Відповідно до ч. 1 ст. 553 ЦК України поручитель змушений здійснити зобов'язання замість основного боржника лише за умови, коли останній його не виконав або виконав неналежним чином. Проте також потрібно враховувати наявні юридичні факти, що можуть звільнити боржника і поручителя від відповідальності (неустойки). Цими юридичними факторами можуть виступати певні обставини, за яких боржник не міг об'єктивно виконати своє зобов'язання.

Ч. 2 ст. 553 ЦК України передбачає виконання зобов'язання частково або у повному обсязі. Порука у повному обсязі характеризується загальним обов'язком поручителя не тільки виконання самого зобов'язання, але й відшкодування збитків, завданих кредитору при порушенні зобов'язання (неустойки), при зазначенні цих умов в договорі. Часткова ж порука застосовується тоді, коли поручитель зобов'язується відшкодувати лише певну суму (частину) від усього боргу.

Отже, порука є одним з найефективніших способів забезпечення зобов'язань, що базується на обов'язку поручителя перед кредитором нести відповідальність за порушення боржником своїх зобов'язань.

Список використаних джерел

1. Науково-практичний коментар до статті 553 Цивільного кодексу України. URL: https://ips.ligazakon.net/document/view/KK000544 (дата звернення: 23.03.2020).

2. Домошенко С. Порука як засіб забезпечення виконання зобов'язань. URL: https://ips.ligazakon.net/document/DG060799 (дата звернення: 23.03.2020).

3. Майоренко М. Порука та гарантія: правові аспекти. URL: https://uteka.ua/ua/publication/commerce-12-xozyajstvennye-operacii-9-poruchitelstvo-i-garantiya-pravovye-aspekty (дата звернення: 23.03.2020).

4. Цивільний кодекс України: Закон України від 16.01.2003 р. № 435-IV. Дата оновлення: 13.02.2020. URL: https://zakon.rada.gov.ua/laws/show/435-15 (дата звернення: 23.03.2020).

Коконєва І.

студентка І курсу магістратури
юридичного факультету
Тернопільського національного
економічного університету
Науковий керівник: к.ю.н., доцент, доцент
кафедри безпеки, правоохоронної діяльності
та фінансових розслідувань ТНЕУ
Зайцева-Калаур І.В.

СИСТЕМНИЙ ПІДХІД ДО РОЗГЛЯДУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В нинішньому світі інформація стає все більш важливою цінністю, а провідною галуззю діяльності – індустрія отримання, обробки і захисту інформації, куди з кожним роком вкладають все більш значні капітали. Вже найближчим часом політичну й економічну роль окремих держав на світовій арені будуть визначати саме розвиток інформаційної сфери та рівень інформаційної безпеки.

Розгляд інформаційної безпеки з позиції системного підходу дозволяє виділити чотири групи інформаційно-технологічних небезпек для суспільства і держави, зумовлених досягненнями науково-технічного прогресу [1, с. 51].

До першої групи варто віднести інтенсивний розвиток нового вигляду зброї – інформаційної, що здатна ефективно впливати на інформаційно-технологічну інфраструктуру держави та психіку людей.

Друга група пов'язана з новим виглядом соціальних злочинів, який націлений на використання досягнень сучасних інформаційних технологій: комп'ютерне хуліганство (впровадження «вірусів»); незаконне копіювання технологічних рішень, махінації з

банківськими операціями та інше. Провідні дослідники в цій області вважають, що найбільш обіцяючим знаряддям злочину стає комп'ютер. За останні десять років електронні викрадення в економічній сфері у 20 разів перевищили збройні пограбування.

Третя група полягає в електронному контролі за життям, планами настроєм громадян, діяльністю політичних організацій, тотальному комп'ютерному контролі за населенням країни. Немалі масиви даних про здоров'я, соціальну активність, політичні думки, зв'язки, фінансові справи населення високі інформаційні технології дозволяють накопичувати, зберігати та використовувати.

Четверта група являє собою використання інформаційних технологій в політичній боротьбі. Однією з домінуючих тенденцій сучасного суспільного розвитку є зростання впливу засобів масової інформації на зміст та хід політичних процесів, функціонування механізму влади.

Крім того, слід наголосити на ще один важливий аспект інформаційної безпеки – захист комп'ютерної інформації від розкрадань. Останнім часом проглядається чітка тенденція до зростання загроз, які стосуються кількості спроб несанкціонованого втручання в роботу телекомунікаційних та інформаційних систем і несанкціонованого доступу до інформації, яка в них циркулює. З цього випливає, що існує реальна загроза національному інформаційному простору України та, якщо необхідні заходи не будуть прийняті, то у найближчому майбутньому це призведе до втрати державою контролю над частиною інформаційного простору та зробить неможливим забезпечення прав громадян у цій сфері.

Засобів несанкціонованого доступу до інформації є безліч, але жоден засіб захисту, окремо взятий не зможе гарантувати адекватну безпеку. Надійний захист допустимий тільки, якщо створений механізм комплексного забезпечення безпеки. Основні складові такого комплексу:

– нормативно-правові;

– технічні;

– організаційні засоби.

Нормативно-правові засоби захисту виділяються законодавчими актами держави, що суворо встановлюють правила використання, обробки та передачі інформації обмеженого доступу та встановлюють ступінь відповідальності у разі порушень цих правил.

У ст. 34 Конституції України розглядається право громадян України на інформацію, забезпечення інформаційних процесів [2].

Технічні засоби поділяються на апаратно-програмні та фізичні і включають в себе механічні, електричні, електромеханічні та електронні пристрої. Апаратні технічні засоби розташовують в обчислювальній техніці, в телекомунікаційній апаратурі чи в пристроях, що пов'язані з схожою апаратурою через стандартний інтерфейс. Програмні засоби - програмне забезпечення, що здійснює функції захисту інформації. Фізичні засоби реалізуються у вигляді автономних систем та пристроїв, які здійснюють функції загального захисту об'єктів, за допомогою яких обробляється інформація.

До організаційних засобів захисту належать організаційно-технічні та організаційно-правові, що використовуються в процесі створення та функціонування кожної структури. Інакше кажучи, тільки на основі нормативно-правової бази та за наявності апаратно-програмних засобів можливе ефективне керування в умовах широкого впровадження нових інформаційних технологій.

Щодо державної політики, то у сфері інформаційної безпеки – спрямована на накопичення та захист національних інформаційних ресурсів, розробку та впровадження сучасних безпечних інформаційних технологій, побудову захищеної національної інформаційної інфраструктури, формування і розвиток інформаційних стосунків тощо. Вона повинна реалізовуватись шляхом створення і забезпечення ефективного функціонування в Україні цілісної системи інформаційної безпеки, а також вдосконалення існуючої і розробки нової нормативно-правової бази, яка регулює відносини в сфері інформаційної безпеки, встановлює вимоги і правила провадження діяльності у цій сфері.

Головним завданням інформаційної безпеки за умов глобалізації світових інформаційних процесів є захист національних інтересів України. Держава має запропонувати адекватні реальній ситуації засоби, методи та інструменти оперативного реагування на інформаційні диверсії, поширення неправдивої інформації та упередження формування негативного іміджу України та її громадян, викривлення та тенденційного підбору фактів історичного минулого. У свою чергу зберігаючи національно-культурні та духовні цінності України необхідно забезпечити створення національного інформаційного продукту який би ідентифікував Україну і світовому інформаційному просторі утверджуючи таким чином активну позицію України у побудові інформаційного суспільства.

Важливим аспектом розбудови інформаційного суспільства є гарантування інформаційної безпеки окремого громадянина, його прав на конфіденційність та невтручання у приватне життя. Необхідно обмежити вплив органів держаної влади на інформаційні потоки, які використовує людина встановивши стандарт безпеки громадянина (заборона прослуховування, втручання і блокування інформаційних потоків, встановлення мінімального рівня інформаційно-фінансового забезпечення, який забороняється блокувати тощо).

Для вирішення цих всіх проблем, перш за все, необхідно: створити повнофункціональну інформаційну інфраструктуру держави та забезпечити захист її критичних елементів; підвищити рівень координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігти таким загрозам та забезпечити ліквідації їх наслідків, здійснити міжнародне співробітництво з цих питань; вдосконалити нормативно-правову базу щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері.

Список використаних джерел

1. Аспекти публічного управління : у 12 т. / ред. рада : Серьогін С. та ін. Основні складові інформаційної безпеки. Дніпропетровськ: Наук. журнал, 2019. Т. 5 63 с.

2. Конституція України : офіц. текст. Київ : КМ, 2013. 96 с.

Комарніцька А.
студентка III курсу
юридичного факультету
Тернопільського національного
економічного університету
Науковий керівник: к.ю.н., доцент
кафедри конституційного, адміністративного
та фінансового права ТНЕУ
Ментух Н.Ф.

ПОРІВНЯЛЬНА РЕКЛАМА ЯК ФОРМА НЕДОБРОСОВІСНОЇ КОНКУРЕНЦІЇ

Кожен суб’єкт господарювання зацікавлений у реалізації своєї продукції на ринку. Саме реклама є одним із найефективніших способів, що сприяють просуванню товарів та послуг шляхом створення впізнаваного бренду.

Враховуючи той факт, що конкуренція – необхідна умова для стабільного функціонування економіки, держава повинна докладати зусиль для того, щоб створити систему захисту суб’єктів господарювання та споживачів від недобросовісної конкуренції та посилити контроль за зловживанням у цій сфері. Зокрема, йде мова про порівняльну рекламу, яка досить часто використовується для того, щоб показати «кращу сторону» своїх товарів чи послуг у порівнянні з іншими. Некоректне порівняння може призвести до дискредитації конкурента та заподіяти йому значної матеріальної або моральної шкоди.