Київський університет імені Бориса Грінченка

А.Ю. Нашинець-Наумова

ІНФОРМАЦІЙНЕ ПРАВО

Навчальний посібник

Київ — 2020

УДК 342.732(075.8)
Н37

Рекомендовано до друку Вченою радою
Київського університету імені Бориса Грінченка
(протокол № 7 від 29 серпня 2019 року)

Рецензенти:

Нікітенко О.І., завідувач кафедри публічно-правових дисциплін Білоцерківського національного аграрного університету, доктор юридичних наук, професор, заслужений юрист України;

Світличний О.П., професор кафедри цивільного та господарського права Національного університету біоресурсів і природокористування України, доктор юридичних наук, доцент;

Севрюков Д.Г., професор кафедри теорії права та держави Юридичного факультету Київського національного університету імені Тараса Шевченка, доктор юридичних наук, професор.

Нашинець-Наумова А.Ю.

Н37 Інформаційне право: навчальний посібник / А.Ю. Нашинець-Наумова. — К. : Київ. ун-т ім. Б. Грінченка, 2020. — 136 с.

ISBN 978-617-658-077-5

У навчальному посібнику розглядаються в єдності теорія й практика інформаційного права як чинник формування й розвитку інформаційного суспільства, кодифікації інформаційного законодавства та практики його застосування.

Навчальний посібник розрахований на студентів, магістрантів, аспірантів закладів вищої освіти. Він також буде корисним викладачам, науковим та практичним працівникам, усім, кого цікавлять інформаційні правовідносини, культура та безпека як складові інформаційної політики України.

УДК 342.732(075.8)

ISBN 978-617-658-077-5

ЗМІСТ

ЗМІСТОВИЙ МОДУЛЬ ІІ «Інформаційна безпека»

ПЕРЕДМОВА

Інформація як феномен так і не розкрила науці свою природу до кінця. Вона продовжує формувати як матеріальну, так і віртуальну реальність сучасності. Природно, що, користуючись інформацією у формі відомостей, документів, даних, знань, людина хоче знати про цей предмет якомога більше. Це бажання виникло несьогодні і не тільки у зв'язку з народженням глобальних комунікацій і технологій. Великі уми давнини прагнули до пізнання механізму знань, до того, щоб зрозуміти, як з індивідуальних спостережень і висновків виникають шляхи наступності, як утворюється естафета передачі й сприйняття того, що людина вже пізнала і продовжує освоювати.

Сьогодні питання щодо обґрунтування важливості інформаційного права не вимагає додаткових аргументів. Це комплексна галузь права, що визначає суспільні відносини щодо інформації, технологій її поширення, одержання та зберігання в усіх сферах життєдіяльності людей, їх спільнот, суспільства, держави, міжнародного співтовариства. Це система правових норм, що регулює множину дій, спрямованих на задоволення інформаційних потреб громадян, юридичних осіб і держави.

Майже понад двісті юрисдикцій різних держав визначають правила реалізації прав людини на інформацію та створюють відповідні структури надання та захисту інформації, одночасно забезпечуючи механізми убезпечення людини від шкідливої інформації. Існують і сили з протилежними цілями. Інформація є і зброєю, і товаром поряд з її основною функцією — нести знання. Завдання держави, права, всіх інститутів суспільства —

опанувати інформацію і використовувати її на благо людини. Допоможе нам в цьому нова галузь юридичних знань — інформаційне право. Саме ця галузь повинна відповісти на питання: навіщо, для чого, як використовувати ресурс інформаційної сфери сьогодні, щоб забезпечити вільне, справедливе і впорядковане завтра?

Наукова громадськість, молоде покоління — студенти нашого часу, практики в галузі створення і застосування нових технологій та інформаційного оздоровлення світу — не можуть відмовитися від моральних основ права, від його організуючої ролі в житті суспільства. Керуючись цим, автор пропонує цей навчальний посібник і сподівається, що він буде корисним у справі виховання нового покоління юристів і всіх, хто працює у сфері формування інформаційного суспільства.

Перша версія цього посібника «Основи інформаційного права» (2015) була підготовлена на базі раніше виданого практикуму, створеного за участі автора. Робота викликала великий інтерес, і в даний час з'явилася можливість оновити її з урахуванням не тільки динамічного життя, освоєння засобів інформатизації, Інтернету, а й з урахуванням еволюції законодавства в цій сфері. Тільки за останні роки в Україні прийнято чимало нових законів, ще більше створено проєктів нормативно-правових актів, що вимагають ретельного обговорення та знаходження відповідей на непрості запитання. Саме з цим пов'язана необхідність оновлення і доповнення даного посібника.

Перший змістовний модуль посібника «Основні положення інформаційного права» об'єднує проблематику, що дозволяє усвідомити специфіку інформаційного права як нової й комплексної галузі в системі права України. У ньому розглядаються проблеми предмета, сфери дії, цілі галузі; форми реалізації інформаційного права; питання складу суб'єктів і видів інформаційної діяльності; принципи правового регулювання; методи регулюван-

ня правовідносин у цій сфері, а також питання категорій, дефініцій і підстави виділення інститутів цієї галузі права. Чотири теми першого модуля дають загальне уявлення про специфіку галузі і готують студентів до глибшого розуміння проблем правового регулювання окремих інститутів.

У змістовному модулі 2 «Інформаційна безпека» вводяться базові поняття, пов'язані із забезпеченням інформаційної безпеки, розглядаються основні загрози безпеці та засоби протидії ним. Також робиться огляд формальних моделей безпеки і сучасних стандартів у цій галузі.

Крім того, до кожної теми подаються схеми, ситуаційні завдання, питання для самоперевірки та методичні рекомендації щодо вирішення задач і виконання завдань, перелік тем рефератів.

Усім причетним до обговорення проблем інформаційного права в тій чи іншій формі автор висловлює щиру подяку і сподівається на те, що спільними зусиллями будуть подолані складності в засвоєнні теорії та практики нової галузі українського права — права інформаційного.

КОРОТКИЙ ЗМІСТ НАВЧАЛЬНОЇ ДИСЦИПЛІНИ «ІНФОРМАЦІЙНЕ ПРАВО»

ЗМІСТОВИЙ МОДУЛЬ І

ОСНОВНІ ПОЛОЖЕННЯ ІНФОРМАЦІЙНОГО ПРАВА

Тема 1. Предмет інформаційного права та його принципи. Методи інформаційного права

Правова природа інформаційного права в Україні. Поняття, предмет, принципи інформаційного права. Інформаційне право як наука і як навчальна дисципліна. Методи інформаційного права. Предмет інформаційного права. Функції інформаційного права. Інформаційне право як наука та навчальна дисципліна. Предмет, методи та функції інформаційного права. Місце інформаційного права в системі правових наук. Взаємодія інформаційного права з іншими галузями права. Система інформаційного права. Державна політика у сфері суспільних інформаційних відносин. Модель інформаційної сфери. Процеси пошуку, отримання і споживання інформації.

Особливості створення і розповсюдження інформації, формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг. Поняття інформаційного простору. Єдиний інформаційний простір. Ознаки єдиного інформаційного простору.

Об'єкти інформаційного права. Поняття інформаційної сфери. Інформаційні процеси. Основні об'єкти інформацій-

ної сфери. Структура інформаційної сфери. Інформація як основний об'єкт інформаційної сфери. Особливості правової інформації.

Поняття та види інформаційних систем. Об'єкти інформаційних систем. Інформаційні технології як об'єкт інформаційних правовідносин.

Тема 2. Джерела інформаційного права

Поняття джерел інформаційного права та їх форми. Зовнішні форми інформаційного права. Інформаційне законодавство. Міжнародно-правові стандарти у сфері інформаційного права. Інформаційно-правові договори. Інформаційно-правовий акт. Підзаконні інформаційно-правові акти. Інформаційне законодавство — головне джерело інформаційного права. Становлення інформаційного законодавства України.

Загально-правові та спеціально-правові акти, що регулюють суспільні інформаційні правовідносини.

Конституційно-правове, цивільно-правове, адміністративно-правове, кримінально-правове регулювання інформаційних відносин.

Синтетичні міжгалузеві комплексні інститути права.

Структура інформаційного законодавства України.

Поняття джерел інформаційного права. Рівні та структура джерел інформаційного права.

Тема 3. Поняття і класифікація інформації

Поняття «інформація». Класифікація інформації. Право на інформацію та її обмеження. Конституційні положення щодо правового регулювання суспільних відносин, пов'язаних з інформацією. Поняття та види публіч-

ної інформації. Режими доступу до публічної інформації. Інформаційне суспільство.

Інформаційна інфраструктура. Інформація, інформаційна діяльність як об'єкт суспільних відносин. Співвідношення понять «інформація», «відомості», «дані», «коди», «сигнали», «знання», «таємниця», «телекомунікація» тощо в суспільних відносинах. Зміст терміна «документ» в інформаційній діяльності. Інформаційні ресурси як предмет суспільних відносин. Інформаційний простір як об'єкт інформаційної діяльності. Поняття та сутність глобального інформаційного простору.

Тема 4. Інформаційні відносини

Поняття та ознаки інформаційних відносин. Елементи інформаційних відносин. Види інформаційних відносин.

Інформаційні відносини, що виникають в процесі пошуку, отримання і споживання інформації, інформаційних ресурсів, інформаційних продуктів, інформаційних послуг.

Інформаційні відносини, що виникають при створенні й використанні інформаційних систем та мереж, засобів і методів інформаційної безпеки.

ЗМІСТОВИЙ МОДУЛЬ ІІ
ІНФОРМАЦІЙНА БЕЗПЕКА

Тема 5. Загальна характеристика інформаційної безпеки

Поняття інформаційної безпеки. Джерела загроз інформаційної безпеки України. Основні складові інформаційної безпеки. Основні функції інформаційної безпеки. Основні принципи побудови концепції інформаційної безпеки. Основні категорії інформаційної безпеки.

Забезпечення інформаційної безпеки. Тектологія інформаційної безпеки. Загрози національним інтересам в інформаційній сфері. Методологія інформаційної безпеки.

Терміни, що визначають предметну основу інформаційної безпеки.

Терміни, що визначають характер діяльності щодо забезпечення інформаційної безпеки.

Доступність інформації. Конфіденційність інформації. Цілісність інформації.

Стандарти інформаційної безпеки. Стандарт забезпечення захисту. Доктрина інформаційної безпеки.

Тема 6. Система забезпечення інформаційної безпеки

Поняття системи забезпечення інформаційної безпеки. Рівні інформаційної безпеки. Органи (служби) інформаційної безпеки. Нормативно-правові засади побудови, поточної діяльності та розвитку системи забезпечення інформаційної безпеки України.

Загрози інформаційної безпеки. Функції системи забезпечення інформаційної безпеки.

Мета забезпечення інформаційної безпеки.

Методи забезпечення інформаційної безпеки.

Види загроз інформаційної безпеки. Оборонна, охоронна та захисна функції держави щодо інформаційних ресурсів єдиного інформаційного простору України. Охорона та захист інформації в автоматизованих (комп'ютерних) системах як вид інформаційної діяльності. Особливості правової охорони комп'ютерної інформації: комп'ютерних програм, автоматизованих баз даних і знань. Інтернет-правовідносини.

Тема 7. Забезпечення інформаційної безпеки в інтернет-просторі

Правове регулювання інформаційних відносин, що виникають при забезпеченні інформаційної безпеки в інтернет-просторі.

Кібербезпека. Інформаційна безпека в кібернетичному (віртуальному) просторі.

Кіберзлочини. Кіберзахист критичної інфраструктури.

Кібербезпекова політика.

Конвергенція і глобалізація комп'ютерних мереж.

Специфіка інформаційної безпеки суспільства в умовах формування глобальної кіберцивілізації.

Тема 8. Забезпечення інформаційної безпеки Інтернету речей

Загальна характеристика Інтернету речей. Структура Інтернету речей.

Основні компоненти Інтернету речей. Розумні пристрої. Оцінка небезпек для Інтернету речей.

Технології Інтернету речей. Big Data (Великі дані).

Інтеграція Інтернету речей в життя людини.

ЗМІСТОВИЙ МОДУЛЬ І
ОСНОВНІ ПОЛОЖЕННЯ ІНФОРМАЦІЙНОГО ПРАВА

Тема 1. ПРЕДМЕТ ІНФОРМАЦІЙНОГО ПРАВА ТА ЙОГО ПРИНЦИПИ. МЕТОДИ ІНФОРМАЦІЙНОГО ПРАВА

Значення інформації в житті людини сьогодні важко переоцінити. Діяльність щодо отримання та обробки інформації займає досить багато часу. Тому мимоволі людина стикається з величезною кількістю джерел інформації і є, відповідно, частиною глобального інформаційного обміну. У той же час, в умовах розвитку інформаційних технологій, процес пошуку й обробки інформації істотно прискорився, стали доступними практично будь-які джерела інформації в умовах реального часу.

У країні, як і в усьому світі, відбувається поступове становлення інформаційного суспільства, економічною основою якого є створення і вдосконалення технічних і технологічних способів і засобів виробництва, отримання і поширення інформації на основі створення та використання інформаційно-комунікаційних технологій, що є найважливішими ознаками сучасної інформаційної епохи. Підвищення економічної складової ІКТ вимагає створення і відповідної правової основи їх виробництва і використання.

Важливо також підкреслити зв'язок процесів інформатизації суспільства з його історичним розвитком.

Як відзначають фахівці у сфері інформаційних проблем, інформатизація життя сприяє зародженню і зміцненню основ прогресивного сучасного етапу суспільного розвитку — грома-

дянського суспільства. Крім того, серед стратегічних напрямів розвитку, забезпечення умов та державної підтримки становлення та формування інформаційного суспільства було визначено «електронні» сектори економіки (торгівлі, надання комунальних і банківських послуг тощо), системи у сферах охорони здоров'я, освіти, науки, культури, охорони довкілля, культурологічні питання оцифровування культурної спадщини держави, розвиток державно-адміністративних інститутів, притаманних інформаційному суспільству тощо.[1]

Право, виконуючи економічні та соціально-політичні функції та взаємодіючи з державою в особі уповноважених на правотворчість органів, постійно розвивається, вдосконалюється і змінюється. Це пов'язано з різними стратегічними завданнями і цілями, які ставляться в той чи інший історичний період часу державою.

Зараз метою переходу України до інформаційного суспільства є розвиток громадянського суспільства та демократичних традицій, а також подолання інформаційної нерівності при входженні громадян України в глобальне інформаційне співтовариство на основі поваги до прав людини, в тому числі права на вільний доступ до інформації, права на захист персональних даних і обов'язків розкриття інформації з боку державних, громадських і комерційних організацій.

Потреби суспільного розвитку спонукають державу не тільки розвивати і вдосконалювати правове регулювання сформованих сфер людського буття і діяльності, а й встановлювати загальнообов'язкові правила поведінки в нових сферах діяльності членів суспільства. До однієї з таких нових сфер відноситься інформаційне право.

Інформаційне право — це комплексна галузь права, яка являє собою сукупність правових норм, що закріплюють і регулюють суспільні відносини, які виникають у процесі створен-

[1] Новицький А.М. Правове регулювання інституціоналізації інформаційного суспільства в Україні: монографія. Ірпінь: НУ ДПС України, 2011. С. 65.

ня, перетворення, зберігання, розповсюдження та споживання інформації, тобто практично у всіх сферах людської діяльності, пов'язаної з інформацією або діяльністю в інформаційній сфері.

Оскільки сфера інформатики та інформаційних відносин активно розвивається, природно, що і правова термінологія теж розширюється.

Для інформаційного права особливе значення мають дефінітивні норми. Вони встановлюють терміни і поняття, що використовуються в усіх галузях права, в тому числі й в інформаційному, у зв'язку з регулюванням соціальних інститутів в інформаційній сфері. До таких термінів і понять відносять: інформаційні ресурси, державні інформаційні ресурси, документ, документовану інформацію, комп'ютерні системи, технології та засоби їх забезпечення, захист інформації, інформацію про громадян, інтелектуальну власність, систему моніторингу навколишнього середовища тощо. Внаслідок формування інформаційного права і становлення системи інформаційного законодавства з'являються нові поняття, терміни, яким необхідні конкретні визначення для правильного застосування в регулятивних нормах. Крім загальних проблем, що стосуються інформації безпосередньо і її окремих видів, багато дефініцій зосереджено в конкретних сферах відносин (наука, культура, виборча система тощо).

Завдання інформаційного права — здійснити аналіз стану цієї частини законодавства і запропонувати підходи до уніфікації термінології і всього понятійного апарату у сфері інформаційних відносин, регульованих законодавством.

Зважаючи на вищезазначене, **інформаційне право** — це наука про предмети, принципи та методи правового регулювання, формування і використання інформаційних ресурсів, технологій і комунікацій та їх мереж, організації управління процесами інформатизації та забезпечення інформаційної безпеки громадян, держави і суспільства з метою задоволення їх інформаційних потреб.

Інформаційні відносини, пов'язані зі стрімким розвитком інформаційно-комунікаційних технологій, розширюють сферу їх правового регулювання і роблять актуальним питання про відокремлення інформаційного права в окрему галузь права. У доктрині інформаційного права сформовані кілька точок зору щодо місця інформаційного права в правовій системі, які умовно можна розділити на дві групи: інформаційне право — частина традиційних галузей права й інформаційне право — самостійний елемент системи права.

1. Інформаційне право як частина традиційних галузей права:
   - цивільного права;
   - адміністративного права.

Тут слід зазначити, що таке розуміння інформаційного права не охоплює всього масиву норм в інформаційній сфері, хоча вони і містяться в складі різних галузей права. Наприклад, окремі норми інформаційного права містяться:

- в Конституції України (закріплено право на інформацію, свободу засобів масової інформації, захист інформації про приватне життя фізичної особи та персональних даних тощо);
- в Цивільному кодексі України (одержання, розміщення, надання інформації; правове регулювання службової та комерційної таємниці; правове регулювання захисту честі, гідності та ділової репутації; виняткові права на результати інтелектуальної діяльності тощо);
- Кодексі України про адміністративні правопорушення (незаконна відмова в наданні інформації, надання завідомо неправдивої інформації, незаконне використання або розголошення відомостей, порушення правил захисту інформації, недотримання вимог до інформації, розголошення комерційної або іншої таємниці, несанкціонований доступ до комп'ютерної інформації, відповідальність за адміністративні правопорушення в галузі зв'язку та інформації);

- Кримінальному кодексі України;
- банківському, земельному, митному праві; тут закріплюються особливості обороту різних видів інформації, інформаційних систем і застосування інформаційних технологій у різних сферах господарської діяльності.

2. Інформаційне право — самостійний елемент системи права:
   - комплексна галузь права;
   - міжгалузевий комплексний інститут права.

Під інформаційним законодавством ми розуміємо комплексний масив, що складається із сукупності всіх діючих нормативно-правових актів різної юридичної сили, що спеціалізуються на регулюванні інформаційних відносин щодо обігу інформації в інформаційній сфері. Аналіз теоретичних розробок показує, що в якості первинного елемента інформаційного законодавства виступає нормативно-правовий акт, а для інформаційного права — норма. Юридичний нормативний акт є носієм, формою закріплення і вираження норм права, і саме цим обумовлена його нормативність.

Системно-структурний підхід зумовлює поділ інформаційного права на структурні частини: Загальну і Особливу.

У даний час чітка структура системи інформаційного права відсутня, проте в доктрині права є погляди щодо переліку норм права, що складають Загальну частину, серед них норми, що регулюють: загальні положення (поняття і види інформації, суб'єкти інформаційного права, система інформаційного права, взаємозв'язок інформаційного права з іншими галузями права тощо); принципи; предмет і метод правового регулювання; джерела інформаційного права; юридичну відповідальність в інформаційній сфері та інші питання.

Що стосується Особливої частини, то вона складається з окремих інститутів інформаційного права, в яких згруповані близькі за значенням і сутністю інформаційні правові норми. Зв'язок між ними носить «об'єктивний характер».

Особлива частина інформаційного права включає: структурні підрозділи (норми, інститути, субінститути), які групуються у дві основні підгалузі інформаційного права:

- інформаційне економічне право (регулює порядок здійснення в інформаційній мережі електронної економічної діяльності: електронної торгівлі, інтернет-банкінгу, електронного консалтингу, електронного рекламінгу, інтернет-страхування тощо);
- інформаційне гуманітарне право (регулює порядок здійснення в інформаційній мережі економічної гуманітарної діяльності щодо забезпечення державою інформаційних прав фізичних осіб, у тому числі шляхом створення та функціонування систем електронного адміністрування).

Іншим напрямком виступає забезпечення державою інформаційних прав громадян, у тому числі на вільний обіг незахищеної (що знаходиться у відкритому доступі) інформації, її збір, обробку і поширення в електронній формі.

Таким чином, якщо Загальна частина інформаційного права представлена переважно з сукупності норм, що регулюють загальні положення різногалузевих інформаційних відносин, то Особлива частина представлена з сукупності норм, окремих правових інститутів, що регулюють різногалузеві інформаційні відносини. Виділяють ще й спеціальну частину в структурі інформаційного права, яка, наприклад, включає: правовідносини у сфері засобів масової інформації (медіаправо); правовідносини у сфері інформатизації, у сфері науки, інформаційної культури, бібліотечної, архівної, статистичної та інших галузей інформаційної діяльності; правовідносини в інформаційному праві; в інших сферах діяльності.

Інформація не обмежується рамками комп'ютера або систем комп'ютерів. Завдяки розвитку засобів зв'язку, зокрема супутникових систем, сформувалася ще одна сфера відносин, яка перебуває в найтіснішому контакті з інформаційним ресурсом — це система комунікацій інформації — телекомунікація.

Проблематика забезпечення безпеки в інформаційній сфері, вирішення конфліктів, реалізації відповідальності за правопорушення в цій галузі відносин не може викликати сумнівів. Однак і тут є проблеми, до яких належить звернутися. З урахуванням складності структури предмета інформаційного права питання щодо методів цієї галузі є не менш важливими.

Оскільки інформація супроводжує практично всі сфери людської діяльності, то для регулювання інформаційних відносин застосовуються різні існуючі методи публічного і приватного права в залежності від виду й призначення інформації та характеру поведінки суб'єктів.

В інформаційному праві застосовуються диспозитивні методи, тобто при регулюванні відносин інформаційної власності (речової та інтелектуальної), при створенні й використанні інформаційних технологій і засобів їх забезпечення (право автора й право власності, відношення замовника й розробника інформаційних технологій та засобів їх забезпечення) тощо. Цей метод заснований на рівних можливостях суб'єктів, їх самостійності при вступі в інформаційні відносини, самостійності здійснення ними своїх прав, відповідальності.

Також в інформаційному праві діє метод імперативного регулювання інформаційних відносин. Це використання владовідносин («команда – виконання»), відсутність згоди сторін, наявність нерівноправних сторін, сувора зв'язаність суб'єктів права правовими рамками (суб'єкти публічного права діють на свій розсуд, але лише в межах наданих законом повноважень). Існують поєднання переконання і примусу, також позитивне зобов'язання — діяти в певному напрямку для досягнення тих чи інших цілей. Оскільки інформаційне право як нова наукова дисципліна тільки формується, не можна точно дати відповідь на питання, який же метод переважає. Можна припустити, що все-таки домінує імперативний метод. Він застосовується, наприклад, при здійсненні дій, пов'язаних з державною реєстрацією інформаційних ресурсів та інформаційних систем,

при регулюванні інформаційних відносин в галузі масової інформації, при вирішенні органами державної влади й іншими структурами завдань у сфері ліцензування певних видів діяльності та сертифікації продуктів і послуг в інформаційній сфері, при формуванні й реалізації відповідними структурами державної політики щодо формування та розвитку інформаційного суспільства.

Схеми до теми

Інформаційне право — це комплексна галузь права, що вивчає сукупність правових норм, які регулюють суспільні відносини, що виникають між суб'єктами щодо пошуку, передачі, отримання, виробництва та розповсюдження інформації, використання інформаційних технологій та інформаційних ресурсів та захисту інформації.

Об'єктом інформаційного права є суспільні відносини, які пов'язані зі створенням, формуванням, зберіганням, обробкою, поширенням, використанням інформаційних продуктів, наданням інформаційних послуг, управлінням процесом формування й використання інформаційного продукту та надання інформаційних послуг, розвитком і застосуванням нових технологій роботи з інформацією та її передачі в системах і мережах комунікацій, посиленням безпеки в інформаційній сфері, а також з юридичною відповідальністю суб'єктів права у цих відносинах.

Предмет інформаційного права визначається відповідно до суті інформаційного законодавства й практики розвитку нових суспільних відносин щодо інформації. *Провідний предмет* — це інформація. *Безпосередніми предметами* є конкретні види та форми інформації щодо конкретних інформаційних відносин, інформаційної діяльності й технологій об'єктивізації відомостей, даних, сигналів, кодів тощо.

Методи правового регулювання в галузі інформації — це системне комплексне застосування методів конституційного, цивільного, адміністративного, трудового та кримінального права та методів приватно-правового регулювання (на рівні правочинів, угод, звичаїв, традицій тощо).

Методи інформаційного права

Загальні:
— диспозитивний та імперативний;
— автономії й рівності сторін;
— індивідуальний метод регулювання.

Часткові:
— наказу, зв'язування, заборони, дозволу;
— узгодження, рекомендацій, координації, заохочення.

Принципи інформаційного права базуються на положеннях основних конституційних норм, що закріплюють інформаційні права і свободи та гарантують їх здійснення, а також на особливостях та юридичних властивостях інформації як об'єкта правовідносин.

Принципи інформаційного права

Принцип пріоритетності прав особистості в інформаційній сфері

Принцип вільного виробництва та розповсюдження будь-якої інформації, на яку не встановлені заборони законодавством

Принцип заборони виробництва та розповсюдження інформації, шкідливої і небезпечної для розвитку особистості, суспільства, держави

Система інформаційного права

Загальна

У Загальній частині зосереджені норми, які встановлюють основні поняття, загальні принципи, правові форми та методи правового регулювання діяльності в інформаційній сфері.

Особлива

Особлива частина включає окремі інститути інформаційного права, в яких згруповані близькі за змістом інформаційно-правові норми.

Ситуаційні завдання до теми

Задача 1

Студент Історико-філософського факультету Київського університету імені Б. Грінченка Шелест під час написання дипломної роботи звернувся до бібліотеки навчального закладу із запитом — підібрати йому неопубліковані роботи та іншу інформацію, яка стосується діяльності Радянського інформаційного бюро і центральних газет у роки Великої Вітчизняної війни. У бібліотеці Шелесту відмовили в проханні, спираючись на те, що ці джерела знаходяться в спеціальному сховищі бібліотеки, до якого студенти не мають доступу. Шелест поскаржився на працівників бібліотеки ректору університету, але й останній відмовив йому, зауваживши, що подібна інформація підбирається лише в наукових цілях. Шелест написав скаргу до Міністерства освіти і науки України.

➤ *Чи правомірними є дії працівників бібліотеки з точки зору інформаційно-правових відносин?*

Задача 2

Інженер-програміст Іванов був прийнятий на роботу в приватне акціонерне товариство «Онор», де виконував функції оператора ЕОМ. Його обов'язками було введення інформації щодо норм чинного законодавства в інформаційну базу, яку «Онор» продавав на комерційній основі підприємствам легкої промисловості. У вільний від введення інформації час Іванову вдалося розробити і впровадити більш досконалий алгоритм обробки правової інформації в інформаційній базі, що помітно підвищило її цінність і призвело до отримання значного прибутку. На зборах засновників приватного акціонерного товариства «Онор»

було запропоновано преміювати Іванова, а його розробку використовувати в ході реалізації модернізованої програми на вигідних комерційних умовах. Однак Іванов заявив керівництву товариства, що воно порушує його авторські права, і зажадав, щоб йому відраховували весь прибуток за використання його програмного продукту.

➤ *Як вирішити цей спір з позиції норм інформаційного права?*

Завдання 1

Здійснити в мережі Інтернет пошук відомостей щодо джерел інформаційного права. Результати пошуку обробити аналітично.

Завдання 2

У відповідних джерелах, у тому числі й у мережі Інтернет, знайти визначення поняття «інформація».

Завдання 3

Проаналізуйте та виділіть схематично основні ознаки теорій формування та розвитку інформаційного суспільства М. Кастельса, Ф. Махлупа та Г. Шиллера.

Завдання 4

Розкрийте передумови формування та динамічного розвитку інформаційного права. Чи можна вважати структуру та зміст системи інформаційного права сформованими? Яких недоліків формування даної галузі права дає змогу уникнути виділення Загальної та Особливої частин інформаційного права? Відповідь обґрунтуйте.

Завдання 5

Проаналізуйте наукові підходи вітчизняних вчених до визначення поняття «інформаційне право». Заповніть таблицю.

Інформаційне право	
Автор	*Визначення*
А.І. Марущак	
Р.А. Калюжний	
В.С. Цимбалюк	
М.Я. Швець	
Б.А. Кормич	
К.І. Бєляков	

Завдання 6

Проаналізуйте сучасні наукові джерела та визначте основні ознаки європейської, американської та азіатської моделей інформаційного суспільства. Відповідь подайте у вигляді таблиці.

Завдання 7

На основі історичних наукових джерел визначте основні етапи інформаційної революції та охарактеризуйте кожен із них, виділивши основні ознаки. Спрогнозуйте наступні (майбутні) етапи інформаційної революції суспільства.

Питання для самоперевірки

1. *Дайте визначення поняття «інформаційне право».*
2. *Охарактеризуйте методологію інформаційного права.*
3. *Виділіть основні принципи інформаційного права.*
4. *Дайте визначення поняття «інформаційне суспільство».*
5. *Визначте міжгалузевий зв'язок інформаційного права з самостійними галузями права, зокрема правовою інформатикою, правовою кібернетикою, та іншими науками гуманітарного і соціально-технічного спрямування, пов'язаними з інформаційною діяльністю.*

Тема 2.
ДЖЕРЕЛА ІНФОРМАЦІЙНОГО ПРАВА

Під джерелами інформаційного права розуміють форми закріплення волі держави у сфері реалізації інформаційних процесів.

До джерел регулювання інформаційних правовідносин відносяться інформаційне законодавство, нормативно-правові акти, інформаційні угоди, договори на надання інформаційної підтримки тощо.

Інформаційне законодавство являє собою відносно самостійну систему нормативно-правових актів, що регулює інформаційні відносини. Систематизацію норм інформаційного законодавства можна розглянути, виходячи з критерію безпосереднього об'єкта правового регулювання, і представити у нижчеподаному вигляді.

Загально-правові норми містяться в нормативно-правових актах, які встановлюють правові основи регулювання всіх видів об'єктів інформаційних відносин.

До таких актів належать: 1) загальновизнані норми і принципи міжнародного права; 2) норми Конституції України; 3) закони, що закріплюють загально-правові поняття і критерії.

Спеціально-правові (інформаційно-правові) норми містяться в нормативно-правових актах, які встановлюють спеціальні норми, що стосуються правового регулювання окремих видів об'єктів інформаційних відносин, які поділяються на п'ять груп.

1. Інформаційно-правові норми, які безпосередньо регулюють особливості формування текстів рекламного, пропагандистського й іншого характеру (плакати, стенди, календарі тощо).

2. Інформаційно-правові норми, які безпосередньо регулюють відносини, що виникають у локальних і глобальних комп'ютерних мережах.

3. Інформаційно-правові норми, які безпосередньо регулюють відносини щодо поширення масової інформації на телебаченні і радіо.

4. Інформаційно-правові норми, які безпосередньо регулюють відносини щодо поширення масової інформації пресою (газети, журнали, альманахи тощо).

5. Інформаційно-правові норми, які безпосередньо регулюють відносини щодо створення творів мистецтва (кіно- і відеопродукція, книги, компакт-диски, аудіокасети та інші об'єкти, які є інформаційними продуктами).

Інформаційно-правові норми є різновидом правових норм, а отже, мають таку саму структуру. Особливістю інформаційно-правових норм є те, що вони регулюють відокремлені групи суспільних відносин стосовно особливостей інформаційної сфери. Вони регламентують права, обов'язки, відповідальність суб'єктів права при виробництві, розповсюдженні та використанні інформації з урахуванням специфіки інформаційних відносин.

Отже, правові норми покликані регулювати особливий вид правовідносин, а саме інформаційні, та мають такі ознаки:

1) об'єктом їх регулювання є інформаційні процеси, тобто процеси створення інформації, володіння, передачі іншим особам, захисту інформації та їх власників;

2) вони створюються від імені держави уповноваженими особами при безпосередньому сприянні технічних фахівців у сфері інформаційних систем;

3) забезпечуються системою державних гарантій і санкцій, у тому числі заходами примусового характеру;

4) регулюють не тільки реальні, а й «віртуальні» відносини, що виникають в інформаційних мережах і системах (наприклад, електронна комерція, коли вибір товару і його оплата

(часто електронними грошима) здійснюється в інформаційній системі);

5) мають внутрішню структуру (гіпотезу, диспозицію, санкцію);

6) закріплюють заохочений державою варіант поведінки.

Таким чином, інформаційно-правові норми регулюють специфічні відносини, що виникають в інформаційній сфері у зв'язку з реалізацією інформаційних прав і свобод та здійсненням інформаційних процесів при зверненні інформації.

Однією з універсальних функцій норм права і, зокрема, інформаційних норм є інформування суб'єктів правовідносин про належний і можливий варіант їх поведінки.

Варто зазначити, що найбільш ґрунтовними в цьому аспекті є джерела, що регламентують права і свободи громадян у сфері інформації. І це не дивно, адже світова практика державотворення й теорія правової держави, на якій ця практика, починаючи з другої половини XX ст., була побудована, вимагають закріплення прав і свобод людини в конституції як нормативно-правовому акті найвищої сили. Отже, ми вправі вважати саме Конституцію України основою правової бази політики інформаційної безпеки. У Конституції України доцільно виділити, насамперед, джерела, якими визначені базові (політичні або громадянські) права у сфері інформації. Це, зокрема, ст. 34 Конституції (свобода думки і слова), ст. 31 Конституції (таємниця листування), ст. 32 Конституції (таємниця приватного життя) тощо. Крім того, існує низка похідних від цих прав норм, якими врегульовані окремі аспекти інформаційних відносин.

Так, норми ст. 19 Загальної декларації прав людини і громадянина встановлюють право на свободу слова, а норми ст. 12 цієї Декларації — таємницю приватного життя. Положення Загальної декларації прав людини і громадянина згодом розвинуто в Міжнародному пакті про громадянські й політичні права та Міжнародному пакті про економічні, соціальні й культурні права; у Європейській конвенції про захист основних прав

і свобод людини тощо. Існує також багато галузевих міжнародно-правових актів, якими врегульовані окремі питання інформаційних прав людини — доступ до екологічної інформації, захист персональних даних тощо. Причому в цих актах інформаційні права людини значною мірою конкретизовано й, що є ще важливішим, досить жорстко регламентовано випадки та можливості обмежень цих прав з боку держави. Отже, окрім безпосереднього встановлення умов, за яких фізична особа бере участь в інформаційних відносинах, цими нормами встановлено певні межі й напрями державної діяльності в інформаційній сфері, що зумовлює один із елементів взаємозалежності між інформаційними правами людини та державною політикою у сфері інформаційної безпеки.

Наступною групою норм є:

- захист та обмеження свободи інформації з боку держави;
- захист національної інформаційної інфраструктури;
- проблеми безпеки інформаційного розвитку держави.

У вищезазначених групах ці правові норми, як правило, створюються державою на власний розсуд, і говорити про загальновизнані міжнародно-правові стандарти в цій сфері ми не можемо. Але, знову ж таки, виявляється взаємозалежність між категорією інформаційних прав людини та державною політикою інформаційної безпеки в тому аспекті, що остання обмежується чинними гарантіями (національними та міжнародними) прав людини. Крім того, у міжнародному праві, зокрема в підписаній Україною Європейській конвенції про захист прав і основних свобод людини та у практиці створеного згідно із цією Конвенцією Європейського суду з прав людини, є визнаним принцип «найменшого зла», тобто будь-які дії держави для захисту своєї безпеки повинні завдавати мінімально можливої шкоди правам людини.

Інший елемент взаємозалежності між правовими нормами та політичними механізмами держави ґрунтується на розумінні того, що інформаційні права людини не можуть бути реалізова-

ні, а отже, не стануть реальними безпечними умовами для людини й суспільства за відсутності в державі механізмів їх реалізації та захисту. Так само жодна програма державного розвитку не може бути успішною без системи органів і системи нормативно-правових актів, які втілюють програмні положення в життя.

Названі механізми визначаються внутрішньодержавним законодавством і підзаконними актами. Ключовим наразі в українському законодавстві, як у сфері інформаційного права, так і в галузі інформаційної безпеки, є, безперечно, Закон України «Про інформацію». Цей Закон покликаний урегулювати найголовніші суспільні відносини в інформаційній сфері, включаючи питання реалізації інформаційних прав і свобод та захисту інформаційної безпеки, захисту інформації та інформаційної інфраструктури держави. Тобто, на цьому етапі ми вже бачимо поєднання в нормативно-правовому акті як норм, що є частиною природного права, так і норм, які мають суто державне походження. Але варто зазначити, що чинний Закон України «Про інформацію» створювався, по-перше, ще до прийняття нової Конституції, по-друге, в той час, коли інформаційний простір України ще лише починав розбудовуватися разом із проголошеною незалежною державою. Отже, цей Закон, попри численні зміни, не повністю відповідає темпам розвитку інформаційних відносин в Україні. Крім того, наголошується на необхідності якомога скорішого прийняття Закону України «Про інформаційну безпеку України», оскільки Концепція (основи державної політики) національної безпеки України, на думку багатьох фахівців, «не виконала функцію базового документа побудови системи забезпечення інформаційної безпеки України».

Водночас зарубіжний і вітчизняний досвід забезпечення безпеки суб'єктів свідчить, що для боротьби з усією сукупністю потенційно можливих загроз, пов'язаних із конфіденційною інформацією, захистом ноу-хау та підтриманням конкурентоспроможності суб'єкта, необхідна стрункa й цілеспрямована організація процесу протидії.

Схеми до теми

Джерела інформаційного права — це обставини, що спонукають появу і дію інформаційного права. Термін «джерело інформаційного права» юриспруденції відомий давно. Ще римський історик Тит Лівій називав закони джерелом особистого і приватного інформаційного права.

Джерела інформаційного законодавства як комплексної галузі можуть бути класифіковані наступним чином:

1. Норми Конституції України, що закріплюють інформаційні права та свободи, встановлюють права та обов'язки суб'єктів інформаційних відносин щодо створення та поширення інформації певного виду, а також встановлюють обмеження щодо обігу інформації в державі та суспільстві.

2. Галузі законодавства, що повністю присвячені питанням регулювання інформаційних відносин.

Особливістю інформаційного права є різноманітність і значна кількість його джерел. Це зумовлено тим, що нормами зазначеної галузі регламентується широке коло суспільних відносин. Специфікою таких джерел є те, що всі вони:

- Ґрунтуються на Конституції й законах України
- Приймаються органами виконавчої влади, органами місцевого самоврядування, іншими державними (недержавними) інституціями
- Мають різну юридичну силу
- До джерел належать і деякі міжнародні договори й рішення Конституційного Суду України
- Приймаються одноособово й колегіально

Форми інформаційного права

Під *внутрішньою формою* розуміють систему інформаційного права, що має об'єктивний характер своєї побудови, який виявляється в єдності й узгодженості всіх її норм, диференційованих за правовими комплексами, галузями, підгалузями, інститутами і нормами інформаційного права. Внутрішня форма інформаційного права — це структура і зв'язки. До неї відносять систему інформаційного права, горизонтальну і вертикальну структури співпідпорядкованості всіх її елементів.

Зовнішня форма інформаційного права — це спосіб об'єктивізації форми інформаційного права, зовнішнього прояву, матеріальної фіксації. У сучасній науковій літературі різні автори вважають, що поняття інформаційного права відбиває державну волю, а формами інформаційного права виступають інформаційні норми. Проте, на думку більшості науковців, більш близькими до істини є вчені, які поняття інформаційного права визнають не як державну волю (це його сутність), а як інформаційні норми, і в цьому зв'язку формою вони називають джерела інформаційного права. Тому інформаційна норма це — не форма інформаційного права, а саме інформаційне право.

Зовнішні форми інформаційного права

Інформаційно-правовий прецедент — виражене зовні рішення органу виконавчої влади з конкретної справи, якому надається формальна обов'язковість при розв'язанні наступних аналогічних справ.

Інформаційно-правовий договір — угода двох чи більше суб'єктів інформаційного права про встановлення, зміну або припинення інформаційних прав чи обов'язків.

Інформаційно-правовий акт — письмовий документ компетентного органу держави, в якому закріплено забезпечуване нею формально обов'язкове правило поведінки в інформаційній сфері.

Інформаційно-правовий прецедент
Прецедентом є такі дії влади, що мали місце лише один раз, але можуть бути прикладом для подібних дій цієї влади в подальшому. Інакше кажучи, інформаційно-правовий прецедент — це рішення юрисдикційних органів щодо інформаційно-правової справи, що згодом приймається за загально обов'язкове правило.

Інформаційно-правові договори — це угода двох чи більше суб'єктів інформаційного права щодо встановлення, зміни або припинення інформаційних прав чи обов'язків. У цих документах міститься волевиявлення сторін щодо інформаційних прав та обов'язків, визначається їхнє коло і послідовність, а також закріплюється добровільна згода виконувати взяті зобов'язання. Вони мають широке поширення в інформаційному праві.

Інформаційно-правовий акт — одна з основних найбільш виражених зовнішніх форм інформаційного права. Це державний акт нормативного характеру.

Міжнародно-правові стандарти у сфері інформаційного права

1) Конвенція Ради Європи про доступ до офіційних документів від 8.06.2009;
2) Конвенція про доступ до інформації, участь громадськості в процесі прийняття рішень та доступ до правосуддя з питань, що стосуються довкілля (ратифікована Законом України № 832-XIV від 06.07.99 р.);
3) Йоганнесбурзькі принципи. Національна безпека, свобода висловлювань і доступ до інформації;
4) документи міжнародної організації «Артикль 19» (Article 19), зокрема: «Право громадськості знати. Принципи законодавства про свободу інформації», «Модельний закон про свободу інформації»;
5) «Про доступ до офіційних документів», рекомендація Rec (2002) 2 Комітету Міністрів Ради Європи від 21.02.2002;
6) «Про доступ до інформації, що перебуває в розпорядженні державних органів», рекомендація № R (81) 19 Комітету Міністрів Ради Європи від 25.11.1981;
7) «Про доступ громадськості до інформації, що є в розпорядженні державних органів, і свободу інформації», рекомендація № 854 (1979) Парламентської Асамблеї Ради Європи;
8) «Про право на недоторканність приватного життя», резолюція № 1165 (1998) Парламентської Асамблеї Ради Європи;
9) практика Європейського суду з прав людини.

Ситуаційні завдання до теми

Задача 1

На закритому хімічному підприємстві, яке розташоване в межах міста і знаходиться поблизу державного кордону, в результаті аварії стався викид шкідливих речовин в атмосферу. Міська адміністрація вжила необхідних заходів щодо евакуації громадян із заражених територій і запобігла витоку небажаної інформації про аварію. При цьому вона заборонила керівництву підприємства передавати вітчизняним та зарубіжним ЗМІ інформацію про масштаби аварії та відомості, що стосуються життя населених пунктів, які входять в зону досяжності поширення шкідливих речовин. Водночас адміністрація, приймаючи таке рішення, посилалася на закритість виробництва хімічного підприємства.

➤ *Чи правомірні дії міської адміністрації з точки зору норм інформаційного права?*

Задача 2

Юридичне агентство «Гомер» звернулося до Комітету Національної комісії з цінних паперів та фондового ринку з питань корпоративного управління, емісії та обігу пайових цінних паперів з проханням надати йому право на поширення інформації про цінні папери комерційних банків та інших кредитних організацій. Керівництво Комітету, розглянувши заяву та нотаріально завірені копії реєстраційних документів агентства, відмовило йому в укладенні договору на поширення вказаної інформації на тій підставі, що агентство «Гомер» займається лише експертизою проєктів законів. Керівництво юридичного агентства

«Гомер», посилаючись на Статут агентства, повідомило керівництву Комітету про спеціалізацію його працівників у сфері поширення будь-якої соціально-правової інформації. Опираючись на ці факти, агентство оскаржило рішення Комітету Національної комісії з цінних паперів та фондового ринку з питань корпоративного управління.

➤ *Чи правомірними є дії Комітету Національної комісії з цінних паперів та фондового ринку?*

Завдання 1

Проаналізувавши систему національного інформаційного законодавства, визначте (із посиланням на норму відповідного нормативно-правового акту) норми, в яких містяться основні принципи інформаційного права.

Завдання 2

Проаналізуйте основні міжнародні нормативно-правові акти в інформаційній сфері та вкажіть схематично положення, в яких містяться норми щодо інформаційних прав та свобод громадян.

Завдання 3

Проаналізуйте міжнародні стандарти в інформаційно-правовій сфері та зазначте їх положення, відображенні в чинному законодавстві України (у вигляді таблиці).

Завдання 4

Порівняйте визначення терміна «інформація», закріплене в Законі України «Про інформацію», із визначеннями,

закріпленими в міжнародних нормативно-правових актах у сфері інформації. Проаналізуйте виявлені відмінності.

Завдання 5

Проаналізуйте основні проблеми розвитку та реформування інформаційного законодавства та визначте шляхи їх вирішення.

Питання для самоперевірки

1. *Охарактеризуйте міжнародне інформаційне законодавство.*
2. *Охарактеризуйте інформаційне законодавство України.*
3. *Визначте структуру інформаційного законодавства.*
4. *Проаналізуйте джерела інформаційного права.*
5. *Визначте основні проблеми розвитку та реформування інформаційного законодавства.*

Тема 3.
ПОНЯТТЯ І КЛАСИФІКАЦІЯ ІНФОРМАЦІЇ

Наразі вже ні в кого не викликає сумніву той факт, що сучасне суспільство перебуває на такому етапі свого розвитку, коли інформація стає одним з ключових елементів нашого сьогодення. При цьому право як соціальний регулятор має адекватно і своєчасно реагувати на суспільні відносини, що змінюються. Але й саме право в цифрову епоху отримує нові форми свого вираження і реалізації, такі як, наприклад, електронна демократія, електронна держава, електронний уряд, електронне опублікування, електронні державні послуги тощо. У зв'язку з цим одним з вихідних понять інформаційної держави буде поняття інформації, правової інформації.

Визначення інформації дуже близьке до філософського, де під інформацією розуміється повідомлення, інформування про стан справ, відомості про що-небудь. Життя і праця людини, існування живої природи, робота технічних систем — невід'ємні від діяльності з інформацією. Природа фізичних законів з'явилася задовго до людини як біологічного виду і тим більше — людської цивілізації. У цьому сенсі будь-який матеріальний об'єкт, будь-який процес, що виникає в природі, сам по собі є первинним джерелом інформації, адже, незалежно від того, чи існує розумний спостерігач, яблуко буде червоним або зеленим, а гуркіт грому буде сигналізувати про дощ.

Отже, **інформація** — це міра зміни в часі і просторі структурного розмаїття систем.

Філософи, дискутуючи в питаннях, пов'язаних з предметною сферою інформації, змогли виділити три підходи до розуміння інформації.

Перший підхід — антропно-комунікативний, коли одна особа (відправник) хоче передати факт, ідею, думку чи іншу інформацію комусь іншому (одержувачу). Ця інформація має значення для відправника незалежно від того, чи вона проста й конкретна, чи складна й абстрактна.

Другий підхід — функціональний. Йдеться про сприйняття інформації, яка об'єднана функціями органічних, громадських, кібернетичних систем.

Третій підхід — системний, передбачає, що всі природні явища і катаклізми, наші економічні негаразди і проблеми, соціальна нестабільність, інші процеси перебувають в логічному взаємозв'язку з певними подіями і діями людини, а тому мають свою причину і прогнозовані. Що стосується інформаційних процесів (де б вони не протікали) — без системного бачення і системного аналізу не можна з'ясувати причини, мотиви, наслідки і перспективи тих чи інших подій і процесів.

Отже, представникам функціонального підходу властиво при розгляді феномену інформації пов'язувати його тільки з діяльністю саморозвитку, тоді як прихильникам атрибутивного підходу властиво кваліфікувати феномен інформації як особливість всіх матеріальних об'єктів.

Розглядаючи інформацію з позиції філософії, можна сказати, що вона являє собою той особливий тип дійсності, який здатний існувати нарівні з матеріальним і ідеальним. І якщо матеріальному притаманні просторові й тимчасові форми, яких ідеальне буття не має, то інформаційне життя володіє просторовими формами.

Інформації притаманний ряд відмінних рис, головні з яких виражаються у взаємозв'язку з носіями (матеріальними або ідеальними); єдності, системності (полягає в тому, що наявна в будь-якому повідомленні інформація не представляє собою арифметичну суму, що складається з елементів цього повідомлення й існує можливість розташувати її в будь-якому поряд-

ку); демонстраційному характері (тобто здатність інформації виходити за рамки зовнішнього світу) тощо.

Як онтологічний феномен інформація пов'язана з генезою предметно-практичної діяльності людини і спроможністю людської психіки не тільки операціоналізувати світ у певних абстракціях (поняттях, символах, знаках), але й реагувати на прояви зовнішнього світу через емоційні стани, вчинки, практику і поведінку. Це те головне, що відрізняє людину від будь-якої істоти живої природи. У людському соціумі феномен інформації присутній у вербальній і невербальній формах, теоріях і законах, категоріях і поняттях, які стали результатам накопичення знання у процесі багатогранної людської діяльності.

Отже, людина бачить світ виключно крізь призму людської свідомості, яка ті чи інші речі й явища, що існують у ній, обгортає в інформаційну обкладинку, тобто поняття.

Для передачі суб'єктивних властивостей і ознак застосовують інформаційний діалектичний синтез, який має здатність вивести зі своєї справжньої обмеженості будь-який з об'єктів і в загальних рисах змусити його бути присутнім безмежно в часі.

Проблема класифікації інформації в цьому аспекті є досить дискусійним питанням. У працях вітчизняних дослідників у сфері інформаційного права і теорії інформаційної безпеки були зроблені спроби класифікації інформації. Її поділяють на загальнодоступну і з обмеженим доступом.

Закріплені два типи класифікації інформації: по категорії доступу і в залежності від порядку надання або поширення інформації.

Також поділяють інформацію, яка вільно поширюється; інформацію, яка надається за згодою осіб; інформацію, яка відповідно до законів підлягає поширенню; інформацію, яка обмежується або забороняється.

Звернемося тепер до правової інформації як різновиду інформації в цілому.

Виділяють наступні види інформації за змістом:

- правову (нормативно-правові акти);
- загальну інформацію про органи влади;
- нормативно-технічну;
- наукову;
- санітарно-епідеміологічну;
- екологічну;
- соціальну;
- статистичну;
- фінансово-економічну та багато інших.

Як бачимо, в цьому випадку до правової інформації віднесені тільки правові акти.

Правову інформацію можна розглядати як масив правових актів і тісно пов'язаних з ним довідкових, нормативних та інших матеріалів, що охоплюють всі сфери правової діяльності. У даному підході вже простежується спроба переходу до широкого розуміння правової інформації, але на перше місце, як і раніше, виноситься не інформація, а право і правові акти. Але обмежувати правову інформацію рамками джерел права не можна хоча б тому, що саме право не обмежується тільки законами і його зміст набагато ширший. Наприклад, судове повідомлення містить правову інформацію, оскільки державний орган з його допомогою повідомляє громадянина про необхідність вчинити певні юридично-значимі дії. Така ж природа і податкових повідомлень. Звичайно, це найнижчий рівень правової інформації, але для простих громадян він має найбільше значення, саме з такою правовою інформацією людина стикається найчастіше.

Тому всю іншу правову інформацію відносимо до ненормативної, серед якої виділяють:

- економічну правову інформацію;
- кримінологічну правову інформацію;

- криміналістичну правову інформацію;
- статистичну правову інформацію;
- судово-експертну правову інформацію;
- оперативно-розшукову правову інформацію;
- правову інформацію, що міститься в кримінальних та цивільних справах;
- судову та іншу правозастосовну практику;
- індивідуально-правові акти;
- нормативи і стандарти;
- інформацію про цивільно-правові відносини, договірні та інші зобов'язання;
- інформацію про стан законності і правопорядку;
- інформацію ефективності прокурорського нагляду;
- інформацію про форми і способи захисту прав громадян;
- науково-юридичну правову інформацію.

Раніше було сформульовано визначення інформації як міри зміни в часі і просторі структурного розмаїття систем. Тепер же можна з упевненістю констатувати, що в якості такої системи буде виступати правова система з усіма її елементами, а не тільки джерелами права. У цьому випадку правову інформацію слід визначити як міру зміни в часі і просторі структурного розмаїття правових систем. При цьому родові властивості інформації відповідним чином переносяться на конкретний вид інформації — правову інформацію. Зокрема, правова інформація зменшує ентропію правової системи, оскільки нові (прийняті) правові норми покликані врегулювати невизначеність в існуючих суспільних відносинах.

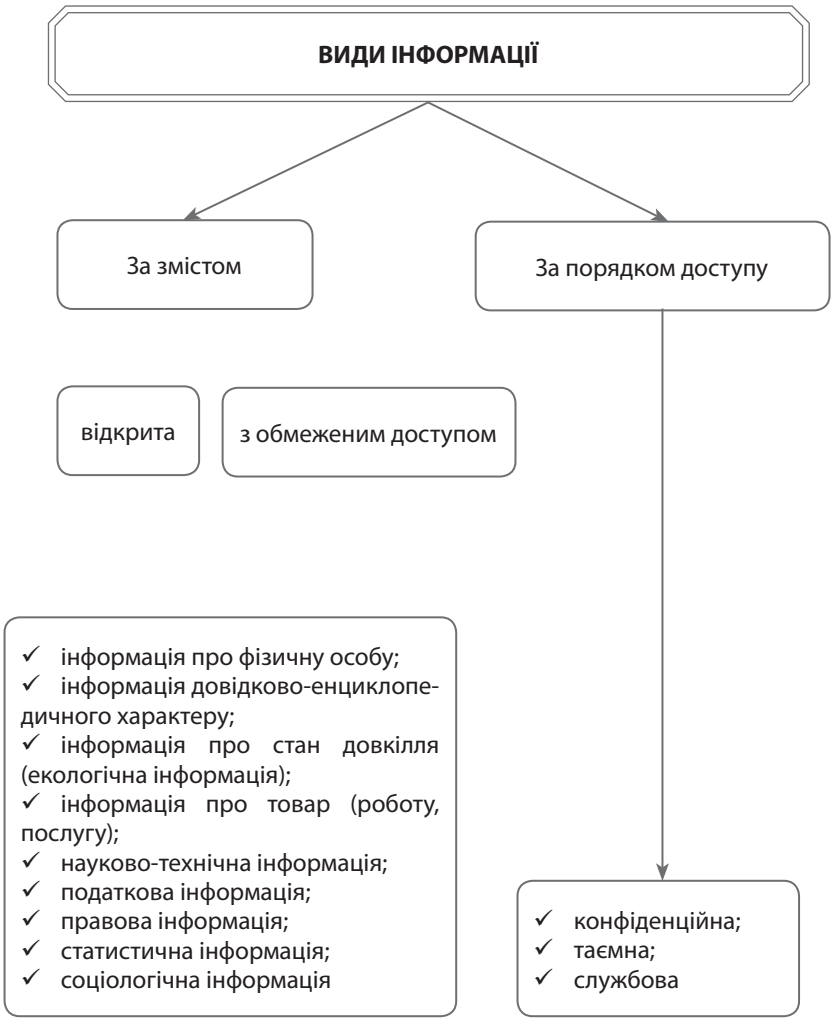
Схеми до теми

Відповідно до ст. 1 Закону України «Про інформацію» від 2 жовтня 1992 р. ***інформацією*** є будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Ст. 200 Цивільного Кодексу України від 16 січня 2003 р. також містить визначення поняття «інформація», зміст якого повністю співпадає із визначенням у Законі.

Основними властивостями інформації є:
- ✓ фізична невідчужуваність інформації;
- ✓ відокремленість інформації;
- ✓ екземплярність інформації;
- ✓ властивість інформаційного об'єкта;
- ✓ властивість або ознака тиражування (розповсюджуваності) інформації;
- ✓ організаційна форма.

Інформація — документовані або публічно оголошені відомості про події та явища, що відбуваються у суспільстві, державі та навколишньому природному середовищі.

Відповідно до ст. 10 Закону України «Про інформацію» є *такі* ***види інформації за змістом***:
- ✓ інформація про фізичну особу;
- ✓ інформація довідково-енциклопедичного характеру;
- ✓ інформація про стан довкілля (екологічна інформація);
- ✓ науково-технічна інформація;
- ✓ податкова інформація;
- ✓ інформація про товар (роботу, послугу);
- ✓ правова інформація;
- ✓ статистична інформація;
- ✓ соціологічна інформація;
- ✓ інші види інформації.


ВИДИ ІНФОРМАЦІЇ
За змістом
За порядком доступу
відкрита
з обмеженим доступом
✓ інформація про фізичну особу;
✓ інформація довідково-енциклопедичного характеру;
✓ інформація про стан довкілля (екологічна інформація);
✓ інформація про товар (роботу, послугу);
✓ науково-технічна інформація;
✓ податкова інформація;
✓ правова інформація;
✓ статистична інформація;
✓ соціологічна інформація
✓ конфіденційна;
✓ таємна;
✓ службова

Інформація класифікується

За роллю в правовій системі

За ступенем доступності

Юридично значимі ознаки, які зумовлюють специфіку інформації як об'єкта правового регулювання

✓ Нематеріальний характер («самостійність відносно носія», тобто цінність інформації полягає в її суті, а не в матеріальному носії, на якому вона зафіксована).
✓ Суб'єктивний характер («інформація виникає в результаті діяльності суб'єкта, який наділений свідомістю», тобто вона є результатом інтелектуальної діяльності):

✓ необхідність об'єктивації для включення у правовий обіг;
✓ кількісна визначеність;
✓ неспоживчість, можливість багаторазового використання;
✓ зберігання інформації у суб'єкта, який її передає;
✓ здатність до відтворення, копіювання, збереження і накопичення.

Інформація про фізичну особу
Відповідно до ст. 11 Закону України «Про інформацію» *інформація про фізичну особу (персональні дані)* — відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

При цьому не допускаються збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та захисту прав людини.

Інформація довідково-енциклопедичного характеру
Відповідно до ст. 12 Закону України «Про інформацію» *інформація довідково-енциклопедичного характеру* — це систематизовані, документовані, публічно оголошені або іншим чином поширені відомості про суспільне, державне життя та навколишнє природне середовище.

Інформація про товар (роботу, послугу)
Відповідно до ст. 14 Закону України «Про інформацію» *інформація про товар (роботу, послугу)* — це відомості та/або дані, які розкривають кількісні, якісні та інші характеристики товару (роботи, послуги).

Соціологічна інформація
Відповідно до ст. 19 Закону України «Про інформацію» *соціологічна інформація* — це будь-які документовані відомості про ставлення до окремих осіб, подій, явищ, процесів, фактів тощо.

Інформація про стан довкілля
Відповідно до ст. 13 Закону України «Про інформацію» *інформація про стан довкілля (екологічна інформація)* — це відомості та/або дані про:

- ✓ стан складових довкілля та його компоненти, включаючи генетично модифіковані організми та взаємодію між цими складовими;
- ✓ фактори, що впливають або можуть впливати на складові довкілля (речовини, енергія, шум та випромінювання, а також діяльність або заходи, включаючи адміністративні, угоди в галузі навколишнього природного середовища, політику, законодавство, плани і програми);
- ✓ стан здоров'я та безпеки людей, умови життя людей, стан об'єктів культури і споруд тією мірою, якою на них впливає або може вплинути стан складових довкілля;
- ✓ інші відомості та/або дані.

Науково-технічна інформація
Відповідно до ст. 15 Закону України «Про інформацію» *науково-технічна інформація* — це будь-які відомості та/або дані про вітчизняні та зарубіжні досягнення науки, техніки і виробництва, одержані в ході науково-дослідної, дослідно-конструкторської, проектно-технологічної, виробничої та громадської діяльності, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Службова інформація
Відповідно до ст. 9 Закону України «Про доступ до публічної інформації» — це інформація:
✓ що міститься в документах суб'єктів владних повноважень, які становлять внутрівідомчу службову кореспонденцію, доповідні записки, рекомендації, якщо вони пов'язані з розробкою напряму діяльності установи або здійсненням контрольних, наглядових функцій органами державної влади, процесом прийняття рішень і передують публічному обговоренню та/або прийняттю рішень;
✓ зібрана в процесі оперативно-розшукової, контррозвідувальної діяльності, у сфері оборони країни, яку не віднесено до державної таємниці.

Статистична інформація
Відповідно до ст. 18 Закону України «Про інформацію» *статистична інформація* — це документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства.

Інформація з обмеженим доступом — це відомості конфіденційного або таємного характеру, правовий статус яких передбачений законодавством України, які визнані такими відповідно до встановлених юридичних процедур і доступ до яких обмежений власником таких відомостей.

Конфіденційна інформація — це відомості, які знаходяться у володінні, користуванні або розпорядженні окремих фізичних чи юридичних осіб і поширюються за їх бажанням відповідно до передбачених умов.

Таємна інформація — це інформація, що містить відомості, які становлять державну та іншу передбачену законодавством таємницю (банківську, комерційну, службову, професійну, адвокатську тощо), розголошення якої завдає шкоди особі, суспільству і державі.

Податкова інформація
Відповідно до ст. 16 Закону України «Про інформацію» *податкова інформація* — це сукупність відомостей і даних, що створені або отримані суб'єктами інформаційних відносин у процесі поточної діяльності і необхідні для реалізації покладених на контролюючі органи завдань і функцій у порядку, встановленому Податковим кодексом України від 2 грудня 2010 р.

Правова інформація
Відповідно до ст. 17 Закону України «Про інформацію» *правова інформація* — це будь-які відомості про право, його систему, джерела, реалізацію, юридичні факти, правовідносини, правопорядок, правопорушення і боротьбу з ними та їх профілактику тощо.

Ознаки інформації

Ідеальність і *несамостійність* інформації

Невичерпність інформації

Ознака *наступності* інформації

Трансформування інформації

Універсальність інформації

Комплексна якість інформації

До *національних інформаційних ресурсів* належать:

В обов'язковому порядку — інформаційні продукти, створені органами державної влади й органами місцевого самоврядування в порядку здійснення основної діяльності цих органів

Похідний результат інших робіт, що виконують із залученням державного бюджету, — після завершення виконання таких робіт або їх окремих етапів

Інформаційні продукти, створені за рахунок позабюджетних коштів їх власників або виробників на основі угоди із власником або виробником

Міждержавні та міжнародні інформаційні продукти на основі відповідних міждержавних або міжнародних угод

Ситуаційні завдання до теми

Задача 1

Наприкінці року по телебаченню повідомили, що всі борги по зарплаті працівникам бюджетної сфери погашені. У той же час у деяких районах Волинської області вчителі оголосили страйк у зв'язку з невиплатою заробітної плати за останні чотири місяці. Журналіст Сухінін звернувся до адміністрації Волинської області з проханням надати йому документи, що містять докладні відомості про використання бюджетних коштів області за минулий рік. Йому в цьому проханні відмовили, посилаючись на те, що запитувана інформація є обмеженого доступу. Журналіст написав скаргу до Національної спілки журналістів України.

➤ *Чи правий Сухінін? Дайте інформаційно-правову оцінку позиції адміністрації області.*

Задача 2

Державна архівна служба України (Укрдержархів) з дозволу Уряду України передала Державному архіву однієї з республік колишнього СРСР у постійне користування документи про особисте життя і діяльність керівників колишнього СРСР — уродженців цієї республіки. Дочка одного із зазначених керівників оскаржила в суді дії Укрдержархіву, посилаючись на Закон України «Про Національний архівний фонд та архівні установи» і вимагаючи негайно повернути всі документи до Києва.

➤ *Зробіть юридичний аналіз ситуації.*

Завдання 1

Здійснити пошук наукової інформації про предмет, методи, функції та систему інформаційного права в електронних каталогах провідних наукових бібліотек України.

Завдання 2

Заповніть таблицю за зразком.

Вид інформації	**Відомості, що відносяться до виду інформації**
Інформація про фізичну особу	Відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована

Питання для самоперевірки

1. *Дайте визначення поняття «інформація».*
2. *Розкрийте наукові погляди на правову природу інформації.*
3. *Виділіть основні правові ознаки інформації.*
4. *Назвіть основні види та джерела інформації.*
5. *Охарактеризуйте інформацію з обмеженим доступом.*

Тема 4.
ІНФОРМАЦІЙНІ ВІДНОСИНИ

Сутність інформаційних відносин полягає в тому, що як інформація пронизує всі сфери людської діяльності, так й інформаційні відносини, що виникають у зв'язку з її обігом, є абстрактними, науково відокремленими від інших соціальних відносин. Наукове відокремлення дозволило вирішити ряд правових конфліктів у сфері володіння інформацією та захисту інформації від доступу третіх осіб.

Інформаційні правовідносини є різновидом відносин, що виникають у суспільстві, однак для цілей правового регулювання необхідно виявити такі ознаки даного виду правовідносин:

1) конкретний об'єкт — інформація (незалежно від форми);
2) форма правомірної поведінки;
3) інформаційно-правові норми;
4) поєднання суб'єктивних прав і обов'язків кореспондуючого характеру, коли реалізація права одним суб'єктом знаходиться в безпосередній залежності від виконання відповідних обов'язків іншим суб'єктом;
5) суб'єктами правовідносин можуть бути тільки особи, що володіють правосуб'єктністю;
6) суб'єктивні права і обов'язки реалізуються учасниками інформаційних правовідносин під захистом держави, забезпеченої системою державних гарантій та інструментами юридичної відповідальності.

Таким чином, відносини щодо інформації, що не відповідають зазначеним ознакам (наприклад, інформаційні відносини побутового характеру), не можуть розглядатися в якості правових відносин.

Правоздатність фізичних та/або юридичних осіб виникає в силу проголошеної законом можливості кожного бути автором творів науки, літератури і мистецтва без якого б то не було додаткового дозволу. Дієздатність автора не має значення для володіння правами на інформаційний об'єкт, проте впливає на можливість реалізації майнових прав на інформаційний об'єкт (в даному випадку застосовуються норми цивільного права).

Суб'єктами інформаційних правовідносин також є і власники засобів індивідуалізації.

Фізичні особи — це особи, які мають ім'я, що складається з власне імені, по батькові та прізвища (хоча ім'я може формуватися й інакше, в залежності від національних особливостей). При цьому фізична особа має право захищати своє ім'я, в тому числі вимагати відтворення його без яких би то не було помилок, а також оцінювати ім'я і давати право на його використання в якості внеску до статутного капіталу господарських товариств.

Крім того, ім'я може стати товарним знаком, наприклад, товарний знак популярного актора «Antonio Banderas», під яким випускаються парфумерні вироби. У сучасній практиці прикладів, коли ім'я відомої особи використовується в рекламних цілях, достатньо, в тому числі і для просування свого товару на ринку.

Юридичні особи мають фірмове найменування, товарний знак, право на використання яких може бути передано будь-якій особі за договором комерційної концесії.

Юридична особа має також ділову репутацію, захист якої здійснюється в рамках цивільного законодавства, хоча ділова репутація також може бути об'єктом договору, тобто бути таким собі інформаційним ресурсом, який сам може стати засобом отримання прибутку.

Держава також має власне ім'я і деякі виняткові права на об'єкти промислової власності та інформацію, що становлять державну таємницю.

Держава може передавати право на використання свого імені з комерційною метою, однак користувачі в такому випад-

ку повинні сплачувати обов'язкові платежі за подібне використання (таким обов'язком не обкладаються суб'єкти, які використовують державне найменування в суспільно корисних цілях, а також відповідно до цілей своєї діяльності, наприклад, суд, нотаріуси, державні органи та освітні установи, громадські організації).

Відповідно кожен, хто відноситься до перерахованого, повинен володіти правосуб'єктністю для того, щоб вступати в інформаційні правовідносини. Правоздатність зазначених осіб є спільною, проте дієздатність фізичних осіб може бути обмежена. При цьому обмеження встановлюється уповноваженим на те органом, а формально тим об'єктом, через який особи вступають у правовідносини, тобто статусом самої інформації — загальнодоступна вона або обмежена в користуванні, або взагалі вилучена з користування.

Звертаючись до загальних принципів класифікації суб'єктів правовідносин, суб'єктів інформаційних правовідносин можна поділити на:

- індивідуальні суб'єкти — фізичні особи, які беруть участь в інформаційному процесі (обіг інформації — створення, передача, використання);
- колективні суб'єкти — юридичні особи, незалежно від форм власності та організаційно-правових форм.

Визначаючи об'єкт інформаційних правовідносин, необхідно звернути увагу на два різних підходи до розуміння об'єкта правовідносин як правової категорії. Один з підходів — моністичний — теорія єдиного об'єкта. Згідно з ним об'єктом правовідносин є те, на що спрямовано або на що впливає право. Оскільки впливати право може тільки на поведінку людей, то поведінка зобов'язаної особи і становить юридичний об'єкт правовідносин. Подібний підхід піддавався критиці в науковій літературі у зв'язку з тим, що він не може бути застосований до всіх правовідносин. Тому другий підхід — плюралістичний або ціннісний (теорія множинності об'єктів) — більш прийнятний

тому, що не зводить об'єкт правовідносин тільки до поведінки зобов'язаної особи, а розуміє під ним різні соціальні блага (соціальні цінності).

У даних правовідносинах інформація є факультативним (додатковим) об'єктом правовідносин, який не є інформаційним. Наприклад, при укладанні угоди купівлі-продажу металевих дверей самі двері не є носієм інформації, однак укладення угоди передує пошуку контрагентів, який здійснюється шляхом інформування (тобто публічного поширення інформації), вираженого у формі реклами чи громадської оферти; інформація супроводжує укладення угоди, коли сторони обумовлюють її умови; і, нарешті, інформація супроводжує виконання угоди, коли сторони сповіщають одна одну про час і місце виконання, уточнюють дані, параметри або в подальшому їх змінюють. Крім того, сам договір або замовлення є письмово оформленим фіксуючим волю сторін документом, який підтверджує дійсність волевиявлення. При цьому договір не є метою даного виду правовідносин, а лише супроводжує їх.

Для характеристики відносин, що становлять предметну сферу інформаційного права, і в теорії права, і в законодавстві використовується поняття «інформаційна сфера».

З огляду на те, що відносини, які виникають в інформаційній сфері, не є однорідними, для з'ясування сутності предмета інформаційно-правового регулювання прийнято поділяти дані відносини на наступні групи:

- відносини, пов'язані зі створенням і перетворенням інформації (до цієї групи входять відносини: пов'язані зі створенням об'єктів інтелектуальної власності; пов'язані зі створенням офіційної інформації органами державної влади і управління, місцевого самоврядування; зі створенням масової інформації тощо);
- відносини щодо зберігання інформації (відносини щодо обов'язкового зберігання окремих видів інформації, наприклад, інформації обмеженого доступу тощо);

- відносини, пов'язані з передачею і розповсюдженням інформації (відносини щодо поширення правової інформації, відносини, пов'язані з розповсюдженням інформації за допомогою використання мережі Інтернет тощо);
- відносини, пов'язані зі споживанням інформації (відносини щодо реалізації права людини на пошук і отримання інформації; відносини у сфері бібліотечної справи, архівної справи тощо).

Схеми до теми

Інформаційні відносини — це суспільні відносини, врегульовані нормами цивільного та інформаційного права щодо виробництва, розповсюдження, використання інформації та охорони і захисту прав на неї, учасники яких наділені суб'єктивними правами та юридичними обов'язками.

ІНФОРМАЦІЙНІ ВІДНОСИНИ
поділяються на:

Відносні	Абсолютні	Квазіабсолютні

Переважна частина інформаційних відносин має *відносний характер* і походить від зобов'язальних відносин.
Відповідно *абсолютний характер* інформаційні відносини будуть мати, коли це стосуватиметься таємниці особистості та прав особистості на приватну сферу. Право особи на свою приватну сферу абсолютне (це таємниця життя, лікарська таємниця, таємниця сповіді, сюди також слід віднести банківську таємницю, оскільки кожна особа має право вимагати від необмеженого кола осіб обов'язкової заборони на збирання вказаних відомостей, а якщо ці відомості стали відомими особі у зв'язку з її професійною діяльністю, то — нерозголошення).
Квазіабсолютні відносини притаманні нерозкритій інформації, тому що однакове право на один і той самий об'єкт можуть одночасно мати декілька осіб. Це право не може бути визнане абсолютним, воно закріплює монополію, хоч і обмежену, але якої достатньо для пуску об'єкта в економічний обіг, і дозволяє користуватись правами, а також здійснювати захист засобами, значною мірою характерними для абсолютних прав.

Основними *принципами* інформаційних відносин є:

Гарантованість права на інформацію

Відкритість, доступність інформації та свобода її обміну

Об'єктивність, вірогідність інформації

Повнота і точність інформації

Законність одержання, використання, поширення та зберігання інформації

***Учасниками* інформаційних відносин є:**

Громадяни

Юридичні особи

Держава

***Основними* учасниками інформаційних відносин є:**

Споживачі

Автори

Зберігачі (охоронці) інформації

Поширювачі

Об'єктами інформаційних відносин є документована або публічно оголошувана інформація про події та явища в галузі політики, економіки, культури, охорони здоров'я, а також у соціальній, екологічній, міжнародній та інших сферах.

Суб'єкти інформаційних відносин ***мають право*** одержувати (виробляти, добувати), використовувати, поширювати та зберігати інформацію в будь-якій формі з використанням будь-яких засобів, крім випадків, передбачених законом.

Кожний учасник інформаційних відносин для забезпечення його прав, свобод і законних інтересів ***має право*** на одержання інформації про:
- ✓ діяльність органів державної влади;
- ✓ діяльність народних депутатів;
- ✓ діяльність органів місцевого і регіонального самоврядування та місцевої адміністрації;
- ✓ те, що стосується його особисто.

Суб'єкти інформаційних відносин ***зобов'язані***:
- ✓ поважати інформаційні права інших суб'єктів;
- ✓ використовувати інформацію згідно з законом або договором (угодою);
- ✓ забезпечувати додержання принципів інформаційних відносин;
- ✓ забезпечувати доступ до інформації усім споживачам на умовах, передбачених законом або угодою;
- ✓ зберігати інформацію в належному стані протягом встановленого терміну і надавати іншим громадянам, юридичним особам або державним органам у передбаченому законом порядку;
- ✓ компенсувати шкоду, заподіяну при порушенні законодавства про інформацію.

Ситуаційні завдання до теми

Задача 1

Начальник Управління міжнародних відносин Міністерства інфраструктури України Костюченко рекомендував підвідомчому об'єднанню «Простір» терміново включити до складу коштів міжнародного інформаційного обміну з російською фірмою «Пілон» інформаційні системи та мережі, для яких раніше були встановлені специфічні правила доступу до інформаційних ресурсів. Генеральний директор об'єднання «Простір» Логінов відмахнувся від Костюченка і розповів про його рекомендації заступнику міністра Семенову. Останній зауважив: «У нас горить договір з російською стороною, виконуй рекомендацію». Логінов не став заперечувати і вчинив так, як звелів керівник.

➤ *Чи порушені в цій ситуації правила міжнародного інформаційного права?*

Задача 2

У телепрограмі «Наука: реалії сьогодення», що транслювалася на Першому національному каналі українського телебачення, доктор біологічних наук, професор Гончарук заходився міркувати про вплив аварії на Чорнобильській АЕС на здоров'я дітей, що проживають в ураженій 30-кілометровій зоні. На закінчення він сказав: «А взагалі, шановні чорнобильці, я раджу вам на деякий час вивезти своїх дітей з прилеглих до АЕС територій, оскільки зараз станція продовжує "диміти", а в її роботі виявлені неполадки. Хоч би вона знову не вибухнула!». Ведучий телепрограми Шинкарук беззастережно підтримав вче-

ного, відзначивши його великий внесок у дослідження біологічних проблем заражених територій після вибуху на Чорнобильській АЕС. Наступного дня після трансляції телепрограми голови адміністрацій Чернігівської області України та Гомельської області Республіки Білорусь зажадали від керівництва Першого національного негайно спростувати брехливу інформацію, яка вводить в оману постраждале населення, і суворо покарати ведучого Шинкарука. Професор Гончарук і журналіст Шинкарук відмовилися від спростування переданої інформації, посилаючись на публікації в пресі та власні погляди.

➤ *Чи допущені в цьому випадку зловживання свободою слова?*

Завдання 1

Віднайдіть у практиці Європейського суду з прав людини прецеденти, що стосуються прав особи в інформаційно-правовій сфері, проаналізуйте їх та складіть коротке резюме.

Завдання 2

Зобразіть графічно склад інформаційних правовідносин, використавши наведену нижче таблицю.

Суб'єкт	Об'єкт	Зміст

Завдання 3

На прикладі трьох правових норм із різних джерел інформаційного права визначте структуру інформаційних правовідносин, що виникають на підставі цих норм. Подайте у вигляді таблиці:

Відповідна стаття правової норми	**Структура інформаційних правовідносин**

Завдання 4

Проаналізуйте та представте схематично основні ознаки, які відрізняють інформаційні правовідносини від правовідносин в інших галузях права за такими категоріями: учасники правовідносин; характер виникнення правовідносин (вольовий чи примусовий); строк дії правовідносин; правовий режим інформаційного об'єкта; необхідність наявності юридичного факту.

Завдання 5

Керівник нафтовидобувної компанії видав наказ, який забороняє його працівникам давати представникам засобів масової інформації будь-які коментарі, що стосуються діяльності компанії, без особистої вказівки на те самого директора або його першого заступника. Визначте елементи інформаційних правовідносин та надайте юридичну оцінку такої заборони.

Завдання 6

Редактор газети «За здоровий спосіб життя» з метою здійснення щомісячного моніторингу зловживання населення тютюновими виробами та алкогольними напоями вирішив провести соціальне опитування трьох мереж супермаркетів міста Запоріжжя, про що надіслав власникам закладів відповідний запит.

У запиті містились такі запитання:

- Який обсяг тютюнових та алкогольних виробів було реалізовано супермаркетом протягом останнього місяця?
- Як касир-продавець визначає вік покупця даних виробів?
- Як підвищення цін на дані вироби впливає на обсяг продажів?

Керівниками цих супермаркетів було проігноровано запит.

Проаналізуйте ситуацію. Визначте коло інформаційних правовідносин. Визначте чітко всі елементи інформаційних правовідносин та дайте правову оцінку діям керівників супермаркетів та редактора.

Питання для самоперевірки

1. *Визначте поняття та зміст інформаційних правовідносин.*
2. *Виділіть суб'єктивні права та обов'язки сторін інформаційних правовідносин.*
3. *Охарактеризуйте об'єкт інформаційних правовідносин?*
4. *Назвіть види інформаційних правовідносин.*
5. *Виділіть основні принципи інформаційних правовідносин.*

ЗМІСТОВИЙ МОДУЛЬ ІІ
ІНФОРМАЦІЙНА БЕЗПЕКА

Тема 5.
ЗАГАЛЬНА ХАРАКТЕРИСТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Тематика інформаційної безпеки привертає сьогодні увагу вчених різних правових, соціально-гуманітарних і технічних наук, що зумовлено міждисциплінарним характером інформаційної безпеки й залежністю від неї практично всіх сфер суспільного життя.

Першими дослідженнями, в яких почато розвиток поняття «інформаційна безпека», є дослідження сфери національної безпеки. Саме вони сформували розповсюджений сьогодні підхід, за яким інформаційна безпека розглядається як важливий складник національної безпеки. Очевидно, що поняття «національна безпека», «інформаційна безпека» значною мірою пов'язані з поняттям «безпека», сутнісно-філософське наповнення якого є далеко не тривіальним завданням, на що звернули увагу ще в античні часи.

У філософських і політико-правових ученнях античних мислителів була спроба розглядати проблему забезпечення безпеки громадян як засіб досягнення загального блага. Так Аристотель у роздумах щодо ідеального державного облаштування та способів управління суспільством висував критерій безпеки громадян. Відомий мислитель Бенедикт Спіноза головною метою створення «громадянського суспільства» називав «мир і безпеку життя», а не менш відомий мислитель Ж.-Ж Руссо стверджував, що найважливішою турботою держави має бути «турбота про самозбереження».

Проте вважається, що першим, хто із системних позицій проаналізував проблеми безпеки й виживання держави, суспільства та окремого індивіда в контексті їх взаємодії, був Т. Гоббс. На його думку, страх перед загрозами власній безпеці змушує людину жити в суспільстві й шукати в ньому засоби колективного захисту від зазначених загроз. Тому, як справедливо зазначають О.М. Гончаренко, Р.Д. Джангужин, Е.М. Лисицин, спираючись на Т. Гоббса, пошук безпечних умов розвитку й життєдіяльності суспільства зумовлює прогрес цивілізації.

У контексті сказаного заслуговує на увагу й те, що Статут ООН визначив об'єднання зусиль міжнародного співтовариства для підтримки безпеки як одну з головних цілей створення та діяльності цієї організації, а учасники ОБСЄ в статті 5 Заключного акту від 1 серпня 1975 року записали: «... воздерживаться от любых действий, которые могут ухудшить положение в такой степени, что будет поставлено под угрозу поддержание ... безопасности». Тобто в цьому випадку під безпекою розуміється деяка якість міжнародних відносин, яка ставиться в залежність від того чи іншого рівня міжнаціональних правовідносин.

Водночас безпечний і сталий розвиток соціальної системи можна розглядати як особливу форму буття, яке може бути охарактеризоване такими філософськими категоріями, як якість, кількість і структура, оскільки якість характеризує цілісність, нероздільну визначеність предметів і явищ, а структура, яка залежить від кількості (наприклад, елементів структури), одночасно тісно пов'язана з якістю й характеризує розподіл і взаємодію в просторі елементів системи і програму їх розвитку.

Загальновідомо, що головна особливість структури системи — її цілісність і якісна відмінність від складових її елементів, а зміна структури завжди пов'язана зі зміною якості й навпаки.

У контексті сказаного є підстави стверджувати, що хоч би як це не було сумно, але чималою загрозою для безпеки кожної людини та людства загалом є розмаїття філософсько-світоглядних здобутків, ідеологій і, відповідно, ціннісних орієнтацій народів

і цивілізацій. На жаль, указане різноманіття не тільки збагачує різнокольорову палітру культурного надбання людства в процесі його розвитку. За певних умов це розмаїття цінностей може стати рушійною силою небувалих катаклізмів, які поки що міжнародному співтовариству вдається більш-менш приборкувати на рівні локальних міжетнічних і міжконфесійних конфліктів, до того ж, досить часто із застосуванням засобів збройної боротьби.

Отже, не будучи чимось матеріальним, безпека є своєрідною характеристикою й необхідною передумовою життєдіяльності, прогресивного розвитку та життєздатності об'єктів реального світу. Указані об'єкти існують і розвиваються в середовищі, параметри якого формуються під впливом різноманітних, часто взаємопов'язаних і взаємозумовлених факторів, інтегральний складник яких, як правило, створює деякий інтегральний імовірний рівень загроз безпеці. Тому органи державної влади мають гарантувати певний рівень захисту й можливостей щодо задоволення життєвих потреб людини, суспільства, держави. Очевидно, досягнутий рівень безпеки залежить від можливостей, які наявні в розпорядженні держави, ефективності практичних заходів щодо реалізації державою вказаних можливостей у ході прогнозування, виявлення, нейтралізації загроз безпеці або принаймні зниження їх інтегрального рівня.

Особливо яскраво це прослідкується у війні 2003 році між Іраком і коаліцією на чолі із США, як до її початку, так і після її закінчення. Сукупність проблемних питань, породжених указаною війною у сфері забезпечення міжнародної, національної та інформаційної безпеки, міжнародного права й міжнародних відносин, безумовно, виходить далеко за межі «іракської проблеми».

Загалом дослідження генезису наукової думки та правової практики у сфері забезпечення інформаційної безпеки України дало змогу виділити чотири основні етапи становлення.

Перший етап розвитку інформаційної безпеки України — 1991–1996 рр.: від моменту появи незалежної держави, і відпо-

відно проблеми безпеки України, до кінця 1996 р. На першому етапі було забезпечено створення необхідної вихідної нормативно-правової бази, що регулює сферу інформаційної безпеки; отримала початок розробка фундаментальних концептуальних положень інформаційної безпеки з позиції єдності інтересів всіх об'єктів інформаційної безпеки — особистості, суспільства і держави.

Другий етап охоплює період з 1997 по 2000 рік. У ці роки сформувалися концептуальні засади державної політики забезпечення безпеки особистості, суспільства і держави від зовнішніх і внутрішніх загроз у всіх сферах життєдіяльності суспільства. У ці роки спектр внутрішніх і зовнішніх загроз інформаційної безпеки країни розширюється, проте, як і раніше, основні загрози залежать від стану вітчизняної економіки.

Третій етап — 2001–2013 рр. Цей етап характеризується значними внутрішньополітичними і соціально-економічними змінами. Ми можемо відзначити перехід до домінуючого обліку зовнішніх факторів впливу на загальний рівень інформаційної безпеки та розширення тимчасових горизонтів розробки заходів щодо забезпечення інформаційної безпеки особистості, суспільства і держави.

Четвертий етап — з 2014 р. по теперішній час. Зараз триває четвертий етап формування системи інформаційної безпеки. Сьогодні цей етап пов'язаний передусім із формуванням кіберпростору, передумова розвитку якого передбачена низкою індустріальних революцій, а також інформаційною революцією. Інформаційна революція, по-перше, зумовила виникнення сучасного інформаційного суспільства; по-друге, призвела до синтезу двох інформаційно-комунікаційних технологій — комп'ютерної (інформаційної) та телекомунікаційної; по-третє, сприяла формуванню двох простих, але дуже змістовних законів. Перший закон сформульовано одним із засновників корпорації «Intel» Гордоном Муром. Говорячи, що «кількість транзи-

сторів у процесорах збільшуватиметься вдвічі кожних півтора роки», він фактично пояснює формування на межі тисячоліть інформаційного простору. Другий закон належить Роберту Маткалфу, винахіднику найпоширенішої сьогодні технології комп'ютерної мережі Internet. Говорячи, що «цінність мережі знаходиться у квадратичній залежності від кількості вузлів, які є її складниками», він констатує, що основу сучасного інформаційного суспільства становлять ІТ-системи та мережі різного призначення, домінування яких у всіх процесах життєдіяльності людства зумовило появу та формування кібернетичного простору. Вплив на ці глобальні субстанції нині: 1) відіграє суттєву роль в економічному й соціальному розвитку більшості держав світу і свідчить про їх вступ до якісно нової фази взаємовідносин — інформаційного та кіберпротиборств; 2) сприяє отриманню державами світу як значних переваг, так і виникненню низки проблем — передусім їх інфосфери вразливі до загроз, які пов'язані з особливостями існування та передачі інформації. При цьому саме вибухове зростання обсягів інформації, до яких отримали доступ пересічні громадяни, винайдення потужних комп'ютерів і вбудованих мікроконтролерів, що сприяло розвитку промисловості, не лише привело більшість країн світу до глобальної інтелектуалізації, а й зробило більш вразливими передусім критично-важливі сегменти та об'єкти їхньої економіки до загроз антропогенного й техногенного характеру, а також природних катаклізмів.

Отже, перші праці, в яких зроблена спроба узагальнити наукові знання й деталізувати основи інформаційної безпеки, з'явилися на початку 90-х років минулого століття. Визнання інформаційної безпеки як важливої функції держави, зі своїми цілями та завданнями, складною структурою, властивою тільки їй характеристиками, викликало необхідність більш детального вивчення питання про кодифікацію інформаційного законодавства, яке підтримується багатьма вченими й дослідниками національного інформаційного простору.

Але за будь-яких обставин у сучасних умовах задоволення потреби в безпеці на всіх її рівнях (індивідуальному, суспільному, інформаційному, національному, міжнародному) передбачає застосування системного підходу щодо всебічного врахування низки факторів, які впливають на безпечний розвиток соціальної системи.

Схеми до теми

Основні етапи становлення правової практики у сфері забезпечення інформаційної безпеки України

Перший етап (1991–1996 рр.). На цьому етапі спостерігається відсутність фундаментальної інформації дослідницької складової національної безпеки. У більшості випадків науково-дослідні роботи присвячені національній безпеці, в контексті якої автори згадують лише поверхово про необхідність поділу її інформаційної складової, при чому не надаючи пріоритету іншим складовим. Інформаційна безпека в основному ототожнюється з безпекою інформації. Автори виділяють ряд головних недоліків інформаційної безпеки України, які, як правило, мають внутрішній характер і пов'язані, перш за все, з нестачею кваліфікованих кадрових ресурсів та політичною нестабільністю в країні.

Другий етап (1996–2000 рр.). Розгляд інформаційної безпеки стоїть на першому місці щодо системи національної безпеки, про що свідчить конституційне визнання інформаційної безпеки в якості однієї з важливих функцій держави. У той же час науково-інформаційна складова дослідження розглядається через висвітлення проблем інформаційної безпеки держави, залишаючи осторонь інші важливі об'єкти — права людини і громадянина, а також суспільства. Ще однією особливістю дослідження цього періоду є те, що наголошується на необхідності вживання превентивних заходів щодо захисту з метою забезпечення інформаційної безпеки України. З'являються перші ґрунтовні дисертаційні дослідження політологічного та юридичного спрямування, предметом розгляду яких є інформаційна безпека. Численні наукові дослідження вказують на появу нового виду тероризму, інформаційного — кіберзлочинності як виду злочину, а також нової загрози інформаційній безпеці України як маніпулювання людською свідомістю, громадянином і суспільством в цілому.

Третій етап (2001–2018 рр.). З огляду на те, що інформаційні питання носять транснаціональний характер і вимагають узгоджених дій з боку всього міжнародного співтовариства, характерною особливістю цього етапу є активізація досліджень міжнародних принципів інформаційної безпеки. Крім того, проголошена зовнішня політика України щодо інтеграції в Європейський Союз призвела до появи наукових статей про досвід інформаційної безпеки в європейській спільноті, розпочався процес узгодження (адаптації) національного законодавства до європейського. З огляду на специфіку термінології, яка використовується для визначення деяких аспектів інформаційної безпеки, черговою віхою для вітчизняної науки в цій галузі є поява численних словників, глосаріїв тощо. Слід зазначити, що для цього періоду характерними є інтенсифікація досліджень про роль, місце та проблеми органів виконавчої влади у сфері інформаційної безпеки в Україні, а також ретельна деталізація окремих положень інформаційних правовідносин.

Інформаційна безпека — це стан захищеності життєво важливих інтересів особистості, суспільства і держави в інформаційній сфері від внутрішніх та зовнішніх загроз.

Складові інформаційної безпеки

Конфіденційність — стан інформації, при якому доступ до неї здійснюють тільки суб'єкти, що мають на нього право.

Цілісність — уникнення несанкціонованої модифікації інформації.

Доступність — уникнення тимчасового або постійного приховування інформації від користувачів, що отримали права доступу.

Конфіденційність — найбільш опрацьований у нас в країні аспект інформаційної безпеки. На жаль, практична реалізація заходів щодо забезпечення конфіденційності сучасних інформаційних систем натрапляє на серйозні труднощі. По-перше, відомості про технічні канали просочування інформації є закритими, тому більшість користувачів позбавлена можливості уявлення про потенційні ризики. По-друге, на шляху призначеної для користувача криптографії як основного засобу забезпечення конфіденційності стоять численні законодавчі перепони і технічні проблеми.

Цілісність можна поділити на *статичну* (тобто незмінність інформаційних об'єктів) і *динамічну* (що відноситься до коректного виконання складних дій (транзакцій)). Засоби контролю динамічної цілісності застосовуються, зокрема, при аналізі потоку фінансових повідомлень з метою виявлення крадіжки, переупорядковування або дублювання окремих повідомлень.

Цілісність виявляється найважливішим аспектом ІБ в тих випадках, коли інформація служить «керівництвом до дії». Рецептура ліків, наказані медичні процедури, набір і характеристики комплектуючих виробів, хід технологічного процесу — все це приклади інформації, порушення цілісності якої може призвести до смерті. Неприпустиме і спотворення офіційної інформації, такої, наприклад, як текст закону або сторінка вебсервера якої-небудь урядової організації.

Особливо яскраво основна роль *доступності* виявляється в різного роду системах управління: виробництвом, транспортом тощо. Зовні менш драматичні, але також вельми неприємні наслідки — і матеріальні, і моральні — може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей (продаж залізничних та авіаквитків, банківські послуги тощо).

ЗАХОДИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Законодавчі заходи
(забезпечення інформаційної безпеки)

Процедурні заходи
(заходи безпеки, орієнтовані на людей)

Адміністративні заходи
(накази й інші дії керівництва організацій, пов'язані з інформаційними системами, що захищаються)

Програмно-технічні заходи

Закони і нормативні акти орієнтовані на всі суб'єкти інформаційних відносин незалежно від їх організаційної приналежності (це може бути як юридична, так і фізична особа) в межах країни (міжнародні конвенції мають навіть ширшу область дії). ***Адміністративні заходи*** — на всі суб'єкти в межах організації, ***процедурні*** — на окремих людей (або невеликі категорії суб'єктів), ***програмно-технічні*** — на устаткування і програмне забезпечення.

ВИДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

За джерелами походження:

— *ненавмисні*, викликані помилковими чи ненавмисними діями людини (наприклад, помилковий запуск програми, ненавмисне допущення інсталяції закладок через недотримання правил безпеки роботи в Інтернеті тощо);

— *навмисні* (інспіровані), результат навмисних дій людей (наприклад, навмисна інсталяція програм, які передають інформацію на інші комп'ютери, навмисне зараження вірусами, навмисна дезінформація тощо).

За повторюваністю вчинення:

— *повторювані* — такі загрози, які мали місце раніше;

— *продовжувані* — неодноразове здійснення загроз, що складається з ряду тотожних загроз, які мають спільну мету.

За рівнем детермінізму:

— *закономірні* — такі загрози, які носять стійкий, повторюваний характер, що зумовлено об'єктивними умовами існування та розвитку системи інформаційної безпеки;

— *випадкові* — такі загрози, які можуть трапитися або не трапитися. До таких загроз належать загрози хакерів дестабілізувати інформаційні системи органів державного управління.

За структурою впливу:

— *системні* — загрози, що впливають одразу на всі складові елементи системи управління національною безпекою;

— *структурні* — загрози, що впливають на окремі структури системи;

— *елементні* — загрози, що впливають на окремі елементи структури системи. Дані загрози мають постійний характер і можуть бути небезпечними лише за умови неефективності або непроведення їх моніторингу.

За характером реалізації:

— *реальні* — активізація алгоритмів дестабілізації є неминучою і не обмежена часовим інтервалом і просторовою дією;

— *потенційні* — активізація алгоритмів дестабілізації можлива за певних умов середовища функціонування органу державного управління.

За сферою інформаційної діяльності:

— загрози у зовнішньополітичній сфері;
— у внутрішньополітичній сфері;
— у воєнній сфері;
— в економічній сфері;
— у соціальній та гуманітарній сферах;
— у науково-технологічній сфері;
— в екологічній сфері.

За суб'єктами:

— *інформаційна безпека особи* (фізична особа, юридична особа);

— *суспільства;*

— *держави.*

За рівнем поширення:

— *міжнародні;*

— *національні;*

— *локальні;*

— *приватні.*

За формою прояву:

— *внутрішні;*

— *зовнішні.*

Ситуаційні завдання до теми

Задача 1

Журналісти газети «Факти» вирішили відвідати судове засідання районного суду у справі громадянина Порохова, обвинуваченого в розкраданні предметів, що мають особливу історичну і художню цінність. Судовий пристав-виконавець, нічим не мотивуючи свої дії, не пустив журналістів до зали суду.

➤ *Які принципи правового регулювання у сфері інформації в цьому випадку були порушені?*

Задача 2

Програміст Назаров кілька років працював на підприємстві з іноземними інвестиціями «Стенол». Однак під час прийому на роботу в трудовому договорі не обговорювалися і не були прописані його майнові права на програми, які він розроблятиме. За час трудової діяльності Назаров розробив ефективну систему автоматизації обліку товарів на підприємстві. Але заробітна плата його не задовольняла, і він вирішив звільнитись, запропонувавши керівництву підприємства «Стенол» свої платні послуги із супроводження та модернізації програмного забезпечення створеної ним системи. Керівництво визнало запитану Назаровим оплату занадто високою і відхилило його пропозицію. Згодом на підприємство «Стенол» був прийнятий на роботу програміст Навроцький, на якого теж були покладені обов'язки щодо розвитку та супроводження системи автоматизованого обліку товарів на підприємстві. Навроцький відчував, що йому не вдасться домогтися бажаної угоди з адміністрацією підприємства, модифікував

свою програму, яка згодом припинила нормально функціонувати. Це практично паралізувало всю систему обліку в «Стенол».

➤ *Оцініть ситуацію, що склалася з інформаційно-правової позиції. Як кваліфікувати дії програміста Назарова?*

Задача 3

Міжнародна фірма «Нок» купила у правовласника за готівку програмний продукт, який знадобився цій фірмі для розробки власних електронних карт. Програмне забезпечення було встановлено на 25 ЕОМ з метою його використання в автоматизованій інформаційно-правовій системі.

➤ *Чи порушила в цьому випадку міжнародна фірма «Нок» інформаційне законодавство?*

Завдання 1

Проаналізуйте рішення Європейського суду з прав людини у справі «Pinto Coelho проти Португалії». Якими критеріями користувався суд для визначення правомірності розкриття інформації?

Завдання 2

Запитувач звернувся до розпорядника інформації, Міністерства екології та природних ресурсів, з проханням надати інформацію щодо об'єктів, які є найбільшими забруднювачами навколишнього природного середовища. Відповідь на даний запит було отримано запитувачем через 10 днів із зазначенням, що з даною інформацією можна ознайомитися на офіційному вебсайті

міністерства. Проаналізуйте ситуацію, визначте коло інформаційних правовідносин. Чи правомірні дії суб'єкта владних повноважень при наданні відповіді на інформаційний запит?

Завдання 3

Студентська організація «Майбутнє України» звернулася до суб'єкта владних повноважень — Міністерства освіти та науки, з пропозицією щодо внесення змін до розміщеного на вебсайті проєкту нормативно-правового акту у сфері надання освітніх послуг. Визначте порядок та строки розгляду даних пропозицій уповноваженою посадовою особою зазначеного органу.

Питання для самоперевірки

1. *Дайте визначення поняття «інформаційна безпека».*
2. *Охарактеризуйте джерела загроз інформаційної безпеки України.*
3. *Визначте основні складові інформаційної безпеки.*
4. *Охарактеризуйте кримінально-правову охорону та захист інформаційних відносин.*
5. *Які є види відповідальності за поширення недостовірної інформації, отриманої в мережі Інтернет.*
6. *Визначте проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій.*

Тема 6.
СИСТЕМА ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Система забезпечення інформаційної безпеки в Україні має відповідні структури і певний регламентований процес прийняття й реалізації управлінських рішень у сфері управління інформаційною безпекою. Підтвердженням цього є те, що 1 травня 2014 р. виконувач обов'язків Президента України, Голова Верховної Ради України Олександр Турчинов підписав Указ № 449/2014 про рішення РНБО «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28 квітня 2014 р. Виходячи з необхідності вдосконалення нормативно-правового забезпечення, запобігання потенційним і реальним загрозам інформаційній безпеці й нейтралізації їх, Рада національної безпеки й оборони України доручила Кабінету Міністрів України в місячний строк розробити й подати на розгляд Верховної Ради України законопроєкти про внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав.

Очевидним є те, що система забезпечення інформаційної безпеки є сукупністю окремих елементів, якими зазвичай є об'єкт, суб'єкти і їх види. Водночас окремими її складниками є основні характеристики, рівні інформаційної безпеки та перелік загроз.

Отже, система забезпечення інформаційної безпеки — це внутрішня структура, систематизована сукупність, єдність, взаємозв'язок і диференціація окремих її елементів (об'єкт, суб'єкти, основні характеристики, рівні інформаційної безпеки та перелік загроз).

У питанні про об'єкт інформаційної безпеки звертаємо увагу на те, що законодавець подає перелік об'єктів національної безпеки: людина та громадянин — їхні конституційні права і свободи; суспільство — його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності; інформаційне й навколишнє природне середовище і природні ресурси; держава — її конституційний лад, суверенітет, територіальна цілісність і недоторканність.

Отже, очевидною є необхідність доповнення цього переліку (на прикладі інформаційної безпеки) такими об'єктами, як інформація, інформаційна діяльність, інформаційне суспільство.

Законодавство не містить чіткого переліку суб'єктів інформаційної безпеки, а в Законі України «Про основи національної безпеки України» подано лише систему суб'єктів забезпечення національної безпеки. Проте в Законі України «Про інформацію» суб'єктами визначені фізичні особи, юридичні особи, об'єднання громадян і суб'єкти владних повноважень. Інший перелік ми можемо переглянути в Законі України «Про доступ до публічної інформації», де суб'єктами визнано запитувачів інформації (фізичні, юридичні особи, об'єднання громадян без статусу юридичної особи, крім суб'єктів владних повноважень); розпорядників інформації.

Проте вищеперераховані чинники можуть відображатися й у внутрішньополітичному середовищі: сьогодні відсутня чітка межа між двома зазначеними видами загроз у сфері інформаційної діяльності. Використовуючи такий підхід, ми спостерігаємо вплив різних компонентів інформаційної впливової дії на внутрішню структуру (структуру інтересів — життєвих цінностей, соціальних пріоритетів, внутрішніх настанов), на соціальні об'єкти (соціальні групи, зокрема особистість), а отже, і на зовнішню структуру. У цьому контексті, на наш погляд, очевидним є те, що саме залежність між зовнішньополітичними та внутрішньополітичними структурами зумовлює причини соціальних конфліктів у суспільстві.

Отже, наявність можливості (і вміння) здійснювати цілеспрямований інформаційний вплив на зазначені структури суспільства визначає можливість вирішення цих конфліктів політичними засобами, що, у кінцевому підсумку, характеризує рівень інформаційної й національної безпеки держави.

До найбільш важливих об'єктів забезпечення інформаційної безпеки України в зовнішньополітичній сфері належать такі: інформаційні ресурси органів виконавчої влади, що реалізують зовнішню політику України, українські представництва та організації за кордоном, представництва України при міжнародних організаціях; блокування діяльності українських засобів масової інформації з роз'яснення зарубіжній аудиторії цілей і основних напрямів державної політики України, її думки щодо соціально значимих подій українського й міжнародного життя.

Із зовнішніх загроз інформаційної безпеки України в зовнішньополітичній сфері найбільшу небезпеку становлять: інформаційний вплив іноземних політичних, економічних, військових та інформаційних структур на розроблення й реалізацію стратегії зовнішньої політики України; поширення за кордоном дезінформації про зовнішню політику України; порушення прав українських громадян і юридичних осіб в інформаційній сфері за кордоном; спроби несанкціонованого доступу до інформації та впливу на інформаційні ресурси, інформаційну інфраструктуру органів виконавчої влади, що реалізують зовнішню політику України, українських представництв та організацій за кордоном, представництв України при міжнародних організаціях.

З внутрішніх загроз інформаційної безпеки України в зовнішньополітичній сфері найбільшу небезпеку становлять: порушення встановленого порядку збирання, оброблення, зберігання та передачі інформації в органах виконавчої влади, що реалізують зовнішню політику України; інформаційно-пропагандистська діяльність політичних сил, громадських об'єднань,

засобів масової інформації та окремих осіб, що спотворює стратегію й тактику зовнішньополітичної діяльності України; недостатня інформованість населення про зовнішньополітичну діяльність України.

Основними заходами щодо забезпечення інформаційної безпеки України в зовнішньополітичній сфері є розроблення основних напрямів державної політики в галузі вдосконалення інформаційного забезпечення зовнішньополітичного курсу України; розроблення та реалізація комплексу заходів щодо посилення інформаційної безпеки інформаційної інфраструктури органів виконавчої влади, що реалізують зовнішню політику України, українських представництв та організацій за кордоном, представництв України при міжнародних організаціях; створення українськими представництвами й організаціями за кордоном умов для роботи з нейтралізації поширюваної там дезінформації про зовнішню політику України; вдосконалення інформаційного забезпечення роботи з протидії порушенням прав і свобод українських громадян і юридичних осіб за кордоном; удосконалення інформаційного забезпечення суб'єктів України з питань зовнішньополітичної діяльності, які входять до їхньої компетенції.

Останнім часом безпосередньо у військовій справі рівень інформаційного потенціалу все більшою мірою зумовлює оперативність прийняття рішень, структуру і якість озброєнь, оцінювання рівня їх достатності, дієвість пропаганди, ефективність дій союзників і власних збройних сил і, в підсумку, результат збройного протистояння. Значущість інформаційної безпеки як складника воєнної безпеки України пояснюється залежністю реалізації найбільш важливих інтересів України у воєнній сфері від інформаційних загроз. З аналізу найбільш небезпечних загроз важливим національним інтересам України у воєнній сфері випливає, що реалізаційною основою більшості цих загроз є інформаційна. Наведемо найбільш показові приклади. Зокрема, з-поміж інших загроз стабілізації воєнно-політично-

го стану в Центральній Європі та недопущення збройних конфліктів наведено такі: висунення територіальних претензій до України; втручання у внутрішні справи України; нестабільність воєнно-політичного стану навколо України; активізація сепаратистських сил і підтримання їх ззовні; заяви й акції, що дискредитують внутрішню та зовнішню політику України; войовничість політичного керівництва сусідніх країн; загострення міжетнічних і міжконфесійних суперечностей; нестабільність соціально-політичного стану в деяких країнах Центральної Європи. Не викликає сумніву те, що всі ці загрози тією чи іншою мірою реалізуються на інформаційному рівні, причому їх інформаційний складник досить вагомий. Варто зазначити, що йдеться не про абсолютизацію інформаційних факторів у реалізації наведених загроз, а про те, що вони поряд з економічними, політичними, соціальними та іншими факторами є домінуючими. Проблема інформаційної безпеки базується на вже сформованій залежності всіх сфер життєдіяльності суспільства й держави — економіки, політики, науки, культури, забезпечення національної та міжнародної безпеки — від нормального обміну інформацією, надійного функціонування інформаційних і телекомунікаційних систем. Тим самим для розвинених країн створюється спокуса використовувати наявні в них переваги (електронно-цифровий розрив) в інформаційних технологіях і засобах маніпулювання суспільною свідомістю для експансії у вищевказаних сферах життєдіяльності, використовуючи поки не обмежений ніякими положеннями міжнародного права абсолютно новий вид зброї — інформаційний. У сучасних умовах застосування інформаційної зброї як засобу ведення війн може викликати наслідки, цілком порівнянні за силою своєї дії з «традиційною» зброєю масового знищення. Ця теза аж ніяк не випадкова. Аналіз використання сучасних технологій іншими державами вимагає здійснення системи спеціальних заходів щодо забезпечення інформаційної безпеки, в тому числі міжнародної.

Останнім часом ми спостерігаємо, як Російська Федерація поширює недостовірну, неповну, упереджену інформацію про Україну, через що намагається маніпулювати суспільною свідомістю в Україні та за її межами, що призводить до необхідності вдосконалення нормативно-правового забезпечення, запобігання потенційним і реальним загрозам національній безпеці в інформаційній сфері й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері. Тому ефективність своєчасного виявлення та нейтралізації розглянутих загроз національній безпеці у воєнній сфері істотно залежить від виваженості й активності заходів щодо забезпечення воєнної безпеки на інформаційному рівні.

Одним із найважливіших ресурсів будь-якого суб'єкта є інформація, роль якої зростає в міру розвитку бізнесу та посилення конкуренції. Володіння інформацією необхідного обсягу в потрібний час і в потрібному місці є запорукою успіху в будь-якому виді господарської діяльності.

Інформаційна безпека в економічній сфері, захист її від несанкціонованого використання, знищення або зміни набувають в умовах ринкової конкуренції першочергового значення. Забезпечення безпеки економічних інформаційних систем — це комплекс заходів, спрямований на захист конфіденційних відомостей у виробничо-господарській, управлінській, науково-технічній і фінансовій сферах. Інформаційна безпека в економічній сфері являє собою комплексну проблему, що охоплює всі стадії оброблення та зберігання важливої документації, включаючи бухгалтерську звітність, договори з партнерами, персональні дані клієнтів та іншу фінансово-економічну інформацію, витік якої може призвести до серйозних фінансових збитків і незворотних наслідків. Перехід до ринкових відносин в економіці викликав появу на внутрішньому українському ринку товарів і послуг великої кількості вітчизняних і зарубіжних комерційних структур, у тому числі виробників і споживачів інформації, засобів інформатизації та захисту інформації.

Безконтрольна діяльність цих структур щодо створення й захисту систем збирання, оброблення, зберігання та передачі статистичної, фінансової, біржової, податкової, митної інформації створює реальну загрозу безпеці України в економічній сфері. Аналогічні загрози виникають під час безконтрольного залучення іноземних фірм до створення подібних систем, оскільки при цьому складаються сприятливі умови для несанкціонованого доступу до конфіденційної економічної інформації і для контролю за процесами її передачі та оброблення з боку іноземних спецслужб. Широке використання імпортних засобів інформатизації, телекомунікації, зв'язку та захисту інформації створює загрозу виникнення технологічної залежності України в цій сфері від іноземних держав.

Недостатність нормативної правової бази, що визначає відповідальність суб'єктів за недостовірність чи приховування відомостей про їхню комерційну діяльність, про споживчі властивості вироблених ними товарів і послуг, про результати їхньої господарської діяльності, про інвестиції тощо, перешкоджає нормальному функціонуванню економіки країни загалом. З іншого боку, істотний економічний збиток суб'єктам може бути завдано внаслідок розголошення інформації, яка містить комерційну таємницю, розголошення інсайдерської інформації. У системах збирання, оброблення, зберігання та передачі фінансової, податкової, митної інформації найбільш небезпечними є протиправні копіювання інформації або її спотворення внаслідок навмисних порушень технології роботи з інформацією та несанкціонованого доступу до неї.

Схеми до теми

Система забезпечення інформаційної безпеки — це внутрішня структура, систематизована сукупність, єдність, взаємозв'язок і диференціація окремих її елементів (об'єкт, суб'єкти, основні характеристики, рівні інформаційної безпеки та перелік загроз).

Рівні інформаційної безпеки

Нормативно-правовий рівень — закони, нормативно-правові акти тощо.

Адміністративний рівень — дії загального характеру, які вживаються органами державного управління.

Процедурний рівень — конкретні процедури забезпечення інформаційної безпеки.

Програмно-технічний рівень — конкретні технічні заходи забезпечення інформаційної безпеки.

На законодавчому рівні розрізняють дві групи заходів:

- ✓ заходи, спрямовані на створення і підтримку в суспільстві негативного (у тому числі із застосуванням покарань) ставлення до порушень і порушників інформаційної безпеки (назвемо їх заходами обмежувальної спрямованості);
- ✓ направляючі й координуючі заходи, що сприяють підвищенню освіченості суспільства в галузі інформаційної безпеки, що допомагають у розробці та поширенні засобів забезпечення інформаційної безпеки (заходи творчої спрямованості).

Найважливіше (і, ймовірно, найважче) на законодавчому рівні — створити механізм, що дозволяє узгодити процес розробки законів з реаліями і прогресом інформаційних технологій. Закони не можуть випереджати життя, але важливо, щоб відставання не було занадто великим, оскільки на практиці, крім інших негативних моментів, це веде до зниження інформаційної безпеки.

До адміністративного рівня інформаційної безпеки відносяться дії загального характеру. Головна мета заходів адміністративного рівня — сформувати програму робіт в галузі інформаційної безпеки та забезпечити її виконання, виділяючи необхідні ресурси і контролюючи стан справ. Основою програми є політика безпеки, що відображає підхід організації до захисту своїх інформаційних активів. Керівництво кожної організації має усвідомити необхідність підтримки режиму безпеки і виділення на ці цілі значних ресурсів. Політика безпеки будується на основі аналізу ризиків, які визнаються реальними для інформаційної системи організації. Коли ризики проаналізовані та стратегія захисту визначена, складається програма забезпечення інформаційної безпеки. Термін «політика безпеки» є не зовсім точним перекладом англійського словосполучення «security policy», проте в даному випадку калька відображає сенс цього поняття краще, ніж лінгвістично правильний переклад «правила безпеки». Тут мова йде не про окремі правила або їх набори, а про стратегію організації у галузі інформаційної безпеки. Для вироблення стратегії і втілення її в життя потрібні політичні рішення, що приймаються на найвищому рівні керівництва організації, установи чи підприємства.

Політика безпеки — сукупність документованих рішень, прийнятих керівництвом організації і спрямованих на захист інформації та асоційованих з нею ресурсів.

Процедурний рівень орієнтований на людей, а не на технічні засоби. Саме люди формують режим інформаційної безпеки, і вони ж виявляються головною загрозою, тому «людський фактор» заслуговує особливої уваги. Слід усвідомити ту ступінь залежності від комп'ютерної обробки даних, в яку потрапило сучасне суспільство. Акцент слід робити не на військовому чи кримінальному боці справи, а на цивільних аспектах, пов'язаних з підтриманням нормального функціонування апаратного та програмного забезпечення, тобто концентруватися на питаннях доступності та цілісності даних.

Програмно-технічний рівень, тобто рівень, спрямований на контроль комп'ютерних сутностей — обладнання, програм та/або даних, який утворює останній і найважливіший рубіж інформаційної безпеки. Наголошуємо, що збиток наносять в основному дії легальних користувачів, по відношенню до яких процедурні регулятори малоефективні. Головні вороги — некомпетентність і неакуратність при виконанні службових обов'язків, і тільки програмно-технічні заходи здатні їм протистояти.

Методи запобігання та нейтралізації загроз інформаційної безпеки

Правові методи передбачають розробку та реалізацію комплексу нормативно-правових актів, що регламентують інформаційні відносини в суспільстві, забезпечують інформаційну безпеку. Так, зокрема, в Законі України «Про захист інформації в інформаційно-телекомунікаційних системах України» від 05 липня 1994 р. серед інших принципів захисту правової інформації був названий принцип кримінальної відповідальності за несанкціонований доступ до інформації.

Програмно-технічні методи включають використання різних технічних засобів захисту інформації при її передачі по каналах зв'язку.

Організаційно-економічні методи передбачають формування системи захисту таємної та конфіденційної інформації за допомогою їх сертифікації, ліцензування, стандартизації на предмет відповідності вимогам інформаційної безпеки.

Ситуаційні завдання до теми

Задача 1

Національне інформаційне агентство, використовуючи можливості контролю телефонних каналів зв'язку, перешкоджало недержавному підприємству «Пегас» в реалізації його функцій міжнародного інформаційного обміну та пропонувало укласти договір про надання послуг у галузі експлуатації каналів зв'язку. Однак умови, на яких пропонувалося укласти цей договір, були для підприємства «Пегас» невигідні: згідно з умовами договору підприємство повинно було передати національному інформа-

ційному агентству за послуги свої майнові права на 25 % акцій.

➤ *Чи правомірні дії національного агентства з точки зору законодавства щодо міжнародного інформаційного обміну?*

Задача 2

Комерційний банк «Укрсоцбанк» уклав договір з юридичною фірмою «Nactua» про впровадження у своєму юридичному відділі найсучасніших інформаційних систем «Банківське право» і «Правові основи роботи з цінними паперами». Юридична фірма встановила в банку названі системи, отримала обумовлену винагороду і, попередивши банк про конфіденційність отриманих ним відомостей про системи, приступила до виконання нового замовлення. Президент банку «Укрсоцбанк» Сміян вирішив зробити приємне своєму колезі, голові правління банку «Юст» Шахову, і передав його ІТ-спеціалістам всю інформацію про нові системи. Дізнавшись про це, генеральний директор юридичної фірми «Nactua» Безсонов подав позов до суду на банк «Укрсоцбанк» і зажадав відшкодування заподіяної шкоди за розголошення конфіденційних відомостей.

➤ *Які норми інформаційного законодавства були порушені і яке рішення має прийняти суд?*

Завдання 1

Проаналізуйте Рішення Європейського суду з прав людини у справі «Aditions Plon проти Франції». Який підхід застосований судом для визначення правомірності обмеження поширення інформації? Чи може аналогічний підхід застосовуватися і до обмеження доступу до інформації?

Завдання 2

На підставі законодавчих та підзаконних нормативно-правових актів проаналізуйте та виділіть п'ять правових норм, що характеризують способи регулювання інформаційної діяльності.

Завдання 3

Проаналізуйте спеціальне законодавство у сфері інформаційної діяльності та оформіть його основні положення щодо порядку здійснення такої діяльності у вигляді таблиці із зазначенням назви нормативно-правового акту та відповідної норми.

Завдання 4

Проаналізуйте нормативно-правові акти, що регулюють діяльність засобів масової інформації, та зобразіть схематично види інформаційної діяльності, які здійснюють ЗМІ.

Питання для самоперевірки

1. *Дайте визначення поняття «система забезпечення інформаційної безпеки».*
2. *Охарактеризуйте рівні інформаційної безпеки.*
3. *Визначте загрози інформаційної безпеки.*
4. *Дайте визначення понять «загроза», «небезпека».*
5. *Назвіть основні характеристики загроз інформаційної безпеки України.*
6. *Визначте види загроз за певними критеріями.*

Тема 7.
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ІНТЕРНЕТ-ПРОСТОРІ

Сьогодні простір мережі Інтернет поступово перетворився на арену ведення бойових дій, де все більш активно діють відповідні спецпідрозділи іноземних держав. Це проявляється в збільшенні кількості та потужності кібератак та кіберінцидентів, які становлять нові загрози національній та міжнародній безпеці. Тобто, *кібербезпекою* є інформаційна безпека в кібернетичному (віртуальному) просторі, а *кіберзлочином*, відповідно, — суспільно небезпечне винне діяння в кіберпросторі. Засобом для здійснення кіберзлочину є комп'ютер, мережі зв'язку. З кримінально-правової точки зору його характеристикою є умисел, а суб'єктом — осудна фізична особа.

Однак слід зрозуміти, що важливою особливістю кіберпростору є його висока динамічність та мінливість загрози. Це обумовлює неможливість створення Стратегії, яка б охоплювала період більш ніж 3–5 років. Щонайменше кожні два роки Стратегія забезпечення кібербезпеки України потребує корегування відповідно до нових викликів і загроз, а також змін у геополітичному безпечному середовищі. Таким чином, процес перегляду Стратегії має бути тісно пов'язаний з системною роботою над річними або дворічними Оглядами. Швидше за все такий Огляд матиме дві складові: відкриту і закриту. Необхідність другої складової пов'язана з загальним місцем кібербезпекової проблематики в системі національної безпеки держави та оцінці реального стану та можливостей українських безпекових відомств протидіяти кібератакам противників або проводити власні спеціальні операції в кіберпросторі. У багатьох випадках розголошення таких даних дійсно може

призвести до послаблення можливостей ефективного використання кіберпростору в національних інтересах.

Забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя керівництво провідних держав світу приділяє посилену увагу створенню та удосконаленню ефективних систем захисту критичної інфраструктури від зовнішніх і внутрішніх загроз кібернетичного характеру. У багатьох провідних країнах світу вже сформовані загальнодержавні системи кібернетичної безпеки — як найбільш оптимальні організаційні структури, що здатні за короткий проміжок часу акумулювати сили та засоби різних державних органів і приватного сектору для протидії кіберзагрозам. В Україні також відбувається процес формування системи кібернетичної безпеки.

Для України кіберзлочинність є надзвичайно актуальною проблемою, адже наша країна вже досить довгий час лідирує у списку країн, де кіберзлочини є надзвичайно поширені і становлять загрозу для суспільства та держави в цілому. Для подолання цієї проблеми варто акумулювати всі національні ресурси, чітко визначити державну політику в даній сфері, орієнтуючись на позитивний досвід європейських країн.

Через більш ніж десять років після появи мережі Інтернет у світі почала активно розроблятися правова база, спрямована на припинення злочинів у сфері комп'ютерної інформації.

В умовах ведення гібридної війни періодичне спланованe здійснення кібератак, об'єктом ураження яких є зокрема державні установи, загрожує інформаційній безпеці суспільства та держави в цілому.

Встановлено, що стан захищеності інформаційно-технічної інфраструктури у державних установах пропорційний рівню обізнаності державних службовців щодо безпечного використання технологій мережі Інтернет та недопущення кіберінцидентів.

Зокрема, в таких умовах вбачається необхідність організації та проведення заходів, спрямованих на підвищення кіберкомпетентності держслужбовців, що передбачає отримання ними знань, набуття вмінь та навичок щодо безпечного користування сервісами електронної пошти, інформаційними ресурсами мережі Інтернет та забезпечення необхідного рівня кібербезпеки.

За оцінками 2018 року, кібератаки за своїм негативним впливом зайняли друге місце у списку глобальних світових ризиків. У світі та в українському суспільстві зокрема стає дедалі більше людей, що розуміють важливість кібербезпеки й тих проблем, які необхідно вирішувати. У Верховній Раді на розгляд подано ряд законопроєктів, які розробляються з метою створення дієвих механізмів, спрямованих на оперативне виявлення, реагування, попередження, запобігання, нейтралізацію кіберзагроз, кібератак та кіберзлочинів. Зокрема, пропонувалося внести зміни до законодавства, яке регулює правоохоронну діяльність в інформаційно-телекомунікаційній сфері, спрямовані на посилення рівня відповідальності та підвищення розміру штрафних санкцій по відношенню до операторів, провайдерів телекомунікацій, що надають послуги доступу до Інтернету за порушення умов і правил, що регламентують діяльність у сфері телекомунікацій та користування радіочастотним ресурсом України, передбачену ліцензіями, дозволами, а також порядку та умов надання послуг зв'язку в мережах загального користування.

Проте вимоги, які висувають автори таких законопроєктів, є неприйнятними для представників громадськості, а також засобів масової інформації. На їх думку, прийняття таких законів призведе до руйнуванням засад політичної свободи та демократії.

Отже, в умовах ведення гібридної війни проти України, національний сегмент мережі Інтернет перетворено на ключову арену інформаційного протиборства. Сплановані та орга-

нізовані спеціальні інформаційні операції, що мають на меті деструктивний вплив на особу та суспільство в цілому, становлять надзвичайну небезпеку для інформаційного простору України. Здійснюються такі операції переважно через мережу Інтернет, що виражається у поширенні фейкової інформації з використанням певних методів, зокрема таких, як дезінформування, диверсифікація громадської думки, поширення чуток, пропаганда, психологічний тиск тощо.

Тому інформаційна безпека є важливою самостійною сферою забезпечення національної безпеки, що характеризує стан захищеності національних інтересів в інформаційній сфері.

На нашу думку, в умовах ведення інформаційної війни проти України та враховуючи високий рівень вразливості національного інформаційного простору, застосування певних обмежувальних заходів свободи Інтернету є доречним. Проте ці обмеження повинні бути пропорційні існуючим загрозам і не суперечити конституційним правам та свободам людини та основним принципам державної інформаційної політики.

Проаналізувавши стан правового регулювання питань забезпечення інформаційної безпеки в Інтернет-просторі відповідно до вимог сьогодення, доцільно підтримати здійснення відповідної політики. Вагомими здобутками у цьому напрямку вже стало прийняття Доктрини інформаційної безпеки України, Стратегії кібербезпеки України, Закону України «Про основні засади забезпечення кібербезпеки України».

За останній час відбулися деякі організаційно-структурні зміни щодо системи захисту національної інформаційної безпеки, в тому числі і кібербезпеки. Зокрема, було створено Міністерства інформаційної політики України; у складі Національної поліції України — Департамент кіберполіції; Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України, що здійснює координацію та контроль за діяльністю суб'єктів сек-

тора безпеки і оборони, що забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України; Ситуаційний центр забезпечення кібернетичної безпеки, створений на базі Департаменту контррозвідувального захисту інтересів держави в галузі інформаційної безпеки Служби безпеки України тощо.

Проте питання забезпечення безпеки в Інтернет-просторі завжди залишатиметься відкритим, враховуючи стрімкий розвиток інформаційно-комунікаційних технологій, постійне зростання користувачів мережі та під'єднаних до неї пристроїв, ведення інформаційних протиборств між країнами із застосуванням усіх методів зовнішньої інформаційної агресії та спеціальних інформаційних операцій, інформаційний тероризм, розробка нових видів інформаційної зброї тощо.

В українському суспільстві майже відсутня змістовна дискусія щодо пошуку можливих рішень проблем, що стосуються функціонування інтернету та інформаційного простору. Значна частина дискусій на ці теми відбувається у форматі суперечок та взаємних звинувачень. Багато в чому це обумовлюється низьким рівнем довіри між представниками стейкхолдерів, які часто мають не просто різні погляди на ситуацію, але й різний когнітивний, лексичний та смисловий апарат для їх формулювання.

Значна частина законодавчих ініціатив у 2017–2018 рр. від депутатів ВРУ на тему інформаційного простору та розвитку інтернету була негативно сприйнята суспільством через потенційну загрозу свободі інтернету та обмеження цифрових прав користувачів. Подібні ініціативи не завжди беруть за основу вимір прав людини та не враховують європейський досвід в частині обмежень. Зокрема, законодавці у своїх ініціативах рідко беруть до уваги принцип пропорційності, що практикує Європейський суд з прав людини, вирішуючи дилему правомірності обмежень прав людини.

Ситуаційні завдання до теми

Задача 1

Керівник служби безпеки фірми «Тегола» склав для персоналу фірми інструкцію по роботі з документами, що становлять комерційну таємницю. Відповідно до цієї інструкції працівники фірми повинні були давати відповідну підписку про її нерозголошення, або це зобов'язання мало включатися у вигляді окремого пункту в трудову угоду того чи іншого працівника. Якщо відомості, що становлять комерційну таємницю, доводилося розголошувати своїм діловим партнерам або клієнтам фірми, то положення про нерозголошення таємниці обов'язково повинні були включатися у відповідні договори з учасниками правовідносин. З метою запобігання витоку комерційної інформації співробітникам фірми заборонялося передавати будь-яку інформацію правоохоронним органам; інформацію могли передавати лише керівник фірми і керівник служби безпеки. Також в інструкцію були введені положення, що дозволяють здійснювати фото- та кінозйомку службових та інших приміщень з письмового дозволу директора фірми «Тегола».

➤ *Дайте правову оцінку положень цієї інструкції з точки зору законодавства про інформаційну безпеку.*

Задача 2

Публіцист Волков надрукував у газеті «Вісті» цікаву статтю під назвою «Скарби України», в якій привів отримані від експерта Служби Безпеки України Нестерова загальні відомості про державні запаси дорогоцінних металів і каменів, а також назвав розміри золотого запасу та валютних резервів України. Керівник відділу Служби Безпеки

України Романов, прочитавши в газеті статтю Волкова і з'ясувавши, звідки він отримав інформацію, поставив перед своїм керівництвом питання про притягнення до відповідальності Нестерова за розголошення відомостей, які відносяться до державної таємниці.

➤ *Проаналізуйте цю ситуацію з точки зору законодавства про інформаційну безпеку.*

Задача 3

Депутати Оболонської районної в місті Києві ради звернулися до Міністерства освіти і науки України з проханням направити до районного архіву копії документів жителів Оболонського району, які захистили кандидатські і докторські дисертації за останні десять років, з тим, щоб сформувати власний масив інформації про науковий потенціал району. У цьому проханні було відмовлено на тій підставі, що всі масиви документів, що зберігаються в базах даних Міносвіти України, є виключно державними інформаційними ресурсами і відносяться до інформації з обмеженим доступом.

➤ *Чи є в даній ситуації порушення інформаційного законодавства, що регулює безпеку інформаційних ресурсів в Україні?*

Завдання 1

Розробіть проєкт Доктрини інформаційної безпеки.

Завдання 2

Сформулюйте професіограму фахівця у сфері управління інформаційною безпекою.

Завдання 3

Проаналізуйте рішення Європейського суду з прав людини у справі «Бенедік проти Словенії (Case of Benedik v. Slovenia (Application №62357/14)». Якими критеріями користувався суд для визначення правомірності процедури доступу та передачі персональних даних посадових осіб?

Питання для самоперевірки

1. *Охарактеризуйте поняття «Інтернет-простір».*
2. *Визначте основні нормативно-правові акти, які характеризують Інтернет-простір в нашій країні.*
3. *Визначте, які загрози належать до сфери Інтернет-простору.*

Тема 8.
ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ІНТЕРНЕТУ РЕЧЕЙ

Саме впровадження та розвиток Інтернету речей на сьогодні є новітнім етапом у процесі розвитку глобальної мережі Інтернет. Прикладами використання Інтернету речей є технології розумного будинку, розумного міста, розумної ферми, розумного авто, годинника тощо.

Інтернет речей створює умови для появи синергетичного ефекту від поєднання можливостей штучного інтелекту, хмарних обчислень, безлічі сенсорів, математичних алгоритмів обробки великих даних (Big Data), роботизованих пристроїв різного призначення, систем передачі даних (мережі Інтернет), що дозволяє надавати різноманітні послуги та проводити всілякі роботи за участю чи без участі людей.

Сьогодні постало актуальне питання щодо врегулювання інформаційних відносин, які виникають у зв'язку з впровадженням технологій Інтернету речей та визначення можливих правових проблем.

Об'єктом даних правовідносин, як і будь-яких інших інформаційних правовідносин, є інформація, але та, що знаходиться у формі Big Data, зберігається у хмарних середовищах, продукується штучним інтелектом тощо.

Суб'єктний склад даних правовідносин може бути різним. Наприклад, держава, до якої звертається фізична особа із запитом на отримання публічної інформації, що знаходиться у формі відкритих даних, фізичні особи, що використовують офіційні хмарні технології для зберігання даних, юридичні особи, що надають такі можливість, тощо.

Особливої уваги на сьогодні заслуговує новий вид суб'єктів таких правовідносин — «штучний інтелект». «Штучний інтелект» як феномен інженерної думки переживає період інтенсивного розвитку. Це досягається завдяки розробці нових типів нейронних мереж. Однак невирішеним залишається питання правового регулювання даного явища, його основ і умов існування, інтеграції в інші системи, в першу чергу — в людське життя. Причина тому — відставання теорії права від науково-технічного прогресу: відсутність правової регламентації у сфері взаємодії людини і «штучного інтелекту», проблеми моралі, безпеки, правосуб'єктності, відповідальності, недоторканності приватного життя. Окрема увага повинна бути приділена питанням правовідносин, коли для сфери «штучного інтелекту» має активно застосовуватися цивільне, адміністративне, інформаційне та інші галузі законодавства.

Яскравим прикладом появи нових учасників правовідносин є робот Софія, створений у 2016 році. У 2017 році Софія отримала громадянство Саудівської Аравії. Але чи можуть існувати правовідносини між людиною і машиною? Дане питання викликало у світових наукових колах чималий дисонанс, і суперечки щодо нього триватимуть ще довго.

Водночас доцільно визначити надважливі питання у сфері Інтернету речей, серед яких захист персональних даних та забезпечення інформаційної безпеки користувачів даних технологій.

Варто звернути увагу на такі аспекти інформаційних відносин, що виникають щодо використання Інтернету речей, як наявність згоди суб'єкта на використання персональних даних та можливість управляти своїми даними та рівнем доступу до них інших суб'єктів.

Проаналізувавши запропоновані принципи правового регулювання, варто зауважити, що лише за їх реалізації можна забезпечити необхідний рівень інформаційної безпеки, особливо в контексті режиму доступу до персональних даних.

Отже, мережа Інтернет як важливий елемент суспільного життя в найближчі роки святкуватиме свій півстолітній ювілей з дати створення, зрозуміло, що за цей період його технології заполонили світ, вдосконалились і зазнають подальшого розвитку. Тому сьогодні новітнім етапом в розвитку мережі є технології Інтернету речей. Людство поступово ввійшло в еру «розумних пристроїв», штучного інтелекту, хмарних технологій. Такими поняттями, як «Smart house», «Smart town», «Smart car», «Smart watch» тощо, вже нікого не здивуєш.

Проте на сьогодні постало актуальне питання щодо врегулювання інформаційних відносин, які виникають у зв'язку з впровадженням технологій Інтернету речей та визначенням можливих правових проблем.

Проаналізувавши особливості використання даних технологій та врахувавши можливі правові проблеми, необхідно розробити концепцію правового регулювання Інтернету речей. Неодмінно в законодавстві має бути визначено термінологію та принципи регулювання відповідних відносин, що виникають із використанням даних технологій, встановлено юрисдикцію учасників, чітко виокремлено коло суб'єктів таких відносин.

Схеми до теми

Інтернет речей (англ. Next Generation Network — мережа наступного покоління) — це мультисервісна мережа зв'язку, яка підтримує інтеграцію послуг передавання мови, даних та мультимедіа та базується на IP-мережі (на відміну від ISDN). Основна відмінність мереж наступного покоління від традиційних мереж в тому, що вся інформація, яка циркулює в мережі, розбита на дві складові. Це сигнальна інформація, що забезпечує комутацію абонентів та надання послуг і безпосередньо даних користувача, що містять корисну інформацію, призначену абоненту (голос, відео, дані). Шляхи проходження сигнальних повідомлень і даних користувача можуть не збігатися.

Офіційне визначення Інтернету речей наведено в Рекомендації МСЕ-Т Y.2060, згідно з якою IoT — глобальна інфраструктура інформаційного суспільства, яка забезпечує передові послуги за рахунок організації зв'язку між речами (фізичними або віртуальними) на основі існуючих і таких, що розвиваються, сумісних інформаційних і комунікаційних технологій.

Базові принципи Інтернету речей

Можливість кожного об'єкта відправляти і отримувати дані за допомогою персональної мережі або мережі Інтернет, до якої він підключений	Повсюдно поширена комунікаційна інфраструктура	Глобальна ідентифікація кожного об'єкта

Відмінності Інтернету речей від існуючого Інтернету людей

- ✓ фокус на речах, а не на людині;
- ✓ істотно більша кількість підключених об'єктів;
- ✓ істотно менші розміри об'єктів і невисокі швидкості передачі даних;
- ✓ фокус на зчитуванні інформації, а не на комунікаціях;
- ✓ необхідність створення нової інфраструктури і альтернативних стандартів.

Відмінності понять «Інтернет речей» і «інтернет-річ»

Під інтернет-річчю розуміється будь-який пристрій, який:

- ✓ має доступ до мережі Інтернет з метою передачі або запиту будь-яких даних;
- ✓ має конкретну адресу в глобальній мережі або ідентифікатор, за яким можна здійснити зворотний зв'язок з річчю;
- ✓ має інтерфейс для взаємодії з користувачем.

Напрямки практичного застосування IoT

На основі Інтернету речей можуть бути реалізовані всілякі «розумні» (smart) додатки в різних сферах діяльності й життя людини. ***«Розумна планета»*** — людина зможе буквально «тримати руку на пульсі» планети — своєчасно реагувати на проблеми щодо планування господарств, забруднення та інших екологічних проблем, а значить, ефективно розпоряджатися невідновлюваними ресурсами. ***«Розумне місто»*** — міська інфраструктура і супутні муніципальні послуги, такі як освіта, охорона здоров'я, громадська безпека, ЖКГ, стануть більше пов'язаними і ефективними. ***«Розумний будинок»*** — система буде розпізнавати конкретні ситуації, що відбуваються в будинку, і реагувати на них відповідним чином, що забезпечить мешканцям безпеку, комфорт і ресурсозбереження. ***«Розумна енергетика»*** — буде забезпечена надійна і якісна передача електричної енергії від джерела до приймача в потрібний час і в необхідній кількості. ***«Розумний транспорт»*** — переміщення пасажирів з однієї точки простору в іншу стане зручнішим, швидшим і безпечнішим. ***«Розумна медицина»*** — лікарі й пацієнти зможуть отримати віддалений доступ до медичного обладнання або до історії хвороби в будь-якому місці, буде реалізована система віддаленого моніторингу здоров'я, автоматизована видача лікарських препаратів хворим тощо.

Ситуаційні завдання до теми

Задача 1

Між ПАТ «ТЕРРА БАНК» та Міжнародною юридичною фірмою «Gide Loyretee Nouel» підписана угода про надання останнім послуг. Керівник ПАТ «ТЕРРА БАНК» Клименко відмовив в наданні копії договору Міжнародній юридичній фірмі «Gide Loyretee Nouel», надавши тільки інформацію, яка, на його думку, стосувалася умов отримання бюджетних коштів та надання відповідних послуг. При цьому підставою для відмови в наданні копії самого договору, за словами Клименка, стало те, що договір може містити та-

кож комерційну таємницю та іншу конфіденційну інформацію.

➤ *Чи слід вважати відмову Клименка в цій ситуації правомірною?*

Задача 2

Видавнича група «Фламмаріон» видала книгу з секретною медичною історією колишнього Президента Франції Міттерана (зокрема про те, що він був хворий на рак і приховував це близько 10 років, перебуваючи на посаді президента). Книга вийшла через 9 днів після смерті президента. Сім'я Міттерана подала позов до суду на видавничу групу «Фламмаріон».

➤ *Яке рішення повинен винести суд з точки зору норм міжнародного інформаційного права?*

Задача 3

Юридичне агентство «Гомер» звернулося до Комітету Національної комісії з цінних паперів та фондового ринку з питань корпоративного управління, емісії та обігу пайових цінних паперів з проханням надати йому право на поширення інформації про цінні папери комерційних банків та інших кредитних організацій. Керівництво Комітету, розглянувши заяву та нотаріально завірені копії реєстраційних документів агентства, відмовило йому в укладенні договору на поширення вказаної інформації на підставі того, що агентство «Гомер» займається лише експертизою проєктів законів. Керівництво юридичного агентства «Гомер», посилаючись на Статут агентства, повідомило керівництву Комітету про спеціалізацію його працівників у сфері поширення будь-якої соціально-правової інфор-

мації. Опираючись на ці факти, агентство оскаржило рішення Комітету Національної комісії з цінних паперів та фондового ринку з питань корпоративного управління.

➤ *Чи правомірними є дії Комітету Національної комісії з цінних паперів та фондового ринку?*

Завдання 1

Визначте види юридичної відповідальності за правопорушення у сфері інформації, нормативно-правові акти, які встановлюють такий вид відповідальності, та наведіть приклади інформаційних правопорушень.

Відповідь оформіть у вигляді таблиці.

Завдання 2

Проаналізуйте норми Кодексу України про адміністративні правопорушення, виділіть серед них правопорушення у сфері інформації та надайте власні пропозиції щодо систематизації таких правопорушень.

Питання для самоперевірки

1. *Розкрийте поняття «Інтернет речей».*
2. *Дайте визначення державно-правового механізму інформаційної безпеки Інтернету речей. У чому полягають його особливості?*
3. *Визначте, які основні напрями державної політики в інформаційній сфері закріплені законодавчо в контексті нормативно-правового регулювання Інтернету речей.*

ЗАГАЛЬНІ МЕТОДИЧНІ РЕКОМЕНДАЦІЇ ДО ВИРІШЕННЯ ЗАДАЧ (ТА/АБО ВИКОНАННЯ ЗАВДАНЬ)

Однією із форм навчальних занять, під час яких студенти набувають знань та умінь із інформаційного права, є практичні заняття.

Практичне заняття — вид навчального заняття, під час якого для студентів організовується аналіз окремих теоретичних положень з дисципліни «Інформаційне право», формуються навички і вміння їх практичного застосування через індивідуальне виконання відповідно сформульованих завдань. Основними завданнями практичного заняття є поглиблення та уточнення знань, здобутих на лекціях і в процесі самостійної роботи; накопичення первинного досвіду організації роботи та технікою управління; оволодіння початковими навиками роботи із нормативними документами.

Структура практичного заняття: попередній контроль знань, навичок і вмінь студентів; формулювання загальної проблеми та її обговорення за участю студентів; розв'язування задач та їх обговорення.

Перш ніж приступити до вирішення задачі, необхідно визначити, яких правовідносин у сфері правого регулювання інформаційно-правових інститутів вона стосується, вивчити відповідну навчально-методичну літературу, необхідні нормативні акти.

Відповіді на поставлені в задачі питання повинні бути повними, обґрунтованими. Необхідно не тільки вказати на можливі порушення норм чинного законодавства, а й визначити наслідки такого порушення, відновлення порушеного права і засоби захисту прав сторін у інформаційно-правових інституту-

тах. Водночас необхідно посилатися на конкретні статті, пункти нормативних актів та використовувати нормативно-правову базу України.

При вирішенні задач студенти мають використовувати наступний алгоритм їх розв'язання.

Вирішення правового спору здійснюється у 3 етапи:

1. З'ясовуюча частина.
2. Підготовча частина.
3. Письмова частина.

На першому етапі *(з'ясовуюча частина)* відбувається:

1) з'ясування спірних обставин або тих, що порушують права чи інтереси осіб;

2) кваліфікація усіх обставин відповідно до норм чинного законодавства;

3) попереднє вирішення проблеми відповідно до чинного законодавства.

Підготовча частина складається із наступних дій:

1) встановлення порядку захисту порушених прав чи інтересів (відповідальність за порушення законодавства про доступ до публічної інформації; адміністративна відповідальність за порушення інформаційного законодавства; відповідальності за порушення умов зберігання, використання архівних документів та їх знищення; відповідальність за порушення законодавства про бібліотечну справу тощо);

2) встановлення форми захисту (позовна заява, скарга, заява тощо);

3) перевірка дотримання строку позовної давності;

4) визначення винної особи та особи, яка має право на звернення;

5) визначення підвідомчості спору;

6) визначення підсудності.

Третій етап — *письмова частина* — полягає власне у написанні розв'язання.

Письмова відповідь має містити:

1) вказівку на суть порушеного права чи інтересу, у тому числі наводяться необхідні розрахунки (якщо умова задачі дозволяє це зробити);

2) при викладенні суті спору обов'язковим є мотивування власної позиції, тобто посилання на нормативно-правові акти, які регулюють спірні відносини та вирішують спір по суті. При цьому обов'язково потрібно враховувати положення щодо юридичної сили та дії нормативно-правових актів у часі та просторі;

3) за кожним порушенням права чи інтересу наводиться попередній висновок;

4) у кінці наводиться загальний висновок, який і є відповіддю на поставлене у задачі завдання.

ТЕМИ РЕФЕРАТІВ ДЛЯ ПРЕЗЕНТАЦІЙ НА СЕМІНАРСЬКОМУ ЗАНЯТТІ

1. Теорія правової інформатики.
2. Наука інформаційного права.
3. Електронне право високих технологій як галузевий інститут інформаційного права.
4. Методи інформаційного права та методологія електронного права високих технологій.
5. Основні принципи, об'єкти і суб'єкти високотехнологічного інформаційного права.
6. Синергетична концепція інноваційного розвитку інформаційного права.
7. Законодавство у сфері рекламної діяльності та правова регуляція електронної реклами в Інтернеті.
8. Законодавство у сфері цифрового телебачення, національного радіомовлення і кінематографії України.
9. Організаційно-правові засади здійснення видавничої справи та види електронних видань.
10. Консолідація інформаційного законодавства.
11. Інформаційне законодавство США та Англії.
12. Інформаційна сфера як сфера обігу інформації та правового регулювання.
13. Інформація як основний об'єкт інформаційної сфери та системи права.
14. Визначення поняття «інформація».
15. Класифікація інформації в залежності від доступу до неї.
16. Юридичні особливості й властивості інформації.

17. Модель інформаційної сфери.
18. Сфера пошуку, отримання та споживання інформації.
19. Сфера створення та розповсюдження вихідної й похідної інформації.
20. Область формування інформаційних ресурсів, підготовки інформаційних продуктів, надання інформаційних послуг.
21. Правове регулювання інформаційних правовідносин.
22. Органи державної влади як суб'єкти інформаційних правовідносин.
23. Правове регулювання персональних даних.
24. Становлення та розвиток системи охорони інформації про фізичну особу.
25. Місце інформаційних відносин в державному управлінні та їх значення у забезпеченні демократизації суспільства.
26. Правові основи редакційно-видавничої та інформаційної діяльності преси в електронному форматі.
27. Правовий статус та особливості діяльності інформаційних агентств та електронної пошти.
28. Організація бібліотечної діяльності та правові проблеми електронних бібліотек.
29. Правові особливості організації архівної діяльності та системи електронних архівів.
30. Організаційно-правова діяльність державного експерта з питань таємниць.
31. Суб'єкти та об'єкти правових відносин у сфері державної таємниці.
32. Питання власності у зв'язку з інформацією, що становить державну таємницю.
33. Захист державної таємниці.
34. Контроль і нагляд за забезпеченням захисту державної таємниці.

35. Кримінально-правова охорона та захист інформаційних відносин.
36. Питання відповідальності за поширення недостовірної інформації, отриманої в мережі Інтернет.
37. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій.
38. Охорона та захист інформаційних ресурсів.
39. Відповідальність за зловживання свободою діяльності друкованих засобів масової інформації.

ДОДАТОК

ПРО СТРАТЕГІЮ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ (проєкт)

Відповідно до частини другої статті 2 Закону України «Про концепцію (основи) національної безпеки України» постановляю:

1. Затвердити Стратегію забезпечення інформаційної безпеки України.
2. Кабінету Міністрів України забезпечити виконання зазначеної Стратегії.
3. Секретарю Ради національної безпеки і оборони України інформувати Президента України про стан реалізації зазначеної Стратегії.

Президент України

ЗАТВЕРДЖЕНО
Указом Президента України

СТРАТЕГІЯ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Стратегія забезпечення інформаційної безпеки України (далі — Стратегія) визначає основні засади державної політики у сфері забезпечення інформаційної безпеки України, спрямованої на захист інформаційних інтересів особи, суспільства і держави від зовнішніх та внутрішніх загроз.

І. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Інформаційна безпека України — це сукупність життєво важливих умов функціонування суб'єктів (особи, суспільства, держави) в інформаційній сфері та суб'єктивних (правових, політичних, інформаційних, наукових, оперативно-розшукових) можливостей їх усвідомлення й контролю.

1.2. Основними характеристиками інформаційної безпеки України є стабільність інформаційної системи держави та стан її захищеності.

1.3. Залежно від характеру загроз існують загрози: за джерелами походження, за повторюваністю вчинення, за рівнем детермінізму, за структурою впливу, за характером реалізації, за суб'єктами, за рівнем поширення, за формою прояву.

1.4. Система забезпечення інформаційної безпеки включає правове, політичне, кадрове, інформаційне, наукове, оперативно-розшукове забезпечення:

— правове забезпечення — створення досконалої правової бази та системи контролю за інформаційною діяльністю з метою забезпечення стабільності інформаційної системи, попередження, виявлення та припинення правопорушень суб'єктами інформаційного права;

— політичне забезпечення — утвердження демократичних форм й інститутів через чітке розмежування компетенції органів законодавчої, виконавчої та судової влади у сфері інформаційної безпеки;

— кадрове забезпечення — діяльність, змістом якої є забезпечення органів з повноваженнями у сфері забезпечення інформаційної безпеки необхідним, відповідаючим певним вимогам, контингентом кадрів, їх соціального захисту;

— інформаційне забезпечення — комплекс організаційних, технічних, технологічних заходів, засобів та методів щодо локалізації потенційних загроз інформаційної безпеки;

— наукове забезпечення — здійснення науково-аналітичної та прогнозної діяльності науково-дослідними установами з метою прогнозування та оцінки можливих внутрішніх і зовнішніх загроз, інформування державних органів про них, проведення наукових досліджень, видання наукових праць у зазначеній сфері;

— оперативно-розшукове забезпечення — сукупність оперативно-розшукових засобів, спрямованих на отримання та обмін необхідною оперативно-розшуковою інформацією щодо фактів правопорушень у сфері інформаційної діяльності.

1.5. Функціями забезпечення інформаційної безпеки є:

— розрахункові — полягають в обробці інформації, яка знаходиться в системі за певними алгоритмами;

— технологічні — полягають в автоматизації всього технологічного циклу або окремих його компонентів;

— аналітичні — полягають у проведенні операцій над даними, результатом яких є прогностична інформація — судження про стан об'єкта в майбутньому;

— функція безпеки — це захищеність інформації та підтримка інфраструктури від випадкових або навмисних впливів природного або штучного характеру, які можуть порушити доступність, цілісність та конфіденційність інформації.

II. ЗАГРОЗИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Загрози інформаційної безпеки України є сукупністю дій або подій, які можуть призвести до порушення достовірності, цілісності,

конфіденційності інформації, яка зберігається, передається або обробляється.

2.1. Основними загрозами інформаційної безпеки України є: розкраданням інформації, копіюванням комп'ютерної інформації, знищення комп'ютерної інформації, пошкодження, модифікація комп'ютерної інформації, блокування комп'ютерної інформації, нав'язування неправдивої інформації.

2.2. Розкрадання інформації — це протиправне вилучення інформації (як таємне, так і відкрите) із законного володіння.

2.3. Копіювання комп'ютерної інформації — це отримання копії певної комп'ютерної інформації шляхом, який технологічно для цього призначений.

2.4. Знищення комп'ютерної інформації — це повна втрата можливості користування відповідною інформацією. Знищенням слід вважати не лише ліквідацію файлу, каталогу тощо, у вигляді яких існувала інформація, а й приведення інформації у такий стан, який виключає можливість використання всієї інформації чи значної її частини. Під знищенням носіїв комп'ютерної інформації слід розуміти фізичне знищення відповідних матеріальних предметів або таку зміну їх властивостей, яка призводить до неможливості подальшого зберігання комп'ютерної інформації на цих носіях.

2.5. Пошкодження — це зміна властивостей майна, при якому істотно погіршується його стан, втрачається значна частина його корисних властивостей і воно стає повністю або частково непридатним для цільового використання.

2.6. Модифікація комп'ютерної інформації — це внесення будь-яких змін, крім пов'язаних з адаптацією програми для ЕОМ або баз даних.

2.7. Блокування комп'ютерної інформації — це штучне ускладнення доступу користувачів до інформації, не пов'язане з її знищенням.

2.8. Нав'язування неправдивої інформації — це умисне перекручення або приховування істини з метою ввести в оману особу, у віданні якої знаходиться інформація, і таким чином домогтися від неї добровільної передачі цієї інформації.

ІІІ. ОСНОВНІ НАПРЯМИ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Державна політика у сфері забезпечення інформаційної безпеки має спрямовуватися на створення умов для ефективного і якісного інформаційного забезпечення, вирішення стратегічних та оперативних завдань соціального та економічного розвитку країни; своєчасне виявлення, попередження і нейтралізацію зовнішніх та внутрішніх загроз інформаційної безпеки; зміцнення законності та правопорядку у сфері інформаційної діяльності. Її основні напрями зазначені нижче.

3.1. У зовнішньополітичній сфері:

— розробка основних напрямів державної політики в галузі вдосконалення інформаційного забезпечення зовнішньополітичного курсу України;

— розробка та реалізація комплексу заходів щодо посилення інформаційної безпеки інформаційної інфраструктури органів виконавчої влади, що реалізують зовнішню політику України, українських представництв та організацій за кордоном, представництв України при міжнародних організаціях;

— створення українськими представництвами та організаціями за кордоном умов для роботи з нейтралізації поширюваної там дезінформації про зовнішню політику України;

— вдосконалення інформаційного забезпечення роботи з протидії порушенням прав і свобод українських громадян і юридичних осіб за кордоном;

— вдосконалення інформаційного забезпечення суб'єктів України з питань зовнішньополітичної діяльності, які входять до їхньої компетенції.

3.2. У внутрішньополітичній сфері:

— розробка та вдосконалення єдиної політики в галузі захисту інформації;

— забезпечення захисту державних секретів;

— протидія технічним розвідкам;

— захист від впливу інформаційної зброї;

— організаційно-технічний захист інформаційних ресурсів, інформаційно-телекомунікаційних систем та інформаційної інфраструктури;

— відповідність інформаційних систем та об'єктів інформатизації вимогам стандартів і нормативних правових актів у галузі інформації та захисту інформації;

— підтвердження відповідності технічних засобів вимогам інформаційної безпеки.

3.3. В економічній сфері:

— організація та здійснення державного контролю за створенням, розвитком і захистом систем і засобів збору, обробки, зберігання та передачі статистичної, фінансової, біржової, податкової, митної інформації;

— корінна перебудова системи державної статистичної звітності з метою забезпечення достовірності, повноти та захищеності інформації, що здійснюється шляхом введення суворої юридичної відповідальності посадових осіб за підготовку первинної інформації, організацію контролю за діяльністю цих осіб та служб обробки та аналізу статистичної інформації, а також шляхом обмеження комерціалізації такої інформації;

— розробка національних сертифікованих засобів захисту інформації та впровадження їх у системи та засоби збору, обробки, зберігання та передачі статистичної, фінансової, біржової, податкової, митної інформації;

— розробка і впровадження національних захищених систем електронних платежів на базі інтелектуальних карт, систем електронних грошей та електронної торгівлі, стандартизація цих систем, а також розробка нормативної правової бази, що регламентує їх використання;

— вдосконалення нормативної правової бази, що регулює інформаційні відносини у сфері економіки;

— вдосконалення методів відбору та підготовки персоналу для роботи в системах збору, обробки, зберігання та передачі економічної інформації.

3.4. У соціальній та гуманітарній сферах:

— прискорення реформування національної медійної та комунікаційної систем, модернізація їх стандартів, створення системи суспільного мовлення;

— забезпечення незалежності та плюралізму засобів масової інформації та їх залучення до інтеграції України у глобальний інформаційний простір;

— впровадження та поширення сучасних інформаційних технологій;

— недопущення монополізації інформаційного ринку України;

— забезпечення вигідного для українських виробників місця у світовому поділі праці у сфері інформаційних послуг;

— забезпечення захисту громадян від інформаційної продукції, що негативно впливає на фізичний, психічний, інтелектуальний та моральний розвиток людини;

— удосконалення національного інформаційного законодавства щодо забезпечення отримання громадянами суспільно значущої інформації і чітке визначення процедури доступу до інформації;

— удосконалення організаційних та правових засад національного інформаційного ринку;

— розвиток електронних інформаційних технологій у системі управлінських структур; активізація державної політики шляхом розробки законодавства у сфері захисту вітчизняного інтернет-простору та розвитку інтернет-послуг, у тому числі для безпеки вітчизняних інтернет-ресурсів і нейтралізації несанкціонованих втручань у користування інформаційними послугами.

3.5. Реалізація державної політики забезпечення інформаційної безпеки України базується на:

— внутрішніх принципах — законності, балансі інтересів особистості, суспільства і держави, комплексності, системності, стабільності та надійності, інтеграції з міжнародними системами безпеки, контролю;

— зовнішніх принципах — суверенітеті, інтегрованості у міжнародні інформаційні системи інформаційної безпеки, взаємовигідному співробітництві між державами, сумлінному виконанні взятих на себе міжнародних зобов'язань, боротьбі з міжнародним інфор-

маційним тероризмом і піратством, пріоритеті загальновизнаних норм і принципів міжнародного права перед нормами і принципами національного права.

3.6. Повноваження здійснювати державну політику у сфері забезпечення інформаційної безпеки України надані на стратегічному рівні — Раді національної безпеки і оборони України та Кабінету Міністрів України; на тактичному рівні — центральним органам виконавчої влади; на оперативному рівні — місцевим органам виконавчої влади.

Основним змістом системи забезпечення інформаційної безпеки є реалізація сукупності науково-обґрунтованих і апробованих на практиці з урахуванням світового і вітчизняного досвіду заходів у контексті реалізації державної політики інформаційної безпеки.

Основними функціями суб'єктів забезпечення інформаційної безпеки є: аналіз стану і можливих загроз національній безпеці України в інформаційній сфері та узагальнення міжнародного досвіду щодо формування та реалізації інформаційної політики; удосконалення системи правового та наукового забезпечення інформаційної безпеки України; здійснення аналізу питань інформаційної безпеки та присутності України у світовому просторі; розробка рекомендацій щодо встановлення стандартів, норм і правил експлуатації програмно-технічних засобів інформатизації, єдиних класифікаторів інформації, інформаційних реєстрів і ресурсів, прогнозування, виявлення та оцінка потенційних та можливих загроз інформаційній безпеці, дестабілізуючих чинників, причин їх виникнення, наслідків прояву, запобігання й усунення їх впливу на інформаційні інтереси.

IV. ПОВНОВАЖЕННЯ СУБ'ЄКТІВ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

4.1. Верховна Рада України:

— визначає засади зовнішньої та внутрішньої політики держави в інформаційній сфері;

— здійснює законодавче регулювання політики національної безпеки України в інформаційній сфері (нормативно закріплює

права і свободи людини і громадянина в інформаційній сфері, гарантії цих прав і свобод; основні обов'язки громадянина; закріплює основи національної безпеки, засади цивільно-правової відповідальності; визначає діяння, які є злочинами, адміністративними або дисциплінарними правопорушеннями, та відповідальність за них);

— створює правові засади функціонування системи забезпечення національної безпеки в інформаційній сфері;

— затверджує загальнодержавні програми в цій сфері та контролює хід їх виконання;

— затверджує бюджетні асигнування для фінансування діяльності із забезпечення національної безпеки в інформаційній сфері;

— визначає порядок створення та повноваження Ради національної безпеки і оборони України;

— призначає за поданням Президента України, Прем'єр-міністра України, Міністра оборони України, Міністра закордонних справ України, Голови Служби безпеки України;

— призначає на посади та звільняє половину складу Національної ради України з питань телебачення і радіомовлення.

4.2. Президент України здійснює загальне керівництво у сфері інформаційної безпеки України, а саме:

— очолює Раду національної безпеки і оборони України;

— здійснює керівництво в інформаційній та інших сферах національної безпеки та оборони України;

— здійснює контроль і координацію діяльності державних органів у забезпеченні національної безпеки в інформаційній та інших сферах;

— вживає оперативні заходи з метою нейтралізації загроз національним інтересам України в межах компетенції, визначеної Конституцією;

— один раз на рік на сесії Верховної Ради звітує перед народом України про стан національної безпеки України;

— забезпечує взаємодію усіх гілок державної влади між собою, а також із недержавною складовою системи забезпечення національної безпеки в інформаційній сфері;

— видає нормативно-правові акти з питань забезпечення національної безпеки в інформаційній сфері;

— визначає реальні та потенційні загрози та небезпеки для національної безпеки в інформаційній сфері та вживає необхідних заходів з її забезпечення.

4.3. Кабінет Міністрів України у сфері забезпечення інформаційної безпеки:

— забезпечує інформаційний суверенітет України, здійснення внутрішньої і зовнішньої інформаційної політики держави, виконання Конституції і законів України, актів Президента України, що стосуються інформаційної безпеки;

— вживає заходів щодо забезпечення прав і свобод людини і громадянина в інформаційній сфері;

— забезпечує проведення державної політики інформаційної безпеки;

— спрямовує і координує роботу усієї системи органів державного управління з питань, що стосуються інформаційної безпеки;

— визначає потреби у витратах на забезпечення інформаційної безпеки, забезпечує виконання затвердженого Верховною Радою України Державного бюджету України щодо фінансування заходів у сфері інформаційної безпеки у визначених обсягах;

— організовує розроблення і виконання державних програм з розвитку інформаційної інфраструктури органів державного управління;

— здійснює передбачені законодавством заходи щодо формування, розміщення, фінансування та виконання державного оборонного замовлення на поставку (закупівлю) продукції, виконання робіт, надання послуг для потреб органів, що забезпечують інформаційну безпеку;

— встановлює порядок надання суб'єктам забезпечення інформаційної безпеки у користування державного майна, засобів зв'язку і радіочастотного ресурсу, комунікацій, інших об'єктів інфраструктури держави, навігаційної, топогеодезичної, метеорологічної, гідрографічної та іншої інформації;

— забезпечує комплектування особового складу сил забезпечення інформаційної безпеки;

— утворює, реорганізовує, ліквідовує науково-дослідні установи, навчальні заклади та окремі кафедри (відділення, факультети) суб'єктів забезпечення інформаційної безпеки;

— забезпечує реалізацію права на соціально-економічний захист відповідно до законодавства України, що регламентує діяльність окремих суб'єктів забезпечення інформаційної безпеки;

— здійснює у визначених законом випадках регулювання господарської діяльності у суб'єктах забезпечення інформаційної безпеки;

— встановлює відповідно до закону порядок реалізації та утилізації об'єктів інформаційної інфраструктури, інформаційних ресурсів;

— забезпечує здійснення, передбачених законодавством заходів, щодо цивільної оборони України, надання військової допомоги іншим державам, направлення підрозділів Збройних сил України до інших держав, допуску та умов перебування підрозділів збройних сил інших держав на території України та участі України в міжнародних миротворчих операціях;

— контролює виконання законів у сфері оборони, здійснює відповідно до законів інші заходи щодо забезпечення обороноздатності України, координує і контролює їх виконання та несе, в межах своїх повноважень, відповідальність за забезпечення оборони України.

4.4. Міністерства та інші центральні органи виконавчої влади в межах своїх повноважень:

— забезпечують реалізацію законів України, указів та розпоряджень Президента України, концепцій, доктрин, програм, постанов органів державного управління у сфері інформаційної безпеки;

— забезпечують створення, підтримку в готовності і застосування сил та засобів забезпечення інформаційної безпеки, а також управління їх діяльністю;

— у межах своєї компетенції розробляють нормативні правові акти в інформаційній сфері і представляють їх Президентові України та Кабінету Міністрів України;

— вносять в органи виконавчої влади пропозиції щодо удосконалення функціонування системи забезпечення інформаційної безпеки України;

— керують діяльністю підвідомчих організацій з планування і проведення заходів по забезпеченню інформаційної безпеки;

— забезпечують дотримання прав і законних інтересів громадян, організацій і держави, законів та інших нормативно-правових актів в інформаційній сфері;

— притягують до відповідальності посадових осіб, дії яких призводять до порушення національних інтересів в інформаційній сфері, створюють умови або безпосередню загрозу інформаційній безпеці України.

4.5. Органи місцевого самоврядування та місцеві державні адміністрації забезпечують вирішення питань у сфері інформаційної безпеки України у відповідних адміністративно-територіальних одиницях, а саме:

— забезпечують виконання Конституції та законів України, рішень Конституційного Суду України, актів Президента України, Кабінету Міністрів України, інших органів державної влади у сфері забезпечення інформаційної безпеки;

— забезпечують здійснення заходів щодо охорони громадської безпеки, громадського порядку, боротьби зі злочинністю в інформаційній сфері;

— здійснюють заходи щодо організації правового інформування та інформаційного виховання населення;

— проводять роботу, пов'язану з розробленням та здійсненням заходів щодо інформаційного забезпечення біженців, а також депортованих осіб, які добровільно повертаються в регіони їх колишнього проживання;

— забезпечують виконання законодавства щодо національних меншин і міграції, про свободу думки і слова, свободу світогляду і віросповідання;

— оголошують у разі стихійного лиха, аварій, катастроф, епідемій, епізоотій, пожеж, інших надзвичайних подій зони надзвичайної ситуації; здійснюють передбачені законодавством заходи, пов'язані із забезпеченням інформаційної безпеки, захистом інформаційних прав особи;

— забезпечують своєчасне інформування населення про загрозу виникнення або виникнення надзвичайних ситуацій під час

проведення потенційно небезпечних заходів в умовах присутності цивільного населення за участю особового складу Збройних сил України, інших військових формувань та правоохоронних органів з використанням озброєння і військової техніки.

4.6. Діяльність МВС України в інформаційній сфері держави здійснюється властивими їй формами та методами, передбаченими законами України «Про міліцію», «Про оперативно-розшукову діяльність», «Про боротьбу з тероризмом», «Про боротьбу з корупцією», «Про організаційно-правові основи боротьби з організованою злочинністю», у тісній взаємодії з іншими суб'єктами забезпечення національної безпеки та спрямована на нейтралізацію загроз національним інтересам і національній безпеці України.

Відповідно до п. 3 Указу Президента України «Про Положення про Міністерство внутрішніх справ України» серед основних завдань МВС України є:

— організація і координація діяльності органів внутрішніх справ щодо захисту прав і свобод громадян, інтересів суспільства і держави в інформаційній сфері від протиправних посягань на них, охорони громадського порядку і забезпечення громадської безпеки в інформаційній сфері;

— участь у розробленні та реалізації державної політики щодо боротьби із кіберзлочинністю та кібертероризмом;

— забезпечення запобігання злочинам в інформаційній сфері, їх припинення, розкриття і розслідування, розшуку осіб, які вчинили злочини, вжиття заходів щодо усунення причин і умов, що сприяють вчиненню правопорушень;

— організація охорони та оборони внутрішніми військами особливо важливих державних об'єктів, зокрема об'єктів критичної інфраструктури держави тощо.

4.7. Діяльність Служби безпеки України в інформаційній сфері держави здійснюється властивими їй формами та методами, передбаченими законами України «Про Службу безпеки України», «Про оперативно-розшукову діяльність», «Про контррозвідувальну діяльність», «Про боротьбу з тероризмом», «Про боротьбу з корупцією», «Про організаційно-правові основи боротьби з організованою злочинністю», у тісній взаємодії з іншими суб'єктами забезпечен-

ня національної безпеки та спрямована на нейтралізацію загроз національним інтересам і національній безпеці України, визначеними у ст. 7 Закону України «Про основи національної безпеки України»:

— постійний моніторинг впливу на національну безпеку процесів, що відбуваються, в першу чергу, в інформаційній, політичній, соціальній, економічній, екологічній, науково-технологічній, воєнній та інших сферах, релігійному середовищі, міжетнічних стосунках; прогнозування змін, що відбуваються в них, та потенційних загроз національній безпеці;

— систематичне спостереження за станом і проявами міжнародного та інших видів тероризму (зокрема й кібертероризму);

— прогнозування, виявлення та оцінка можливих загроз, дестабілізуючих чинників і конфліктів, причин і умов їх виникнення та наслідків прояву;

— комплексне інформаційно-аналітичне забезпечення діяльності вищих органів державної влади та інших суб'єктів забезпечення національної безпеки України в інформаційній сфері;

— розроблення науково обґрунтованих пропозицій і рекомендацій щодо прийняття управлінських рішень з метою захисту національних інтересів України;

— запобігання та нейтралізація впливу загроз і дестабілізуючих чинників на національну безпеку та національні інтереси в інформаційній сфері;

— локалізація, деескалація та врегулювання конфліктів, ліквідація їх негативних наслідків або впливу дестабілізуючих чинників;

— оцінка результативності дій щодо забезпечення національної безпеки в інформаційній сфері та визначення витрат на ці цілі;

— участь у двосторонньому і багатосторонньому співробітництві в галузі інформаційної безпеки, якщо це відповідає національним інтересам України;

— спільне проведення планових та оперативних заходів з компетентними структурами іноземних держав у рамках міжнародних організацій та договорів у галузі безпеки.

4.8. Державна служба спеціального зв'язку та захисту інформації України:

— забезпечує формування і реалізацію державної політики у сферах захисту державних інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, криптографічного та технічного захисту інформації, використання і захисту державних електронних інформаційних ресурсів, телекомунікацій, користування радіочастотним ресурсом України;

— приймає участь у формуванні і реалізації державної політики у сфері електронного документообігу органів державної влади та органів місцевого самоврядування, розробленні та впровадженні електронного цифрового підпису в органах державної влади та органах місцевого самоврядування;

— забезпечує в установленому порядку урядовим зв'язком Президента України, Голови Верховної Ради України, Прем'єр-міністра України, інших посадових осіб органів державної влади, місцевого самоврядування, органів військового управління, керівників підприємств, установ і організацій у мирний час, в умовах надзвичайного та воєнного стану, а також у разі виникнення надзвичайної ситуації;

— забезпечує функціонування безпеки та розвитку державної системи урядового зв'язку і Національної системи конфіденційного зв'язку;

— розробляє та здійснює заходи щодо розвитку телекомунікаційних мереж, поліпшення їх якості, забезпечення доступності і сталого функціонування;

— сприяє інтеграції сфер телекомунікацій, користування радіочастотним ресурсом України у світовий інформаційно-комунікаційний простір.

4.9. Суди загальної юрисдикції здійснюють судочинство у справах про злочини, що завдають шкоди інформаційній безпеці України.

4.10. Прокуратура України здійснює повноваження щодо забезпечення національної безпеки України в інформаційній сфері відповідно до Конституції України та Закону України «Про прокуратуру України». Прокуратура України становить єдину систему, на яку покладаються:

— підтримання державного обвинувачення в суді, зокрема за справами щодо посягань у сфері інформаційних правовідносин;

— представництво інтересів громадянина або держави в суді у випадках, визначених законом;

— нагляд за додержанням законів органами, які проводять оперативно-розшукову діяльність, дізнання, досудове слідство за справами щодо посягань у сфері інформаційних правовідносин;

— нагляд за додержанням законів під час виконання судових рішень у кримінальних справах щодо посягань у сфері інформаційних правовідносин, а також під час застосування інших заходів примусового характеру, пов'язаних з обмеженням особистої свободи громадян, зокрема в інформаційній сфері;

— нагляд за додержанням прав і свобод людини і громадянина в інформаційній сфері, додержанням законів з цих питань органами виконавчої влади, органами місцевого самоврядування, їх посадовими і службовими особами.

4.11. Правовий статус Ради національної безпеки і оборони України щодо забезпечення національної безпеки України в інформаційній сфері визначений у Конституції України, в законах України «Про основи національної безпеки України» та «Про Раду національної безпеки і оборони України». Серед основних завдань є:

— внесення пропозицій Президентові України щодо реалізації засад внутрішньої і зовнішньої політики в інформаційній та інших сферах національної безпеки і оборони;

— координація та здійснення контролю за діяльністю органів виконавчої влади в інформаційній та інших сферах національної безпеки й оборони у мирний час;

— координація та здійснення контролю за діяльністю органів виконавчої влади в інформаційній та інших сферах національної безпеки й оборони в умовах воєнного або надзвичайного стану та під час виникнення кризових ситуацій, що загрожують національній безпеці України.

4.12. Основними завданнями Міжвідомчої комісії з питань інформаційної політики та інформаційної безпеки є:

— здійснення аналізу стану і можливих загроз національній безпеці України в інформаційній сфері та узагальнення міжнародного досвіду щодо формування та реалізації інформаційної політики;

— аналіз здійснення галузевих програм і виконання заходів, пов'язаних із реалізацією міністерствами та іншими центральними органами виконавчої влади державної політики в інформаційній сфері;

— розроблення і внесення Президентові України та РНБО України пропозицій щодо:

— визначення національних інтересів України в інформаційній сфері, концептуальних підходів до формування державної інформаційної політики та забезпечення інформаційної безпеки держави;

— здійснення системних заходів, спрямованих на вдосконалення інформаційної політики України, реалізацію державної стратегії розвитку і захисту національного інформаційного простору та входження України у світовий інформаційний простір;

— удосконалення системи правового та наукового забезпечення інформаційної безпеки України;

— розвиток інформаційної інфраструктури в державі, зокрема з питань модернізації її матеріально-технічної бази та належного фінансового забезпечення;

— організація та порядок міжвідомчої взаємодії міністерств, інших центральних органів виконавчої влади у сфері забезпечення інформаційної безпеки;

— удосконалення системи оперативного інформаційно-аналітичного забезпечення Президента України, зокрема альтернативною інформацією у сфері національної безпеки й оборони.

4.13. Основними завданнями Державного комітету телебачення і радіомовлення України з питань інформаційної політики та інформаційної безпеки є:

— участь у формуванні та забезпечення реалізації державної політики в інформаційній та видавничій сферах, державної політики у сфері захисту суспільної моралі;

— міжгалузева координація та функціональне регулювання з питань діяльності інформаційної та видавничої сфер;

— здійснення управління в інформаційній та видавничій сферах;

— сприяння реалізації конституційного права на свободу слова, забезпечення розвитку інформаційної сфери, розширення національного інформаційного простору.

4.14. Державне агентство з питань електронного урядування України є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України через Віце-прем'єр-міністра України — Міністра регіонального розвитку, будівництва та житлово-комунального господарства і який реалізує державну політику у сфері інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства.

Основними завданнями Агентства є:

— реалізація державної політики у сфері інформатизації, електронного урядування, формування і використання національних електронних інформаційних ресурсів, розвитку інформаційного суспільства;

— координує діяльність органів виконавчої влади, пов'язану із створенням та інтеграцією електронних інформаційних систем і ресурсів в Єдиний вебпортал органів виконавчої влади та наданням інформаційних та інших послуг через електронну інформаційну систему «Електронний Уряд»;

— створення та функціонування інформаційної системи електронної взаємодії державних електронних інформаційних ресурсів;

— розробляє і здійснює разом з іншими органами виконавчої влади та органами місцевого самоврядування заходи щодо розвитку інформаційного суспільства;

— координує адміністрування адресного простору українського сегмента Інтернету;

— визначає у межах повноважень, передбачених законом, особливості захисту державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом тощо.

4.15. Державний комітет телебачення і радіомовлення України є головним у системі центральних органів виконавчої влади з формування та реалізації державної політики у сфері телебачення і радіомовлення, в інформаційній та видавничій сферах.

Основними завданнями Держкомтелерадіо України є формування та реалізація державної політики у сфері телебачення і радіомовлення, інформаційній та видавничій сферах, поліграфії.

Держкомтелерадіо України відповідно до покладених на нього завдань:

— розробляє заходи щодо запобігання внутрішньому і зовнішньому інформаційному впливу, який загрожує інформаційній безпеці держави, суспільства, особи;

— бере участь у формуванні єдиного інформаційного простору, сприянні розвитку інформаційного суспільства;

— реалізує разом з іншими державними органами завдання щодо забезпечення інформаційної безпеки тощо.

4.16. Національна комісія з утвердження свободи слова та розвитку інформаційної галузі здійснює свою діяльність відповідно до Положення про Національну комісію з утвердження свободи слова та розвитку інформаційної галузі, затвердженого Указом Президента України № 493/2006 від 6 червня 2006 р.

Основними завданнями Комісії є:

— підготовка пропозицій щодо виконання зобов'язань України, які випливають з її членства в Раді Європи, ОБСЄ, інших міжнародних організаціях, а також досягнення Україною відповідності політичній складовій Копенгагенських критеріїв 1993 року щодо набуття членства в ЄС в частині забезпечення стабільності та ефективності функціонування відповідних інститутів, які гарантують демократію, принципи свободи слова та розвиток засобів масової інформації та виконання відповідних положень Плану дій «Україна — ЄС»;

— проведення моніторингу ефективності реалізації законів та інших нормативно-правових актів щодо свободи слова та розвитку інформаційної галузі, їх відповідності стандартам Ради Європи, ОБСЄ, інших міжнародних організацій та вимогам політичної складової Копенгагенських критеріїв і відповідних положень Плану дій «Україна — ЄС» та підготовка проєктів відповідних законодавчих, інших нормативно-правових актів;

— підготовка довідкових матеріалів з питань відповідності стандартам Ради Європи, ОБСЄ, інших міжнародних організацій, вимогам політичної складової Копенгагенських критеріїв, виконання відповідних положень Плану дій «Україна — ЄС», вжиття заходів до висвітлення цієї роботи в засобах масової інформації;

— опрацювання пропозицій щодо запровадження європейських стандартів в інформаційній галузі, зокрема щодо:

— реформування державних та комунальних засобів масової інформації;

— створення та розвитку системи суспільних (громадських) засобів масової інформації;

— впровадження цифрового телебачення та інших новітніх інформаційних технологій;

— розвитку українського сегменту мережі Інтернет;

— вдосконалення системи підготовки та перепідготовки працівників засобів масової інформації.

V. ОСНОВНІ НАПРЯМИ ЗАПОБІГАННЯ ТА НЕЙТРАЛІЗАЦІЇ ЗАГРОЗ ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ УКРАЇНИ

5.1. Основними напрямами запобігання та нейтралізації загроз інформаційній безпеці України є

у зовнішньополітичній сфері:

— удосконалення системи забезпечення інформаційної безпеки українського сегменту глобальних інформаційних та телекомунікаційних систем і мереж зв'язку;

— удосконалення правового регулювання діяльності іноземних і спільних з нерезидентами компаній на українському інформаційному ринку;

— прийняття нормативних актів, які б забезпечували конкурентоспроможність вітчизняних виробників в умовах лібералізації національного і міжнародного інформаційного ринку;

— організація взаємодії правоохоронних структур України й інших держав в галузі виявлення, попередження і припинення злочинів в інформаційній сфері;

— розробка та впровадження загальнодержавної системи визначення та моніторингу порогових значень показників (індикаторів), що характеризують рівень захищеності національних інтересів у різних сферах життєдіяльності та виникнення реальних загроз національній безпеці;

у внутрішньополітичній сфері:

— прийняття Стратегії забезпечення інформаційної безпеки України;

— удосконалення системи повноважень державних органів з питань, що пов'язані з різними аспектами забезпечення інформаційної безпеки України;

— удосконалення системи захисту національних інформаційних і телекомунікаційних мереж і нормативно-правового забезпечення її безпечного функціонування;

— приведення законодавства з питань охорони державної таємниці до європейських стандартів;

у економічній сфері:

— розробка правових положень щодо визначення розміру матеріального збитку, заподіяного інтересам особистості, суспільства чи держави правопорушеннями в інформаційній сфері;

— створення державної системи контролю над використанням спеціальних технічних засобів негласного одержання інформації;

у соціальній та гуманітарній сферах:

— удосконалення правових норм, що регламентують відповідальність за правопорушення у галузі забезпечення інформаційної безпеки (включаючи посилення відповідальності за несанкціонований доступ до інформації, її протиправне копіювання, знищення, блокування, модифікацію і протизаконне використання, навмисне поширення недостовірної інформації, протиправне розкриття інформації з обмеженим доступом, її використання в злочинних та корисливих цілях);

— конкретизація механізмів недопущення поширення певних видів інформації, а також пропаганди чи агітації, що розпалюють соціальну, расову, національну і релігійну ненависть та ворожнечу;

— встановлення уніфікованого переліку умов для надання чи обмеження права на доступ до інформації, переліку видів інформації з обмеженим доступом і механізмів реалізації цих обмежень, принципів і організаційних механізмів доступу до інформації ор-

ганів державної влади, органів місцевого самоврядування, громадських організацій, фізичних та юридичних осіб;

— розробка та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, в тому числі з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність.

VI. КОНТРОЛЬ ЗА РЕАЛІЗАЦІЄЮ СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

6.1. Контроль за реалізацією Стратегії здійснюють Верховна Рада України, Президент України, Кабінет Міністрів України, Рада національної безпеки і оборони України, Служба безпеки України, Центральні органи виконавчої влади, правоохоронні органи, інші органи виконавчої влади, місцеві державні адміністрації та органи місцевого самоврядування в межах їх повноважень.

6.2. Стратегія є базою для розробки конкретних програм, проєктів та планів заходів за складовими державної політики у сфері забезпечення інформаційної безпеки та механізмів їх реалізації.

Президент України

СПИСОК РЕКОМЕНДОВАНИХ ДЖЕРЕЛ

1. Загальна декларація прав людини 1948 року // Голос України, 2008. — 10 груд.
2. Конвенція про захист прав людини і основоположних свобод 1950 року // Голос України. — 2001. — 10 січ.
3. Конвенція про захист осіб стосовно автоматизованої обробки даних особистого характеру від 28 січня 1981 року [Електронний ресурс]. — Режим доступу : http://zakon4.rada.gov.ua/laws/show/994_326
4. Конвенція про оцінку впливу на навколишнє середовище у транскордонному контексті від 25 лютого 1991 року [Електронний ресурс]. — Режим доступу: http://zakon1.rada.gov.ua/laws/show/995_272
5. Угода про співробітництво в галузі інформації від 09.10.1992 р. // Офіційний вісник України. — 2004. — № 40. — Ст. 2700.
6. Директива 95/46/ЄС Європейського Парламенту і Ради Європи «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних» від 24.10.1995 р. // Офіційний журнал L 281, 23/11/1995. — С. 0031–0050.
7. Директива 97/66/ЄС Європейського Парламенту і Ради Європи «Стосовно обробки персональних даних і захисту права на невтручання в особисте життя в телекомунікаційному секторі» // Офіційний журнал L 024, 30/01/1998 — С. 0001–0008.
8. Окінавська Хартія глобального інформаційного суспільства від 22.07.2000 р. // Дипломатический вестник. — 2000. — № 8. — С. 51–56.
9. Конвенція про кіберзлочинність від 23 листопада 2001 року // Офіційний вісник України. — 2007. — № 65.
10. Декларація принципів «Побудова інформаційного суспільства — глобальне завдання в новому тисячолітті» від 12.12.2003 р. [Електронний ресурс]. — Режим доступу : http://zakon1.rada.gov.ua/laws/show/995_c57

11. Резолюція 60/45, прийнята Генеральною Асамблеєю Організації Об'єднаних Націй, «Досягнення у галузі інформатизації та телекомунікацій в контексті міжнародної безпеки» від 08.12.2005 р. [Електронний ресурс]. — Режим доступу : http://zakon1.rada.gov.ua/laws/show/995_e45
12. Конституція України // Відомості Верховної Ради України. — 1996. — № 30. — Ст.141.
13. Кодекс України про адміністративні правопорушення від 27.12.1984 року // Відомості Верховної Ради Української РСР. — 1984. — Додаток до № 51. — Ст. 1122.
14. Кримінальний кодекс України від 05.04.2001 року // Відомості Верховної Ради України. — 2001. — № 25–26. — Ст. 131.
15. Цивільний кодекс України від 16.01.2003 року // Відомості Верховної Ради України. — 2003. — № 40. — Ст. 356.
16. Закон України «Про інформацію» від 02.10.1992 року // Відомості Верховної Ради України. — 1992. — № 48. — Ст. 650.
17. Закон України «Про друковані засоби масової інформації (пресу) в Україні» від 16.11.1992 року // Відомості Верховної Ради України. — 1993. — № 1. — Ст. 1.
18. Закон України «Про науково-технічну інформацію» від 25 червня 1993 року // Відомості Верховної Ради України. — 1993. — № 33. — Ст. 345.
19. Закон України «Про Національний архівний фонд та архівні установи» від 24.12.1993 року // Відомості Верховної Ради України. — 1994. — № 15. — Ст. 86.
20. Закон України «Про державну таємницю» від 21.01.1994 року // Відомості Верховної Ради України. — 1994. — № 16. — С. 93.
21. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 року // Відомості Верховної Ради України. — 1994. — № 31. — Ст. 286.
22. Закон України «Про бібліотеки і бібліотечну справу» від 27.01.1995 року // Відомості Верховної Ради України. — 1995. — № 7. — Ст. 45.
23. Закон України «Про інформаційні агентства» від 28.02.1995 року // Відомості Верховної Ради України. — 1995. — № 13. — Ст. 83.
24. Закон України «Про звернення громадян» від 02.10.1996 року // Відомості Верховної Ради України. —1996. — № 47. — Ст. 256.
25. Закон України «Про державну підтримку засобів масової інформації та соціальний захист журналістів» від 23.09.1997 року // Відомості Верховної Ради України. — 1997. — № 50. — Ст. 302.

26. Закон України «Про національну програму інформатизації» від 04.02.1998 року // Відомості Верховної Ради України. — 1998. — № 27–28. — Ст. 181.
27. Закон України «Про електронні документи та електронний документообіг» від 22.05.2003 року // Відомості Верховної Ради України. — 2003. — № 36. — Ст. 275.
28. Закон України «Про телекомунікації» від 18.11.2003 року // Відомості Верховної Ради України. —2004. — № 12. — Ст. 155.
29. Закон України «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки» від 09.01.2007 року // Відомості Верховної Ради України. — 2007. — № 12. — Ст. 102.
30. Закон України «Про доступ до публічної інформації» від 13.01.2011 року // Відомості Верховної Ради України. — 2011. — № 32. — Ст. 314.
31. Розпорядження Кабінету Міністрів України від 15.05.2013 року № 386-р «Про схвалення Стратегії розвитку інформаційного суспільства в Україні» // Урядовий кур'єр. — 2013. — № 105.
32. Постанова Кабінету Міністрів України від 09.08.1993 року № 611 «Про перелік відомостей, що не становлять комерційної таємниці» [Електронний ресурс]. — Режим доступу: http://zakon4.rada.gov.ua/laws/show/611-93-%D0%BF
33. Звід відомостей, що становлять державну таємницю, затверджений наказом Служби безпеки України від 12.08.2005 року № 440 // Офіційний вісник України, 2005. — № 34. — С. 172. — Ст. 2089.
34. Про деякі заходи щодо поліпшення доступу фізичних та юридичних осіб до електронних послуг / Указ Президента України // Урядовий кур'єр. — 2019. — № 144.
35. Про деякі заходи з покращення доступу до мобільного Інтернету / Указ Президента України // Урядовий кур'єр. — 2019. — № 128.
36. Про внесення змін до Правил надання та отримання телекомунікаційних послуг / Постанова Кабінету Міністрів України // Урядовий кур'єр. — 2019. — № 547.
37. Про затвердження Положення про інтегровану систему електронної ідентифікації / Постанова Кабінету Міністрів України // Урядовий кур'єр. — 2019. — № 211.
38. Про затвердження Загальних вимог до кіберзахисту об'єктів критичної інфраструктури / Постанова Кабінету Міністрів України // Урядовий кур'єр. — 2019. — № 118.
39. Про внесення змін до Положення про формування та виконання Національної програми інформатизації / Постанова Кабінету Міністрів України // Урядовий кур'єр. — 2019. — № 103.

40. Інтернет речей: теоретико-методологічні основи правового регулювання. Т. 1: Сфери застосування, ризики і бар'єри, проблеми правового регулювання: монографія / О.А. Баранов; НДІІП НАПрН України. — К. : Видавничий дім «АртЕк», 2018. — 344 с.
41. Кормич Б.А. Інформаційне право: підручник. — Харків : БУРУН і К., 2011. — 334 с.
42. Ліпкан В.А. Теоретичні основи та елементи національної безпеки України: монографія. — К. : «Текст», 2003. — 600 с.
43. Марущак А.І. Інформаційне право України. — К. : ЦУЛ, 2011. — 456 с.
44. Марущак А.І. Інформаційне право: регулювання інформаційної діяльності : навчальний посібник. — К. : ЦУЛ, 2008. — 342 с.
45. Основи інформаційного права України : навч. посіб. / В.С. Цимбалюк, В.Д. Гавловський та ін.; за ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. — К.: Знання, 2004. — 274 с.
46. Науково-практичний коментар до Закону України «Про доступ до публічної інформації» [Електронний ресурс] / Верховна Рада України : [сайт]. —Режим доступу : http://www.president.gov.ua/docs/comment_api_final.pdf
47. Нашинець-Наумова А.Ю. Практикум з інформаційного права : навчально-методичний посібник / А.Ю. Нашинець-Наумова. — К. : Типографія «Планета», 2014. — 128 с.
48. Нашинець-Наумова А.Ю. Основи інформаційного права навчальний посібник / А.Ю. Нашинець-Наумова. — К. : Вив-во «Сталь», 2015. — 198 с.
49. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання : монографія / А.Ю. Нашинець-Наумова. — К. : Видавничий дім «Гельветика», 2017. — 169 с.
50. Нашинець-Наумова А.Ю. Інформаційна безпека суб'єктів господарювання: проблеми теорії та практики правозастосування : монографія / А.Ю. Нашинець-Наумова ; під заг. ред. д.ю.н. В.І. Курила. — Херсон : Видавничий дім «Гельветика», 2017. — 386 с.
51. Нашинець-Наумова А.Ю. Правове забезпечення інформаційної безпеки: міжнародний досвід і можливість використання // Право і суспільство. — Дніпро, 2018. — № 6. — С. 159–164.
52. Нашинець-Наумова А.Ю. Принципи забезпечення системи національної безпеки: конституційно-правовий аспект // Науковий вісник міжнародного гуманітарного університету: Збірник наукових праць. Серія: Юриспруденція. — Одеса, 2018. — № 35. — Т. 1. — С. 50–56.

53. Нашинець-Наумова А.Ю. До питання щодо боротьби з кібершпіонажем: вивчення та осмислення // Актуальні проблеми правознавства : зб. наук. праць. — Тернопіль, 2019. — Вип. 1 (17). — С. 126–132.
54. Нашинець-Наумова А.Ю. Світовий досвід законодавчої регламентації режимів конфіденційної інформації // Підприємництво, господарство і право. —Київ, 2019. — № 4. — С. 166–171.
55. Нашинець-Наумова А.Ю. Протидія комп'ютерній злочинності в кібернетичному просторі // Вісник кримінологічної асоціації України : зб. наук. праць. — Харків, 2019. — № 1(20). — С. 108–117.
56. Сучасні правові стандарти Європейського Союзу у сфері захисту персональних даних. Збірник документів; [неофіційний пер. з англ. І. Майстренко; за ред. В. Брижко; передмова В. Пилипчука]. (Науково-дослідний інститут інформатики і права Національної академії правових наук України). — К. : ТОВ «Видавничий дім» АртЕк», 2018. — 180 с.
57. Цимбалюк В.С. Основи інформаційного права України: навч. посіб. / В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін; за ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. — К. : Знання, 2004. — 274 с.
58. Ткачук Т.Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. — К. : ТОВ «Видавничий дім «АртЕк», 2018. — 411 с.
59. Цимбалюк В.С. Основи інформаційного права України : навч. посіб. / В.С. Цимбалюк, В.Д. Гавловський, В.В. Гриценко та ін; за ред. М.Я. Швеця, Р.А. Калюжного та П.В. Мельника. — К : Знання, 2004. — 274 с.
60. Юдін О.К. Інформаційна безпека держави : навч. посібник / О.К. Юдін, В.М. Богуш. — Х. : Консул, 2013. — 576 с.
61. Юридична відповідальність за правопорушення в інформаційній сфері та основи інформаційної деліктології : монографія / І.В. Арістова, О.А. Баранов, О.П. Дзьобань та ін.; за заг. ред. проф. К.І. Бєлякова. — Київ : КВІЦ, 2019. — 344 с.

Навчальне видання

НАШИНЕЦЬ-НАУМОВА Анфіса Юріївна

ІНФОРМАЦІЙНЕ ПРАВО

Навчальний посібник

За зміст і якість поданих матеріалів відповідає автор

Науково-методичний центр видавничої діяльності
Київського університету імені Бориса Грінченка

Завідувач НМЦ видавничої діяльності *М.М. Прядко*
Відповідальна за випуск *А.М. Даниленко*
Над виданням працювали:
О.А. Марюхненко, Т.В. Нестерова, Н.І. Погорєлова

Підписано до друку 09.01.2020 р. Формат 60х84/16.
Ум. друк. арк. 7,9. Обл.-вид. арк. 7,06. Наклад 50 пр. Зам. № 9-152.

Київський університет імені Бориса Грінченка,
вул. Бульварно-Кудрявська, 18/2, м. Київ, 04053.
Свідоцтво суб'єкта видавничої справи ДК № 4013 від 17.03.2011 р.