, яка забезпечується Законом України "Про інформацію", Законом України "Про захист інформації в автоматизованих системах" та ст. 361-363 Кримінального Кодексу України. Крім цих документів до нормативно-правової бази, яка регулює інформаційні правовідносини, належать.

Положення про Державний комітет України з питань державних секретів та технічного захисту інформації. Затверджено Указом Президента України від 05.11.96р. № 1047\96.

Положенням визначено основні завдання Держкомсекретів України, його обов'язки та права щодо реалізації Державної політики у сфері забезпечення охорони державної таємниці та технічного захисту інформації у межах, встановлених законами України, а також щодо координації режимно-секретної діяльності та функціонування системи технічного захисту інформації центральних і місцевих органів виконавчої влади, підприємств, установ і організацій всіх форм власності, дипломатичних представництв та інших об'єктів України за кордоном.

Положення про технічний захист в Україні. Затверджено постановою Кабінету Міністрів України від 09.09.94р. № 632.

Положення визначає об'єкт захисту та мету технічного захисту інформації (ТЗІ), структуру та основні завдання складових частин системи ТЗІ, порядок та організацію комплексного технічного захисту інформації з обмеженим доступом на об'єктах різного призначення і організацію контролю за ефективністю ТЗІ.

Постанова Кабінету Міністрів України від 13.01.95р. № 24 "Про заходи щодо виконання постанови Верховної Ради України від 05.07.94р.

№80", "Про введення в дію Закону України "Про захист інформації в автоматизованих системах"" та статті 34 Закону України "Про Державну таємницю".

Цією постановою також схвалена "Програма робіт з організації стандартизації та сертифікації в галузі технічного захисту інформації на 1995-1998 роки".

Положення про порядок видачі суб'єктам підприємницької діяльності спеціальних дозволів (ліцензій) на здійснення окремих видів діяльності. Затверджено постановою Кабінету Міністрів України від 17.05.94р. № 316.

Положення визначає види діяльності, на які передбачено законодавчими актами України видачу спеціальних дозволів (ліцензій), в тому числі виробництво та сервісне обслуговування систем і засобів виконання робіт, надання послуг, що забезпечують технічний захист інформації. Положення також визначає умови і правила одержання ліцензій.

Інструкція щодо умов і правил здійснення діяльності у галузі технічного захисту інформації та контролю за її дотриманням. Затверджено наказом ДСТЗІ від 26.05.94р. № 46, зареєстровано в Мінюсті України 01.06.94р. №120\329.

Інструкція визначає умови і правила здійснення діяльності у галузі ТЗІ з виробництва та сервісного обслуговування систем і засобів, виконання робіт, надання послуг, що забезпечують технічний захист інформації.

Положення про порядок опрацювання, прийняття, перегляду та скасування міжвідомчих нормативних документів системи технічного перегляду та скасування міжвідомчих нормативних документів системи технічного захисту інформації. Затверджено наказом ДСТЗІ від 01.07.96р. № 44, зареєстровано в Мінюсті України 18.07.96р. № 366\1391.

Положення визначає порядок розроблення, погодження, затвердження, реєстрацію та виконання нових, перегляду та скасування чинних міжвідомчих нормативних документів технічного характеру (норми, методики, положення, інструкції тощо) системи технічного захисту інформації, що не належать до нормативних документів із стандартизації, але є обов'язковими для виконання всіма центральними місцевими органами виконавчої влади, Урядом Автономної Республіки Крим, органами місцевого самоврядування, військовими частинами всіх військових формувань, створених відповідно до законодавства, підприємствами, установами й організаціями незалежно від форм власності, діяльність яких пов'язана з технічним захистом інформації.

5.2. Стандартизація в галузі захисту інформації

Жодне суспільство не може існувати без технічного законодавства

та нормативних документів, які регламентують правила, процеси, методи виготовлення і контролю якості товарів, робіт та послуг, а також гарантують безпеку життя, здоров'я і майна людей та навколишнього середовища. Стандартизація якраз і є тією діяльністю, яка виконує ці функції.

Стандартизація – діяльність, що полягає у встановленні положень для загального і багаторазового застосування щодо наявних чи можливих завдань з метою досягнення оптимального ступеня впорядкування у певній сфері, результатом якої є підвищення ступеня відповідності продукції, процесів та послуг їх функціональному призначенню, усуненню бар'єрів у торгівлі і сприянню науково-технічному співробітництву.

Відносини, пов'язані з діяльністю у сфері стандартизації та застосування її результатів, регулюються Законом України "Про стандартизацію" від 17.05.01р. № 2408-III. Цей Закон встановлює правові та організаційні засади стандартизації в Україні і спрямований на забезпечення єдиної технічної політики у цій сфері.

Об'єктом стандартизації є продукція, процеси та послуги, зокрема матеріали, складники, обладнання, системи, їх сумісність, правила, процедури, функції, методи чи діяльність.

Метою стандартизації в Україні є забезпечення безпеки життя та здоров'я людини, тварин, рослин, а також майна та охорони довкілля, створення умов для раціонального використання всіх видів національних ресурсів та відповідності об'єктів стандартизації своєму призначенню, сприяння усуненню технічних бар'єрів у торгівлі.

Державна політика у сфері стандартизації базується на таких принципах:

- забезпечення участі фізичних і юридичних осіб в розробленні стандартів та у вільному виборі ними видів стандартів при виробництві чи постачанні продукції;
- відкритості та прозорості процедур розроблення і прийняття стандартів з урахуванням інтересів усіх заінтересованих сторін, підвищення конкурентоспроможності продукції вітчизняних виробників;
- доступності стандартів та інформації щодо них для користувачів;
- відповідності стандартів законодавству;
- адаптації до сучасних досягнень науки і техніки з урахуванням стану національної економіки;
- пріоритетності прямого впровадження в Україні міжнародних та регіональних стандартів;
- дотриманні міжнародних та європейських правил і процедур стандартизації;
- участі у міжнародній (регіональній) стандартизації.

Суб'єктами стандартизації є:

- центральний орган виконавчої влади у сфері стандартизації;
- рада стандартизації;

- інші суб’єкти, що займаються стандартизацією.

Залежно від рівня суб’єкта стандартизації, який приймає чи схвалює стандарти, розрізняють:

- національні стандарти, кодекси усталеної практики та класифікатори, прийняті чи схвалені центральним органом виконавчої влади у сфері стандартизації, видані ним каталоги та реєстри загальнодержавного застосування;

- стандарти, кодекси усталеної практики та технічні умови, прийняті чи схвалені іншими суб’єктами, що займаються стандартизацією.

Застосування стандартів чи їх окремих положень є обов’язковим:

- для всіх суб’єктів господарювання, якщо це передбачено в технічних регламентах чи інших нормативно-правових актах;

- для учасників угоди (контракту) щодо розроблення, виготовлення чи постачання продукції, якщо в ній (ньому) є посилання на певні стандарти;

- для виробника чи постачальника продукції, якщо він склав декларацію про відповідність продукції певним стандартам чи застосував позначення цих стандартів у її маркуванні;

- для виробника чи постачальника, якщо його продукція сертифікована щодо дотримання вимог стандартів.

Міжнародні (регіональні) стандарти та стандарти інших країн, якщо їх вимоги не суперечать законодавству України, можуть бути застосовані в Україні в установленому порядку шляхом посилання на них у національних та інших стандартах.

До загальнодержавних нормативних актів з питань захисту інформації відносяться:

Державний стандарт України. ***ДСТУ 3396.0-96.*** *Захист інформації. Технічний захист інформації. Основні поняття.* Затверджено наказом Держстандарту України від 11.10.96р. № 423, введено в дію 01.01.97р.

Стандарт установлює об’єкт захисту, мету, основні організаційно-технічні поняття технічного захисту інформації (ТЗІ), неправомірний доступ до якої може завдати шкоди громадянам, організаціям (юридичним особам) та державі, а також етапи побудови системи захисту інформації та категорії нормативних документів з ТЗІ.

Вимоги стандарту обов’язкові для підприємств та установ усіх форм власності та підпорядкування, громадян – суб’єктів підприємницької діяльності, органів державної влади, органів місцевого самоврядування, військових частин всіх формувань, представництв України за кордоном, які володіють, користуються та розпоряджаються інформацією, що підлягає технічному захисту.

Метою ТЗІ є запобігання витоку чи порушення цілісності інформації з обмеженим доступом.

Технічний захист інформації здійснюється поетапно:

1 етап – визначення й аналіз загроз;

2 етап – розробка системи захисту інформації;

3 етап – реалізація плану захисту інформації;

4 етап – контроль функціонування та керування системою захисту інформації.

Нормативні документи розробляються в ході проведення комплексу робіт із стандартизації та нормування у галузі ТЗІ. Вони поділяються на (рис. 13):

- нормативні документи із стандартизації в галузі технічного захисту інформації;

- державні стандарти та прирівняні до них нормативні документи;

- нормативні акти міжвідомчого значення, що регулюються у Міністерстві юстиції України;

- нормативні документи міжвідомчого значення технічного характеру, що реєструються органом, уповноваженим Кабінетом Міністрів України;

- нормативні документи відомчого значення органів державної влади та органів місцевого самоврядування.

Державний стандарт України. ***ДСТУ 3396.1-96.*** *Захист інформації. Технічний захист інформації. Порядок проведення робіт.* Затверджено наказом Держстандарту України від 19.12.96р. № 51, введено в дію 01.01.97р.

Рис. 13. Класифікація нормативних документів з технічного захисту інформації

Цей стандарт установлює вимоги до порядку проведення робіт з

технічного захисту інформації, який за наказом керівника підприємства передбачає:

- організацію проведення обстеження;
- організацію розроблення системи захисту інформації;
- реалізацію організаційних заходів захисту;
- реалізацію первинних технічних заходів захисту;
- реалізацію основних технічних заходів захисту;
- прийняття, визначення повноти та якості робіт.

Для участі в роботах, подання методичної допомоги, оцінювання повноти та якості реалізації заходів захисту можуть залучатися спеціалісти з ТЗІ сторонніх організацій, які мають ліцензію органу, уповноваженого Кабінетом Міністрів України.

Державний стандарт України. ***ДСТУ 3396.2-97.*** *Захист інформації. Технічний захист інформації. Терміни та визначення.* Затверджено наказом Держстандарту України від 11.04.97р. № 200, введено в дію 01.01.98р.

Цей стандарт установлює терміни та визначення понять у сфері технічного захисту інформації.

Терміни, регламентовані у цьому стандарті, обов'язкові для використання в усіх видах організаційної та нормативної документації, а також для робіт зі стандартизації і рекомендовані для використання у довідковій та навчально-методичній літературі, що належить до сфери технічного захисту інформації.

Терміни стандарту є обов'язковими для використання підприємствами та установами усіх форм власності і підпорядкування, громадянами – суб'єктами підприємницької діяльності, міністерствами (відомствами), центральними і місцевими органами державної виконавчої влади, військовими частинами всіх військових формувань, представництвами України за кордоном, які володіють, використовують та розпоряджаються інформацією, що становить державну чи іншу передбачену законом таємницю або є конфіденційною інформацією, яка належить державі.

ДСТУ 1.3-93. *Порядок розроблення, побудови, оформлення, узгодження, затвердження, позначення та реєстрації технічних умов.* Затверджено та введено в дію наказом Держстандарту України від 29.07.93 р. № 116.

Стандарт установлює порядок розроблення, побудови, викладу, оформлення, узгодження, затвердження, позначання та державної реєстрації технічних умов на продукцію (послуги), що виготовляються в усіх галузях народного господарства України, крім розроблюваної та виготовленої на замовлення Міністерства оборони, а також змін до них.

Вимоги цього стандарту є обов'язковими для підприємств, установ і організацій, що діють на території України, а також для громадян – суб'єктів підприємницької діяльності незалежно від форм власності і видів діяльності.

Державні будівельні норми України. **ДБН А.2.2-2-96.** Проектування. Технічний захист інформації. Загальні вимоги до організації проектування та документації для будівництва. Затверджено наказом Держкоммістобудування України від 02.09.96 р. № 156 і введено в дію 01.01.97р.

Стандарт установлює норми та вимоги до організації проектування, проектної документації для нового будівництва, розширення, реконструкції підприємств та капітального ремонту будівель і споруд об'єктів, де є необхідність проведення робіт з ТЗІ. Заходи з ТЗІ можуть виконуватися організаціями, які мають відповідні ліцензії Держкоммістобудування України або іншими організаціями, які мають ліцензії Держкомсекретів України відповідно до завдання замовника. Положення норм обов'язкові для застосування суб'єктами інвестиційної діяльності України та представництвами України за кордоном при виконанні проектних та будівельних робіт з урахуванням вимог технічного захисту інформації, які містять відомості, що становлять державну або іншу передбачену законодавством України таємницю, а також конфіденційну інформацію, що є державною власністю.

Норми можуть бути використані суб'єктами, професійна діяльність яких пов'язана з захистом конфіденційної інформації, що не є власністю держави.

Керівний нормативний документ. ***КНД 50-009-93.*** *Типова побудова технічних умов. Методичні вказівки.* Затверджено та введено в дію наказом Держстандарту України від 29.07.93р. № 116.

Керівний нормативний документ зі стандартизації поширюється на методи та зміст робіт із розроблення технічних умов, правила викладу їхніх розділів. Положення цього керівного нормативного документа можуть використовуватись підприємствами, установами і організаціями, що діють на території України, а також громадяни – суб'єктами підприємницької діяльності незалежно від форм власності і видів діяльності.

Тимчасові рекомендації з технічного захисту інформації у засобах обчислювальної техніки, автоматизованих системах і мережах від витоку каналами побічних електромагнітних випромінювань і наводок ***(ТР ЕОТ-95).*** Нормативний документ системи ТЗІ затверджено наказом ДСТЗІ від 09.06.96р. № 25.

Тимчасові рекомендації щодо розроблення розділу із захисту інформації в технічному завданні на створення автоматизованої системи ***(ТРАС-96).*** Нормативний документ системи ТЗІ затверджено наказом ДСТЗІ від 03.07.96р. № 47.

Правила побудови, викладення, оформлення та позначення нормативних документів системи ***ТЗІ.НД ТЗІ*** *1.6-001-96.* Нормативний документ системи ТЗІ затверджено наказом ДСТЗІ від 26.07.96р. № 51.

Інструкція про порядок надання дозволу на використання імпортних

засобів ТЗІ а також продукції, яка містить їх у своєму складі. Нормативний документ системи ТЗІ затверджено наказом ДСТЗІ від 31.05.95р. № 13 і зареєстровано в Мінюсті України 12.07.95р. № 215\751.

На цей час більшу частину нормативно-технічних документів (НТД) ТЗІ в Україні складають НТД Держтехкомісії (ДТК) колишнього СРСР, які рекомендовані до використання керівним листом ДСТЗІ від 01.03.94р. На основі Постанови Верховної Ради України № 1545-12 від 12.09.91р. "Про порядок тимчасової дії на території України окремих актів законодавства Союзу РСР".

До загальнодержавних нормативних актів з питань захисту інформації треба додати *відомчі накази та інструкцію МВС України.*

Цю інструкцію розроблено відповідно до вимог законів України "Про державну таємницю", "Про захист інформації в автоматизованих системах", затверджених Кабінетом Міністрів України положень "Про державного експерта з питань таємниць", "Про порядок і умови надання органам державної виконавчої влади, підприємствам, установам і організаціям дозволу (ліцензії) на здійснення діяльності, пов'язаної з державною таємницею, та про особливий режим цієї діяльності", "Про технічний захист інформації в Україні", "Про режимно-секретні органи в міністерствах, відомствах, Уряді Автономної Республіки Крим, місцевих органах виконавчої влади, виконкомах Рад, на підприємствах, в установах і організаціях", "Про Держкомітет України з питань державних секретів та технічного захисту інформації", інших чинних нормативних актів з питань захисту державних секретів. Вона визначає режим секретності, є основним керівним документом, обов'язковим для виконання в МВС України, головних управліннях МВС України в Криму, в місті Києві та Севастополі, управліннях МВС України в областях і на транспорті, міських, районних та лінійних управліннях, міськрайфінорганах, установах виконання покарань, навчальних закладах, науково-дослідних установах, інших підрозділах системи МВС України, діяльність яких пов'язана з державною таємницею.

5.3. Сертифікація захищеності інформаційних технологій

У всіх сферах суспільного життя використання інформаційних систем (ІС) постійно зростає. Така тенденція підвищує вимоги до безпеки застосовуваних інформаційних технологій.

В сучасних умовах уже не тільки функціональні можливості ІС, але і їх захищеність стали для користувача важливим критерієм вибору. Ступінь захищеності ІС визначається у процесі тестування і оцінювання їх компонентів за обов'язковими критеріями незацікавленими організаціями.

Під сертифікацією продукції за вимогами безпеки інформації розуміється комплекс організаційно-технічних заходів, у результаті яких за допомогою спеціального документа-сертифіката і знака відповідності з

визначеним ступенем вірогідності підтверджується, що продукція відповідає вимогам стандартів з безпеки інформації чи інших нормативно-технічних документів.

При сертифікації можуть підтверджуватися як окремі характеристики, так і увесь комплекс характеристик продукції, зв'язаних з забезпеченням безпеки інформації, зокрема технічних, програмно-технічних, програмних засобів, систем, мереж обчислювальної техніки і зв'язку, засобів захисту і засобів контролю ефективності захисту за вимогами безпеки інформації.

При сертифікації продукції підтверджуються вимоги до захисту інформації:

- від несанкціонованого доступу (дії), у тому числі від комп'ютерних вірусів;
- шляхом криптографічних перетворень;
- від витоку за рахунок побічних електромагнітних випромінювань і наведень (ПЕМВІН) чи від дій на неї спеціальних пристроїв, влаштованих у технічні засоби.

Мета сертифікації – зробити захищеність ІС очевидною і порівняною так, щоб з однієї сторони, надати користувачам деталізовану інформацію і допомогу при виборі системи, а з іншої – дати зацікавленим виготовлювачам підтвердження якості їх продукції.

Умовою видачі сертифіката на продукції служить її відповідність вимогам встановлених стандартів чи нормативних документів.

Сертифікат безпеки свідчить про якості захищеної техніки. Вони такі:

- *достовірність ефективності захисту* – досягається точним описом захисних функцій продукту в зв'язку з характерними загрозами і наявністю оцінки ступеня стійкості механізмів захисту проти цих загроз;
- *надійність* – досягається тестуванням всіх аспектів безпеки при розробці, виробництві, постачанні і застосуванні продуктів у відповідності з Європейськими критеріями безпеки інформаційних технологій (ITSEC);
- *коректність застосування* – досягається точним описом порядку і області застосування продукту, описуються також слабкі місця і рекомендації щодо запобігання негативних наслідків.

Наведемо приблизний перелік продукції, процесів і послуг, що підлягають сертифікації на відповідність вимогам забезпечення безпеки компонентів ІС.

1. Засоби і процеси фізичного (об'єктового) захисту інформаційних систем:

- технічні засоби контролю доступу на об'єкт системи обчислювальної техніки (СОТ);
- процедура встановлення доступу на об'єкт СОТ;
- сертифікація екранованих приміщень спеціального призначення;
- сертифікація систем енергопостачання комп'ютерних систем і

об’єктів;

- технічні засоби виявлення на об’єктах активних джерел електромагнітного випромінювання;
- системи просторового зашумлення і їх елементи;
- системи лінійного зашумлення і їх елементи;
- перешкодозаглушувальні фільтри у мережах живлення, зв’язку і сигналізації;
- спеціальні фільтри і пристрої захисту проводових ліній зв’язку;
- технічні засоби виявлення несанкціонованого під’єднання до ліній зв’язку комп’ютерних систем.

2. Технічні засоби ІС:

- засоби обчислювальної техніки загального призначення;
- захищені засоби обчислювальної техніки;
- засоби зв’язку і периферійні пристрої;
- локальні обчислювальні мережі.

3. Системи комплексного захисту інформації в ІС:

- сертифікація класифікованого рівня захищеності наявних і проектованих систем;
- процедури забезпечення достатності систем захисту;
- процедури забезпечення безперервного захисту інформації.

4. Захист комп’ютерних систем від витоку інформації каналами ПЕМВІН:

- захищеність СОТ загального призначення і периферійних пристроїв від витоку інформації ПЕМВІН;
- відповідність захищеності СОТ нормативним рівнем ПЕМВІН;
- відповідність несучих конструкцій і елементної бази СОТ необхідним рівнем ПЕМВІН;
- відповідність рівнів ПЕМВІН СОТ вимогам стандартів;
- відповідність засобів передачі інформації в комп’ютерних системах необхідним рівнем ПЕМВІН;
- відповідність СОТ вимогам відсутності влаштованих засобів розвідки і руйнувань.

5. Захист від несанкціонованого доступу (НСД):

- програмні, апаратні та програмно-апаратні засоби захисту від НСД;
- програмні та апаратні засоби криптографічного захисту інформації в СОТ загального призначення;
- програмні засоби антивірусного захисту в СОТ і обчислювальних мережах;
- процедури встановлення розмежування і контролю доступу в СОТ і обчислювальних мережах;
- відповідність програмного забезпечення комп’ютерних систем вимогам відсутності програмних засобів розвідки і руйнування інформації.

Даний перелік продукції при проведенні акредитації органу сертифікації може бути уточнений і розширений у відповідності з

можливостями організації і конкретними умовами.

Обов'язковій сертифікації за вимогами безпеки інформації підлягають засоби і системи обчислювальної техніки і зв'язку, призначені для обробки (передачі) секретної (конфіденційної) інформації, для використання в управлінні екологічно небезпечними об'єктами, озброєнням і воєнною технікою, а також засоби захисту і контролю ефективності захисту такої інформації.

Ліцензування у галузі захисту інформації

Окремими видами діяльності суб'єкти господарювання можуть займатися тільки на підставі спеціального дозволу (ліцензії), виданого уповноваженим органом з питань ліцензування.

Ліцензія – документ державного зразка, який засвідчує право ліцензіата на провадження зазначеного в ньому виду господарської діяльності протягом визначеного строку за умови виконання ліцензійних умов.

Ліцензійні умови – установлений з урахуванням вимог законів вичерпний перелік організаційних, кваліфікаційних та інших спеціальних вимог, обов'язкових для виконання при провадженні видів господарської діяльності, що підлягають ліцензуванню.

Ліцензування – видача, переоформлення та анулювання ліцензій, видача дублікатів ліцензій, ведення ліцензійних справ та ліцензійних реєстрів, контроль за додержанням ліцензіатами ліцензійних умов, видача розпоряджень про усунення ліцензійних умов, а також розпоряджень про усунення порушень законодавства у сфері ліцензування.

Основними принципами державної політики у сфері ліцензування є:

- забезпечення рівності, законних інтересів усіх суб'єктів господарювання;
- захист прав, законних інтересів, життя та здоров'я громадян, захист навколишнього природного середовища та забезпечення безпеки держави;
- встановлення єдиного переліку видів господарської діяльності, що підлягають ліцензуванню;
- встановлення єдиного порядку ліцензування видів господарської діяльності на території України.

Ліцензування не може використовуватись для обмеження конкуренції у провадженні господарської діяльності.

Ліцензування у сфері захисту інформації проводиться з метою:

- забезпечення ефективності систем і засобів захисту інформації;
- обмеження монополізму і розвитку конкуренції;
- створення рівних умов для розвитку господарської діяльності в галузі захисту інформації;
- сприяння становленню сучасного ринку послуг, його захист від

недобросовісних послуг у галузі захисту інформації;

- забезпечення надання послуг за встановленими рівнями якості;
- забезпечення використання сертифікованих та дозволених до використання засобів захисту інформації;
- забезпечення доступності послуг.

Перелік видів діяльності, що підлягають ліцензуванню, а також порядок одержання дозволу (ліцензії) для здійснення такої діяльності встановлюється ***Законом України "Про ліцензування певних видів господарської діяльності"*** від 1 червня 2000р. № 1775-III (зі змінами і доповненнями станом на 01.01.2004р.).

Відповідно до цього Закону у галузі захисту інформації ліцензуванню підлягають:

- розроблення, виготовлення спеціальних засобів для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації, торгівля спеціальними технічними засобами для зняття інформації з каналів зв'язку, інших засобів негласного отримання інформації;
- розроблення, виробництво, використання, експлуатація, сертифікаційні випробування, тематичні дослідження, експертиза, ввезення, вивезення криптосхем і засобів криптографічного захисту інформації, надання послуг в галузі криптографічного захисту інформації, торгівля криптосистемами і засобами криптографічного захисту інформації;
- розроблення, виробництво, впровадження, сертифікаційні випробування, ввезення, вивезення голографічних захисних елементів;
- розроблення, виробництво, впровадження, обслуговування, дослідження ефективності систем і засобів технічного захисту інформації, надання послуг з технічного захисту інформації;
- виготовлення бланків цінних паперів, документів суворої звітності.

Наказом Державного комітету України з питань регуляторної політики та підприємництва, Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України № 89/67 від 29.12.2000р. затверджено: *"Ліцензійні умови проведення господарської діяльності, пов'язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів технічного захисту інформації, наданням послуг у галузі технічного захисту"*.

Ліцензійні умови визначають кваліфікаційні, організаційні, технологічні та інші вимоги до суб'єктів господарювання, виконання яких є обов'язковими для виконавців робіт та надання певних видів послуг у межах господарської діяльності, пов'язаної з розробленням, виробництвом, впровадженням, обслуговуванням, дослідженням ефективності систем і засобів у галузі технічного захисту інформації.

Об'єкт господарювання, який має намір провадити певний вид

господарської діяльності, що ліцензується, особисто або через упроваджений ним орган чи особу, звертається до відповідного органу ліцензування із заявою встановленого зразка про видачу ліцензії.

У *заяві про видачу ліцензії повинні міститися такі дані:*

1) відомості про суб'єкта господарювання – заявника:

- найменування, місцезнаходження, банківські реквізити, ідентифікаційний код – для юридичних осіб;

- прізвище, ім'я, по батькові, паспортні дані (серія, номер паспорта, ким і коли виданий, місце проживання), ідентифікаційний номер фізичної особи-платника податків та інших обов'язкових платежів – для фізичної особи;

2) вид господарської діяльності, на провадження якого заявник має намір одержати ліцензію.

До заяви про видачу ліцензії додається копія свідоцтва про державну реєстрацію суб'єкта підприємницької діяльності або копія довідки про внесення до єдиного державного реєстру підприємств та організацій України, засвідчена нотаріально або органом, який видав оригінал документа.

Контрольні питання

1. Охарактеризуйте загальні положення з питань захисту інформації.
2. Поясніть суть положень державних органів з питань технічного захисту інформації.
3. Дайте визначення стандартизації, об'єктів та суб'єктів стандартизації.
4. Розкажіть про принципи державної політики у сфері стандартизації.
5. Наведіть класифікацію стандартів за рівнем суб'єктів стандартизації.
6. Опишіть завдання, вимоги та мету державного стандарту України ДСТУ 3396.0-96.
7. Наведіть класифікацію нормативних документів з технічного захисту інформації.
8. Поясніть суть вимог до порядку проведення робіт з технічного захисту інформації.
9. Розкажіть про вимоги, встановлені ДСТУ 3396.2-97, до застосування термінів з технічного захисту інформації.
10. Поясніть суть основних положень державних будівельних норм України ДБН А.2.2-2-96.
11. Наведіть класифікацію тимчасових рекомендацій з технічного захисту інформації.
12. Дайте визначення сертифікації продукції за вимогами безпеки ін-

формації.

13. Наведіть перелік продукції, процесів і послуг, що підлягають сертифікації.

14. Перерахуйте засоби і процеси фізичного захисту інформаційних систем, що підлягають сертифікації.

15. Наведіть перелік технічних засобів ІС та систем комплексного захисту інформації в ІС, що підлягають сертифікації.

16. Опишіть послуги із захисту комп'ютерних систем від витоку інформації каналами ПЕМВІН, що підлягають сертифікації.

17. Перерахуйте заходи і засоби захисту від несанкціонованого доступу, що підлягають сертифікації.

18. Дайте означення основних термінів ліцензування.

19. Наведіть класифікацію основних принципів державної політики у сфері ліцензування.

20. Обґрунтуйте необхідність ліцензування окремих видів діяльності в галузі захисту інформації.

21. Охарактеризуйте основні нормативно-правові документи з ліцензування певних видів господарської діяльності.

Глава 6. Відповідальність за порушення законодавства про інформацію

6.1. Види юридичної відповідальності

Юридична відповідальність – це міра покарання правопорушника шляхом позбавлення його певних соціальних благ або цінностей, які йому належали від імені держави і суспільства, на підставі чинного законодавства з метою попередження правопорушень з боку самого правопорушника та інших осіб і відновлення втрачених прав або відшкодування шкоди.

Правопорушення – це суспільно небезпечне або шкідливе, протиправне, винне діяння (дія або бездіяльність) деліктоздатної (або осудної) особи, яке передбачене чинним законодавством і за яке встановлена юридична відповідальність. Всі правопорушення поділяються на кримінальні злочини(передбачені кримінальним кодексом) і проступки: адміністративні, дисциплінарні, цивільні, земельні, екологічні, конституційні, процесуальні, господарські(економічні) та ін.

Основними видами юридичної відповідальності є (рис. 14): дисциплінарна, адміністративна, цивільно-правова, кримінальна відповідальність.

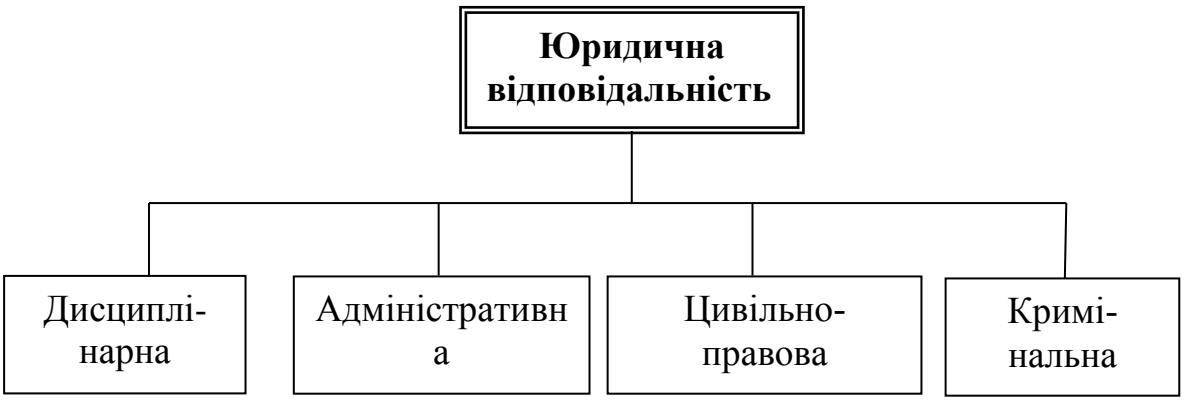

Рис. 14. Основні види юридичної відповідальності

Під ***дисциплінарною відповідальністю*** розуміється обов'язок працівника відповісти перед власником підприємства, установи, організації або уповноваженим ним органом за скоєний дисциплінарний проступок і понести ті стягнення, які вказані у дисциплінарних санкціях трудового права. Дисциплінарний проступок, будучи підставою дисциплінарної відповідальності, являє собою винне протиправне порушення трудових обов'язків працівниками, за скоєння якого може бути вжито заходів дисциплінарного або громадського впливу.

За *ст. 147 Кодексу законів про працю України за порушення трудової дисципліни до працівника можна застосувати тільки одну з таких мір стягнення: догана, звільнення. Законодавством, статутами і положеннями про дисципліну можуть бути передбачені для окремих категорій працівників й інші дисциплінарні стягнення* (пониження у посаді, зниження кваліфікаційного класу, переведення на роботу з нижчою оплатою тощо).

Адміністративна відповідальність – це міра державного примусу, яка виражається в позбавленні певних соціальних благ правопорушника за адміністративний проступок, який передбачений законодавством про адміністративні правопорушення.

За адміністративне правопорушення можуть застосовуватись такі види адміністративних стягнень:

- *офіційне попередження*, яке фіксується установленим способом або виноситься в письмовій формі;

- *штраф* – грошове стягнення, яке накладається на порушників за адміністративне правопорушення в розмірах і у випадках, встановлених кодексом про адміністративні правопорушення і законами України;

- *оплатне вилучення предмета*, який став знаряддям вчинення або безпосереднім об'єктом адміністративного правопорушення;

- *конфіскація предмета*, який належав власнику і став знаряддям вчинення або безпосереднім об'єктом адміністративного правопорушення – полягає в примусовій безоплатній передачі цього предмета у власність держави;

- *позбавлення спеціального права*, наданого даному громадянинові (права керування транспортними засобами, права полювання);

- *виправні роботи* – застосовується судом на строк до 2 місяців за місцем постійної роботи особи і з відрахуванням до 20% її заробітку в доход держави;

- *адміністративний арешт* – до 15 діб у виняткових випадках за окремі види правопорушень.

Цивільно-правова відповідальність – це такий вид юридичної відповідальності, яка наступає за невиконання або неналежне виконання зобов'язань(договорів), передбачена в чинному законодавстві і конкретною угодою сторін (боржника і кредитора), що не суперечить чинному законодавству.

До мір відповідальності відносять покладення обов'язку відшкодування збитків, сплату неустойки, позбавлення порушника суб'єктивного права тощо.

Кримінальна відповідальність – це вид юридичної відповідальності, яка встановлена кримінальним законодавством як негативна оцінка і кара як особливий вид державного примусу, який має публічний характер, у формі вироку до особи, яка винна у вчиненні злочину.

6.2. Поняття кримінальної відповідальності за Кримінальним кодексом України

Таким чином, кримінальна відповідальність за своїм змістом є карою. *Покарання – це така міра примусу, яка застосовується лише судом, у певній формі і в таких видах, які передбачені в санкціях кримінального законодавства.*

Відповідно до ст. 51 КК України передбачається лише *види кримінальних покарань* до осіб, визнаних винними у вчиненні злочину (рис. 15):

- штраф;
- позбавлення військового, спеціального звання, рангу, чину або кваліфікаційного класу;
- позбавлення права обіймати певні посади або займатися певною діяльністю;
- громадські роботи;
- виправні роботи;

- службові обмеження для військовослужбовців;
- конфіскація майна;
- арешт;
- обмеження волі;
- тримання в дисциплінарному батальйоні військовослужбовців;
- позбавлення волі на певний строк;
- довічне позбавлення волі.

Штраф – це грошове стягнення, що накладається судом у випадках і межах, встановлених в Особливій частині КК України.

Позбавлення військового, спеціального звання, рангу, чину або кваліфікаційного класу – засуджена за тяжкий чи особливо тяжкий злочин особа, яка має військове чи спеціальне звання, ранг, чин або кваліфікаційний клас, може бути позбавлена за вироком суду цього звання, рангу, чину або кваліфікаційного класу.

Позбавлення права обіймати певні посади або займатися певною діяльністю – може бути призначене як основне покарання на строк від 2 до 5 років або як додаткове покарання на строк від 1 до 3 років і в тому випадку, якщо воно непередбачено в санкції статті Особливої частини КК України.

Громадські роботи – полягають у виконанні засудженими у вільний від роботи чи навчання час безоплатних суспільно корисних робіт, вид яких визначають органи місцевого самоврядування. Громадські роботи

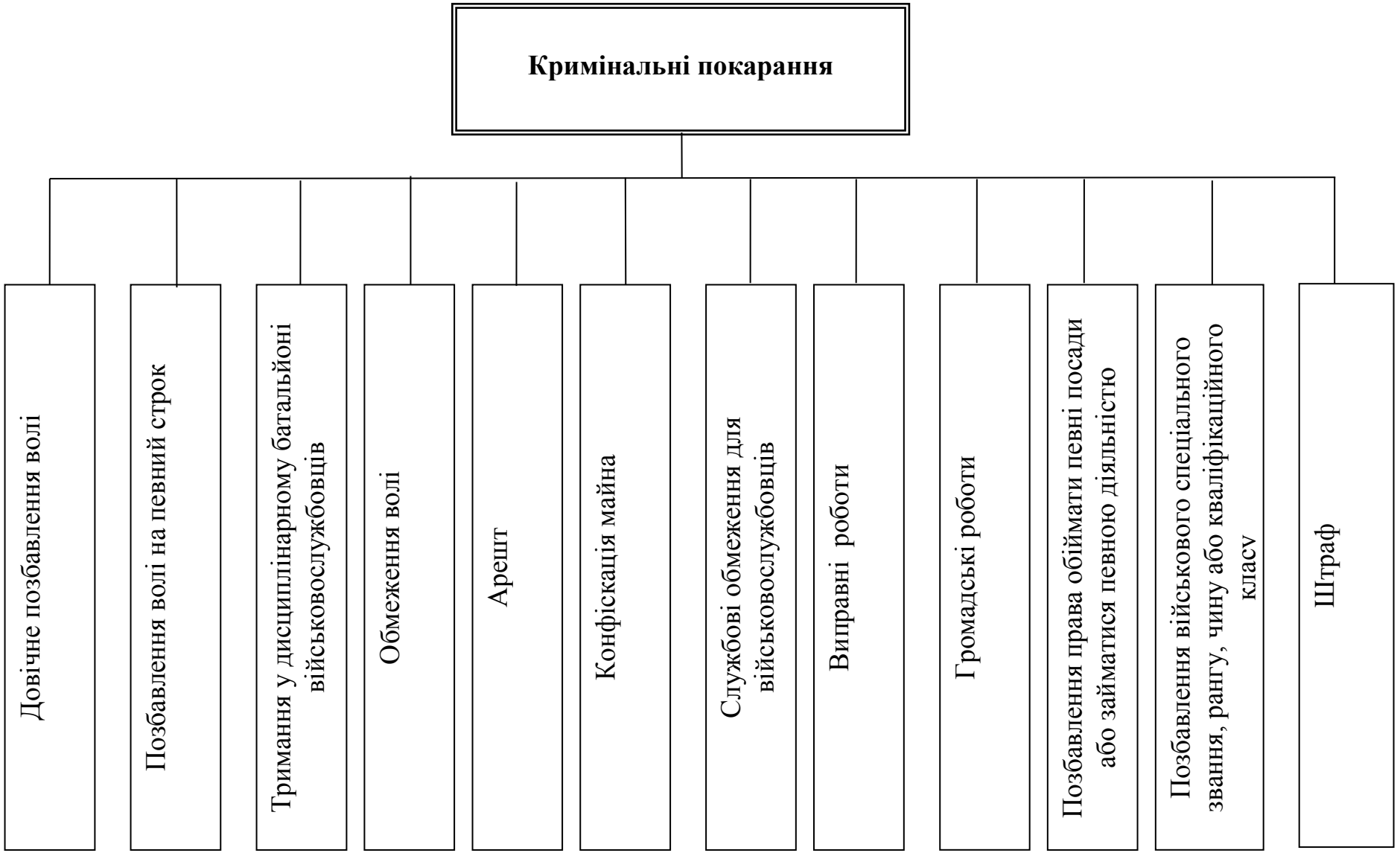

Рис. 15. Види кримінальних покарань

встановлюються на строк від шістдесяти до двохсот сорока годин і відбуваються не більше як чотири години на день. Громадські роботи не призначаються особам, визнаних інвалідами першої або другої групи, вагітним жінкам, особам, які досягли пенсійного віку, а також військовослужбовцям строкової служби.

Виправні роботи – встановлюються на строк від 6 місяців до 2 років і відбуваються за місцем роботи засудженого з вирахуванням в дохід держави від 10 до 20 відсотків зарплати. Виправні роботи не застосовуються до вагітних жінок, жінок, які перебувають у відпустці по догляду за дитиною, до непрацездатних, до осіб, які не досягли 16 років, до пенсіонерів тощо.

Службове обмеження для військовослужбовців – застосовується до засуджених військовослужбовців, крім військовослужбовців строкової служби, на строк від 6 місяців до 2 років у випадках, передбачених КК України або замість обмеження волі чи позбавлення волі враховуючи обставини справи. Під час відбуття цього покарання проводиться відрахування в дохід державі від 10 до 20 відсотків із суми грошового забезпечення. В цей час засуджений не може бути підвищений на посаді, у військовому званні, строк покарання не зараховується йому в строк вислуги років для присвоєння чергового військового звання.

Конфіскація майна – це покарання полягає в примусовому безоплатному вилученні у власність держави всього або частини майна, яке є власністю засудженого. Конфіскація майна встановлюється за тяжкі та особливо тяжкі корисливі злочини і може бути призначена лише у випадках, прямо передбачених в Особливій частині КК України.

Перелік майна, що не підлягає конфіскації, визначається законом України.

Арешт – це такий вид покарання, який полягає в триманні засудженого в умовах ізоляції встановлюється на строк від 1 до 6 місяців. Військовослужбовці відбувають арешт на гауптвахті. Арешт не застосовується до осіб віком до 16 років, вагітних жінок та до жінок, які мають дітей віком до 8 років.

Обмеження волі – цей вид покарання полягає в триманні особи в кримінально-виконавчих установахого типу без ізо без ізоляції від суспільства в умовах здійснення за нею нагляду з обов'язковим залученням засудженого до праці. Обмеження волі встановлюється на строк від 1 до 5 років. Це поке застосовується до неповнолітніх, вагітних жінок і жінок, які мають дітей вікомей віком до 14 років, до пенсіонерів, військовослужбовців строкової служби та до інвалідів першої і другої груп.

Тримання в дисциплінарному батальйоні військовослужбовців – призначається військовослужбовцям строкової служби на строк від 6 місяців до 2 років або замість позбавлення волі на строк не більше 2 років.

Позбавлення волі на певний строк – полягає в ізоляції засудженого та поміщення його на певний строк (від 1 до 15 років) у кримінально-виконавчі установи.

Довічне позбавлення волі – встановлюється за вчинення особливо тяжких злочинів і застосовується лише у випадках, спеціально передбачених КК, якщо суд не вважає за можливе застосувати позбавлення волі на певний строк. Цей вид покарання не застосовується до осіб, що вчинили злочин у віці до 18 років, і до осіб віком понад 65 років, а також до жінок, що були в стані вагітності під час вчинення злочину або на момент винесення вироку.

Основними покараннями є громадські роботи, виправні роботи, службові обмеження для військовослужбовців, арешт, обмеження волі, тримання в дисциплінарному батальйоні військовослужбовців, позбавлення волі на певний строк, довічне позбавлення волі. Додатковими покараннями є позбавлення військового, спеціального звання, рангу, чину або кваліфікаційного класу та конфіскація майна. Штраф та позбавлення права обіймати певні посади або займатися певною діяльністю можуть бути як основними, так і додатковими покараннями.

За один злочин може бути призначене лише одне основне покарання, передбачене в санкції статті Особливої частини КК України. До основного покарання може бути приєднане одне чи декілька додаткових покарань у випадках та порядку, передбачених кримінальним кодексом. Кримінальні покарання можуть призначатися лише за вироком суду. Ухилення від покарання, призначеного вироком суду, несе відповідальність, передбачену статтями 389 та 390 КК України.

6.3. Відповідальність за інформаційні правопорушення

Юридична відповідальність в Україні за правопорушення у сфері інформаційних відносин передбачається такими нормативними актами:

- Закон України „Про інформацію”;
- Закон України „Про державну таємницю”;
- Закон України „Про авторське право”;
- Закон України „Про науково-технічну інформацію”;
- Закон України „Про захист інформації в автоматизованих системах”;
- Кримінальний кодекс України.

Стаття 47. Відповідальність за порушення законодавства про інформацію Закону України „Про інформацію” визначає, що порушення законодавства України „Про інформацію” тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно з законодавством України.

Відповідальність за порушення законодавства про інформацію несуть особи, винні у вчиненні таких порушень:

- необґрунтована відмова від надання відповідної інформації;
- несвоєчасне подання інформації;
- навмисне приховування інформації;
- примушення до поширення або перешкоджання поширення певної інформації, а також цензура;
- поширення відомостей, що не відповідають дійсності, ганьблять честь і гідність особи;
- безпідставна відмова від поширення певної інформації;
- використання і поширення інформації стосовно особистого життя громадянина без його згоди особою, яка є власником відповідної інформації внаслідок виконання своїх службових обов'язків;
- розголошення державної або іншої таємниці, що охороняється законом, особою, яка повинна охороняти цю таємницю;
- порушення порядку зберігання інформації;
- навмисне знищення інформації;
- необґрунтоване віднесення окремих видів інформації до категорії відомостей з обмеженим доступом.

У Законі України „Про державну таємницю" (ст. 1) зазначається, що *державна таємниця* – секретна інформація – вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим законом, державною таємницею і підлягають охороні державою.

Стаття 39. Відповідальність за порушення законодавства про державну таємницю.

Посадові особи та громадяни винні у:

- розголошенні державної таємниці;
- втраті документів та інших матеріальних носіїв секретної інформації;
- недодержанні встановленого законодавством порядку передачі державної таємниці іншій державі чи міжнародній організації;
- засекречуванні інформації, зазначеної у частинах третій і четвертій статті 8 цього закону;
- навмисному віднесенні до державної таємниці інформації, розголошення якої може завдати шкоди інтересам національної безпеки України, а також необґрунтованому заниженні ступеня секретності або необґрунтованому розсекречуванні секретної інформації;
- безпідставному засекречуванні інформації;

- наданні грифа секретності матеріальним носіям конфіденційної або іншої таємної інформації, яка не становить державної таємниці, або ненаданні грифа секретності матеріальним носіям інформації, що становить державну таємницю, а також безпідставному скасуванні чи зниженні грифа секретності матеріальних носіїв секретної інформації;

- порушенні встановленого законодавством порядку надання допуску та доступу до державної таємниці;

- порушенні встановленого законодавством режиму секретності та невиконанні обов'язків щодо збереження державної таємниці;

- невжитті заходів щодо забезпечення охорони державної таємниці та незабезпеченні контролю за охороною державної таємниці;

- провадженні діяльності, пов'язаної з державною таємницею, без одержання в установленому порядку спеціального дозволу на провадження такої діяльності, а також розміщенні державних замовлень на виконання робіт, доведення мобілізаційних завдань, пов'язаних з державною таємницею в органах державної влади, органах місцевого самоврядування, на підприємствах, установах, організаціях, якщо не надано спеціального дозволу на проводження діяльності пов'язаної з державною таємницею;

- недодержанні вимог законодавства щодо забезпечення охорони державної таємниці під час здійснення міжнародного співробітництва, прийому іноземних делегацій, груп, окремих іноземців та осіб без громадянства і проведення роботи з ними;

- невиконанні норм і вимог технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення цілісності цієї інформації або просочування її технічними каналами, – несуть дисциплінарну, адміністративну та кримінальну відповідальність згідно з законом.

Стаття 19. Відповідальність за порушення законодавства України про науково-технічну інформацію визначає, що порушення законодавства України про технічну інформацію тягне за собою відповідальність згідно з чинним законодавством.

Стаття 17. Відповідальність за порушення порядку і правил захисту інформації.

Особи, винні в порушенні порядку і правил захисту оброблюваної в АС інформації, несуть дисциплінарну, адміністративну, кримінальну чи матеріальну відповідальність згідно з чинним законодавством України.

Стаття 52. Способи цивільно-правового захисту авторського права і суміжних прав.

1. При порушеннях будь-якою особою авторського права і (або) суміжних прав, недотриманні передбачених договором умов використання творів і (або) об'єктів суміжних прав, використанні творів і об'єктів суміжних прав з обходом технічних засобів захисту чи з підробленням

інформації і (або) документів про управління правами чи створенні загрози неправомірного використання об'єктів авторського права і (або) суміжних прав та інших порушеннях особистих немайнових прав і майнових прав суб'єктів авторського права і (або) суміжних прав мають право звернутися до суду з позовом про поновлення прав та відшкодування збитків (матеріальної шкоди) та моральної (немайнової) шкоди.

2. Суд має право постановити рішення чи ухвалу про:

а) відшкодування моральної (немайнової) шкоди, завданої порушенням авторського права і (або) суміжних прав з визначенням розміру відшкодування;

б) відшкодування збитків, завданих порушенням авторського права і (або) суміжних прав;

в) стягнення з порушника авторського права і (або) суміжних прав доходу, отриманого внаслідок порушення;

г) виплату компенсації, що визначається судом, від 10 до 50000 мінімальних заробітних плат, замість відшкодування збитків або стягнення доходу;

д) заборону опублікування творів, їх виконань чи постановок, випуску примірників фонограм, відеограм, їх сповіщення, припинення їх розповсюдження, вилучення (конфіскацію) контрафактних примірників творів, фонограм, відеограм чи програм мовлення та обладнання і матеріалів, призначених для їх виготовлення і відтворення, публікацію у пресі інформації про допущене порушення тощо, якщо у ході судового розгляду буде доведено факт порушення авторського права і (або) суміжних прав або факт наявності дій, що створюють загрозу порушення цих прав;

е) вимагати від осіб, які порушують авторське право і (або) суміжні права, і інформацію про третіх осіб, задіяних у виробництві та розповсюдженні контрафактних примірників творів та об'єктів суміжних прав, засобів обходу технічних засобів та про канали розповсюдження.

У главі XVI Кримінального Кодексу України „Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж" передбачаються такі види юридичної відповідальності.

1. Незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, їх систем чи мереж, що призвело до перекручення чи знищення комп'ютерної інформації або носіїв такої інформації, а також розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в ці машини, системи чи комп'ютерні мережі та здатних спричинити перекручення чи знищення комп'ютерної інформації, чи носіїв такої інформації (ст. 361) – караються штрафом до 70 неоподаткованих мінімальних доходів громадян,

або виправними роботами на строк до двох років, або обмеженням волі на той самий строк.

2. Ті самі дії (п.1), якщо вони заподіяли істотну шкоду або вчинені повторно чи за попередньою змовою групою осіб, – *караються обмеженням волі на строк до п'яти років або позбавленням волі на строк від трьох до п'яти років.*

3. Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовою особою своїм службовим становищем (ст. 362) – *караються штрафом від п'ятдесяти до двохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років.*

4. Ті самі дії (п.3), вчинені повторно або за попередньою змовою групою осіб, – *караються штрафом від ста до чотирьохсот неоподатковуваних мінімумів громадян або обмеженням волі на строк до трьох років, або позбавленням волі на такий же самий строк.*

5. Дії, передбачені п.п.3 і 4, якщо вони заподіяли істотну шкоду, – *караються позбавленням волі на строк від двох до п'яти років.*

6. Порушення правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж особою, яка відповідає за їх експлуатацію, якщо це спричинило викрадення, перекручення чи знищення комп'ютерної інформації або істотне порушення роботи таких машин, їх систем чи комп'ютерних мереж (ст. 363),– *карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або позбавлення права обіймати певні посади чи займатися певною діяльністю на строк до п'яти років, або виправними роботами на строк до двох років.*

7. Те саме діяння (п.6), якщо воно заподіяло істотну шкоду, – *карається штрафом до ста неоподаткованих мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на строк до п'яти років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.*

Якщо внаслідок порушення правил експлуатації АЕОМ, їх систем чи комп'ютерних мереж особою, яка відповідає за їх експлуатацію, матиме місце витік, викрадення, перекручення чи знищення комп'ютерної інформації або істотне порушення роботи АЕОМ, їх систем чи комп'ютерних мереж, то особи несуть юридичну відповідальність за ст. 362 та ст. 363 КК.

6.4. Цивільне законодавство щодо захисту інформації

Новий Цивільний кодекс України, прийнятий Верховною Радою 16 січня 2003 року і підписаний Президентом України 27 лютого, набрав

чинності з 1 січня 2004 року. Кодекс ґрунтується на принципово новій – ***приватноправовій*** – концепції регулювання особистих немайнових та майнових відносин (цивільних відносин), що засновані на юридичній рівності, вільному волевиявленні, майновій самостійності їх учасників в умовах переходу до ринкових відносин.

В статті 302 Цивільного кодексу закріплено за кожною фізичною особою право на інформацію, а саме :

- *фізична особа має право вільно збирати, зберігати, використовувати і поширювати інформацію. Збирання, зберігання, використовування і поширення інформації про особисте життя фізичної особи без її згоди не допускається, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Не допускається також збирання інформації, яка є державною таємницею або конфіденційною інформацією юридичної особи;*

- *фізична особа, яка поширює інформацію, зобов'язана переконатися в її достовірності;*

- *вважається, що інформація, яка надається посадовою, службовою особою при виконанні нею своїх обов'язків, а також інформація, яка міститься в офіційних джерелах (звіти, стенограми, повідомлення засобів масової інформації, засновниками яких є відповідні державні органи місцевого самоврядування), є достовірною. Фізична особа, яка поширює таку інформацію, не зобов'язана перевіряти її достовірність і не відповідає у разі її спростування.*

Під поняттям „інформація" слід розуміти документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі (ст. 1 Закону України „Про інформацію"). При цьому об'єктом даного права є всі види інформації, до яких відносять :

- статистичну інформацію;
- адміністративну інформацію (дані);
- масову інформацію;
- інформацію про діяльність державних органів влади та органів місцевого і регіонального самоврядування;
- правову інформацію;
- інформацію про особу;
- інформацію довідково-енциклопедичного характеру, соціологічну інформацію (ст. 18 Закону України „Про інформацію"), а також науково-технічну інформацію (ст. 1 Закону України „Про науково-технічну інформацію").

Право на інформацію полягає в можливості вільного збирання, використання поширення та зберігання відомостей, необхідних їм для реалізації ними своїх прав, свобод і законних інтересів, здійснення завдань і функцій.

Під поняттям „збирання інформації" слід розуміти надану законом можливість набуття, придбання, накопичення відповідно до чинного

законодавства України документованої або публічно оголошуваної інформації фізичними особами. Що стосується „зберігання інформації", то це повноваження включає в себе можливість забезпечення належного стану інформації та її матеріальних носіїв. Повноваження „використання інформації" означає, що фізична особа може задовольнити свої інформаційні потреби будь-яким незабороненим чинним законодавством способом. Терміном „поширення інформації" законодавець визначає можливість фізичної особи розповсюджувати, обнародувати, реалізовувати у встановленому законом порядку документовану або публічно оголошувану інформацію.

Проте здійснення фізичними особами права на інформацію не повинне порушувати громадянські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб.

Здійснення права на інформацію забезпечується цілою низкою гарантій, передбачених ст. 10 Закону України „Про інформацію":

- обов'язком органів державної влади, а також органів місцевого і регіонального самоврядування інформувати про свою діяльність та прийняті рішення;
- створенням у державних органах спеціальних служб або систем, що забезпечували б у встановленому порядку доступ до інформації;
- вільним доступом суб'єктів інформаційних відносин до статистичних даних, архівних, бібліотечних і музейних фондів. Обмеження цього доступу зумовлюється лише специфікою цінностей та особливими умовами їх зберігання, що визначається законодавством;
- створенням механізму здійснення права на інформацію;
- здійсненням державного контролю за додержанням законодавства про інформацію;
- встановленням відповідальності за порушення права на інформацію (ст. 49 Закону України „Про інформацію").

Статтею 418 Цивільного кодексу України визначається право інтелектуальної власності, а саме:

- *право інтелектуальної власності – це право особи на результат інтелектуальної, творчої діяльності або на інший об'єкт права інтелектуальної власності, визначений цим кодексом та іншим законом;*
- *право інтелектуальної власності становить особисті немайнові права інтелектуальної власності та (або) майнові права інтелектуальної власності, зміст яких щодо певних об'єктів права інтелектуальної власності визначається цим кодексом та іншим законом;*
- *право інтелектуальної власності є непорушним. Ніхто не може бути позбавленим права інтелектуальної власності чи обмежений у її здійсненні, крім випадків, передбачених законом.*

Можна назвати низку законів, що стосуються інтелектуальної власності. Основним з них є Конституція України, у ст. 41 якої передбачено, що кожен має

право володіти, користуватися і розпоряджатися результатами своєї інтелектуальної, творчої діяльності.

Початком становлення законодавства України про інтелектуальну власність є прийняття Закону України „Про власність" від 7 лютого 1991р., який містив спеціальний розділ VI „Право інтелектуальної власності". Починаючи з 1992р. Верховна Рада України прийняла пакет законів про інтелектуальну власність: закони України „Про охорону прав на сорти рослин", „Про охорону прав на винаходи і корисні моделі", „Про охорону прав на промислові зразки", „Про охорону прав на знаки для товарів і послуг", „Про авторське право і суміжні права", „Про державну таємницю", „Про наукову та науково-технічну експертизу", „Про науково-технічну інформацію", „Про охорону прав на топографії інтегральних схем" тощо.

За статтею 420 Цивільного кодексу об'єктами інтелектуальної власності є:

- *літературні та художні твори;*
- *комп'ютерні програми;*
- *компіляції даних (бази даних);*
- *виконання;*
- *фонограми, відеограми, передачі (програми) організацій мовлення;*
- *наукові відкриття;*
- *винаходи, корисні моделі, промислові зразки;*
- *компонування (топографії) інтегральних мікросхем;*
- *раціоналізаторські пропозиції;*
- *сорти рослин, породи тварин;*
- *комерційні (фірмові) найменування, торговельні марки (знаки для товарів і послуг), географічні позначення;*
- *комерційні таємниці.*

Наведений у ст. 420 перелік об'єктів права інтелектуальної власності певною мірою пов'язано з положеннями Стокгольмської Конвенції 1967р., згідно п. VIII ст.2 якої інтелектуальна власність включає права, що стосуються:

- літературних, художніх і наукових творів;
- виконавської діяльності артистів, звукозапису радіо і телевізійних передач;
- винаходів у всіх сферах людської діяльності;
- наукових відкриттів;
- промислових зразків;
- товарних знаків, знаків обслуговування, фірмових найменувань і комерційних позначень;
- захисту проти недобросовісної конкуренції.

Крім того, до об'єктів інтелектуальної власності Конвенція зараховує також усі інші права, що стосуються інтелектуальної діяльності у виробничій, науковій, літературній і художній сферах.

Стаття 421 кодексу визначає осіб, які можуть бути ***суб'єктами права інтелектуальної власності***. При цьому в ній розрізняються два види суб'єктів:

- творець (творці) об'єкта права інтелектуальної власності;

- інші особи, яким належать особисті немайнові та (або) майнові права інтелектуальної власності.

Цивільний кодекс передбачає дві групи захисту права інтелектуальної власності: загальні цивільно-правові засоби і спеціальні засоби захисту інтелектуальної власності. Ці засоби встановлюються статтею 432, в якій зазначається.

1. *Кожна особа має право звернутися до суду за захистом свого права інтелектуальної власності відповідно до статті 16 ЦК.*

2. *Суд у випадках та в порядку, встановлених законом, може постановити рішення, зокрема, про:*

- *застосування негайних заходів щодо запобігання порушенню права інтелектуальної власності та збереження відповідних доказів;*

- *зупинення пропуску через митний кордон України товарів, імпорт чи експорт яких здійснюється з порушенням права інтелектуальної власності;*

- *вилучення з цивільного обороту товарів, виготовлених або введених у цивільний оборот з права інтелектуальної власності;*

- *вилучення з цивільного обороту матеріалів та знарядь, які використовувалися переважно для виготовлення товарів з порушенням права інтелектуальної власності;*

- *застосування разового грошового стягнення замість відшкодування збитків за неправомірне використання об'єкта права інтелектуальної власності. Розмір стягнення визначається відповідно до закону з урахуванням вини особи та інших обставин, що мають істотне значення;*

- *опублікування в засобах масової інформації відомостей про порушення права інтелектуальної власності та зміст судового рішення щодо такого порушення.*

Слід звернути увагу на те, що з метою запобігання порушенню права інтелектуальної власності та збереження відповідних доказів суд має право:

- заборонити відповідачеві чи іншій особі вчинити певні дії;

- винести ухвалу про накладання арешту і вилучення всієї партії виробів товару, щодо яких припускається, що вони є контрфактними, а також матеріалів і обладнання, призначених для їх виготовлення і розповсюдження.

Якщо дії порушення права інтелектуальної власності мають ознаки злочину, за який передбачено кримінальну відповідальність, орган дізнання, слідства або суд зобов'язані вжити заходів для забезпечення вчиненого або можливого в майбутньому цивільного позову шляхом розшуку і накладення арешту на:

- вироби (товари), щодо яких припускається, що вони є контрфактами;

- матеріали та обладнання, призначенні для виготовлення і використання зазначених виробів (товарів);

- документи, рахунки та інші предмети, що можуть бути доказом вчинення дій, за які відповідно до чинного законодавства передбачено кримінальну відповідальність.

6.5. Регулювання господарських відносин у сфері захисту інформації

Визначення основних засад господарювання в Україні та регулювання господарських відносин, які виникають у процесі організації та здійснення господарської діяльності між суб'єктами господарювання, а також між цими суб'єктами та іншими учасниками відносин у сфері господарювання здійснюється на основі Господарського кодексу України, що набрав чинності з 1 січня 2004 року.

„Учасником відносин у сфері господарювання, – зазначено у ст. 2 Господарського кодексу, *– є суб'єкти господарювання, споживачі, органи державної влади та органи місцевого самоврядування, наділені господарською компетенцією, а також громадяни, громадські та інші організації, які виступають засновниками суб'єктів господарювання чи здійснюють щодо них організаційно-господарські повноваження на основі відносин власності."*

Для розуміння суті господарської діяльності як предмета регулювання Кодексом виділяються такі основні риси господарської діяльності, що мають бути присутні комплексно:

- діяльність суб'єктів господарювання за своїм економічним змістом є виготовленням і реалізацією продукції (виконання робіт, надання послуг), тобто здійснюється у виробничій сфері;
- продукт цієї діяльності має грошову оцінку (цінову визначеність), причому незалежно від того, чи є така діяльність підприємницькою.

В основу концепції Господарського кодексу України щодо суб'єктів відповідних правовідносин накладено постулат, що головним суб'єктом господарювання є господарська організація – підприємство, об'єднання підприємств. Так, за класифікацією Кодексу до суб'єктів господарювання належать:

- господарські організації – юридичні особи, створені відповідно до Цивільного кодексу України та інші юридичні особи, що здійснюють господарську діяльність та зареєстровані у встановленому порядку державні, комунальні та інші підприємства, створені на підставі Кодексу;
- громадяни України, іноземні особи без громадянства, які здійснюють господарську діяльність та зареєстровані відповідно до закону як підприємці;
- філіали, підприємства, інші відокремлені підрозділи господарських організацій, що створені ними для здійснення господарської діяльності і не мають статусу юридичної особи.

Регламентація захисту прав суб'єктів господарювання та споживачів наведена у ст. 20 Кодексу.

1. Держава забезпечує захист прав законних інтересів суб'єктів господарювання та споживачів.

2. Кожний суб'єкт господарювання та споживач має право на захист своїх прав і законних інтересів.

Права та законні інтереси зазначених суб'єктів захищаються шляхом:

- *визнання наявності або відсутності прав;*
- *визнання повністю або частково недійсними актів органів державної влади та органів місцевого самоврядування, актів інших суб'єктів, що суперечать законодавству, ущемляють права та законні інтереси суб'єкта господарювання або споживачів;*
- *визнання недійсними господарських угод з підстав, передбачених законом;*
- *відновлення становища, яке існувало до порушення прав та законних інтересів суб'єктів господарювання;*
- *припинення дій, що порушують право або створюють загрозу його порушення;*
- *присудження до виконання обов'язку в натурі;*
- *відшкодування збитків;*
- *застосування штрафних санкцій;*
- *застосування оперативно-господарських санкцій;*
- *застосування адміністративно-господарських санкцій;*
- *установлення, зміни і припинення господарських відносин;*
- *іншими способами, передбаченими законом.*

3. Порядок захисту прав суб'єктів господарювання та споживачів визначається цим Кодексом, іншими законами.

Регулювання господарського судочинства, визначення основних принципів діяльності судів при розгляді господарських спорів, гарантування захисту прав та інтересів усіх учасників судового процесу, забезпечення повного, всебічного та об'єктивного вирішення усіх спорів відповідно до закону регламентується Арбітражним (господарським) процесуальним кодексом України, чинним з 1 березня 1992 року.

Згідно ст.1 Кодексу право на звернення до господарського суду мають:

- підприємства, установи, організації, інші юридичні особи (у тому числі іноземні), громадяни, які здійснюють підприємницьку діяльність без створення юридичної особи і в установленому порядку набули статусу підприємницької діяльності;

- державні та інші органи, громадяни, що не є суб'єктами підприємницької діяльності, у випадках передбачених законодавчими актами України.

Відповідно до ст. 2 процесуальною формою такого звернення є позов, викладений у відповідній письмовій заяві, яка повинна відповідати встановленим вимогам.

Правом звернення з позовними заявами до арбітражного суду мають також прокурори для захисту інтересів державних органів, державних підприємств і організацій.

6.6. Адміністративне законодавство щодо захисту інформації

Адміністративне законодавство складається з Кодексу України про адміністративні правопорушення, прийнятого і введеного у дію 7 грудня 1984 року (з подальшими змінами та доповненнями) та інших законів України.

Завданням Кодексу є охорона прав і свобод громадян, власності конституційного ладу України, прав і законних інтересів підприємств, установ і організацій, встановлення правопорядку, зміцнення законності, запобігання правопорушенням, виховання громадян в дусі точного і неухильного додержання Конституції і законів України, поваги до прав, честі та гідності інших громадян, до правил співжиття, сумлінного виконання своїх обов'язків, відповідальності перед суспільством.

Адміністративним правопорушенням Кодексом (стаття 9) визначається протиправна, умисна чи необережна дія чи бездіяльність, яка посягає на громадський порядок, на встановлений порядок управління і за яку передбачено адміністративну відповідальність. Адміністративна відповідальність за правопорушення, передбачені цим Кодексом, настає, якщо ці порушення не тягнуть за собою відповідальність за Кримінальним кодексом.

Мірою відповідальності за адміністративні правопорушення *є* такі *адміністративні стягнення* (стаття 24):

- попередження;
- штраф;
- оплатне вилучення предмета, який став знаряддям вчинення або безпосереднім об'єктом адміністративного правопорушення;
- конфіскація предмета, який став знаряддям або безпосереднім об'єктом адміністративного правопорушення;
- стягнення грошей, одержаних внаслідок вчинення адміністративного правопорушення;
- позбавлення спеціального права, наданого даному громадянинові (права полювання, права керування транспортними засобами);
- виправні роботи;
- адміністративний арешт;

Обставинами, що обтяжують відповідальність за адміністративні правопорушення, згідно зі статтею 35 Кодексу, визначаються:

- продовження протиправної поведінки незважаючи на вимогу уповноважених на те осіб припинити її;
- повторне протягом року вчинення однорідного правопорушення, за яке особу вже було піддано адміністративному стягненню;
- вчинення правопорушення особою, яка раніше вчинила злочин;
- втягнення неповнолітнього в правопорушення;
- вчинення правопорушення групою осіб;
- вчинення правопорушення в умовах стихійного лиха або за інших надзвичайних ситуаціях;
- вчинення правопорушення в стані сп'яніння.

Найбільш важливими щодо захисту інформації в Кодексі України про адміністративні правопорушення є статті 51^2, 145, 146, 147, 148^2, 148^3, 148^4 та 212^2, які передбачають такі міри відповідальності:

- незаконне використання об'єкта права інтелектуальної власності (літературного чи друкованого твору, їх виконання, фонограми, передачі організації мовлення, комп'ютерної програми, бази даних, наукового відкриття, винаходу, корисної моделі, промислового зразка для товарів і послуг, топографії інтегральної мікросхеми, раціоналізаторської пропозиції, сорту рослин тощо), привласнення права на такий об'єкт або інше умисне порушення прав на об'єкт права інтелектуальної власності, що охороняється законом, – тягне за собою *накладання штрафу у розмірі від десяти до двохсот неоподатковуваних мінімумів доходів громадян з конфіскацією незаконно виготовленої продукції та обладнання і матеріалів, які призначені для її виготовлення (ст. 51^2);*
- порушення умов і правил, що регламентують діяльність у галузі зв'язку передбачену ліцензіями, – тягне за собою накладання штрафу на посадових осіб підприємств і організацій усіх форм власності *у розмірі від десяти до двохсот неоподатковуваних мінімумів доходів громадян;*
- ті самі дії, вчинені повторно протягом року після накладання адміністративного стягнення за порушення умов і правил, – тягнуть за собою *накладання штрафу на посадових осіб у розмірі від тридцяти до п'ятдесяти неоподатковуваних мінімумів доходів громадян* (ст.145);
- порушення правил охорони ліній і споруд зв'язку або пошкодження кабельної, радіорелейної, повітряної лінії зв'язку, проводового мовлення або споруд чи обладнання, які входять до їх складу, якщо воно не викликало порушення зв'язку, – тягнуть за собою *накладання штрафу на громадян у розмірі від тридцяти до сорока неоподатковуваних мінімумів доходів громадян* (ст..147);
- порушення порядку та умов надання послуг зв'язку в мережах загального користування, – тягнуть за собою *накладання штрафу на посадових осіб у розмірі від тридцяти до ста неоподатковуваних мінімумів доходів громадян* (ст..148^2);

- використання засобів зв'язку з метою, що суперечить інтересам держави, з метою порушення громадського порядку та посягання на честь і гідність громадян, – тягнуть за собою *накладання штрафу в розмірі від п'ятдесяти до ста неоподатковуваних мінімумів доходів громадян* (ст..148^3);

- використання технічних засобів та обладнання, що застосовуються в мережах зв'язку загального користування, без сертифіката відповідності або без погодження з адміністрацією зв'язку України, – тягнуть за собою *накладання штрафу в розмірі від десяти до двохсот неоподаткованих мінімумів доходів громадян* (ст.148^4);

- невиконання норм і вимог технічного захисту секретної інформації, внаслідок чого виникає реальна загроза порушення цілісності цієї інформації або прострочення її технічними каналами, – тягне за собою *накладання штрафу на громадян від одного до трьох неоподатковуваних мінімумів доходів громадян і на посадових осіб – від трьох до десяти неоподатковуваних мінімумів доходів*;

- повторне протягом року вчинення попереднього порушення, за яке особу вже було піддано адміністративному стягненню, – тягне за собою *накладання штрафу на громадян від трьох до восьми неоподатковуваних мінімумів доходів громадян і на посадових осіб – від п'яти до п'ятнадцяти неоподатковуваних мінімумів доходів громадян* (ст. 212^2);

Таким чином, основним покаранням за адміністративні правопорушення є штраф – грошове стягнення, що накладається на громадян і посадових осіб за адміністративні правопорушення.

Справи про адміністративні правопорушення розглядаються:

- адміністративними комісіями при виконавчих комітетах сільських, селищних, міських рад;
- виконавчими комітетами сільських, селищних, міських рад;
- районними (міськими) судами (суддями);
- органами внутрішніх справ, органами державних інститутів та іншими органами (посадовими особами), уповноваженими на те Кодексом України про адміністративні правопорушення.

Контрольні питання

1. Наведіть класифікацію видів юридичної відповідальності.
2. Охарактеризуйте особливості дисциплінарної та цивільно-правової (матеріальної) відповідальності.
3. Поясніть суть адміністративної відповідальності.
4. Наведіть класифікацію видів кримінальних покарань.
5. Опишіть особливості основних кримінальних покарань.
6. Розкажіть про особливості додаткових покарань.

7. Наведіть класифікацію законодавчих актів, що передбачають юридичну відповідальність у сфері інформаційних відносин.

8. Дайте характеристику правопорушень за Законом України „Про інформацію”.

9. Охарактеризуйте особливості відповідальності при роботі з таємною інформацією.

10. Поясніть суть цивільно-правового захисту авторського права і суміжних прав.

11. Опишіть особливості відповідальності за незаконне втручання в роботу ЕОМ, систем комп’ютерних мереж.

12. Охарактеризуйте види покарання при викраденні, привласнені комп’ютерної інформації шляхом шахрайства чи зловживання службовим становищем.

13. Розкрийте суть кримінального покарання осіб, винних у порушенні правил експлуатації автоматизованих електронно-обчислювальних систем.

14. Розкажіть про особливості покарання при порушенні правил експлуатації АЕОС з викраденням, перекрученням чи знищенням комп’ютерної інформації.

15. Поясніть суть права фізичних осіб на інформацію.

16. Розкрийте суть права інтелектуальної власності.

17. Наведіть класифікацію об’єктів інтелектуальної власності.

18. Охарактеризуйте можливі заходи судових органів щодо захисту прав інтелектуальної власності.

19. Наведіть класифікацію об’єктів господарювання.

20. Опишіть заходи захисту прав суб’єктів господарювання та споживачів.

21. Охарактеризуйте склад та завдання адміністративного законодавства.

22. Поясніть особливості стягнень за адміністративні правопорушення.

23. Розкрийте суть мір відповідальності за адміністративні правопорушення у сфері інформатизації.

24. Опишіть особливості відповідальності за порушення цілісності секретної інформації.

Глава 7. Міжнародно-правове регулювання в галузі захисту інформації

7.1. Міжнародна інформаційна діяльність

Згідно зі ст. 50 Закону України „Про інформацію" *міжнародна інформаційна діяльність полягає в забезпеченні громадян, державних органів, підприємств, установ і організацій офіційною документованою або публічно оголошуваною інформацією* про зовнішньополітичну діяльність України, про події та явища в інших країнах, а також у цілеспрямованому поширенні за межами України державними органами і об'єднаннями громадян, засобами інформації та громадянами всебічної інформації про Україну.

Громадяни України мають право на вільний і безперешкодний доступ до інформації через зарубіжні джерела, включаючи пряме телевізійне мовлення, радіомовлення і пресу .

Правове становище і професійна діяльність акредитування в Україні іноземних кореспондентів та інших представників іноземних засобів масової інформації, а також інформаційна діяльність дипломатичних, консульських та інших офіційних представників зарубіжних держав в Україні регулюються законодавством України, відповідними міжнародними договорами, укладеними Україною.

Створення і діяльність спільних організацій в галузі інформації за участю вітчизняних та іноземних юридичних осіб і громадян регулюються законодавством України.

Якщо міжнародним договором встановлені інші правила, ніж ті, які містяться в законодавстві України, що регулює відношення в галузі інформації, то застосовуються норми міжнародного договору, укладеного Україною.

Статтею 52 цього Закону передбачається, що *міжнародне співробітництво* в галузі інформації з питань, які становлять взаємний інтерес, *здійснюється* на *основі міжнародних договорів*, укладених Україною та юридичними особами, що займаються інформаційною діяльністю.

Державні органи та інші юридичні особи, які займаються інформаційною діяльністю, можуть безпосередньо здійснювати зовнішньоекономічну діяльність у власних інтересах індивідуальних і колективних споживачів, яких вони обслуговують і яким гарантують одержання зарубіжної інформації.

За ст.52 експорт та імпорт інформаційної продукції (послуг) здійснюються згідно з законодавством України про зовнішньоекономічну

діяльність.

У Законі України „Про Концепцію Національної програми інформатизації" відмічається, що *у міжнародному співробітництві з питань інформатизації головним є*:- активна участь України в реалізації міжнародних проектів, спрямованих на формування умов для входження до глобальних інформаційних систем;

- захист при виконанні цих проектів національних інтересів;
- реалізація стратегічних цілей української зовнішньої політики.

Необхідно організувати та постійно вдосконалювати взаємозв'язок національних телекомунікаційних систем із комп'ютерними мережами інших країн та глобальною мережею INTERNET забезпечити доступ до міжнародних інформаційних масивів та баз даних і геоінформаційних систем .

Важливим є створення системи інформаційно-телекомунікаційного забезпечення міждержавного співробітництва у сфері торгівлі, охорони здоров'я, боротьби з міжнародною злочинністю, гідрометеорології тощо.

У сфері міждержавної торгівлі передбачається створити систему зовнішньоторговельної інформації стосовно міжнародних, національних, державних і регіональних програм співробітництва, міжнародного та українського законодавства, інформаційно-телекомунікаційну базу для системного вивчення стану світових ринків товарів (продукції, послуг) і маркетингового забезпечення діяльності українських експортерів.

7.2. Міжнародна діяльність у галузі захисту інформації в автоматизованих системах та її правове регулювання

Основні засади міжнародної діяльності України в галузі захисту інформації в автоматизованих системах визначаються у розділі VI Закону України "Про захист інформації в автоматизованих системах".

У ст. 19 Закону мова йде про взаємодію в питаннях захисту інформації в АС. З метою забезпечення міждержавної взаємодії обчислювальних мереж і АС уповноважені Кабінетом Міністрів України органи координують свою роботу щодо захисту інформації з органами захисту інформації інших держав.

Загальні засади забезпечення інформаційних прав України визначаються у ст. 20 цього Закону. Фізичні та юридичні особи в Україні, на підставі Закону України "Про інформацію", можуть встановлювати взаємозв'язки з АС інших держав з метою обробки, обміну, продажу, купівлі відкритої інформації. Такі взаємозв'язки мають виключати можливість несанкціонованого доступу з боку інших держав або їх представників - резидентів України чи осіб без громадянства до інформації, що є в АС України, незалежно від форм власності і підпорядкування, стосовно якої встановлено вимоги нерозповсюдження її за межі України без спеціального дозволу.

Іноземні держави, іноземні фізичні та юридичні особи можуть виступати власниками АС в Україні, власниками інформації, що розповсюджується та обробляється в АС України або засновувати спільні з українськими юридичними та фізичними особами підприємства з метою створення АС, постачання інформації до АС України, обміну інформацією між АС України та АС інших держав. Окремі види такої діяльності здійснюються на підставі спеціального дозволу (ліцензії), що видається уповноваженим на це органом.

Участь України в міжнародних інформаційних відносинах визначається законодавством:

"Про ратифікацію Статуту і Конвенції Міжнародного союзу електрозв'язку" (від 15.07.1994р.);

"Про ратифікацію Угоди про співробітництво в галузі охорони авторського права і суміжних прав" (від 27.01.1995р.);

"Про приєднання України до Бернської конвенції про охорону літературних і художніх творів (Паризького акта від 24 липня 1971р., зміненого 2 жовтня 1979р.)" (від 31.05.1995р.);

"Про ратифікацію Четвертого додаткового протоколу до Статуту Всесвітнього поштового союзу" (від 02.06.1995р.);

"Про ратифікацію Договору про закони щодо товарних знаків" (від 13.10.1995р.);

"Про приєднання України до Статуту Ради Європи" (від 31.10.1995р.);

"Про ратифікацію Конвенції про захист прав і основних свобод людини 1950 року, Першого протоколу та протоколів № 2, 4, 7 та 11 до Конвенції*" (від 17.07.1997р.);

"Про ратифікацію Конвенції про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом, 1990 р." (від 17.12.1997р.);

"Про ратифікацію Угоди щодо співробітництва у розвитку та використанні систем стільникового рухомого зв'язку" (від 03.03.1998р.);

"Про ратифікацію Угоди між Урядом України та Урядом Сполучених Штатів Америки про захист технологій, пов'язаних із запуском Україною ліцензованих США комерційних космічних апаратів" (від 04.12.1998р.).

Щодо захисту персональних даних існують:

Конвенція №108 Ради Європи "Про захист фізичних осіб при автоматизованій обробці даних" (від 28.01.1981р.);

Директива 95/46/ЕС "Про захист фізичних осіб при обробці персональних даних і вільного обігу цих даних" (від 24.10.1995р.);

Директива 97/66/ЕС "Про обробку персональних даних і захист privacy (приватності) у телекомунікаційному секторі та рекомендації щодо захисту даних в інформаційних супермагістралях".

7.3. Правове регулювання охорони та захисту інформації в автоматизованих системах за законодавством різних країн

У різних країнах існують свої правові підходи до вирішення проблем захисту інформації в автоматизованих (комп'ютерних) системах, зокрема щодо боротьби з правопорушеннями, які вчиняються за допомогою комп'ютерних технологій. Ці підходи грунтуються на різних правових доктринах. Провідними серед них є такі:

Правова доктрина системи загального права англо-американської сім'ї права (Великобританія, США та інші країни, що запозичили їх доктрину права). Основний ЇЇ зміст зводиться до публічно-правового і приватно-правового (недержавного) регулювання суспільних відносин, через що існує поділ права на публічне й приватне. При цьому важливим критерієм такого розмежування є визначення соціальної спрямованості інтересу: публічний (суспільства, держави в цілому) та приватний (окремої людини, недержавних спільнот). Державне забезпечення приватно-правового регулювання здійснюється через можливість судового захисту у формі судових прецедентів.

Правова доктрина європейської континентальної сім'ї права, її ще називають романо-германською (ФРН, Франція, Росія та ряд інших). За цією доктриною, право поділяється на галузі, підгалузі, галузеві та міжгалузеві комплексні інституції публічного (державного) права. Серед провідних галузей визначаються: конституційне, адміністративне, цивільне та кримінальне право. На їх основі виникають синтетичні міжгалузеві комплексні інститути права. Такий підхід правового регулювання притаманний і Україні.

Порівняльний аналіз теорії і практики зарубіжного та вітчизняного законодавств свідчить про наявність певних тенденцій концептуального характеру щодо формування соціальної інституції – захисту інформації як об'єкта (предмета) правового регулювання.

Наприклад, нормативна база багатьох країн Європи (Бельгія, Німеччина, Італія, Люксембург та ін.) розвивається за правовою концепцією, за якою у разі несанкціонованого зняття інформації в автоматизованих системах не вважають доцільним застосовувати державні інституції класичних законодавчих положень щодо розкрадання та розтрати майна (речей). За цим підходом вводяться нові норми, що визначають окремі правопорушення, предметом посягання яких є інформація, в тому числі й та, що обробляється за допомогою комп'ютерних технологій. Тобто, речове й інформаційне право, зокрема захист інформації в автоматизованих системах, є автономними інституціями в системі законодавства.

Перші спеціальні закони щодо боротьби з комп'ютерною злочинністю були прийняті в 1973 році в Швеції та в 1976 році в США на федеральному рівні. Згодом, у багатьох країнах світу було поступово затверджено законодавчі акти стосовно цієї категорії злочинів. Розвиток

законодавства стосовно комп'ютерних злочинів у сфері економіки в різних країнах за хронологією виглядає так: 1973р. – Швеція; 1975 – 1976рр. США; 1979р. – Австралія; 1981р. – Великобританія; 1984р. – приймаються нові закони у США; 1985р. – Данія, Канада; 1986р.– ФРН, Швеція; 1987р. – Австралія, Японія, Норвегія; 1988р. – Франція, Греція; 1990р. – нові закони у Великобританії; 1991р. – Фінляндія, Португалія, Туреччина; 1992р. – Швейцарія, Іспанія; 1993р. – Франція, Нідерланди тощо.

В окремих країнах формується законодавство щодо таких суспільних відносин, як захист даних. Тут хронологія така: 1973р. – Швеція; 1974р. – США; 1977р. – ФРН; 1978р. – Данія, Франція, Норвегія; 1979р. – Австрія; 1981р. – Іспанія, Ізраїль; 1982р. – Австралія; 1983р. – Сан-Мари -но; 1984р. – Великобританія; 1985р. – Канада; 1987р. – Фінляндія; 1988р. – Ірландія, Японія, Нідерланди; 1989р. – Ісландія; 1990р. – Словенія; 1991р. – Португалія; 1992р. – Бельгія, Швейцарія, Іспанія, Словаччина, Чехія, Угорщина та ін.

Враховуючи фактор інформатизації, в багатьох країнах відповідним чином адаптується традиційне законодавство, зокрема щодо захисту авторських прав: 1982р. – Швеція, Великобританія, США; 1984р. – Фінляндія; 1986р. – Китай, Данія, Німеччина, Франція; 1988р. – Великобританія, Канада; 1992р. – Угорщина.

Одним із напрямків публічно-правового (державного) захисту інформації стає захист топології (топографії) інтегральних мікросхем. Відповідне спеціальне законодавство протягом 80-х років XX століття було прийнято в ряді країн: 1985р. – Японія; 1986р. – Швеція; 1987р. – Данія, ФРН, Франція, Японія (вдосконалення), Нідерланди, Великобританія; 1988р. – Австрія, Іспанія; 1989р. – Австралія, Італія, Португалія; 1990р. – Бельгія, Канада; 1991р. – Фінляндія, Угорщина тощо.

Розглянемо більш детально деякі аспекти інформаційного права окремих країн щодо захисту інформації в автоматизованих (комп'ютерних) системах.

7.3.1. Інформаційне законодавство ФРН

У лютому 1986 року Бундестагом Німеччини було прийнято Другий Закон щодо боротьби з економічною злочинністю. Завдяки цьому було закладено правову базу для ефективного кримінально-правового переслідування економічних правопорушень нового типу, перш за все злочинів, об'єктом або знаряддям яких є ЕОМ. Ряд нових статей, які введено цим законом, містять спеціально сформульований склад комп'ютерних злочинів. Закон було введено у дію 1 серпня 1986 року.

У Німеччині також були прийнято ряд Федеральних Законів щодо захисту інформації:

27 січня 1977 року "Про захист персоніфікованої інформації від протиправних дій у процесі обробки даних";

3 серпня 1977 року "Про порядок опублікування інформації";

9 лютого 1978 року "Про порядок ведення інформаційних регістрів" та ряд інших актів інформаційного законодавства.

З метою систематизації положень інформаційного законодавства та його інкорпорації в ФРН був прийнятий 20 грудня 1990 року новий Федеральний Закон ФРН "Про удосконалення обробки даних і захист інформації". За цим законом втратили чинність зазначені вище закони. Цей закон, по суті, регулює основні різновиди суспільних відносин, які виникають у процесі збору, обробки і розповсюдження персоніфікованої інформації. В контексті нашої системи права цим законом по суті здійснено кодифікацію законодавства, об'єктом регулювання якого виступають суспільні інформаційні відносини в умовах інформатизації. Основним родовим об'єктом правового регулювання є юридичний захист інформаційних прав громадян. Третій підрозділ Закону від 20 грудня 1990 року закріплює статус і форми діяльності Федерального уповноваженого щодо захисту даних.

Стосовно комп'ютерних злочинів, законодавство ФРН складається з кількох умовно визначених блоків.

1. Економічне кримінальне законодавство: протиправні комп'ютерні маніпуляції; комп'ютерний саботаж; комп'ютерне шпигунство; несанкціонований доступ до комп'ютерних систем або мереж.

2. Законодавство про охорону прав інтелектуальної власності: протизаконне використання робіт, які захищені авторським правом; незаконне виробництво топографій мікроелектронних напівпровідників.

3. Законодавство щодо захисту державної інформації: регулює ступінь відповідальності за злочини, які пов'язані з протизаконним розголошенням захищеної державної інформації.

4. Процесуальне законодавство: регламентує склад злочинів, пов'язаних з протиправним втручанням до комп'ютерних систем, у зв'язку з проведенням процесуальних дій.

Правопорушення, які пов’язані з комп'ютерами та визначені законом, зібрано в статтях Кримінального кодексу:

- інформаційне шпигунство (нелегальне отримання даних) – ст. 202a;
- комп'ютерне шахрайство – ст. 263a;
- фальсифікація даних і речових доказів – ст. 269;
- обман у правовій діяльності, у зв'язку з проведенням процесуальних дій, – ст. 270;
- заміна інформації – ст. 303a;
- комп'ютерний саботаж – ст. 303b.

Зловживання, пов'язані з руйнуванням інформації та внесенням комп'ютерних вірусів, регламентуються статтями 202a, 303a, 303b Кримінального кодексу ФРН.

Інші комп'ютерні правопорушення регламентуються законодавчими

актами:

- протизаконне використання робіт, які захищені авторським правом – ст. 106 Закону "Про авторське право";
- нелегальна передача технології – ст. 34 Закону "Про зовнішню торгівлю";
- протизаконне розголошення захищеної інформації – ст. 43 Закону "Про захист державної інформації";
- незаконне виробництво топографій мікроелектронних напівпровідників – ст. 10 Закону "Про захист напівпровідників".

Розглянемо детальніше зміст складу злочинів, що містяться у КК ФРН: ст. 263а кодексу регламентує склад протизаконних дій, які становлять ***форми комп'ютерних маніпуляцій і пов'язані із заподіянням шкоди.*** Вона передбачає кримінальну відповідальність за неправомочний вплив на кінцеві результати процесу обробки інформації шляхом протизаконного використання невірних та неповних програм і відомостей, технічних засобів.

(Аналогічні статті стосовно кримінальної відповідальності за комп'ютерне шахрайство передбачені законами Фінляндії, Данії, Австрії, Швейцарії та інших країн).

Склад злочину ст. 269 КК ФРН, передбачає кримінальну відповідальність за ***протиправне введення даних до комп'ютера*** (ЕОМ) ***чи їх повну заміну іншими даними (фальсифікація інформації)*** *з* метою сприйняття її у хибному вигляді або подання зміненої інформації в документальному вигляді, використання такої інформації.

Статтею 270 КК ФРН передбачена відповідальність за ***порушення допустимих параметрів, у зв'язку з процесом обробки шляхом обману.***

Порівняльний аналіз свідчить, що його поняття обману у правовідносинах розвинутих країн збігається за змістом з поняттям несанкціонованого втручання в процес обробки інформації. Спосіб втручання не визначається як суттєвий у кваліфікації злочинів.

Аналіз свідчить, що в законодавстві Німеччини про комп'ютерні злочини, як і в більшості європейських країн (наприклад, Нідерландах, Швеції), ***комп'ютерне шахрайство*** *та* ***комп'ютерний підлог,*** *поєднані в блок –* ***" комп'ютерні маніпуляції".***

Строки покарання за такі дії у ФРН – до 5 років позбавлення волі, у Нідерландах – до 6 років, у Швеції – від 3 місяців до 6 років.

Правопорушення, які пов'язані з пошкодженням інформації, переслідуються в судовому порядку тільки при завданні шкоди компанії. У ФРН розслідування може початися протягом 3 місяців після подання компанією заяви та інших необхідних документів, які свідчать про наявність вчинення протиправних дій і заподіяння шкоди, для їх подальшого вивчення та прийняття рішення.

Слід звернути увагу на те, що у випадку, коли вчинення злочину має широкий суспільний резонанс і викликає суспільний інтерес,

судовий орган може провести судовий процес без наявності заяви про заподіяння шкоди фірмі, компанії, банку та іншим потерпілим.

У законодавстві ФРН, як і в законодавстві деяких інших західних країн, існує визначення злочинів, об'єднаних у один блок – ***"комп'ютерний саботаж".*** Кримінальна відповідальність за вчинення або спробу вчинення такого типу злочинів регламентується в Кримінальному кодексі ФРН ст. 303а – "Заміна даних", ст. 303b– "Комп'ютерний саботаж".

Аналогічні склади злочину визначені в кримінальному законодавстві Швеції – ст.12 ч.1,2,3 КК "Кримінальне пошкодження"; ст.13 ч.4,5 КК – "Саботаж"; ст.14 ч.4 КК – "Пошкодження документів" тощо.

Залежно від рівня суспільної небезпеки злочину, строки покарання за такі дії визначаються:

у ФРН за менш небезпечні факти передбачено два роки ув'язнення або штраф, за тяжкі – 5 років або штраф;

- у Швеції – відповідно 6 місяців і 10 років;
- у Нідерландах – 2 роки або штраф 25 000 гульденів і 4 роки або штраф 100000 гульденів;
- у ФРН існує два типи злочинів, що регулюються однією статтею. Це ст.202а КК ***"Інформаційне шпигунство",*** яка встановлює міру відповідальності за отримання без дозволу спеціально захищеної від несанкціонованого доступу інформації.

Нелегальне копіювання та використання комп'ютерного програмного забезпечення – розглядається як порушення авторських прав, згідно зі ст. 69 і 106 Закону ФРН "Про авторське право". Покарання за порушення авторських прав включає тюремне ув'язнення до трьох років або великі штрафи.

Ст. 108 вищеназваного закону регламентує міру відповідальності за ***протизаконне і неодноразове використання програмного продукту з метою одержання прибутку.*** Строк ув'язнення – до 5 років або штраф.

Ст. 10 Закону ФРН "Про захист напівпровідників" обумовлює такий склад правопорушення, як ***незаконне виробництво топографічних копій,*** яке, залежно від способу вчинення, кваліфікується або за ст. 202а "Інформаційне шпигунство", або за ст. 106, чи ст. 108а Закону ФРН "Про авторське право". Порушення, пов'язані з незаконним комерційним використанням та розкриттям комерційної і промислової таємниці з особистої зацікавленості або на користь інших осіб, конкуренція, пошкодження власності, кваліфікується ст. 17 Закону ФРН "Про нечесну конкуренцію", яка передбачає міру покарання від трьох до п'яти років позбавлення волі або штраф.

Покарання за ***порушення приватної таємниці та використання інших секретів*** визначають відповідно до диспозиції статей 203 та 204 Кримінального кодексу ФРН.

7.3.2. Інформаційне законодавство Норвегії

Згідно з законодавством Норвегії, комп'ютерні злочини поділяються на:

- протиправний (несанкціонований) доступ до комп'ютерних систем;
- комп'ютерний саботаж;
- комп'ютерне шпигунство;
- комп'ютерне шахрайство;
- нелегальне копіювання програм;
- злочини, які пов'язані з розповсюдженням нелегальної інформації (порнографія, расистська література).

Склад цих злочинів регламентується такими статтями Кримінального кодексу Норвегії:

- ст. 145 ч.2 – протиправний доступ до комп'ютерних систем;
- ст. 261 та ст.393 – протиправне використання власності;
- ст. 279 параграф 2 – комп'ютерне шахрайство;
- ст. 291 – збитки, які понесені (виникли) внаслідок комп'ютерних злочинів;
- ст. 294 – промислове шпигунство, а також ст. 54 Закону "Про авторське право" – протизаконне копіювання.

7.3.3. Інформаційне законодавство Італії

Щорічні втрати в Італії від комп'ютерних злочинів становлять сотні мільйонів лір. У зв'язку з цим, в Італії законодавчими актами введені основні положення відносно найбільш тяжких комп'ютерних злочинів:

1. Декрет № 518 від 29.12.92 року "Використання положень Європейського Економічного Співтовариства за № 91/250 стосовно офіційного захисту комп'ютерних програм";
2. Закон № 547 від 23.12.93 "Зміна та внесення нових статей стосовно комп'ютерних злочинів у Кримінальний кодекс".

Комп'ютерний злочин, згідно з кримінальним законодавством Італії, – ***це злочин, вчинений з використанням комп'ютерних технологій як від персонального комп'ютера, так і портативних телефонних пристроїв, які створені на базі мікрочіпів.***

Законодавство Італії забезпечує захист урядових організацій, військових об'єктів, банків, компаній, фірм від несанкціонованого доступу в комп'ютерні мережі, протиправного використання захищених банків даних, незаконного копіювання топографій напівпровідників (чіпів), які злочинці використовують для встановлення кодів кредитних і телефонних карток, банківських рахунків тощо.

В Італії було прийнято два важливі законодавчі акти, що стосуються комп'ютерних злочинів.

Перший, щодо програмного захисту, це Закон № 518 від 29.12.92 р. "Про виконання постанови Європейського Економічного Союзу № 91/250

щодо правового захисту комп'ютерних програм".

Другий стосується комп'ютерних злочинів взагалі, це Закон № 547 від 23.12,93 р. "Про зміни та доповнення до розділу Кримінального кодексу про комп'ютерну злочинність".

Згідно з цією постановою, комп'ютерні злочини – це ті злочини, що вчинені з використанням комп'ютерних технологій – від персонального комп'ютера до портативного телефонного апарата, забезпеченого мікрочіпом.

Можливості цього виду обладнання значно більші, і якщо воно пов'язане зі спеціальними мережами, то при належному застосовуванні за його допомогою можливий несанкціонований доступ до баз даних компаній, громадських установ, банків. Подібне обладнання також дозволяє використовувати лінії пошкодженої мережі для захоплення конфіденційної комерційної інформації.

7.3.4. Інформаційне законодавство Франції

Прийнятий у Франції 5 січня 1994 року Закон "Godfrran" (було названо на честь автора) вніс якісні уточнення в питання щодо **несанкціонованого доступу та протидії функціонуванню систем.** Такі правопорушення щорічно завдають збитків, наприклад, страховим компаніям у розмірі 5 мільярдів франків.

Франція володіє повним юридичним арсеналом для боротьби з такою категорією злочинності. У 1994 році з компетентного персоналу було сформовано бригаду поліції, яка спеціалізується на виявленні та розслідуванні комп'ютерних злочинів при тісному співробітництві зі службами безпеки та цивільними (громадськими) організаціями.

З 1 березня 1994 року було введено в дію нову версію Кримінального кодексу, який докорінно змінив внутрішні закони про комп'ютерну злочинність. До кодексу були внесені статті із санкціями проти правопорушень, які пов'язані з обробкою інформації та із злочинами стосовно фальсифікації даних.

7.3.5. Інформаційне законодавство Іспанії

В Іспанії зміст категорії "комп'ютерний злочин" має таке визначення.

1. Дії, які спрямовані на знищення або стирання програм чи їх складових частин, заміну, знищення накопиченої інформації, необґрунтоване використання комп'ютера (ЕОМ).

2. Дії проти держави, національної безпеки, найближчого оточення, майна тощо.

Єдиний закон, який передбачає покарання за комп'ютерні злочини, – це Кримінальний кодекс Іспанії. Диспозиції статей КК сформульовані

відповідно до норм Державного Закону № 5/92 від 2 жовтня 1992 року, який регулює процеси персональної автоматизованої обробки даних і передбачає утворення органу захисту даних для контролю за виконанням цих норм.

Розслідування комп'ютерних злочинів покладено на судову поліцію.

7.3.6. Інформаційне законодавство Швеції

Перші спеціальні закони про боротьбу з комп'ютерною злочинністю були прийняті у Швеції в 1973 році. Шведське законодавство поділяє сферу комп'ютерної злочинності на 4 категорії злочинів:

а) протиправне використання ЕОМ, комп'ютерних програм та банків даних як інструменту для вчинення злочинів;

б) зруйнування інформації, комп'ютерних програм та комп'ютерів із злочинними намірами;

в) протизаконне копіювання, підробка або заміна даних чи комп'ютерного програмного забезпечення;

г) несанкціоноване втручання та використання комп'ютерних систем і мереж.

У період з 1 серпня 1991 року до 30 липня 1993 року поліцією Швеції було розслідувано злочинів: категорії а) – 60; категорії б) – 2; категорії в) – 8; категорії г) –43.

У Швеції як комп'ютерне шпигунство розглядається зміст ст.4 ч.8 КК –"Порушення поштової та телекомунікаційної таємниці", ст.4 ч.9 КК – "Вторгнення до захищених банків даних", ст.4 ч.9а КК – "Підслуховування", частина 21 Закону "Про інформацію".

7.3.7. Інформаційне законодавство Австралії

В Австралії перші законодавчі акти стосовно комп'ютерної злочинності були прийняті у 1979 році.

Сектор комп'ютерних злочинів (CCS) Австралійської федеральної поліції (AFP), який був організований у 1989 році, виконує дві функції. *Перша* – збір розвідувальної (оперативно-розшукової) інформації про спеціальні комп'ютерні злочини та їх розслідування. *Друга* – забезпечення технічної підтримки інших підрозділів щодо дослідження комп'ютерних засобів, які пов'язані зі злочинами або допомогли в їх вчиненні.

Згідно з чинним законодавством Австралії, комп'ютерні злочини поділяються на три загальні види.

1. Специфічні комп'ютерні злочини.
2. Злочини, пов'язані з комп'ютером.
3. Злочини, які вчинені за допомогою комп'ютерів.

Специфічні ***комп'ютерні злочини вміщують правопорушення, в яких комп'ютерна система є об'єктом злочинного посягання.***

Прикладом цього виду злочинів може бути протизаконний доступ до комп'ютерної системи.

До *злочинів, що пов'язані з комп'ютерами, належать правопорушення, в яких комп'ютер виступає в ролі предмета або інструмента здійснення правопорушення.* Одним з прикладів цієї категорії злочинів є крадіжка грошей з банку з використанням комп'ютера як інструмента вчинення злочину.

Третій вид злочинів – правопорушення, в яких інформаційна технологія використовується як допоміжна у його вчиненні. Наприклад, використання синдикатами, які займаються розповсюдженням наркотиків, спеціальних комп'ютерів або комунікаційних засобів для безпечного зв'язку між собою.

У 1989 році в Законодавчий Акт від 1914 року "Про злочинність в Федерації" було введено спеціальний розділ VIa. Статті 76a – 76f цього розділу регламентують склади злочинів проти комп'ютерної мережі і комп'ютерних засобів Федерації комерційних організацій, компаній, банків, фірм та приватних осіб, які, згідно з Актом про телекомунікації (1991р.) та ліцензіями, мають дозвіл на користування системами та комп'ютерними мережами.

Ст. 76a визначає перелік термінів, які використовуються при розгляді комп'ютерних злочинів.

Законодавство цієї країни охоплює чотири категорії комп'ютерних злочинів.

Перша категорія – злочини, пов'язані з несанкціонованим доступом до банків даних державних та недержавних комп'ютерних мереж особами, які не мають доступу до ЕОМ (ст. 76b ч.1a,1b) або особами, які мають доступ до ЕОМ (ст.76o ч. 1). Максимальне покарання – 6 місяців ув'язнення.

Друга – несанкціоноване втручання до банків даних державних та недержавних комп'ютерних мереж з метою обману (підлогу) даних особами, які не мають доступу до ЕОМ (ст.76b ч.2a) або особами, які мають доступ до ЕОМ (СТ.76d ч. 2a). Покарання – до 2 років ув'язнення.

Третя – несанкціоноване втручання до захищених банків даних державних та недержавних комп'ютерних мереж, які вміщують інформацію стосовно:

- безпеки, оборони та міжнародних відносин Австралії;
- перевірки та ідентифікації конфіденційних джерел інформації служб безпеки та поліції;
- захисту населення;
- особистих справ кожної людини;
- торгових та комерційних таємниць;
- записів фінансових організацій, з метою одержання, вивчення та використання інформації (комп'ютерне шпигунство) особами, які не мають доступу до ЕОМ (ст.76b ч.2в, 3a, 3б, 3c) або особами, які мають доступ до

ЕОМ (ст.76d ч.2b, 3a, 3b, 3c). Покарання – до 2 років ув'язнення.

Четверта категорія визначає два типи злочинів, які пов'язані з:

- протиправним втручанням до банків даних державних та недержавних комп'ютерних мереж з метою несанкціонованого руйнування, стирання, заміни або доповнення даних (комп'ютерне шахрайство) особами, які не мають доступу до ЕОМ (ст.76c ч.a, б, c) або особами, які мають доступ до ЕОМ (ст.76e ч.a, б);
- протиправним втручанням до державних та недержавних комп'ютерних мереж та систем ЕОМ з метою блокування їх роботи (комп'ютерний саботаж) особами, які не мають доступу до ЕОМ (ст. 76c ч.d) або особами, які мають доступ до ЕОМ (ст.76e ч.c). Покарання – до 10 років позбавлення волі.

7.3.8. Інформаційне законодавство Росії

Досить активно розвивається інформаційне законодавство в Російській Федерації. У його складі можна назвати такі нормативні акти:

Закон Російської Федерації "Про федеральні органи урядового зв'язку та інформації";

Закон Російської Федерації "Про авторське право і суміжні права";

Закон Російської Федерації "Про правову охорону програм для електронних обчислювальних машин і баз даних";

Закон Російської Федерації "Про інформацію, інформатизацію і захист інформації" тощо.

Кримінальний кодекс Російської Федерації (прийнятий Державною Думою 24 травня 1996 р.) містить ряд статей, що визначають кримінальну відповідальність за злочини, предметом яких є інформація.

Глава 19 "Злочини проти Конституційних прав і свобод людини і громадянина" визначає види злочинів та відповідальність за них.

Стаття 146. Порушення авторських і суміжних прав

1. Незаконне використання об'єктів авторського права або суміжних прав, а так само присвоєння авторства, якщо ці діяння заподіяли великий збиток, – караються штрафом у розмірі від двохсот до чотирьохсот мінімальних розмірів оплати праці або в розмірі заробітної плати чи іншого прибутку засудженого за період від двох до чотирьох місяців або обов'язковими роботами на строк від ста вісімдесяти до двохсот сорока годин, або позбавленням волі на строк до двох років.

2. Ті ж діяння, вчинені неодноразово або групою осіб за попередньою змовою, або організованою групою, – караються штрафом у розмірі від чотирьохсот до восьмисот мінімальних розмірів оплати праці або в розмірі заробітної плати чи іншого прибутку засудженого за період від чотирьох до восьми місяців, або арештом на строк від чотирьох до шести місяців, або позбавленням волі на строк до п'яти років.

Стаття 147. Порушення винахідницьких і патентних прав

1. Незаконне використання винаходу, корисної моделі або промислового зразка, розголошення без згоди автора або заявника сутності винаходу, корисної моделі або промислового зразка до офіційної публікації відомостей про неї, присвоєння авторства або примушення до співавторства, якщо ці діяння заподіяли великий збиток, – караються штрафом у розмірі від двохсот до чотирьохсот мінімальних розмірів оплати праці або в розмірі заробітної плати чи іншого прибутку засудженого за період від двох до чотирьох місяців, або обов'язковими роботами на строк від ста вісімдесяти до двохсот сорока годин, або позбавленням волі на строк до двох років.

2. Ті ж діяння, вчинені неодноразово або групою осіб за попередньою змовою або організованою групою, – караються штрафом у розмірі від чотирьохсот до восьмисот мінімальних розмірів оплати праці або в розмірі заробітної плати чи іншого прибутку засудженого за період від чотирьох до восьми місяців, або арештом на строк від чотирьох до шести місяців, або позбавленням волі на строк до п'яти років.

Розділ VIII визначає злочини у сфері економіки.

У главі 21 визначаються злочини проти власності:

Стаття 164. Розкрадання предметів, що мають особливу цінність

1. Розкрадання предметів або документів, що мають особливу історичну, наукову, художню або культурну цінність, незалежно від способу розкрадання, –карається позбавленням волі на строк від шести до десяти років із конфіскацією майна чи без такої.

2. Те ж діяння:

а) вчинене групою осіб за попередньою змовою або організованою групою;

б) вчинене неодноразово;

в) знищення, що спричинило псування або руйнування предметів або документів, зазначених у частині першій цієї статті, – карається позбавленням волі на строк від восьми до п'ятнадцяти років з конфіскацією майна.

У главі 22 "Злочини у сфері економічної діяльності" містяться статті такого змісту.

Стаття 187. Виготовлення або збут підроблених кредитних чи розрахункових та інших платіжних документів

1. Виготовлення з метою збуту або збут підроблених кредитних чи розрахункових карт, а також інших платіжних документів, що не є цінними паперами, –караються позбавленням волі на строк від двох до шести років із штрафом у розмірі від п'ятисот до семисот мінімальних розмірів оплати праці або в розмірі заробітної плати чи іншого прибутку засудженого за період від п'яти до семи місяців.

2. Ті ж діяння, вчинені неодноразово або організованою групою, – караються позбавленням волі на строк від чотирьох до семи років із кон-

фіскацією майна.

У КК Російської Федерації є глава 28, яка визначає злочини у сфері комп'ютерної інформації:

Стаття 272. Неправомірний доступ до комп'ютерної інформації

1. Неправомірний доступ до комп'ютерної інформації, що охороняється законом, тобто інформації на машинному носії, в електронно-обчислювальній машині (ЕОМ), системі ЕОМ або їх мережі, якщо це діяння спричинило знищення, блокування, модифікацію або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їх мережі, – карається штрафом у розмірі від двохсот до п'ятисот мінімальних розмірів оплати праці або в розмірі заробітної плати чи іншого прибутку засудженого за період від двох до п'яти місяців, або виправними роботами на строк від шести місяців до одного року, або позбавленням волі на строк до двох років.

2. Те ж діяння, вчинене групою осіб за попередньою змовою або організованою групою чи особою з використанням свого службового положення, а так само особою, що має доступ до ЕОМ, системи ЕОМ або їх мережі, – карається штрафом у розмірі від п'ятисот до восьмисот мінімальних розмірів оплати праці або в розмірі заробітної плати чи іншого прибутку засудженого за період від п'яти до восьми місяців, або виправними роботами на строк від одного року до двох років, або арештом на строк від трьох до шести місяців, або позбавленням волі на строк до п'яти років.

Стаття 273. Створення, використання і розповсюдження шкідливих програм для ЕОМ

1. Створення програм для ЕОМ чи внесення змін у існуючі програми, які завідомо призводять до несанкціонованого знищення, блокування, модифікації або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ чи .їх мережі, а так само використання або розповсюдження таких програм чи машинних носіїв з такими програмами, – карається позбавленням волі на строк до трьох років зі штрафом у розмірі від двохсот до п'ятисот мінімальних розмірів оплати праці або в розмірі заробітної плати чи іншого доходу засудженого за період від двох до п'яти місяців.

2. Ті ж діяння, які потягли по необережності тяжкі наслідки, – караються позбавленням волі на строк від трьох до семи років.

Стаття 274. Порушення правил експлуатації ЕОМ, системи ЕОМ чи їх мережі

1. Порушення правил експлуатації ЕОМ, системи ЕОМ чи їх мережі особою, яка має доступ до ЕОМ, системи ЕОМ чи їх мережі, що потягло знищення, блокування або модифікацію інформації, яка охороняється законом, якщо це діяння завдало суттєвої шкоди, – карається позбавленням права обіймати певні посади або займатися певною діяльністю на строк до

п'яти років, або обов'язковими роботами на строк від ста вісімдесяти до двохсот сорока годин, або обмеженням волі на строк до двох років.

7.3.9. Інформаційне законодавство США

У США, як і в багатьох інших країнах, у доктрині загального права (англо-американська система права) на законодавчому рівні існує визначення інформації як товару, як об'єкта права власності. За цією концепцією, не є суттєвим на яких матеріальних носіях знаходиться інформація як об'єкт правового захисту, а отже й захист її здійснюється на загальних підставах, як і матеріальних цінностей. Тобто, при використанні принципу аналогії права на законодавчому рівні та через судові прецеденти змінюється зміст складу правопорушень (вводиться нова редакція норми).

Прикладом може бути прийнятий у 1987 році у США Закон "Про захист комп'ютерної інформації". Він стосується програми комп'ютерних даних у Національному Бюро Стандартів з метою забезпечення захисту даних уряду та підготовки осіб, які займаються забезпеченням захисту й мають відношення до управління, операцій та використання Федеральних комп'ютерних систем. За цим Законом, удосконалення захисту, збереження таємної інформації в Федеральних комп'ютерних системах є в інтересах держави, і нею створюються умови для максимального захисту таких систем, без обмеження використання тих засобів захисту, які заплановані або які вже застосовуються. Закон "Про захист комп'ютерної інформації" вносить доповнення до Закону США, яким було надано повноваження Національному Бюро Стандартів щодо розробки шляхів захисту Федеральних комп'ютерних систем, включаючи відповідальність за розробку методів (шляхів) захисту економічної інформації та таємниці в Федеральних комп'ютерних системах, а також технічну допомогу та поради Національного розвідувального управління.

Для застосування методів (шляхів) захисту переглянуто розділ III (d) Закону від 1949 року "Про федеральну власність та адміністративну службу".

Окремі положення захисту інформації в комп'ютерних системах у США були введені також й іншими нормативно-правовими актами:

- Звід законів США 47c, Закон "Про атомну енергію та умови використання ядерних ресурсів";
- Звід законів США 128 (передача фондів іноземної криптографічної підтримки
- Звід законів США 140a (видатки Міністерства оборони на співробітництво розвідки з іноземними управліннями);
- Звід законів США 140b (використання прибутку Міністерства оборони для розвідки);
- Звід законів США 539 (видатки ФБР на співробітництво розвідки з

іноземними управліннями);

- Звід законів США 1028 (дії розвідки щодо статуту про виявлення підробок);
- Звід законів США 1029 (дії розвідок щодо статуту про захист кредитної картки);
- Звід законів США 1030 (дії розвідки щодо статуту про комп'ютерний обмін);
- Звід законів США 1367 (дії розвідки щодо статуту про перешкоди супутникового зв'язку);
- Звід законів США 1546 (дії розвідки щодо статуту про підробку віз. Інформаційний захист);
- Звід законів США 7342 (захист джерел розвідки та методів роботи ЦРУ щодо отримання іноземної інформації);
- Звід законів США 2577, Закон "Про контроль озброєння та роззброєння", розділ 37 (захист джерел розвідки, методів та осіб, завдяки яким складаються доповіді про контроль озброєння до Конгресу);
- Звід законів США 2656, Закон "Про зв'язок з іноземними країнами" 1979р., розділ 503 (захист джерел розвідки, методів та осіб, що займаються науковим / технічним розвитком, складанням доповідей до Конгресу);
- Звід законів США 2162, Закон "Про атомну енергію" 1954р., розділ 14 (роль Директора ЦРУ в контролюванні обмежень за даними для службового користування відносно програм з атомної енергії інших країн);
- Звід законів США 783 (b) "Про доступ іноземних управлінь до таємної інформації";
- Звід законів США, Додаток 2411, Закон "Про управління експортом" 1979 року, з доповненнями. Розділ 12 (захист джерел розвідки, методи та обробка інформації, пов'язаної з експортом спільно з Центральним фінансово-контрольним управлінням та Міністерством торгівлі).

Це далеко неповний перелік нормативних актів, що регулюють захист інформації в комп'ютерних системах США.

В окремих штатах цієї країни прийняті свої нормативно-правові акти.

У червні 1983 р. Міністерством охорони здоров'я США для Комітету з питань науки і техніки Конгресу була підготовлена доповідь на тему: "Комп'ютерні злочини і правопорушення в урядових установах", в якій було виділено 17 основних способів вчинення комп'ютерних злочинів. У основу доповіді було покладено опитування респондентів про всі випадки комп'ютерних шахрайств і зловживань за період з 1 січня 1978р. по 31 березня 1982р.

Під ***комп'ютерним шахрайством*** авторами доповіді розумілася ***будь-яка незаконна умисна дія (або ряд дій) з метою перекручення даних для отримання вигоди, якщо вона здійснювалася за допомогою***

маніпулювання процесами введення і передачі даних, комунікаціями, операційною системою та обладнанням.

Комп'ютерним зловживанням автори доповіді вважали ***правопорушення, що включає в себе неправомірне використання, знищення або модифікацію оброблюваної інформації.***

У 1994 році у федеральне законодавство США щодо комп'ютерних злочинів були внесені нові поправки, які розширюють коло карних діянь і уточнюють термінологію. Законодавчий "Акт про шахрайство та зловживання за допомогою комп'ютерів", крім відзначених статей про регулювання міри вини за несанкціонований доступ до даних, які зберігаються в комп'ютерах федерального уряду, та злочинів з використанням ЕОМ, котрі були вчинені більш ніж у одному штаті, розширено у 1994 році статтею про відповідальність за передачу *шкідливих кодів (комп'ютерних вірусів)*.

Слово "вірус" мало використовується в правотворчій практиці. Новий законодавчий акт охоплює несанкціоновані передачі програм, інформації, кодів і команд, які викликають ушкодження комп'ютера, комп'ютерної системи, мережі, інформації, даних або програм. Ключові зміни в законі – розділення злочинів з використанням комп'ютерів на два рівні: дії вчинені "з необачним ігноруванням правил", котрі призвели до пошкоджень, класифікуються як адміністративні карні порушення, а навмисні шкідливі акти (дії) підлягають під певні кримінальні злочини.

Щодо кримінального законодавства окремих штатів, то серед головних його ознак слід зазначити, насамперед, варіювання, адже кримінальні кодекси штатів дуже різняться між собою.

Так, деякі штати (Юта, Техас, Коннектикут) пов'язують кримінальну відповідальність із *розмірами збитків* у грошовому відображенні. В інших штатах кримінальна відповідальність настає навіть за відсутності матеріальних збитків, зокрема: у випадках несанкціонованого доступу до конфіденційної інформації (Невада, Вірджинія, Нью-Йорк), результатів медичного обстеження (Нью-Йорк, Вірджинія), даних про трудову діяльність, заробітну платню, надані кредити та приватні справи (Вірджинія). У штаті Небраска будь-який несанкціонований доступ вважається злочином.

Покарання за ці злочини також відрізняються у різних штатах. Зокрема, в штаті Джорджія порушення права доступу в деяких випадках може спричинити ув'язнення терміном до 15 років.

Як ознаку злочину закони деяких штатів передбачають *навмисність дій*. Однак, слід підкреслити, що оскільки навмисність злочинного наміру дуже важко довести, то цей пункт може стати суттєвою перешкодою для притягнення до кримінальної відповідальності за комп'ютерні злочини в Каліфорнії, Де-лаварі, Флориді, Канзасі, Меріленді та Мінесоті.

За законодавством штату Юта, одним з найефективніших критеріїв визначення покарання за скоєне правопорушення є *розмір заподіяної* (чи

такої, що могла бути заподіяна) *шкоди*, адже це дозволяє легко розмежувати випадки настання (використовуючи звичну для нас термінологію) цивільно-правової, адміністративної та кримінальної відповідальності. У такому разі введення чіткої кваліфікації діяння залежно від розміру шкоди дозволить уникнути суб'єктивізму під час призначення покарання.

7.3.10. Інформаційне законодавство Казахстану

В Особливій частині КК Казахстану, серед злочинів у сфері економічної діяльності, міститься *ст. 227 "Неправомірний доступ до комп'ютерної інформації, створення, використання і поширення шкідливих програм для ЕОМ"*. У ній визначені види складів злочину:

1. Неправомірний доступ до комп'ютерної інформації, що охороняється законом, тобто інформації на машинному носії, в електронно-обчислювальній машині (ЕОМ), системі ЕОМ або їх мережі, якщо це діяння спричинило знищення, блокування, модифікацію або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їх мережі, **–** карається штрафом у розмірі від двохсот до п'ятисот місячних розрахункових показників або в розмірі заробітної плати чи іншого прибутку засудженого за період від двох до п'яти місяців, або притягненням до громадських робіт на строк від ста двадцяти до ста вісімдесяти годин, або виправними роботами на строк до одного року, або позбавленням волі на той же строк.

2. Те ж діяння, вчинене групою осіб за попереднім зговором або організованою групою чи особою з використанням свого службового положення, а так само особою, що має доступ до ЕОМ, системи ЕОМ або їх мережі, **–** карається штрафом у розмірі від п'ятисот до восьмисот місячних розрахункових показників або в розмірі заробітної плати чи іншого прибутку засудженого за період від п'яти до восьми місяців, або виправними роботами на строк від одного року до двох років, або позбавленням волі на строк до трьох років.

3. ***Створення програм для ЕОМ або внесення змін в існуючі програми, що завідомо призводять до несанкціонованого знищення, блокування, модифікації чи копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їх мережі, а так само використання чи поширення таких програм або машинних носіїв із такими програмами*** **–** караються штрафом у розмірі від п'ятисот до однієї тисячі місячних розрахункових показників або в розмірі заробітної плати чи іншого прибутку засудженого за період від п'яти місяців до одного року, або виправними роботами на строк до двох років, або позбавленням волі на той же строк.

4. Дії, передбачені частиною третьою цієї статті, що спричинили по необережності тяжкі наслідки, **–** караються позбавленням волі на строк до п'яти років. Як узагальнення, зазначимо, що у

світовій практиці нормотворчої діяльності існують різні погляди на проблему захисту інформації в автоматизованих системах. Наприклад, у деяких країнах форма вираження інформації не має суттєвого значення для кваліфікації правопорушень. Скажімо, крадіжка інформації у вигляді комп'ютерних програм не відрізняється від крадіжки інформації на паперових носіях. Для їх правового захисту застосовуються норми національного авторського права. Правові норми захисту інформації в цих країнах забезпечуються також у межах комплексного міжгалузевого інституту права – права власності, його складової – права інтелектуальної власності чи в рамках правового інституту боротьби з недобросовісною конкуренцією.

Контрольні питання

1. Поясніть суть міжнародної інформаційної діяльності в Україні.
2. Охарактеризуйте положення „Концепції Національної програми інформатизації” у сфері міжнародного співробітництва з питань інформатизації.
3. Розкажіть про засоби міжнародної діяльності України в галузі захисту інформації.
4. Наведіть класифікацію основ правового регулювання захисту інформації в автоматизованих системах в Україні.
5. Дайте характеристику законодавства щодо захисту інформації зарубіжних країн.
6. Опишіть розвиток та формування законодавства щодо боротьби з комп’ютерною злочинністю в різних країнах.
7. Поясніть особливості інформаційного законодавства ФРН.
8. Розкрийте суть комп’ютерних злочинів за інформаційним законодавством ФРН.
9. Охарактеризуйте особливості інформаційного законодавства Норвегії.
10. Дайте характеристику інформаційного законодавства Італії.
11. Розкажіть про основи правового регулювання в сфері інформації у Франції.
12. Поясніть суть інформаційного законодавства Іспанії.
13. Опишіть особливості інформаційного законодавства Швеції.
14. Дайте характеристику видів комп’ютерних злочинів за законодавством Австралії.
15. Охарактеризуйте інформаційне законодавство Росії.
16. Наведіть класифікацію комп’ютерних злочинів за інформаційним законодавством Росії.
17. Розкажіть про основи інформаційного законодавства США.
18. Охарактеризуйте інформаційне законодавство Казахстану.

Додаток 1

Міжнародна класифікація комп'ютерних злочинів

З метою організації протидії міжнародній кіберзлочинності, а також для координації діяльності правоохоронних органів України з правоохоронними органами Інших країн та міжнародними організаціями до впорядкування законодавства України щодо боротьби з комп'ютерними злочинами правоохоронні органи України здійснюють їх класифікацію, кодування та облік відповідно до рекомендацій Інтерполу, міждержавних нормативів таким чином.

QA = Втручання в роботу або перехоплення інформації у комп'ютерній системі.

QAH = Незаконний (несанкціонований) доступ до комп'ютерної системи.

QAI = Перехоплення інформації, що циркулює в комп'ютерній мережі.

QAT = Викрадення часу за надані платні послуги (наприклад, ухилення від сплати за інформаційні послуги телефонного чи комп'ютерного зв'язку в Інтернеті чи переведення їх на іншого користувача подібних послуг).

QAZ = Інші випадки несанкціонованого доступу або перехоплення інформації.

QD = Зміна (модифікація) або пошкодження інформації в автоматизованій (комп'ютерній) системі.

QDL = " Логічна бомба".

QDT = " Троянський кінь".

QDV = "Комп'ютерні програми - віруси ". QDW = "Комп'ютерні програми - черв'яки".

QDZ *= Інші випадки пошкодження інформації в автоматизованій системі.

QF = *комп'ютерне шахрайство.*

QFC = Шахрайство з автоматами видачі готівки (банкоматами).

QFF = Комп'ютерна підробка (підроблення інформації в автоматизованій системі).

OFG = Шахрайство з комп'ютерними ігровими автоматами.

QFM = Шахрайство шляхом неправильного введення/виведення або маніпуляції комп'ютерними програмами.

QFP = Шахрайство з платіжними електронними засобами.

QFT = Телефонне шахрайство.

QFZ = Інші випадки комп'ютерного шахрайства.

QR - Несанкціоноване копіювання комп'ютерних програмних продуктів.

QRG = Несанкціоноване тиражування комп'ютерної гри.

QRS = Несанкціоноване тиражування комп'ютерного програмного забезпечення (комп'ютерних програм).

QRT = Несанкціоноване тиражування напівпровідникової продукції (топологій, топографій інтегральних мікросхем).

QRZ = Інші випадки несанкціонованого копіювання комп'ютерної інформації.

QS = Комп'ютерний саботаж (диверсія).

QSH = Саботаж з технічного забезпечення комп'ютерної системи. QSS = Саботаж з програмного забезпечення комп'ютерної системи. QSZ = Інші види комп'ютерного саботажу.

QZ = Злочини, пов'язані з комп'ютерами (комп'ютерними технологіями).

QZB = Незаконне використання дошки електронних оголошень (BBS).

QZE = Викрадення комерційної таємниці.

QZS = Зберігання або розповсюдження матеріалів, які є об'єктом судового переслідування.

QZZ = Інші випадки вчинення злочинів, пов'язаних з комп'ютерами.

Додаток 2

РОЗДІЛ XVI
ЗЛОЧИНИ У СФЕРІ ВИКОРИСТАННЯ ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ), СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ

Стаття 361. Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж

1. **Незаконне втручання в роботу автоматизованих електронно - обчислювальних машин, їх систем чи комп'ютерних мереж, що призвело до перекручення чи знищення комп'ютерної інформації або носіїв такої інформації, а також розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в ці машини, системи чи комп'ютерні мережі і здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації, – караються штрафом до сімдесяти неоподатковуваних мінімумів доходів громадян, або виправними роботами на строк до двох років, або обмеженням волі на той самий строк.**

2. **Ті самі дії, якщо вони заподіяли істотну шкоду або вчинені повторно чи за попередньою змовою групою осіб, – караються обмеженням волі на строк до п'яти років або позбавленням волі на строк від трьох до п'яти років.**

1. Предметом злочину є:

- автоматизовані електронно-обчислювальні машини (далі – АЕОN1) (комп'ютери) – це комплекси електронних пристроїв, побудованих на основі мікропроцесора, з допомогою яких здійснюються визначені комп'ютерною програмою чи користувачем операції (послідовність дій з обробки інформації і керуванню електронними пристроями) щодо символьної і образної інформації, зокрема, здійснюються її введення та виведення, знищення, копіювання, модифікація, передача інформації у системі чи мережі АЕОМ та інші інформаційні процеси. АЕОМ складається, як правило, із трьох частин: системного блоку, який включає в себе мікропроцесор і інші пристрої, необхідні для її роботи (нагромаджувачі даних, блок живлення тощо), клавіатури, з допомогою якої вводяться в АЕОМ символи, та монітора, на якому відображається текстова і графічна інформація;

- системи АЕОМ або автоматизовані системи (АС) - це системи, що здійснюють автоматизовану обробку даних, до складу яких входять технічні засоби їх обробки (засоби обчислювальної техніки і зв'язку), а також методи і процедури, програмне забезпечення (ст. 1 Закону "Про захист інформації в автоматизованих системах" від 5 липня 1994 р. // ЗУ. Том 7. - К., 1997. –296с.). До складу системи АЕОМ входить, принаймні, одна АЕОМ (комп'ютер) та периферійні пристрої, що працюють на основі

такої АЕОМ: принтер, сканер, модем, мережевий адаптер, стример та ін.;

- комп'ютерна мережа – це комплекс з'єднаних лініями електрозв'язку АЕОМ чи їх систем;

- носії комп'ютерної інформації – фізичні об'єкти, поля і сигнали, хімічні середовища, нагромаджувачі даних в інформаційних системах (ст.24 Положення про технічний захист інформації в Україні, затвердженого постановою Кабінету Міністрів України від 9 вересня 1994 р. №632;

- комп'ютерні віруси – це комп'ютерні програми (програми-віруси), які заражають електронні обчислювальні машини (комп'ютери), внаслідок чого комп'ютер виконує несанкціоновані, небажані дії. Розрізняються "комп'ютерні віруси" і "логічні бомби". Особливістю "комп'ютерних вірусів" є їх здатність відтворювати себе в декількох примірниках, змінювати (модифікувати) комп'ютерну програму, до якої вони приєднались, тим самим порушуючи нормальне функціонування комп'ютерної програми, що використовується конкретним, "зараженим" комп'ютером. "Комп'ютерні віруси" і "логічні бомби" повністю чи частково виводять із ладу програму за певних умов, наприклад, при настанні певного часу. На відміну від "комп'ютерних вірусів", які можуть розповсюджуватися по комп'ютерних мережах, "логічні бомби" не переходять в інші програми, а існують у певній комп'ютерній програмі. Кримінально-правове значення мають лише ті види комп'ютерних вірусів, які призначені не лише для незаконного проникнення в АЕОМ, їх системи чи комп'ютерні мережі, а які здатні спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації;

- комп'ютера інформація – це інформація, що використовується в АЕОМ, яка є сукупністю всіх даних і програм, які використовуються в АЕОМ незалежно від способу фізичного та логічного представлення (ст. 1 Закону від 5 липня 1994 р.), тобто та, що використовується з допомогою АЕОМ (комп'ютера), містить відомості про певні факти, події, предмети, явища, процеси, окремих осіб тощо, а також програми для АЕОМ і бази даних, має ідентифікаційні реквізити власника, який визначив режим (правила) їх використання. Комп'ютерна інформація може знаходитись на носіях інформації в АЕОМ, системі АЕОМ чи мережі АЕОМ;

- програмні і технічні засоби, призначені для незаконного проникнення в автоматизовані електронно-обчислювальні машини, їх системи чи комп'ютерні мережі.

2. **Об'єктивна сторона** злочину характеризується двома видами дій:

- втручання в роботу АЕОМ, їх систем чи комп'ютерних мереж;

- розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в АЕОМ, їх системи чи комп'ютерні мережі і здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв

такої інформації.

3. Незаконне втручання в роботу АЕОМ, їх систем чи комп'ютерних **мереж є злочином з матеріальним складом,** оскільки, крім різних дій у вигляді різного впливу на їх роботу, обов'язковими ознаками об'єктивної сторони цього злочину є також наслідки у вигляді перекручення чи знищення комп'ютерної інформації, тобто порушення її цілісності (руйнування, спотворення, модифікація і знищення) (абз.2 п.2 Положення про технічний захист інформації в Україні), і причинний зв'язок між діями і наслідками. Відсутність наслідків у вигляді перекручення або знищення комп'ютерної інформації чи носіїв такої інформації при втручанні в роботу АЕОМ, їх систем чи комп'ютерних мереж, залежно від мети такого втручання, може кваліфікуватися:

- як замах на вчинення злочину, передбаченого ст.361, якщо метою втручання було спотворити або знищити інформацію, її носії;

- за ст.ст.114, 231 (за наявності ознак цих злочинів), якщо метою втручання в роботу АЕОМ, їх систем чи комп'ютерних мереж було незаконне ознайомлення з інформацією, яка в них обробляється чи зберігається;

- за іншими статтями КК, які передбачають відповідальність за злочини, спосіб вчинення яких може виражатись у незаконному втручанні в роботу АЕОМ, їх систем чи комп'ютерних мереж, наприклад, як розкрадання майна, виготовлення з метою збуту чи використання підроблених недержавних цінних паперів (ст. 224), незаконні дії з документами на переказ та іншими засобами доступу до банківських рахунків (ст.200).

Розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в АЕОМ (комп'ютери), їх системи чи комп'ютерні мережі і здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації, є **злочином з формальним складом,** оскільки об'єктивна сторона цього злочину виражається в самих діях, незалежно від того, спричинили вони чи ні наслідки у вигляді перекручення або знищення комп'ютерної інформації чи носіїв такої інформації.

4. Під **незаконним втручанням у роботу АЕОМ, їх систем чи комп'ютерних мереж** треба розуміти будь-які дії винного, що впливають на обробку ними інформації, яка в них зберігається, або яка вводиться чи передається для обробки в АОЕМ (комп'ютери), їх системи чи комп'ютерні мережі, тобто дії, що впливають на всю сукупність операцій (зберігання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрація), що здійснюються за допомогою технічних і програмних засобів, включаючи обмін по каналах передачі даних. При втручанні в роботу АОЕМ, їх систем чи комп'ютерних мереж здійснюється порушення їх роботи, яке спричиняє спотворення процесу обробки інформації, внаслідок чого перекручується або знищується сама комп'ютерна

інформація чи її носії.

Знищення інформації – це її втрата, коли інформація в АЕОМ, їх системах чи комп'ютерних мережах перестає існувати для фізичних і юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі. Як знищення, втрату інформації треба розглядати і її блокування, тобто припинення доступу до інформації користувачам АЕОМ, їх систем чи комп'ютерних мереж. Втручання в роботу АЕОМ, їх систем чи комп'ютерних мереж може бути і в формі впливу на канали передачі інформації як між технічними засобами її обробки і зберігання всередині АЕОМ, їх систем чи комп'ютерних мереж, так і між окремими АЕОМ, їх системами чи комп'ютерними мережами, внаслідок чого інформація, що передасться для обробки, знищується чи перекручується. Такі дії можуть виражатись, наприклад, в електромагнітному, лазерному та іншому впливі на носії інформації, в яких вона матеріалізується або по яких вона передається; в формуванні сигналів, полів, засобів і блоків програм, вплив яких на інформацію, її носії і засоби технічного захисту викликає порушення цілісності інформації, її знищення чи спотворення; у включенні до бібліотек програм спеціальних програмних блоків, зміни програмного забезпечення та інших подібних діях, що призводять до порушення цілісності інформації.

Перекручення інформації – це зміна її змісту, порушення її цілісності, в тому числі і часткове знищення.

5. Під **розповсюдженням** комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в АОЕМ (комп'ютери), їх системи чи комп'ютерні мережі, і здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації, треба розуміти:

- їх передачу будь-яким способом і на будь-яких підставах (продаж, дарування, обмін, надання можливості скопіювати тощо) з метою їх використання для несанкціонованого доступу до інформації особами, які згідно з правилами розмежування доступу до інформації, встановленими власником інформації чи уповноваженою ним особою, не мають права доступу до такої інформації;

- їх "закладку" в АОЕМ (комп'ютери), їх системи чи комп'ютерні мережі на стадії їх виготовлення, ремонту, реалізації, користування з метою використання в майбутньому для здійснення несанкціонованого доступу до інформації;

- ознайомлення інших осіб із змістом програмних засобів чи технічними характеристиками або технологією виготовлення і використання технічних засобів для незаконного проникнення в АОЕМ (комп'ютери), їх системи чи комп'ютерні мережі.

Програмні засоби, призначені для незаконного проникнення в АОЕМ, їх системи чи комп'ютерні мережі – це спеціальні комп'ютерні програми (програмні блоки, програмне забезпечення), з допомогою яких

можна здійснити несанкціонований доступ до інформації, яка зберігається чи обробляється в АОЕМ, їх системах чи комп'ютерних мережах і які здатні спотворити або знищити інформацію (її носії) шляхом спотворення процесу обробки інформації.

Під комп'ютерною програмою розуміється набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп'ютером, які приводять його у дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах) (див.: ст.1 Закону "Про авторське право і суміжні права" в редакції від 11 липня 2001 р.

Технічні засоби, призначені для незаконного проникнення в АОЕМ, їх системи чи комп'ютерні мережі – це різного роду прилади, обладнання, устаткування тощо, з допомогою яких можливе або безпосереднє підключення до АЕОМ, їх систем або комп'ютерних мереж чи каналів передачі даних, або які здатні шляхом формування сигналів полів, середовищ створити умови для несанкціонованого доступу до інформації з метою ознайомлення з такою інформацією особами, які не мають права доступу до неї, або з метою впливу на процес обробки інформації в АЕОМ, порушення роботи АЕОМ, їх систем чи комп'ютерних мереж, перекручення або знищення комп'ютерної інформації чи її носіїв.

Обов'язковою ознакою (властивістю) програмних і технічних засобів, призначених для незаконного проникнення в АЕОМ, їх системи чи комп'ютерні мережі для визнання їх предметом злочину, що коментується, є їх здатність впливати на процес обробки інформації, його спотворення, в результаті чого інформація (її носії) може бути знищена чи перекручена. Якщо ж такі засоби за своїми технічними характеристиками не мають такої властивості, їх розповсюдження складу злочину, передбаченого ст.361 не утворює. Використання таких програмних і технічних засобів, наприклад, для незаконного ознайомлення з інформацією, яка обробляється чи зберігається в АЕОМ, їх системах чи комп'ютерних мережах, може кваліфікуватися за ст.ст. 114 або 231.

6. **Суб'єктивна сторона** злочину характеризується умислом щодо дій, які вчинюються винним, а психічне ставлення винного до наслідків у вигляді перекручення чи знищення комп'ютерної інформації або її носіїв може характеризуватись як прямим чи непрямим умислом, так і необережністю в обох її видах. При розповсюдженні комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в АЕОМ, їх системи чи комп'ютерні мережі, умисел лише прямий. Втручання в роботу АЕОМ, їх систем чи комп'ютерних мереж, що призводить до перекручення або знищення інформації чи її носіїв, вчинене з метою незаконного отримання інформації, залежно від змісту такої інформації і мети її неправомірного одержання, повинно кваліфікуватися за сукупністю злочинів: за ст.361 і,

відповідно, за ст.ст. 114 чи 231.

7. **Суб'єктом** злочину є особа, яка досягла 16-річного віку. Ним можуть бути особи з персоналу АЕОМ, їх систем чи комп'ютерних мереж і сторонні особи. Суб'єктами злочину у формі розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в АЕОМ, їх системи чи комп'ютерні мережі і здатних спричинити перекручення або знищення комп'ютерної інформації чи її носіїв, можуть бути розробники таких програмних і технічних засобів, їх виготовлювачі, зокрема, виробники (розробники) програм з комп'ютерними вірусами, так звані "технопацюки", "хакери" та інші.

8. В ч.2 ст.361 передбачена відповідальність за три кваліфікованих види складу злочину:

- спричинення істотної шкоди;
- вчинення злочину повторно;
- вчинення злочину за попередньою змовою групою осіб.

9. Визнання заподіяної **шкоди** при порушенні роботи АЕОМ, їх систем чи комп'ютерних мереж **істотно** залежить від багатьох обставин:

- вартості комп'ютерної інформації чи її носіїв, знищених чи перекручених;
- збитків, спричинених неможливістю використання знищеної або перекрученої комп'ютерної інформації чи її носіїв;
- затрат на відновлення змісту перекрученої або знищеної комп'ютерної інформації чи її носіїв;
- збитків внаслідок використання неправомірно одержаної комп'ютерної інформації тощо.

При цьому не повинні враховуватись витрати, які несуть власники, розпорядники і користувачі АЕОМ, їх систем чи комп'ютерних мереж для технічного захисту інформації в них від несанкціонованого доступу до інформації, її приховування, затрати на заході з технічної дезінформації тощо.

10. Про **повторність** злочину див.: ст.32 та коментар до неї.

11. Про вчинення злочину **за попередньою змовою групою осіб** див. ч.2 ст.28 та коментар до неї. При цьому необов'язково, щоб всі особи безпосередньо виконували в повному обсязі дії, зазначені в ч.1 ст.361 (наприклад, одна особа може займатись виготовленням програм з комп'ютерними вірусами, друга – їх тиражуванням, третя – їх реалізацією, четверта – розробкою технічних засобів для незаконного проникнення в АЕОМ, їх систем чи комп'ютерні мережі, неправомірного одержання інформації, яка зберігається чи обробляється в АЕОМ). При цьому дії співучасників, які безпосередньо не вчинили дій, що утворюють об'єктивну сторону незаконного втручання в роботу АЕОМ, їх систем чи комп'ютерних мереж, повинні кваліфікуватися з посиланням на відповідну частину ст.27. У разі вчинення злочину, передбаченого

ст.361. організованою групою з розподілом ролей, дії всіх членів такої групи повинні кваліфікуватися безпосередньо за ст.361.

12. Незаконне втручання в роботу АЕОМ, їх систем чи комп'ютерних мереж може бути способом вчинення інших, найчастіше більш тяжких, злочинів: диверсії (ст.113), шпигунства (ст. 114), розкрадання майна (ст. 190), виготовлення з метою збуту або використання підроблених недержавних цінних паперів (ст. 224) та інших. У таких випадках дії винного повинні кваліфікуватися за сукупністю злочинів: за ст.361 і відповідною статтею КК, яка передбачає відповідальність за злочин, вчинений шляхом незаконного втручання в роботу АЕОМ, їх систем чи комп'ютерних мереж.

Стаття 362. Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем.

1. Викрадення, привласнення, вимагання комп'ютерної ін формації або заволодіння нею шляхом шахрайства чи зловживання службовою особою своїм службовим становищем – караються штрафом від п'ятдесяти до двохсот неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, – караються штрафом від ста до чотирьохсот неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років, або позбавленням волі на той самий строк.

3. Дії, передбачені частинами першою або другою цієї статті, якщо вони заподіяли істотну шкоду, – караються позбавленням волі на строк від двох до п'яти років.

1. **Предметом злочину** є комп'ютерна інформація (див.: підпункт 6 п.1 коментарю до ст.361).

Інформація, в тому числі і комп'ютерна, є об'єктом права власності громадян, організацій (юридичних осіб) і держави, вона може бути об'єктом права власності як у повному обсязі, так і об'єктом лише володіння, користування чи розпорядження. Підставами виникнення права власності на інформацію є її створення своїми силами і за свій рахунок, договір на створення інформації або договір, що містить умови переходу права власності на інформацію до іншої особи. Власник інформації має право здійснювати щодо неї будь-які законні дії (ст.38 Закону "Про інформацію" від 2 жовтня 1992 р.

Комп'ютерна інформація не є окремим видом інформації, вона є формою зберігання статистичної, масової, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру, інформації про діяльність державних органів влади та органів самоврядування, наукової, технічної та іншої інформації. Право власності на комп'ютерну інформацію, створену як вторинну в процесі обробки в АЕОМ, їх

системах чи комп'ютерних мережах, встановлюється з урахуванням норм авторського права на підставі угоди між власником вхідної інформації і користувачем АЕОМ. Якщо такої угоди немає, то така інформація належить користувачу АЕОМ, який здійснив цю обробку. Доступ до інформації, яка зберігається, обробляється і передається в АЕОМ, здійснюється лише згідно з правилами розмежування доступу, встановленими власником інформації чи уповноваженою ним особою (ст.ст.4, 6 Закону "Про захист інформації в автоматизованих системах").

Комп'ютерна інформація є об'єктом права інтелектуальної власності, але не є майном, тобто не є предметом злочинів, передбачених ст.ст. 185-187, 189-191, а тому, незалежно від вартості викраденої інформації чи інформаційної продукції (великий чи особливо великий розмір згідно з примітками 3 та 4 до ст.185) чи розміру завданої її викраденням шкоди (значна шкода згідно з приміткою 2 до ст.185), дії винного не можуть кваліфікуватися як розкрадання за ст.ст. 185-187 чи 189-191. В той же час викрадення комп'ютерної інформації, її привласнення чи заволодіння нею шляхом шахрайства чи зловживання службової особи своїм службовим становищем разом з матеріальним носієм, на якому вона зафіксована, залежно від вартості носія інформації та способу незаконного заволодіння таким носієм має кваліфікуватися, за наявності підстав, за сукупністю злочинів – за ст.362 та ст.ст. 185-187, 189-191 КК, оскільки матеріальний носій є майном, тобто предметом злочинів проти власності.

2. **З об'єктивної сторони** злочин виражається у розкраданні, тобто у заволодінні комп'ютерною інформацією шляхом крадіжки, грабежу чи розбою, її привласненні або заволодінні нею шляхом шахрайства чи зловживання службовою особою своїм службовим становищем, або у вимаганні такої інформації.

Про поняття **"крадіжка", "грабіж", "розбій", "вимагання", "шахрайство", "привласнення", "заволодіння шляхом зловживання службовою особою своїм службовим становищем"** та про момент закінчення таких злочинів дивись коментарі до ст.ст. 185-187, 189-191.

3. Способи викрадення комп'ютерної інформації чи заволодіння нею можуть бути різними: копіювання інформації, вилучення матеріальних носіїв інформації, на яких вона зберігається, чи заволодіння ними. Здебільшого викрадення комп'ютерної інформації вчинюється таємно шляхом несанкціонованого доступу (втручання в роботу) до АЕОМ, їх систем чи комп'ютерних мереж, у яких вона зберігається чи обробляється. Якщо такий несанкціонований доступ буде пов'язаний із перекрученням чи знищенням комп'ютерної інформації чи її носіїв, дії винного мають додатково кваліфікуватися і за ст.361 за наявності всіх інших необхідних ознак передбаченого нею злочину.

Застосування насильства при відкритому викраденні комп'ютерної інформації чи вимаганні не охоплюється ст.362 і має кваліфікуватися

додатково за статтями КК, що передбачають відповідальність за злочини проти здоров'я. Викрадення комп'ютерної інформації шляхом незаконного використання спеціальних технічних засобів негласного отримання інформації має кваліфікуватися за сукупністю злочинів ─ ст.362 та ст.359. Незаконне ознайомлення з інформацією, не пов'язане із її викраденням, чи заволодінням нею, а також її незаконне розголошення, не може кваліфікуватись за ст.362. Такі дії, за наявності підстав, можуть кваліфікуватися за ст.ст. 114, 163, 182, 231 чи 330.

4. Із **суб'єктивної сторони** злочин характеризується лише умисною виною, вид умислу прямий.

5. **Суб'єктом** злочину у формі розкрадання комп'ютерної інформації шляхом крадіжки, грабежу чи розбою, заволодіння нею шляхом шахрайства, а також вимаганні комп'ютерної інформації є особа, що досягла 16-річного віку. Суб'єкт злочину у формі привласнення комп'ютерної інформації та заволодіння нею шляхом зловживання службовою особою своїм службовим становищем спеціальний: особа, що має доступ до комп'ютерної інформації у зв'язку з виконанням нею роботи з управління експлуатації чи обслуговування АЕОМ, їх систем чи комп'ютерних мереж або службова особа.

6. Кваліфікованими видами злочину є його вчинення повторно або за попередньою змовою групою осіб (ч.2), або якщо воно заподіяло істотну шкоду (ч.3).

Повторним слід вважати повторне вчинення особою у будь-якій послідовності передбачених ч.1ст.362 дій за умови, що вони не охоплюються єдиним умислом і не утворюють у своїй сукупності єдиного продовжуваного злочину, тобто умисел на їх вчинення кожен раз виникав самостійно.

Вчиненим за **попередньою змовою групою осіб** викрадення, привласнення, вимагання комп'ютерної інформації чи заволодіння нею шляхом шахрайства чи зловживання службовою особою своїм службовим становищем буде у разі, коли зазначені дії вчинені двома або більше особами, які попередньо домовились про спільне їх вчинення.

Про поняття **істотної шкоди** дивись п.9 коментарю до ст.361.

7. Комп'ютерні програми і комп'ютерні бази даних є об'єктами авторських і суміжних прав, а тому їх викрадення, привласнення чи незаконне заволодіння ними і наступне незаконне відтворення чи розповсюдження має кваліфікуватись за сукупністю злочинів ст.362 та ст. 176.

Викрадення інформації, її привласнення чи незаконне заволодіння інформацією, що містить відомості про об'єкти права промислової власності (винахід, корисна модель, промисловий зразок, кваліфіковане позначення походження товарів, топографія інтегральних схем, сорт рослин) та її наступне незаконне використання має кваліфікуватись за сукупністю злочинів ст.362 та ст.177. База даних – це сукупність творів,

даних або будь-якої іншої незалежної інформації у довільній формі, в тому числі – електронній, підбір і розташування складових частин якої та її упорядкування є результатом творчої праці, і складові частини якої є доступними індивідуально і можуть бути знайдені за допомогою спеціальної пошукової системи на основі електронних засобів (комп'ютера) чи інших засобів (див.: ст.1 Закону "Про авторське право і суміжні права" в редакції від 11 липня 2001р.

Стаття 363. Порушення правил експлуатації автоматизованих електронно-обчислювальних систем

1. Порушення правил експлуатації автоматизованих електронно-обчислювальних машин, їх систем чи комп'ютерних мереж особою, яка відповідає за їх експлуатацію, якщо це спричинило викрадення, перекручення чи знищення комп'ютерної інформації) засобів її захисту, або незаконне копіювання комп'ютерної інформації, або істотне порушення роботи таких машин, їх систем чи комп'ютерних мереж – карається штрафом до п'ятдесяти неоподатковуваних мінімумів доходів громадян або позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до п'яти років, або виправними роботами на строк до двох років.

2. Те саме діяння, якщо воно заподіяло істотну шкоду, – карається штрафом до ста неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або обмеженням волі на строк до п'яти років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого.

1. Технічний захист комп'ютерної інформації в АЕОМ, їх системах та комп'ютерних мережах забезпечується комплексом конструкторських, організаційних, програмних і технічних заходів на всіх етапах їх створення й експлуатації. Основними методами та засобами технічного захисту комп'ютерної інформації є:

- використання захищених засобів; регламентування роботи користувачів, технічного персоналу, програмних засобів, елементів баз даних і носіїв інформації (розмежування доступу); регламентування архітектури автоматизованих систем і засобів обчислювальної техніки; інженерно-технічне оснащення споруд і комунікацій, призначених для експлуатації автоматизованих систем і засобів обчислювальної техніки;
- пошук, виявлення і блокування закладних пристроїв (див. п.п.42, 43 Положення про технічний захист інформації в Україні, затвердженого постановою Кабінету Міністрів України від 9 вересня 1994р.

2. З об'єктивної сторони злочин виражається у порушенні правил експлуатації АЕОМ, їх систем чи комп'ютерних мереж (дія чи бездіяльність), визначених їх 1)власником, уповноваженою ним особою чи розпорядником таких АЕОМ, їх систем чи комп'ютерних мереж чи 2) виробником АЕОМ, їх

систем, комп'ютерних мереж чи їх програмного забезпечення. Обов'язковими ознаками об'єктивної сторони є наслідки у вигляді:

1) витоку інформації внаслідок її викрадення чи копіювання;

2) викрадення засобів захисту комп'ютерної інформації;

3) перекручення або знищення комп'ютерної інформації чи засобів її захисту;

4) істотного порушення роботи АЕОМ, їх систем чи комп'ютерних мереж, а також причинний зв'язок між діяннями і наслідками.

Витік інформації може бути пов'язаний також із її втратою (знищенням чи пошкодженням).

Наслідки у вигляді перекручення або знищення комп'ютерної інформації чи засобів її захисту та істотного порушення роботи АЕОМ, їх систем чи комп'ютерних мереж можуть бути спричинені діями (бездіяльністю) як осіб, які здійснюють їх експлуатацію чи відповідають за технічне чи інше забезпечення їх належної експлуатації, так і діями інших, сторонніх осіб, а у вигляді викрадення комп'ютерної інформації, її копіювання чи викрадення засобів захисту комп'ютерної інформації – лише діями сторонніх осіб, які не є відповідальними за експлуатацію АЕОМ, їх систем чи комп'ютерних мереж.

Порушення правил експлуатації АЕОМ, їх систем чи комп'ютерних мереж може виражатись у порушенні правил експлуатації їх апаратного забезпечення або у порушенні правил експлуатації їх програмного забезпечення. Порушенням правил експлуатації АЕОМ має визнаватись також невиконання чи неналежне виконання обов'язків з технічного забезпечення захисту комп'ютерної інформації, зокрема з пошуку, виявлення і блокування закладних пристроїв.

Порушення встановлених норм і вимог технічного захисту комп'ютерної інформації поділяються на три категорії: перша – невиконання норм і вимог технічного захисту комп'ютерної інформації, в результаті чого створюється реальна можливість порушення цілісності цієї інформації або її витоку технічними каналами; друга – невиконання норм і вимог технічного захисту комп'ютерної інформації, в результаті чого створюються передумови для порушення цілісності цієї інформації або її витоку; третя – невиконання інших вимог технічного захисту інформації з обмеженим доступом (див.: п.63 Положення про технічний захист інформації в Україні).

Про поняття **"викрадення" комп'ютерної інформації, "перекручення чи знищення"** комп'ютерної інформації див.: відповідно п.2 коментарю до ст.362 та п.4 коментарю до ст.361. Викрадення комп'ютерної інформації може бути вчинене шляхом несанкціонованого доступу до неї, приймання й аналізу побічних електромагнітних випромінювань і наводок, використання закладних пристроїв.

Засоби захисту комп'ютерної інформації – це технічні пристрої і (або) технологічні розробки, призначені для створення технологічної перешкоди несанкціонованого доступу до комп'ютерної інформації.

Копіювання комп'ютерної інформації – це її відтворення у електронному вигляді, перенесення на інший носій інформації з використанням програмних та (або) технічних засобів АЕОМ. Копіювання комп'ютерної інформації без використання програмно-технічних засобів АЕОМ, наприклад, шляхом сканування випромінювання монітора спеціальним технічним засобом, має розглядатись як її викрадення.

Визнання порушення роботи АЕОМ, їх систем чи комп'ютерних мереж **істотним** залежить від тривалості переривання їх роботи, складності і тривалості їх ремонту тощо.

3. Із **суб'єктивної сторони** злочин характеризується непрямим умислом чи необережністю щодо наслідків у вигляді викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту, незаконного копіювання комп'ютерної інформації чи істотного порушення роботи АЕОМ, їх систем чи комп'ютерних мереж. Саме ж порушення правил експлуатації АЕОМ, їх систем чи комп'ютерних мереж може бути як навмисним так і ненавмисним.

4. Суб'єкт злочину спеціальний -- особа, яка відповідає за експлуатацію АЕОМ, їх систем чи комп'ютерних мереж.

5. Кваліфікованим видом злочину є порушення правил експлуатації АЕОМ, їх систем чи комп'ютерних мереж, якщо воно заподіяло **істотну шкоду** (ч.2). Шкода може бути як матеріальною, так і нематеріальною. Про поняття істотної шкоди дивись п.9 коментарю до ст.361.

6. Порушення правил експлуатації АЕОМ, їх систем чи комп'ютерних мереж особою, яка відповідає за їх експлуатацію, з метою незаконного копіювання комп'ютерної інформації, її привласнення чи заволодіння нею службовою особою шляхом зловживання своїм службовим становищем, за відсутності інших наслідків, передбачених ст.363, має кваліфікуватися лише за ст.362, оскільки таке порушення є способом вчинення злочину, передбаченого ст.362, і додаткової кваліфікації за ст.363 не потребує. Якщо ж внаслідок зазначеного порушення матиме місце витік, викрадення, перекручення чи знищення комп'ютерної інформації або викрадення засобів її захисту іншими особами, або істотне порушення роботи АЕОМ, їх систем чи комп'ютерних мереж, то дії особи мають кваліфікуватися за сукупністю злочинів (ст.362 та ст.363 КК).

За матеріалами: – **Науково-практичний коментар до кримінального кодексу України** / За редакцією С.С. Яценка. – К.: А.С.К., 2002. - 936 с. – (Економіка. Фінанси. Право).

Додаток 3

ЗАКОН УКРАЇНИ

Про електронний цифровий підпис

Цей Закон визначає правовий статус електронного цифрового підпису та регулює відносини, що виникають при використанні електронного цифрового підпису.

Дія цього Закону не поширюється на відносини, що виникають під час використання інших видів електронного підпису, в тому числі переведеного у цифрову форму зображення власноручного підпису.

Якщо міжнародним договором, згода на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені цим Законом, застосовуються правила міжнародного договору.

Стаття 1. Визначення термінів

У цьому Законі терміни вживаються у такому значенні:

- електронний підпис – дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов'язані та призначені для ідентифікації підписувача цих даних;

- електронний цифровий підпис – 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;

- засіб електронного цифрового підпису – програмний засіб, програмно-апаратний або апаратний пристрій, призначені для генерації ключів, накладення та/або перевірки електронного цифрового підпису;

- особистий ключ – параметр криптографічного алгоритму формування електронного цифрового підпису, доступний тільки підписувачу;

- відкритий ключ – параметр криптографічного алгоритму перевірки електронного цифрового підпису, доступний суб'єктам відносин у сфері використання електронного цифрового підпису;

- засвідчення чинності відкритого ключа – процедура формування сертифіката відкритого ключа;

- сертифікат відкритого ключа (далі – сертифікат ключа) – документ, виданий центром сертифікації ключів, який засвідчує чинність і належність відкритого ключа підписувачу. Сертифікати ключів можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача;

- посилений сертифікат відкритого ключа (далі – посилений сертифікат ключа) – сертифікат ключа, який відповідає вимогам цього Закону, виданий акредитованим центром сертифікації ключів, засвідчувальним центром, центральним засвідчувальним органом;

- акредитація – процедура документального засвідчення компетентності центра сертифікації ключів здійснювати діяльність, пов'язану з обслуговуванням посилених сертифікатів ключів;

- компрометація особистого ключа – будь-яка подія та/або дія, що призвела або може призвести до несанкціонованого використання особистого ключа;

- блокування сертифіката ключа – тимчасове зупинення чинності сертифіката ключа;

- підписувач – особа, яка на законних підставах володіє особистим ключем та від свого імені або за дорученням особи, яку вона представляє, накладає електронний цифровий підпис під час створення електронного документа;

- послуги електронного цифрового підпису – надання у користування засобів електронного цифрового підпису, допомога при генерації відкритих та особистих ключів, обслуговування сертифікатів ключів (формування, розповсюдження, скасування, зберігання, блокування та поновлення), надання інформації щодо чинних, скасованих і блокованих сертифікатів ключів, послуги фіксування часу, консультації та інші послуги, визначені цим Законом;

- надійний засіб електронного цифрового підпису – засіб електронного цифрового підпису, що має сертифікат відповідності або позитивний експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації. Підтвердження відповідності та проведення державної експертизи цих засобів здійснюється у порядку, визначеному законодавством.

Стаття 2. Суб'єкти правових відносин у сфері послуг електронного цифрового підпису

Суб'єктами правових відносин у сфері послуг електронного цифрового підпису є:

- підписувач;
- користувач;
- центр сертифікації ключів;
- акредитований центр сертифікації ключів;
- центральний засвідчувальний орган;
- засвідчувальний центр органу виконавчої влади або іншого державного органу (далі - засвідчувальний центр);
- контролюючий орган.

Стаття 3. Правовий статус електронного цифрового підпису

Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

- електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;
- під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;
- особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті.

Електронний підпис не може бути визнаний недійсним лише через те, що він має електронну форму або не ґрунтується на посиленому сертифікаті ключа.

Стаття 4. Призначення електронного цифрового підпису

Електронний цифровий підпис призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів.

Електронний цифровий підпис використовується фізичними та юридичними особами – суб'єктами електронного документообігу для ідентифікації підписувача та підтвердження цілісності даних в електронній формі.

Використання електронного цифрового підпису не змінює порядку підписання договорів та інших документів, встановленого законом для вчинення правочинів у письмовій формі.

Нотаріальні дії із засвідчення справжності електронного цифрового підпису на електронних документах вчиняються відповідно до порядку, встановленого законом.

Стаття 5. Особливості застосування електронного цифрового підпису

Органи державної влади, органи місцевого самоврядування, підприємства, установи та організації державної форми власності для засвідчення чинності відкритого ключа використовують лише посилений сертифікат ключа.

Інші юридичні та фізичні особи можуть на договірних засадах засвідчувати чинність відкритого ключа сертифікатом ключа, сформованим центром сертифікації ключів, а також використовувати електронний цифровий підпис без сертифіката ключа.

Розподіл ризиків збитків, що можуть бути заподіяні підписувачам,

користувачам та третім особам, які користуються електронними цифровими підписами без сертифіката ключа, визначається суб'єктами правових відносин у сфері послуг електронного цифрового підпису на договірних засадах.

Захист прав споживачів послуг електронного цифрового підпису, а також механізм реалізації захисту цих прав регулюються цим Законом та Законом України "Про захист прав споживачів".

У випадках, коли відповідно до законодавства необхідне засвідчення дійсності підпису на документах та відповідності копій документів оригіналам печаткою, на електронний документ накладається ще один електронний цифровий підпис юридичної особи, спеціально призначений для таких цілей.

Порядок застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності визначається Кабінетом Міністрів України.

Порядок застосування цифрового підпису в банківській діяльності визначається Національним банком України.

Стаття 6. Вимоги до сертифіката ключа

Сертифікат ключа містить такі обов'язкові дані:

- найменування та реквізити центру сертифікації ключів (центрального засвідчувального органу, засвідчувального центру);
- позначення, що сертифікат виданий в Україні;
- унікальний реєстраційний номер сертифіката ключа;
- основні дані (реквізити) підписувача – власника особистого ключа;
- дату і час початку та закінчення строку чинності сертифіката;
- відкритий ключ;
- найменування криптографічного алгоритму, що використовується власником особистого ключа;
- інформацію про обмеження використання підпису.

Посилений сертифікат ключа, крім обов'язкових даних, які містяться в сертифікаті ключа, повинен мати ознаку посиленого сертифіката ключа.

Інші дані можуть вноситися у посилений сертифікат ключа на вимогу його власника.

Стаття 7. Права та обов'язки підписувача

Підписувач має право:

- вимагати скасування, блокування або поновлення свого сертифіката ключа;
- оскаржити дії чи бездіяльність центру сертифікації ключів у

судовому порядку.

Підписувач зобов'язаний:

- зберігати особистий ключ у таємниці;
- надавати центру сертифікації ключів дані згідно з вимогами статті 6 цього Закону для засвідчення чинності відкритого ключа;
- своєчасно надавати центру сертифікації ключів інформацію про зміну даних, відображених у сертифікаті ключа.

Стаття 8. Центр сертифікації ключів

Центром сертифікації ключів може бути юридична особа незалежно від форми власності або фізична особа, яка є суб'єктом підприємницької діяльності, що надає послуги електронного цифрового підпису та засвідчила свій відкритий ключ у центральному засвідчувальному органі або засвідчувальному центрі з дотриманням вимог статті 6 цього Закону.

Обслуговування фізичних та юридичних осіб здійснюється центром сертифікації ключів на договірних засадах.

Центр сертифікації ключів має право:

- надавати послуги електронного цифрового підпису та обслуговувати сертифікати ключів;
- отримувати та перевіряти інформацію, необхідну для реєстрації підписувача і формування сертифіката ключа безпосередньо у юридичної або фізичної особи чи у її уповноваженого представника.

Центр сертифікації ключів зобов'язаний:

- забезпечувати захист інформації в автоматизованих системах відповідно до законодавства;
- забезпечувати захист персональних даних, отриманих від підписувача, згідно з законодавством;
- встановлювати під час формування сертифіката ключа належність відкритого ключа та відповідного особистого ключа підписувачу;
- своєчасно скасовувати, блокувати та поновлювати сертифікати ключів у випадках, передбачених цим Законом;
- своєчасно попереджувати підписувача та додавати в сертифікат відкритого ключа підписувача інформацію про обмеження використання електронного цифрового підпису, які встановлюються для забезпечення можливості відшкодування збитків сторін у разі заподіяння шкоди з боку центру сертифікації ключів;
- перевіряти законність звернень про скасування, блокування та поновлення сертифікатів ключів та зберігати документи, на підставі яких були скасовані, блоковані та поновлені сертифікати ключів;
- цілодобово приймати заяви про скасування, блокування та поновлення сертифікатів ключів;
- вести електронний перелік чинних, скасованих і блокованих сер-

тифікатів ключів;

- забезпечувати цілодобово доступ користувачів до сертифікатів ключів та відповідних електронних переліків сертифікатів через загальнодоступні телекомунікаційні канали;

- забезпечувати зберігання сформованих сертифікатів ключів протягом строку, передбаченого законодавством для зберігання відповідних документів на папері;

- надавати консультації з питань, пов'язаних з електронним цифровим підписом.

Зберігання особистих ключів підписувачів та ознайомлення з ними в центрі сертифікації ключів забороняються.

Стаття 9. Акредитований центр сертифікації ключів

Центр сертифікації ключів, акредитований в установленому порядку, є акредитованим центром сертифікації ключів.

Акредитований центр сертифікації ключів має право:

- надавати послуги електронного цифрового підпису та обслуговувати виключно посилені сертифікати ключів;

- отримувати та перевіряти інформацію, необхідну для реєстрації підписувача і формування посиленого сертифіката ключа, безпосередньо у юридичної або фізичної особи чи її представника.

Акредитований центр сертифікації ключів має виконувати усі зобов'язання та вимоги, встановлені законодавством для центру сертифікації ключів, та додатково зобов'язаний використовувати для надання послуг електронного цифрового підпису надійні засоби електронного цифрового підпису.

Порядок акредитації та вимоги, яким повинен відповідати акредитований центр сертифікації ключів, встановлюються Кабінетом Міністрів України.

Стаття 10. Засвідчувальний центр

Кабінет Міністрів України за необхідності визначає засвідчувальний центр центрального органу виконавчої влади для забезпечення реєстрації, засвідчення чинності відкритих ключів та акредитації групи центрів сертифікації ключів, які надають послуги електронного цифрового підпису цьому органу і підпорядкованим йому підприємствам, установам та організаціям.

Інші державні органи за необхідності, за погодженням з Кабінетом Міністрів України, визначають свої засвідчувальні центри, призначені для виконання функцій, зазначених у частині першій цієї статті.

Засвідчувальний центр по відношенню до групи центрів

сертифікації ключів, зазначених у частині першій цієї статті, має ті ж функції і повноваження, що й центральний засвідчувальний орган стосовно центрів сертифікації ключів.

Засвідчувальний центр відповідає вимогам, встановленим законодавством для акредитованого центру сертифікації ключів.

Засвідчувальний центр реєструється, засвідчує свій відкритий ключ і акредитується у центральному засвідчувальному органі.

Положення про засвідчувальний центр центрального органу виконавчої влади затверджується Кабінетом Міністрів України.

Стаття 11. Центральний засвідчувальний орган

Центральний засвідчувальний орган визначається Кабінетом Міністрів України.

Центральний засвідчувальний орган:

- формує і видає посилені сертифікати ключів засвідчувальним центрам та центрам сертифікації ключів з дотриманням вимог статті 6 цього Закону;

- блокує, скасовує та поновлює посилені сертифікати ключів засвідчувальних центрів та центрів сертифікації ключів у випадках, передбачених цим Законом;

- веде електронні реєстри чинних, блокованих та скасованих посилених сертифікатів ключів засвідчувальних центрів та центрів сертифікації ключів;

- веде акредитацію центрів сертифікації ключів, отримує та перевіряє інформацію, необхідну для їх акредитації;

- забезпечує цілодобово доступ засвідчувальних центрів та центрів сертифікації ключів до посилених сертифікатів ключів та відповідних електронних реєстрів через загальнодоступні телекомунікаційні канали;

- зберігає посилені сертифікати ключів засвідчувальних центрів та центрів сертифікації ключів;

- надає засвідчувальним центрам та центрам сертифікації ключів консультації з питань, пов'язаних з використанням електронного цифрового підпису.

Центральний засвідчувальний орган відповідає вимогам, встановленим законодавством для акредитованого центру сертифікації ключів.

Положення про центральний засвідчувальний орган затверджується Кабінетом Міністрів України.

Стаття 12. Контролюючий орган

Функції контролюючого органу здійснює спеціально уповноважений центральний орган виконавчої влади у сфері

криптографічного захисту інформації.

Контролюючий орган перевіряє дотримання вимог цього Закону центральним засвідчувальним органом, засвідчувальними центрами та центрами сертифікації ключів.

У разі невиконання або неналежного виконання обов'язків та виявлення порушень вимог, встановлених законодавством для центру сертифікації ключів, засвідчувального центру, контролюючий орган дає розпорядження центральному засвідчувальному органу про негайне вжиття заходів, передбачених законом.

Стаття 13. Скасування, блокування та поновлення посиленого сертифіката ключа

Акредитований центр сертифікації ключів негайно скасовує сформований ним посилений сертифікат ключа у разі:

- закінчення строку чинності сертифіката ключа;
- подання заяви власника ключа або його уповноваженого представника;
- припинення діяльності юридичної особи - власника ключа;
- смерті фізичної особи - власника ключа або оголошення його померлим за рішенням суду;
- визнання власника ключа недієздатним за рішенням суду;
- надання власником ключа недостовірних даних;
- компрометації особистого ключа.

Центральний засвідчувальний орган негайно скасовує посилений сертифікат ключа центру сертифікації ключів, засвідчувального центру у разі:

- припинення діяльності з надання послуг електронного цифрового підпису;
- компрометації особистого ключа.

Центральний засвідчувальний орган, засвідчувальний центр, акредитований центр сертифікації ключів негайно блокують посилений сертифікат ключа:

- у разі подання заяви власника ключа або його уповноваженого представника;
- за рішенням суду, що набрало законної сили;
- у разі компрометації особистого ключа.

Скасування і блокування посиленого сертифіката ключа набирає чинності з моменту внесення до реєстру чинних, скасованих і блокованих посилених сертифікатів із зазначенням дати та часу здійснення цієї операції.

Центральний засвідчувальний орган, засвідчувальний центр, акредитований центр сертифікації ключів негайно повідомляють про скасування або блокування посиленого сертифіката ключа його власника.

Блокований посилений сертифікат ключа поновлюється:

- у разі подання заяви власника ключа або його уповноваженого представника;

- за рішенням суду, що набрало законної сили;

- у разі встановлення недостовірності даних про компрометацію особистого ключа.

Стаття 14. Припинення діяльності центру сертифікації ключів

Центр сертифікації ключів припиняє свою діяльність відповідно до законодавства.

Про рішення щодо припинення діяльності центр сертифікації ключів повідомляє підписувачів за три місяці, якщо інші строки не визначено законодавством. Підписувачі мають право обирати за власним бажанням будь-який центр сертифікації ключів для подальшого обслуговування, якщо інше не передбачено законодавством. Після повідомлення про припинення діяльності центр сертифікації ключів не має права видавати нові сертифікати ключів. Усі сертифікати ключів, що були видані центром сертифікації ключів, після припинення його діяльності скасовуються.

Центр сертифікації ключів, що повідомив про припинення своєї діяльності, зобов'язаний забезпечити захист прав споживачів шляхом повернення грошей за послуги, що не можуть надаватися в подальшому, якщо вони були попередньо оплачені.

Акредитований центр сертифікації ключів додатково повідомляє про рішення щодо припинення діяльності центральний засвідчувальний орган або відповідний засвідчувальний центр.

Акредитований центр сертифікації ключів протягом доби, визначеної як дата припинення його діяльності, передає посилені сертифікати ключів, відповідні реєстри посилених сертифікатів ключів та документовану інформацію, яка підлягає обов'язковій передачі, відповідному засвідчувальному центру або центральному засвідчувальному органу.

Порядок передачі акредитованим центром сертифікації ключів посилених сертифікатів ключів, відповідних реєстрів посилених сертифікатів ключів та документованої інформації, яка підлягає обов'язковій передачі, встановлюється Кабінетом Міністрів України.

Стаття 15. Відповідальність за порушення законодавства про електронний цифровий підпис

Особи, винні у порушенні законодавства про електронний цифровий підпис, несуть відповідальність згідно з законом.

Стаття 16. Розв'язання спорів

Спори, що виникають у сфері надання послуг електронного цифро-

вого підпису, розв'язуються в порядку, встановленому законом.

Стаття 17. Визнання іноземних сертифікатів ключів

Іноземні сертифікати ключів, засвідчені відповідно до законодавства тих держав, де вони видані, визнаються в Україні чинними у порядку, встановленому законом.

Стаття 18. Прикінцеві положення

1. Цей Закон набирає чинності з 1 січня 2004 року.

2. До приведення законів України та інших нормативно-правових актів у відповідність із цим Законом вони застосовуються у частині, що не суперечить цьому Закону.

3. Пункт 14 статті 9 Закону України "Про ліцензування певних видів господарської діяльності" (Відомості Верховної Ради України, 2000 р., № 36, ст. 299) після слів "надання послуг в галузі криптографічного захисту інформації" доповнити словами "(крім послуг електронного цифрового підпису)".

4. Кабінету Міністрів України протягом шести місяців з дня набрання чинності цим Законом:

- підготувати та внести до Верховної Ради України пропозиції про внесення змін до законів України, що випливають із цього Закону;
- забезпечити приведення своїх нормативно-правових актів, а також нормативно-правових актів міністерств та інших центральних органів виконавчої влади у відповідність з цим Законом;
- визначити центральний засвідчувальний орган;
- забезпечити прийняття нормативно-правових актів, передбачених цим Законом.

5. Національному банку України протягом шести місяців з дня набрання чинності цим Законом привести свої нормативно-правові акти у відповідність з цим Законом.

6. Кабінету Міністрів України разом з Національним банком України, іншими органами державної влади протягом шести місяців з дня набрання чинності цим Законом розробити та внести на розгляд Верховної Ради України програму заходів щодо впровадження електронного документа, електронного документообігу та електронного цифрового підпису.

Президент України **Л. Кучма**

м. Київ
22 травня 2003 року
№ 852-IV

Додаток4

УКАЗ
ПРЕЗИДЕНТА УКРАЇНИ

Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України"

Відповідно до статті 107 Конституції України **постановляю:**

Увести в дію рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України"

На виконання рішення Ради національної безпеки і оборони України

1. Визнати незадовільним стан виконання Кабінетом Міністрів України, Державним комітетом інформаційної політики, телебачення і радіомовлення України, Державним комітетом зв'язку та інформатизації України Указів Президента України від 21 липня 1997 року № 663 "Про рішення Ради національної безпеки і оборони України від 17 червня 1997 року "Про невідкладні заходи щодо впорядкування системи здійснення державної інформаційної політики та удосконалення державного регулювання інформаційних відносин", від 14 липня 2000 року № 887 "Про вдосконалення інформаційно-аналітичного забезпечення Президента України та органів державної влади", від 31 липня 2000 року № 928 "Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні", вимог Закону України "Про Національну програму інформатизації України", доручень Президента України від 12 квітня 2000 року, від 5 грудня 2000 року та від 25 квітня 2001 року щодо створення та забезпечення функціонування національного каналу супутникового іномовлення.

Кабінету Міністрів України провести службове розслідування причин невиконання зазначених нормативно-правових актів і доручень Президента України та вжити заходів щодо притягнення до відповідальності винних у цьому осіб.

2. Кабінету Міністрів України:

1) у місячний строк:

- подати на розгляд Верховної Ради України законопроекти про ратифікацію Європейської конвенції про транскордонне телебачення та про встановлення кримінальної відповідальності за незаконне втручання в роботу телекомунікаційного обладнання; розглянути питання щодо підписання від імені України Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних, 1981 року;

- розробити пропозиції щодо зупинення видачі ліцензій на надання послуг міжнародного та міжміського телефонного зв'язку до прийняття Закону України "Про телекомунікації" та продажу пакета акцій відкритого акціонерного товариства "Укртелеком" промисловому інвестору;

- ужити заходів до безумовного виконання прийнятих рішень, спрямованих на державну підтримку розвитку і функціонування засобів масової інформації, та Указу Президента України від 31 липня 2000 року „ 928 "Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні";

2) у двомісячний строк:

- подати на розгляд Верховної Ради України проект Концепції національної інформаційної політики та інформаційної безпеки України;

- розробити заходи щодо оптимізації системи державних органів, які реалізують інформаційну політику, забезпечивши чітке розмежування повноважень і налагодження їх взаємодії та координації, створення організаційної структури системи забезпечення інформаційної безпеки;

- проаналізувати виконання Національної програми інформатизації, переглянути проекти програм в інформаційній сфері, які фінансуються з Державного бюджету України, вжити заходів щодо першочергової реалізації та повноцінного фінансування найактуальніших із них;

- подати пропозиції щодо розвитку кабельного телебачення і проводового мовлення в регіонах України, створення Центру безпеки українського сегмента мережі Інтернет і Центру антивірусного захисту інформації;

- затвердити заходи щодо вдосконалення порядку придбання бюджетними організаціями засобів електронно-обчислювальної техніки і програмного продукту;

- підготувати законопроект про внесення змін до законодавства, передбачивши в ньому ліцензування діяльності провайдерів на території України щодо надання доступу до мережі Інтернет;

-;подати пропозиції стосовно створення системи стандартів щодо захисту інформації про озброєння, військову техніку і військово-промислові об'єкти та організаційно-методичного забезпечення системи захисту інформації у сферах взаємодії управлінь озброєння Міністерства оборони України з оборонно-промисловим комплексом;

- здійснити комплексну перевірку ефективності використання бюджетних коштів на виконання Національної програми інформатизації України, для потреб інформатизації поза цією Програмою, а також у Національній телекомпанії України, Національній радіокомпанії України, Концерні радіозв'язку, радіомовлення і телебачення, за результатами якої подати пропозиції щодо вдосконалення системи їх фінансування та оздоровлення фінансово-економічного стану. Забезпечити, починаючи з 2002 року, фінансування проектів інформатизації з Державного бюджету

України в межах Національної програми інформатизації;

- ужити заходів щодо реалізації Положення про державне замовлення на створення і розповсюдження теле- та радіопрограм з урахуванням нагальної потреби підвищення якості інформаційної продукції;

3) у тримісячний строк:

подати на розгляд Верховної Ради України законопроекти:

- про внесення змін до законодавства, що регулює питання боротьби з комп'ютерною злочинністю, та про створення відповідного міжвідомчого центру;

- про кабельне, ефірно-кабельне телебачення і телеінформаційні мережі, про діяльність у сфері інформатизації;

- вивчити питання стосовно права іноземців і осіб без громадянства на заснування друкованого засобу масової інформації, одержання фізичними особами свідоцтва про державну реєстрацію періодичного друкованого видання лише в разі створення ними редакції як юридичної особи та заборони заснування і діяльності засобів масової інформації, у статутному фонді яких більш як 30 відсотків іноземних інвестицій, та в разі необхідності подати на розгляд Верховної Ради України пропозиції про внесення відповідних змін до законодавства України;

- опрацювати заходи щодо дальшого розвитку національного інформаційного ринку на конкурентних засадах, створення сприятливого інвестиційного клімату для розвитку вітчизняних засобів масової інформації та книговидання;

- опрацювати заходи щодо реорганізації ретрансляційної мережі, передбачивши:

- переоснащення і модернізацію парку передавального обладнання Концерну радіозв'язку, радіомовлення і телебачення та перехід на сучасні засоби передачі сигналу;

- забезпечення поточного фінансування Концерну радіозв'язку, радіомовлення і телебачення за надані послуги державних телерадіоорганізацій та включення до проектів державного бюджету, починаючи з 2002 року, погашення заборгованості протягом чотирьох років;

- затвердити в установленому порядку Програму розвитку виробництва засобів зв'язку та інформатизації, забезпечити її фінансування;

- розробити пропозиції щодо створення захищеної інформаційно-телекомунікаційної системи органів державної влади, яка б надавала телекомунікаційні послуги, передбачивши заходи щодо прискорення розробки вітчизняних засобів криптографічного та технічного захисту інформації;

- затвердити Програму створення та розгортання вітчизняного виробництва засобів захисту інформації, національної захищеної інформаційної системи, захищених систем електронного документообігу

та електронного цифрового підпису, сертифікації технічних і програмних засобів інформатизації на відповідність вимогам інформаційної безпеки;

- розробити Єдину систему класифікації та кодифікації продукції оборонного та подвійного призначення, що експортується Україною;
- визначити механізм реалізації повноважень Генерального штабу Збройних Сил України щодо участі в організації і контролі за інформаційним простором держави та його здійснення в особливий період;
- створити міжвідомчу робочу групу з представників заінтересованих міністерств та інших центральних органів виконавчої влади для розроблення Національної геоінформаційної системи;

4) у шестимісячний строк:

- подати на розгляд Верховної Ради України проект Закону України "Про захист інформації в інформаційно-телекомунікаційних системах", передбачивши в ньому, зокрема:
- вимоги та правила захисту в електронних мережах інформації, яка є власністю держави, або інформації з обмеженим доступом, захист якої гарантується державою;
- обов'язкові умови захисту інформації в державних інформаційно - телекомунікаційних системах при наданні послуг із передачі даних, у тому числі з використанням мережі Інтернет;
- механізми проведення моніторингу мереж передачі даних виключно на засадах національного законодавства та міжнародного права, зокрема положень резолюції Ради Європи ENFOPOL 98;
- збереження Інтернет-провайдерами відомостей про Інтернет-трафік протягом шести місяців;
- розробити пропозиції щодо кодифікації законодавства в галузі інформаційних відносин та проект Стратегії впровадження національної інформаційної політики, приділивши увагу таким проблемам, як:
- створення і впровадження дійових механізмів реалізації інформаційних прав і свобод громадянина, суспільства і держави, закріплених у Конституції та законах України;
- дальше вдосконалення законодавства України в інформаційній сфері;
- розвиток на основі сучасних інформаційних технологій національної інформаційної інфраструктури, вдосконалення системи інформаційно-аналітичного забезпечення Президента України та органів державної влади, підвищення конкурентоспроможності національних виробників інформаційного продукту, видів інформаційного виробництва;
- визначення порядку функціонування та механізмів державного контролю за супутниковими, кабельними і комп'ютерними системами передачі інформації;
- формування єдиної державної системи зв'язків з громадськістю;
- дальша лібералізація українського ринку телекомунікацій за умов гарантування реалізації національних інтересів та недопущення

монополізації інформаційних ринків;

- розвиток науково-технічного та кадрового забезпечення інформаційної галузі;

- забезпечення інформаційного суверенітету України та вдосконалення системи захисту національних інформаційних ресурсів;

- затвердити програму розвитку та переоснащення передавального обладнання Концерну радіозв'язку, радіомовлення і телебачення на основі сучасних технічних засобів, передбачивши фінансування будівництва і ремонту ретрансляторів у прикордонних районах України;

- розробити проект Національної програми розвитку вітчизняної теле- та радіоіндустрії з урахуванням довгострокових потреб розвитку телекомунікаційних мереж, засобів зв'язку, національного сегмента мережі Інтернет, супутникових систем передачі інформації, супутникового та кабельного телебачення та вирішити в установленому порядку питання про її затвердження;

- ужити заходів щодо створення та забезпечення функціонування на постійній основі, починаючи з 1 січня 2002 року, національного супутникового каналу іномовлення з використанням наявної технічної бази апаратно-студійного комплексу Національної телекомпанії України та центральної передавальної супутникової станції державного підприємства "Укркосмос" або інших систем;

5) ужити у восьмимісячний строк заходів щодо повного забезпечення спеціальних телекомунікаційних систем України національними ключовими документами.

3. Державному комітету зв'язку та інформатизації України:

затвердити у тримісячний строк у встановленому порядку Положення про національний центр управління мережами зв'язку в системі Держкомзв'язку України;

провести разом з Національною радою України з питань телебачення і радіомовлення у шестимісячний строк координацію частот, що використовуються телерадіоорганізаціями у прикордонних районах України.

4. Міністерству України з питань надзвичайних ситуацій та у справах захисту населення від наслідків Чорнобильської катастрофи, Державному комітету зв'язку та інформатизації України, розробити у тримісячний строк проект створення служби інформації та допомоги населенню.

5. Запропонувати Антимонопольному комітету України провести у тримісячний строк перевірку додержання регіональними телерадіоорганізаціями антимонопольного законодавства України.

6. Державній митній службі України разом з Державним комітетом у справах охорони державного кордону України та Міністерством внутрішніх справ України опрацювати у місячний строк заходи щодо запобігання контрабандному ввезенню на територію України видавничої

продукції та її незаконному розповсюдженню.

7. Міністерству закордонних справ України, Державному комітету зв'язку та інформатизації України, Державному комітету інформаційної політики, телебачення і радіомовлення України опрацювати у двомісячний строк та вжити довгострокових заходів щодо розвитку зовнішньої інформаційної діяльності, інформування світової громадськості про Україну з метою формування позитивного її сприйняття у світі, щодо організації та фінансування теле- і радіомовлення за кордон.

8. Службі безпеки України подати у двомісячний строк пропозиції щодо вдосконалення роботи з протидії інформаційним агресіям та спеціальним інформаційно-пропагандистським операціям, здійснюваним проти України іноземними спецслужбами.

9. Міністерству освіти і науки України:

- опрацювати разом з Департаментом спеціальних телекомунікаційних систем і захисту інформації Служби безпеки України у двомісячний строк заходи щодо підготовки та перепідготовки спеціалістів у сфері інформаційної безпеки;

- підготувати у тримісячний строк типові навчальні програми для середніх і вищих навчальних закладів з навчальної дисципліни "Інформаційна культура";

- опрацювати разом з Міністерством економіки та з питань європейської інтеграції України, Державним комітетом інформаційної політики, телебачення і радіомовлення України, Українською Академією державного управління при Президентові України, Київським національним університетом імені Тараса Шевченка у двомісячний строк заходи щодо підвищення рівня підготовки управлінських, журналістських та технічних кадрів для інформаційної сфери, в тому числі працівників державних органів, урахування сучасних потреб при формуванні державного замовлення на підготовку молодих фахівців.

10. Утворити Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України, на яку покласти функції координації виконання заходів щодо забезпечення формування і захисту національного інформаційного простору, безпеки у цій сфері, розроблення і підготовки проектів відповідних нормативно-правових актів.

Секретареві Ради національної безпеки і оборони України подати у двомісячний строк на затвердження проект положення про зазначену Комісію та пропозиції щодо її персонального складу.

11. Про хід виконання цього Указу заслухати на засіданнях Ради національної безпеки і оборони України у березні і червні 2002 року.

12. Контроль за виконанням цього Указу покласти на Секретаря Ради національної безпеки і оборони України.

Президент України Л. Кучма
м. Київ 6 грудня 2001 року

№ 1193/2001

Додаток 5

ЗАКОН УКРАЇНИ

Про електронні документи та електронний документообіг

Цей Закон встановлює основні організаційно-правові засади електронного документообігу та використання електронних документів.

Розділ I
ЗАГАЛЬНІ ПОЛОЖЕННЯ

Стаття 1. Визначення термінів

У цьому Законі терміни вживаються в такому значенні:

- адресат – фізична або юридична особа, якій адресується електронний документ;
- дані – інформація, яка подана у формі, придатній для її оброблення електронними засобами;
- посередник – фізична або юридична особа, яка в установленому законодавством порядку здійснює приймання, передавання (доставку), зберігання, перевірку цілісності електронних документів для задоволення власних потреб або надає відповідні послуги за дорученням інших суб'єктів електронного документообігу;
- обов'язковий реквізит електронного документа – обов'язкові дані в електронному документі, без яких він не може бути підставою для його обліку і не матиме юридичної сили;
- автор електронного документа – фізична або юридична особа, яка створила електронний документ;
- суб'єкти електронного документообігу – автор, підписувач, адре-сат та посередник, які набувають передбачених законом або договором прав і обов'язків у процесі електронного документообігу.

Стаття 2. Сфера дії Закону

Дія цього Закону поширюється на відносини, що виникають у процесі створення, відправлення, передавання, одержання, зберігання, оброблення, використання та знищення електронних документів.

Стаття 3. Законодавство про електронні документи та електронний документообіг

Відносини, пов'язані з електронним документообігом та використанням електронних документів, регулюються Конституцією України, Цивільним кодексом України, законами України "Про інформацію", "Про захист інформації в автоматизованих системах", "Про державну таємницю", "Про зв'язок", "Про обов'язковий примірник документів", "Про Національний архівний фонд та архівні установи", цим Законом, а також іншими нормативно-правовими актами.

Якщо міжнародним договором України, згода на обов'язковість якого надана Верховною Радою України, встановлено інші правила, ніж ті, що передбачені цим Законом, застосовуються правила міжнародного договору.

Стаття 4. Державне регулювання електронного документообігу

Кабінет Міністрів України та інші органи виконавчої влади в межах повноважень, визначених законом, реалізують державну політику електронного документообігу.

Державне регулювання у сфері електронного документообігу спрямовано на:

- реалізацію 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.

Розділ II
ЕЛЕКТРОННИЙ ДОКУМЕНТ

Стаття 5. Електронний документ

Електронний документ – документ, інформація в якому зафіксована у вигляді електронних даних, включаючи обов'язкові реквізити документа.

Склад та порядок розміщення обов'язкових реквізитів електронних документів визначається законодавством.

Електронний документ може бути створений, переданий, збережений і перетворений електронними засобами у візуальну форму.

Візуальною формою подання електронного документа є відображення даних, які він містить, електронними засобами або на папері у формі, придатній для приймання його змісту людиною.

Стаття 6. Електронний підпис

Електронний підпис є обов'язковим реквізитом електронного документа, який використовується для ідентифікації автора та/або підписувача електронного документа іншими суб'єктами електронного документообігу.

Накладанням електронного підпису завершується створення електронного документа.

Відносини, пов'язані з використанням електронних цифрових підписів, регулюються законом.

Використання інших видів електронних підписів в електронному документообігу здійснюється суб'єктами електронного документообігу на договірних засадах.

Стаття 7. Оригінал електронного документа

Оригіналом електронного документа вважається електронний примірник документа з обов'язковими реквізитами, у тому числі з електронним цифровим підписом автора.

У разі надсилання електронного документа кільком адресатам або його зберігання на кількох електронних носіях інформації кожний з електронних примірників вважається оригіналом електронного документа.

Якщо автором створюються ідентичні за документарною інформацією та реквізитами електронний документ та документ на папері, кожен з документів є оригіналом і має однакову юридичну силу.

Оригінал електронного документа повинен давати змогу довести його цілісність та справжність у порядку, визначеному законодавством; у визначених законодавством випадках може бути пред'явлений у візуальній формі відображення, в тому числі у паперовій копії.

Електронна копія електронного документа засвідчується у порядку, встановленому законом.

Копією документа на папері для електронного документа є візуальне подання електронного документа на папері, яке засвідчене в порядку, встановленому законодавством.

Стаття 8. Правовий статус електронного документа та його копії

Юридична сила електронного документа не може бути заперечена виключно через те, що він має електронну форму.

Допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму.

Електронний документ не може бути застосовано як оригінал:

1) свідоцтва про право на спадщину;

2) документа, який відповідно до законодавства може бути створений лише в одному оригінальному примірнику, крім випадків існування централізованого сховища оригіналів електронних документів;

3) в інших випадках, передбачених законом.

Нотаріальне посвідчення цивільно-правової угоди, укладеної шляхом створення електронного документа (електронних документів), здійснюється у порядку, встановленому законом.

Розділ III
ЗАСАДИ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Стаття 9. Електронний документообіг

Електронний документообіг (обіг електронних документів) – 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.

Порядок електронного документообігу визначається державними органами, органами місцевого самоврядування, підприємствами, установами та організаціями всіх форм власності згідно з законодавством.

Стаття 10. Відправлення та передавання електронних документів

Відправлення та передавання електронних документів здійснюються автором або посередником в електронній формі за допомогою засобів інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем або шляхом відправлення електронних носіїв, на яких записано цей документ.

Якщо автор і адресат у письмовій формі попередньо не домовилися про інше, датою і часом відправлення електронного документа вважаються дата і час, коли відправлення електронного документа не може бути скасовано особою, яка його відправила. У разі відправлення електронного документа шляхом пересилання його на електронному носії, на якому записано цей документ, датою і часом відправлення вважаються дата і час здавання його для пересилання.

Вимоги підтвердження факту одержання документа, встановлені законодавством у випадках відправлення документів рекомендованим листом або передавання їх під розписку, не поширюються на електронні документи. У таких випадках підтвердження факту одержання електронних документів здійснюється згідно з вимогами цього Закону.

Стаття 11. Одержання електронних документів

Електронний документ вважається одержаним адресатом з часу надходження авторові повідомлення в електронній формі від адресата про одержання цього електронного документа автора, якщо інше не передбачено законодавством або попередньою домовленістю між

суб'єктами електронного документообігу.

Якщо попередньою домовленістю між суб'єктами електронного документообігу не визначено порядок підтвердження факту одержання електронного документа, таке підтвердження може бути здійснено в будь-якому порядку автоматизованим чи іншим способом в електронній формі або у формі документа на папері. Зазначене підтвердження повинно містити дані про факт і час одержання електронного документа та про відправника цього підтвердження.

У разі ненадходження до автора підтвердження про факт одержання цього електронного документа вважається, що електронний документ не одержано адресатом.

Якщо автор і адресат у письмовій формі попередньо не домовилися про інше, електронний документ вважається відправленим автором та одержаним адресатом за їх місцезнаходженням (для фізичних осіб – місцем проживання), у тому числі якщо інформаційна, телекомунікаційна, інформаційно-телекомунікаційна система, за допомогою якої одержано документ, знаходиться в іншому місці. Місцезнаходження (місце проживання) сторін визначається відповідно до законодавства.

Стаття 12. Перевірка цілісності електронного документа

Перевірка цілісності електронного документа проводиться шляхом перевірки електронного цифрового підпису.

Стаття 13. Зберігання електронних документів та архіви електронних документів

Суб'єкти електронного документообігу повинні зберігати електронні документи на електронних носіях інформації у формі, що дає змогу перевірити їх цілісність на цих носіях.

Строк зберігання електронних документів на електронних носіях інформації повинен бути не меншим від строку, встановленого законодавством для відповідних документів на папері.

У разі неможливості зберігання електронних документів на електронних носіях інформації протягом строку, встановленого законодавством для відповідних документів на папері, суб'єкти електронного документообігу повинні вживати заходів щодо дублювання документів на кількох електронних носіях інформації та здійснювати їх періодичне копіювання відповідно до порядку обліку та копіювання документів, встановленого законодавством. Якщо неможливо виконати зазначені вимоги, електронні документи повинні зберігатися у вигляді копії документа на папері (у разі відсутності оригіналу цього документа на папері). При копіюванні електронного документа з електронного носія інформації обов'язково здійснюється перевірка цілісності даних на цьому носії.

При зберіганні електронних документів обов'язкове додержання таких вимог:

1) інформація, що міститься в електронних документах, повинна бути доступною для її подальшого використання;

2) має бути забезпечена можливість відновлення електронного документа у тому форматі, в якому він був створений, відправлений або одержаний;

3) у разі наявності повинна зберігатися інформація, яка дає змогу встановити походження та призначення електронного документа, а також дату і час його відправлення чи одержання.

Суб'єкти електронного документообігу можуть забезпечувати додержання вимог щодо збереження електронних документів шляхом використання послуг посередника, у тому числі архівної установи, якщо така установа додержується вимог цієї статті. Створення архівів електронних документів, подання електронних документів до архівних установ України та їх зберігання в цих установах здійснюється у порядку, визначеному законодавством.

Розділ IV
ОРГАНІЗАЦІЯ ЕЛЕКТРОННОГО ДОКУМЕНТООБІГУ

Стаття 14. Організація електронного документообігу

Електронний документообіг здійснюється відповідно до законодавства України або на підставі договорів, що визначають взаємовідносини суб'єктів електронного документообігу.

Використання електронного документа у цивільних відносинах здійснюється згідно із загальними вимогами вчинення правочинів, встановлених цивільним законодавством.

Стаття 15. Обіг електронних документів, що містять інформацію з обмеженим доступом

Суб'єкти електронного документообігу, які здійснюють його на договірних засадах, самостійно визначають режим доступу до електронних документів, що містять конфіденційну інформацію, та встановлюють для них систему (способи) захисту.

В інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах, які забезпечують обмін електронними документами, що містять інформацію, яка є власністю держави, або інформацію з обмеженим доступом, повинен забезпечуватися захист цієї інформації відповідно до законодавства.

Стаття 16. Права та обов'язки суб'єктів електронного документообігу

Суб'єкти електронного документообігу користуються правами та мають обов'язки, які встановлено для них законодавством.

Якщо в процесі організації електронного документообігу виникає необхідність у визначенні додаткових прав та обов'язків суб'єктів електронного документообігу, що не визначені законодавством, такі права та обов'язки можуть встановлюватися цими суб'єктами на договірних засадах.

Стаття 17. Вирішення спорів між суб'єктами електронного документообігу

Вирішення спорів між суб'єктами електронного документообігу здійснюється в порядку, встановленому законом.

Стаття 18. Відповідальність за порушення законодавства про електронні документи та електронний документообіг

Особи, винні в порушенні законодавства про електронні документи та електронний документообіг, несуть відповідальність згідно з законами України.

Розділ V
ПРИКІНЦЕВІ ПОЛОЖЕННЯ

1. Цей Закон набирає чинності через шість місяців з дня його опублікування.

2. Кабінету Міністрів України протягом шести місяців з дня набрання чинності цим Законом:

- підготувати та подати на розгляд Верховної Ради України відповідні пропозиції про внесення змін до законодавчих актів України;
- забезпечити прийняття нормативно-правових актів, передбачених цим Законом;
- забезпечити перегляд і скасування міністерствами, іншими центральними органами виконавчої влади України їх нормативно-правових актів, що суперечать цьому Закону;
- разом з Національним банком України розробити та внести на розгляд Верховної Ради України програму заходів щодо впровадження електронних документів, електронного документообігу та електронного цифрового підпису, стимулювання підприємств, установ і організацій, які впроваджують електронний документообіг.

Президент України **Л. Кучма**

м. Київ

22 травня 2003 року
№ 851-IV

Література

1. Бармен Скотт. Разработка правил информационной безопасности: Пер. с англ. – М.: "Вильямс", 2002. – 208 с.
2. Вертузаєв М.С., Юрченко О.М. Захист інформації в комп'ютерних системах від несанкціонованого доступу: Навч. посібник. За ред. С.Г. Лаптєва. – К.: Вид-во. Європ. ун-ту, 2001. –321с.
3. Голубєв В.О., Говловський В.Д., Цимбалюк В.С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: Навч. посібник. За заг. ред. доктора юридичних наук, професора Р.А. Калюжного – Запоріжжя: ГУ "ЗІДМУ", 2002. – 292с.
4. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты /В.В. Домарев – К.: "ТЧД" "ДС", 2001. – 688с.
5. Ситник В.Ф. та інші. Основи інформаційних систем: Навчальний посібник . –К.: КНЕУ, 2001. – 420с.
6. Ярочкин В.И. Информационная безопасность. Учебное пособие. –М.: Международ. отношения, 2000. – 400с.
7. Конституція України. Прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 р. –К.: Преса України, 1997. –80с.
8. Закон України "Про інформацію" від 02.10.1992р. №2657 –XII.
9. Закон України "Про державну таємницю" від 21.01.1994р. №3855 –XII.
10. Закон України "Про науково-технічну інформацію" від 25.06.1993р. №3322 –XII.
11. Закон України "Про Концепцію Національної програми інформатизації" від 04.02.1998р. №75/98 –ВР.
12. Закон України "Про захист інформації в автоматизованих системах" від 05.07.1994р. №80/94 –ВР.
13. Закон України "Про стандартизацію" від 17.05.2001р. №2408 –III.
14. Закон України "Про ліцензування певних видів господарської діяльності" від 01.06.2000р. №1775 –III.
15. Указ Президента України "Про рішення Ради національної безпеки і оборони України" від 31 жовтня 2001року "Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України" від 06.12.2001р. №1193/2001.
16. Постанова Кабінету Міністрів України "Про затвердження Концепції технічного захисту інформації в Україні" від 08.10.1997р. №1126.
17. Постанова Кабінету Міністрів України "Про деякі питання захисту інформації, охорона якої забезпечується державою" від 13.03.2002р. №281.
18. Кримінальний кодекс України (прийнятий сьомою сесією Верховної Ради України 5 квітня 2001р.). –К.: Офіційний вісник України, 2001.

19. Науково-практичний коментар до Кримінального кодексу України (За ред. М.І. Мельника і М.І. Хавронського) –Київ: “Канноп”, “А.С.К.”, 2001. – 902с.
20. Державний стандарт України ДСТУ 3396.0–96. Захист інформації. Технічний захист інформації. Основні поняття. –К.: Держстандарт України. 1996. –8с.
21. Державний стандарт України ДСТУ 3396.1–96. Захист інформації. Технічний захист інформації. Порядок проведення робіт. –К.: Держстандарт України. 1996. –11с.
22. Державний стандарт України ДСТУ 3396.2–97. Захист інформації. Технічний захист інформації. Терміни та визначення. –К.: Держстандарт України. 1996. –16с.
23. Правила обов’язкової сертифікації засобів обчислювальної техніки (затв. наказом Держстандарту України від 25 червня 1997р. №366).
24. Правила обов’язкової сертифікації технічних засобів охоронної та охоронно-пожежної сигналізації (затв. наказом Держстандарту України від 10 квітня 1997р. №191).
25. Закон України “Про авторське право і суміжні права” від 23.12.1993р. №3792 – XII (в редакції закону України від 11.07.2001р. №2627 –III, з подальшими змінами та доповненнями).
26. Закон України “Про електронні документи та електронний документообіг” від 22.05.2003р. №851 – IV.
27. Закон України “Про електронний підпис” від 22.05 1993р. №852 – IV.
28. Концепція технічного захисту інформації в Україні. Затв. постановою Кабінету Міністрів України від 08.10. 1997р. №1126.
29. Концепція стратегії і тактики боротьби з комп’ютерною злочинністю в Україні (проект). –К.: 2001. –61с.
30. Положення про Державний комітет України з питань державних секретів та технічного захисту інформації (затв. Указом Президента України від 05.11.1996р. №1047/96).
31. Положення про технічний захист інформації в Україні (затв. постановою Кабінету Міністрів України від 09.09.1994р. №632)
32. Науково-практичний коментар до кримінального кодексу України. За редакцією С.С. Яценка –К.: А.С.К., 2002. –936с., (Економіка. Фінанси. Право).
33. Цивільний кодекс України (науково-практичний коментар). Під заг. редакцією д. ю. н., проф.. Є.О. Харитонова. –Х.: 000 “Одіссей”, 2001. – 800с.
34. Європейська конвенція з кіберзлочинів (підписана представниками 30 країн (у т. ч. і України) 23.11.2001р. на Будапештській конференції з проблем боротьби з кіберзлочинністю).
35. Ліцензійні умови провадження господарської діяльності, пов’язаної з розробленням, виробництвом, впровадженням, обслуговувавнням, дослідженням ефективності систем і засобів технічного захисту інформації.

Затв. наказом Державного комітету України з питань регуляторної політики та підприємництва від 29.12.2000р. №89(67).

Навчальне видання

Леонід Іванович Северин
Сергій Леонідович Северин
Андрій Веніамінович Дудатьєв

Правове забезпечення захисту інформації

Навчальний посібник

Оригінал-макет підготовлено Севериним Л.І.

Редактор О. Д. Скалоцька

Навчально-методичний відділ ВНТУ
Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001
21021, м.Вінниця, Хмельницьке шосе, 95, ВНТУ

Підписано до друку
Формат 29,7 х 42 І/4
Друк різографічний
Тираж прим.
Зам. №

Гарнітура Times New Roman
Папір офсетний
Ум. друк. арк.

Віддруковано в комп'ютерному інформаційно-видавничому центрі
Віннцького національного технічного університету
Свідоцтво Держкомінформу України
серія ДК № 746 від 25.12.2001
21021, м.Вінниця, Хмельницьке шосе, 95