“Проблеми протидії правопорушенням в інформаційній сфері: інформаційні війни”: *матеріали науково-практичної конференції, м. Київ, 6 червня 2014 р., НТУУ “КПІ”*

6 червня 2014 року Науково-дослідним інститутом інформатики і права та Науково-дослідним інститутом правового забезпечення інноваційного розвитку Національної академії правових наук України спільно з Навчально-науковим центром інформаційного права та правових питань інформаційних технологій ФСП Національного технічного університету України “Київський політехнічний інститут” було проведено науково-практичну конференцію на тему: “Проблеми протидії правопорушенням в інформаційній сфері: “інформаційні війни”.

З вітальними словами до учасників конференції звернулися директор Науково-дослідного інституту інформатики і права НАПрН України, член-кореспондент НАПрН України Володимир Пилипчук та проректор з науково-педагогічної роботи Національного технічного університету України “Київський політехнічний інститут” Олексій Новіков.

У ході конференції було розглянуто низку актуальних проблем забезпечення інформаційної безпеки та протидії правопорушенням в інформаційній сфері в умовах інформаційної війни. Учасники конференції охопили широке коло питань щодо вказаної проблематики, починаючи від дефініцій термінології, теоретико-правового аналізу, визначення форм та методів проведення інформаційного протиборства до аналізу інформаційної війни як фактора сучасної глобальної політики, а також концептуальні підходи протидії правопорушенням у національному та міжнародному праві. Особливе місце в ході обговорення було відведено соціологічним аспектам дослідження феномену інформаційної війни та правовим гарантіям захищеності людини в процесі інформаційного протиборства. Були запропоновані методики виявлення та аналізу інформаційних операцій і правового моделювання як універсальних засобів попередження та протидії інформаційним війнам.

У конференції взяли участь фахівці з інформаційної безпеки центральних органів виконавчої, правоохоронних органів і військових формувань України, вчені Національної академії наук України і Національної академії правових наук України, представники Національного технічного університету України “Київський політехнічний інститут” та інших вищих навчальних закладів. Активну участь у роботі конференції взяли співробітники Інституту: Ланде Д.В., Баранов О.О., Красноступ Г.М., Бєляков К.І., Савінова Н.А.

Підсумки конференції підвели директор Науково-дослідного інституту інформатики і права НАПрН України, член-кореспондент НАПрН України Володимир Пилипчук та в.о. декана факультету соціології і права НТУУ “КПІ” Анатолій Мельниченко.

Під час підведення підсумків було запропоновано провести окремий семінар серед науковців і фахівці в інформаційній сфері щодо узгодження теоретико-методологічних основ і подальшого вдосконалення правового регулювання відносин в контексті сучасних інформаційних війн.

За результатами конференції було прийняте відповідне рішення.

Т е з и в и с т у п і в.

ІНФОРМАЦІЙНІ ВІЙНИ: ТЕОРЕТИКО-ПРАВОВИЙ АНАЛІЗ

Бєляков К.І., *доктор юридичних наук, професор*

Події, що відбуваються в Україні останнім часом, призвели до загострення політичного та економічного стану країни. На фоні загострення соціальних стосунків, проявів сепаратизму та військових дій гостро відчувається психологічний тиск в інформаційному просторі, який супроводжується засобами масової інформації та соціальних мереж з боку Російської Федерації. Це явище здобуло умовне визначення – “інформаційна війна”, яке потребує ретельного, комплексного дослідження з позицій вивчення сутності, змісту та складу, визначення пов’язаних з ним категорій (“конфлікт”, “агресія”, “експансія” тощо), ролі та місця, його суб’єктів, аналізу

міжнародної практики правового регулювання соціальних відносин, що виникають в процесі негативного інформаційного впливу, проблем формування механізму правового регулювання та відповідних можливостей юридичної відповідальності за скоєння зазначених дій, пов’язаних з ним в чинному законодавстві України, шляхів його вдосконалення, технологічних засобів їх проведення, шляхів і заходів їх попередження та протидії тощо.

Перш за все, необхідно визначити термінологічно-понятійний зміст цього явища, щоб зрозуміти про що йдеться.

В Інтернеті (див. “Вікіпедія”): “Війна – конфлікт між політичними утвореннями – державами, племенами, політичними угрупованнями та ін., що відбувається в формі збройного протиборства, військових (бойових) дій між їх збройними силами”.

Як правило, війна має на меті нав’язування опоненту своєї волі. Один суб’єкт політики намагається змінити поводження іншого, примусити його відмовитися від своєї свободи, ідеології, від прав на власність, віддати ресурси: територію, акваторію й ін.

По формулюванню класиків, “війна є продовження політики іншими, насильницькими засобами”. Основним засобом досягнення цілей війни слугує організована озброєна боротьба як головний і вирішальний засіб, а також економічні, дипломатичні, ідеологічні, інформаційні та інші засоби боротьби. У цьому значенні війна – це організоване озброєне насильство, метою якого є досягнення політичних цілей. Головним засобом у війні є армія.

Інформаційна війна (у класичному її розумінні) – це одна з форм інформаційного протиборства, комплекс заходів щодо інформаційного впливу на масову свідомість для зміни поведінки людей і нав’язування їм цілей, що не відповідають їх інтересам, а також, природно, захист від подібних впливів.

Як відомо, інформаційна війна – це дії, розпочаті для досягнення інформаційної переваги шляхом завдання шкоди інформації та процесам, що базуються на інформації та інформаційних системах ворога при одночасному захисті власної інформації та процесів, що базуються на інформації та інформаційних системах. Основні методи інформаційної війни – блокування або перекручування інформаційних потоків і процесів, прийняття рішень супротивником.

Раніше вважалося, що інформація всього лише забезпечує поінформованість людей про події й факти в навколишньому світі. Інформація сприймалася як корисний ресурс, призначений для розширення людських можливостей. У сучасних умовах інформаційна війна розглядається військовими теоретиками як якісно новий вид бойових дій, активна протидія в інформаційному просторі, а інформація при цьому – як потенційна зброя та зручна ціль. Інформаційна війна розглядає інформацію як окремий об’єкт або зброю, що не завдає фізичної шкоди але може призвести до війни реальної. Інформаційна зброя, як правило, не спрямована на досягнення втрат у живій силі супротивника. Вона не знищує фізично й не руйнує людські, матеріально-технічні та інші ресурси, а підриває основи дії механізмів організації та управління.

Війни в інформаційному середовищі в сучасній науці та військових доктринах, на відміну від журналістської практики, зазвичай прийнято називати інформаційними операціями, наголошуючи, що вони є лише елементами “реальних” багатоаспектних протистоянь. Інформаційні операції є компонентами та супроводом більш загальних процесів. Ареною інформаційних операцій є інформаційний простір.

Основна задача інформаційних операцій полягає в маніпулюванні масовою свідомістю з такими цілями, як, наприклад:

– внесення в суспільну свідомість і свідомість окремих людей певних ідей та поглядів;

– дезорієнтація людей та їх дезінформація;

– ослаблення визначених переконань людей, основ суспільства;

– залякування мас.

Мабуть, немає потреби доводити, що інформаційні аспекти багатьох соціальних явищ винятково важливі для розуміння, проведення та протидії інформаційним операціям. Наприклад, важко уявити виборців, які голосують поза інформаційним контекстом виборчої кампанії або просування продукції без активного впливу на потенційних покупців.

Хоча поняття “інформаційні операції” явно не вживається в нормативних документах багатьох держав, включаючи Україну та Росію, однак такі операції повсюдно здійснюються для забезпечення політичних, економічних та інших інтересів урядів, політичних партій і політичних рухів, для реалізації влади та забезпечення національних інтересів як на території своїх, так і чужих держав. Серед потенційних загроз в інформаційній сфері в Законі України “Про основи національної безпеки України” (стаття 7) відзначаються й ризики інформаційних впливів: “прагнення маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації”. У 2009 році Рада національної безпеки та оборони України схвалила проект Доктрини інформаційної безпеки України, яку введено в дію Указом Президента України. У цьому документі серед основних реальних і потенційних загроз інформаційній безпеці країни у внутрішньополітичній сфері названі “деструктивні інформаційні впливи, у тому числі із застосуванням спеціальних засобів, на індивідуальну, групову та суспільну свідомість”, а також “поширення суб’єктами інформаційної діяльності перекручувань, недостовірної та упередженої інформації”.

На підстави наданого можна зробити висновок про те, що словосполучення “інформаційна війна” є некоректним для вживання в науковому обігу та нормативно-правових актах. Соціальному явищу, що розглядається, відповідає дефініція “інформаційні впливи” – деструктивне маніпулювання суб’єктами інформаційної діяльності суспільною свідомістю шляхом поширення недостовірної, неповної або упередженої інформації із застосуванням спеціальних засобів, на індивідуальну, групову та суспільну свідомість, що відповідає чинному законодавству України.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~

ІНФОРМАЦІЙНА ВІЙНА – КОМПЛЕКС ІНФОРМАЦІЙНИХ ЗАГРОЗ

Скулиш Є.Д., *доктор юридичних наук, професор*
Довгань О.Д. *кандидат юридичних наук, с.н.с.*

Концентрованою реалізацією всього комплексу інформаційних загроз є інформаційна війна. Вона є узгодженою діяльністю з використання інформації як зброї для ведення бойових дій. Головним стратегічним національним ресурсом стає інформаційний простір, тобто інформація, мережева інфраструктура та інформаційні технології.

Інформаційна війна являє собою “мозаїку” різних форм, а не якусь одну певну форму. Серед великого різноманіття способів інформаційних впливів, які реалізуються в інформаційно-телекомунікаційних системах або через них, можна виділити такі: поширення спеціально підібраної інформації (дезінформації). Цей спосіб інформаційних впливів здійснюється у формі: розсилки e-mail (електронних листів); організації новинних груп; створення сайтів з елементами інтерактивної взаємодії їх відвідувачів (чати, оп-line-голосування); розміщення інформації на приватних за змістом веб-ресурсах (блоги, соціальні мережі), в електронних версіях періодичних видань і мережевого мовлення (трансляції передач радіо- і телестанцій) або в мультимедійних архівах, наприклад Youtube; заміна інформаційного змісту веб-сайтів, що полягає в підміні сторінок або їх окремих елементів у результаті проникнення до ресурсів сайту з порушенням процедур, встановлених власником сайту. Такі дії проводяться, в основному, у формі атак для привернення уваги до атакуючої сторони, а також так званих, семантичних атак, що полягають у проникненні до ресурсів веб-сайту і подальшому непомітному розміщенні на них свідомо хибної інформації; реєстрація в пошукових системах сайтів протилежного змісту за однаковими ключовими словами, а також перенаправлення (підміна) посилань на іншу адресу, що призводить до відкриття спеціально підготовлених протидіючою стороною сторінок; зниження ефективності функціонування структурних елементів ІТС, що реалізується шляхом масового розсилання на вузли мережі електронних листів (спаму), проведенням атаки типу “відмова в обслуговуванні”,
~~~~~~~~~~~~~~

впровадженням мережевих комп’ютерних вірусів; віддалене приховане управління ресурсом ІТС за відсутності правомірного доступу до нього. Форми прихованого управління визначаються умовою активізації засобу управління: за часом; за діями, які виконує операційна система; за ключовими повідомленнями; захист ресурсів в інформаційно-телекомунікаційних системах (ІТС) у формах динамічного захисту та захисту від контенту; комп’ютерна розвідка. Основними формами комп’ютерної розвідки є сканування, інвентаризація та розширення прав доступу до ресурсів ІТС.

Дослідниками у цій мозаїці виділяються: війна у сфері управління військами, розвідувально-інформаційна війна, електронна війна, психологічна війна, хакер-війна, економічна інформаційна війна, кібервійна. Набір можливих варіантів для впливу на об’єкт інформаційної війни залежить від власних можливостей нападаючої сторони, системи протидії об’єкта та в кінцевому підсумку, стратегічних завдань нападу.

Локальні війни й збройні конфлікти кінця XX – початку XXI століття свідчать про те, що боротьба в інформаційній сфері стає їх невід’ємною частиною. Зароджується система багаторівневих спеціальних інформаційних операцій і даний напрям реалізації силового тиску відкриває ще небачені раніше перспективи.

Це в свою чергу стимулює провідні країни світу робити помітний акцент на розвиток відповідних технологій, удосконалення доктринальної бази ведення інформаційно-психологічної війни. У зв’язку з глобальними змінами у сфері інформаційних технологій та комунікацій відбувається переформатування підходів до цієї сфери. Найбільш повно організаційні та технічні питання цього спрямування розроблено штабами армій блоку НАТО та відображено у Польових статутах. Ці, а також інші документи армій країн-членів НАТО мають спільну методологічну платформу ведення інформаційно-психологічних операцій (ІПсО) у мирний і у воєнний час. Концептуально ці погляди зведено до таких принципів:

а) командування має розглядати ІПсО як важливий самостійний інструмент впливу на особовий склад армії і населення противника і несе відповідальність за готовність відповідних підрозділів до їх ведення;

б) ІПсО проводяться на плановій основі, з використанням засобів пропаганди та методів психологічного впливу разом з іншими способами впливу на супротивника (з акціями економічного, політичного, спеціального характеру);

в) завдання ІПсО полягають у: відповідному впливі на населення; маскуванні планів дії своїх військ; організації рухів опору; впливі у потрібному напрямі на нейтральні країни; визначають його моральний стан, психолог може прогнозувати поведінку військ супротивника за різних обставин;

г) проведенню ІПсО має передувати: вивчення ідеології супротивника, його культури, релігії, настроїв, менталітету, сильних і слабких місць його морального духу, а також – використання спеціальних підрозділів у тилу супротивника для проведення акцій саботажу, диверсій, терору та “чорної” пропаганди.

Як показує практика, боротьба в інформаційній сфері стає невід’ємною частиною локальних війн і збройних конфліктів (кінець XX – початок XXI століття). Лише останні десять років минулого століття продемонстрували цей факт цілим рядом багаторівневих спеціальних інформаційних операцій: в умовах збройних конфліктів “Морський ангел”, 1991 р.; “Буря в пустелі», 1991-1992 рр.; “Відродження нації”, 1992 р.; “Грім у пустелі”, 1993 р.; “Об’єднаний щит”, 1995 р.; “Спільні зусилля”, 1996 р.; “Лис у пустелі”, 1998 р.; “Союзницька сила”, 1999 р. Нове тисячоліття продовжило цей трагічний перелік, що найбільш резонансно проявилось у “революціях” арабського світу та на Україні.

Наряду з посиленням негативного зовнішнього впливу на інформаційний простір України, зростанням потенційних і реальних інформаційних загроз, руйнівних можливостей інформаційної зброї, що загрожує національній безпеці України, недостатніми залишаються обсяги вироблення конкурентоспроможного національного інформаційного продукту.

Ефективна реалізація стратегічних пріоритетів та основних принципів і завдань державної політики у сфері інформаційної безпеки потребує вдосконалення правових та організаційних

механізмів управління інформаційною безпекою, його відповідного інтелектуально-кадрового і ресурсного забезпечення. Правові аспекти організації інформаційної безпеки мають стати обов’язковим компонентом майбутніх законів, концепцій, доктрин, стратегій і програм, у тому числі Закону України про кібернетичну безпеку України, Стратегії розвитку інформаційного простору України, Стратегії кібернетичної безпеки України, нової редакції Доктрини інформаційної безпеки України та ін., а також внесення змін до деяких законів України (“Про основи національної безпеки України”, “Про інформацію”, “Про захист інформації в інформаційно-комунікаційних системах”, “Про Службу безпеки України” та ін.). Ці компоненти в сукупності мають складати єдине ціле, правову основу безпекового супроводу інформаційних процесів.

Отже, в процесі вдосконалення стратегії національної безпеки України з урахуванням основних тенденцій розвитку інформаційного суспільства набуває особливого значення розробка актуальних проблем організації інформаційної безпеки держави, необхідності прискорення розробки та впровадження національних стандартів і технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, що має сприяти розвитку конструктивного співробітництва.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~

ДИСТАНЦІЙНА КОМУНІКАЦІЯ ЯК КЛЮЧОВИЙ ФАКТОР НЕБЕЗПЕК АГРЕСИВНОЇ ПРОПАГАНДИ

Савінова Н.А., *доктор юридичних наук, с.н.с.*

Сьогоденна наука і політика не мають морального права вдаватися у дискусії з приводу наявності чи відсутності інформаційних війн. Вони є, і ведуться у відношенні нашої країни. Сукупність інформаційних операцій об’єднаних однією спільною метою, по аналогії з триваючим злочином, являють собою єдине, системне, хоча і сегментарне спрямоване явище.

На жаль, до сьогодні догматичне застаріле сприйняття явища “війна” асоціюється виключно з мілітаристичною агресією. Реалії доводять помилковість таких тверджень. Цілеспрямовані інформаційні впливи на свідомість різних груп населення країн та інформаційно-комунікаційні технології (ІТС) сьогодні передують, або супроводжують мілітаристичні впливи, однак, жодним чином не є складовою останніх. Інформаційні і мілітаристичні операції поєднані лише спільним планом, однак їх здійснення не пов’язане одне з одним. Це свідчить про те, що інформаційні війни сьогодні є як складовою війн у цілому, так і самостійним способом здійсненням агресії – інформаційної, комунікативної, маніпулятивної.

Важливим є факт усвідомлення сучасною наукою і відображення сучасними політиками безпеки та правовою політикою того факту, що, по аналогії з ресурсами мілітаристичної агресії (людським та збройним потенціалом), сучасна інформаційна війна характеризується власними особливими ресурсами – ресурсами інформаційного суспільства: інформацією, ІТС та знаннями. Категорія “знання” не стосується суто технічних аспектів, а охоплює всі сфери креативного пошуку, спрямованого на ефективне застосування інформаційних та комунікаційно-техногенних ресурсів, а також всіх інших ресурсів життєдіяльності суспільства, що утворюють попередні шари розвитку людської цивілізації.

Оскільки поняття “війна” асоціюється з використанням зброї, корисно провести вірні паралелі між зброєю мілітаристичної війни та зброєю війни інформаційної.

Виходитимемо з того, що сама по собі традиційна для всіх попередніх часів існування людської цивілізації зброя, хоча і є джерелом підвищеної небезпеки, за умови її незастосування, являє собою засіб стримування агресії: задекларована наявність зброї стримує напад на власника такої. Утім, застосування її при мілітаристичній агресії є очевидним за наслідками такого застосування: фізичних знищень, руйнувань, смертей.
~~~~~~~~~~~~~

Що ж є зброєю інформаційної війни? Така “зброя” інша.

Інформаційна агресія здійснюється з використанням дистанційних комунікацій – технологічно забезпечених віддалених засобів здійснення спілкування, сьогодні фактично не обмежених у часі та відстані здійснення. Такі комунікації можуть спрямовуватися як на технологічні складові інформатизованих сфер життєдіяльності суспільства (інформаційну інфраструктуру, ризикові об’єкти, програмне забезпечення різного рівня тощо), так і на свідомість населення, його груп, особистостей.

Чи є саме дистанційна комунікація зброєю інформаційної війни? Відповідь однозначна: сьогодні – так. На що здатна дистанційна комунікація сьогодні, і чому саме дистанційна (серед іншого – опосередкована) комунікація, а не безпосередня, завдає шкоди суспільним інтересам?

Йдучи від зворотного, запропоную розглянути модель відчуття безпосередньої комунікації. Така комунікація супроводжується особливостями сприйняття опонента у діалозі усіма чуттями: дотиком, слухом, зором, смаком, нюхом. Будь-яка опосередкована комунікація позбавлена кількох з відчуттів, що отримуються органами чуття. При листуванні задіяний лише зір, при прослуховуванні аудіо – лише слух, при перегляді телевізійних програм – зір та слух.

Утім, свідомість людини здатна до “добудовування” відсутніх складових дистанційної (опосередкованої) комунікації повної картини безпосередньої комунікації. Такі прогалини заповнюються за рахунок свідомого і несвідомого, які у сукупності є досвідом людини.

Отже, стає очевидним, що вплив дистанційної комунікації, як технологічної сторони спілкування, забезпечує перцептивну сторону спілкування (сприйняття) за рахунок доповнення отриманої обмеженої інформації власним досвідом людини.

Однак власний досвід людини, яка живе у суспільстві, складається як з її персонального досвіду (побутового, ділового, сексуального тощо), а й з досвіду групи – спільноти, в якій вона перебуває, а також суспільства, у межах якого особа функціонує. Історично досвід спільноти та суспільства формувався за рахунок звичаїв, традицій, моралі, екологічних та біологічних факторів (фактори місцевості), а також з урахуванням соціально-політичних, правових та економічних факторів ареалу країни проживання людини (держави).

Значну роль у даному випадку відіграє історичний досвід. Спільна історія, територія, мова, правова, економічна і політична системи забезпечують наявність у населення механізмів відтворення у свідомості картин ретроспективного досвіду. Такий досвід забезпечує не лише своєрідне, історично нібито доведене, бачення “шаблонних” наслідків, а й екстраполяцію етимології історичних малюнків на реальність. Нав’язана радянською історією пропаганда “злочинів бандерівців” викликає у про радянські налаштованої частини населення відтворення ретроспективної картини світу, до якої вони не мають відношення. Проте, у разі спрямованих “вкидань інформації” на кшталт “бандерівці”, “УПА”, “націоналісти” тощо, у свідомості такої групи людей відбувається формування апріорі агресивних дій націонал-шовіністського характеру на заході України 40-х, 50-х років. Аналогічно діє включення до лексикону активації попереднього досвіду використання у лексиконі маніпуляторів слів “фашисти”, “нелюди” тощо.

Утім, дистанційні комунікації здатні впливати не лише на активацію, а й на саме формування досвіду сучасної людини. ЗМІ та Інтернет, які діють на відносно прогнозовану аудиторію, здатні формувати хибні групи ідентичностей. Вони можуть нав’язувати відповідній аудиторії або викривлені представлення реальності, або в цілому ментально чужу реальність, втягуючи аудиторію у самоідентифікацію із запрограмованими у відповідному продукті мовлення (трансляції, подання) ідентичностями. Так, наприклад, демонстрація на телебаченні патріотичних серіалів країни агресора може формувати у глядачів пасивне і схвальне сприйняття агресії у разі симпатії аудиторії до позитивних героїв або сценарне передбачених “благих цілей” агресії. Аналогічно, демонстрація кримінальних серіалів, де відтворюється свавілля правоохоронців, яке здійснюється нібито в інтересах суспільства, сприймається

аудиторією переважно схвально: симпатія до “хороших хлопців”, які захищають правопорядок будь-якою ціною.

До чого приводить таке сприйняття? Як вказувалося, відбувається переформатуванні ідентичності. Сприймаючи віртуальний продукт як відображення реальності, людина здатна до ідентифікації себе з групою позитивних героїв, або іншими членами суспільства, набувати якостей ментальності, правосвідомості, рівня культури, яке подається у сценарне запрограмованому продукті. При цьому, підсвідоме сприйняття кадрів (фотографій, текстів) насилля, жорстокості, або – навпаки, нездатністю захистити себе та своє оточення, стають складовою людського досвіду (умовно назвемо його “удаваний досвід”). Останній може бути активований безліччю розроблених знаннєво-креативними досягненнями у маніпулюванні свідомістю – починаючи від методик нейролінгвістичного програмування, закінчуючи зомбуванням. Це доводять реалії анексії Криму та нападу на східні регіони з боку Російської Федерації. Ці акти агресії, фактично, не зустріли опору з боку населення таких регіонів, і первинно (зокрема, це стосується Криму) були схвально сприйняті певною частиною населення як прихід “своїх”, “удаваний досвід”, нав’язаний телебаченням, сформував уявну систему ідентичностей населення окремих регіонів з населенням країни агресора. Хибність такої ідентичності стала проявлятися фактично одразу після анексії Криму. Утім, її каталізацією послугували продовжувані агресивні пропагандистські заходи телебачення країни-агресора, які полягали в трансляції перекрученої новинної інформації про події в Україні.

Практики агресивної інформаційної війни доводять, і це підтверджується відкритістю першоджерел, що сьогодні на державному рівні країнами, життєдіяльність яких безпосередньо пов’язана з реалізацією воєнних операцій, системно розробляються напрями інформаційних пригнічень спротиву, інформаційних впливів, маніпулювань свідомістю щодо населення окупованих країн. Таким напрямом, зокрема, у Російській Федерації, є так звана “символічна політика”, до роботи над якою залучені вчені у майже всіх сферах суспільних та гуманітарних наук. Так, проблемою формування внутрішньої і зовнішньої символічної політики займаються історики, соціологи, соціальні психологи, філософи, політологи, юристи і економісти. У закритих дослідженнях у ній беруть участь військові й фахівці у галузі безпеки. Реалізація такої політики покладається на сферу соціальних комунікацій.

Ідея символічної політики полягає у тому, що на базі формування досвіду ідентичностей у країні, на які планується здійснити інформаційну експансію, і, вірогідно, потенційно агресивний напад, утворюється поле позитивного очікування, сприйняття значною частиною регіону нападу агресії не як зла чи шкоди національним інтересам і суверенітету, а як блага, завдяки якому населення увійде до складу хибного, міфічного соціуму ідентичностей, якого насправді нема. Наша держава сьогодні не протистоїть таким заходам, хоча напрацювання механізмів необхідних протидій вітчизняна наука може надати. Для цього необхідні фахівці, експериментальне поле, фактичний досвід ведення попередніх інформаційних операцій щодо України протягом останніх понад десяти років.

Ці тези є лише постановкою проблеми, на основі якої автор намагалась продемонструвати небезпечність сучасного знаряддя інформаційних війн та послідовність його використання при реалізації інформаційних стратегій символічної політики країни агресора. Надшвидкий розвиток подій, пов’язаних з агресією Російської Федерації до України демонструє, що впливи на свідомість людини і безпосередній зв’язок є можливими для здійснення таких маніпуляцій, з метою реалізації стратегій інформаційних війн і мілітаристичних втручань.

З позицій оцінок інформаційної безпеки, кримінально-правової політики, кримінології, інформаційної віктимології та інформаційного права, сьогодні повною мірою зрозуміло, що для представників вітчизняної політики аморально продовжувати ігнорувати позицію вчених щодо оцінки загроз інформаційних війн проти України.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

ОРГАНІЗАЦІЙНО-ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ ІНФОРМАЦІЙНІЙ АГРЕСІЇ ІНОЗЕМНИХ ДЕРЖАВ

Красноступ Г.М., *кандидат юридичних наук, с.н.с.*

Одним з основних завдань держави на сучасному етапі суспільного розвитку є досягнення високого рівня захисту національних інтересів у інформаційній сфері. При цьому, ефективне вирішення цього завдання є можливим лише за умови дієвого організаційно-правового забезпечення інформаційної безпеки України і надання населенню та інститутам громадянського суспільства відповідних державних гарантій.

У наслідок помилок у регулюванні, в національному інформаційному просторі України спостерігається низка негативних явищ, які створюють загрози національній безпеці України.

За умов швидкого розвитку глобального інформаційного суспільства, широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки.

На сьогодні з боку Російської Федерації ведеться цілеспрямована інформаційна операція проти України. Зокрема, з метою маніпулювання суспільною свідомістю в Україні та за її межами через російські засоби масової інформації поширюється недостовірна, неповна та упереджена інформацію про Україну. Ключовими завданнями такої інформаційної операції є деморалізація населення України, особового складу Збройних Сил України, а також спонукання їх до державної зради й переходу на бік супротивної сторони, формування у громадян України та Росії викривленого бачення подій, що відбуваються, а не їх дійсних причин та наслідків.

Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому здійснюється запобігання нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Тому, слід виділити основні напрями реалізації державної інформаційної політики у сфері державної безпеки, якими є:

−забезпечення дієвого захисту інформаційного суверенітету України;

−активне залучення засобів масової інформації до боротьби з проявами корупції та іншими явищами, які загрожують національній безпеці України;

−недопущення будь-яких проявів цензури, інших дій, які перешкоджають провадженню журналістами професійної діяльності.

Відповідно до Закону України “Про Основні засади розвитку інформаційного суспільства в Україні на 2007 – 2015 роки” вирішення проблеми інформаційної безпеки має здійснюватися шляхом:

−створення повнофункціональної інформаційної інфраструктури держави та забезпечення захисту її критичних елементів;

−підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва з цих питань;

−вдосконалення нормативно-правової бази щодо забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп’ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

−розгортання та розвитку Національної системи конфіденційного зв’язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

Практична реалізація державної інформаційної політики за сучасних умов вимагає широкої психологічної кампанії щодо підтримки її головних положень у громадській думці, роз’яснень її соціальної спрямованості, доведення її обґрунтованості.

У березні 2014 року на території Автономної Республіки Крим, крім перебування військового контингенту Російської Федерації, здійснюється психологічний тиск з боку засобів масової інформації вказаної держави, що ведуть “інформаційну операцію” проти України, втягуючи і захоплюючи стратегічні об’єкти української телекомунікаційної інфраструктури, з метою поширення неправдивих відомостей про події, що дійсно відбуваються на півострові. Як зазначив головний редактор газети “Юридичний вісник України” Шаров. В. інформаційна війна триває і “жертв” у ній уже чимало.

За даними громадської організації “Інститут масової інформації” з початку російської окупації Криму зафіксовано щонайменше 62 випадки грубих порушень свободи слова. Мають місце численні перешкоджання професійній діяльності журналістів. При цьому, кількість таких порушень щоденно зростає. Як зазначив директор департаменту інформаційної політики Держкомтелерадіо України Червак Б.О., все це відбувається на тлі масованого і агресивного інформаційного наступу російської пропаганди, яка всупереч європейським стандартами у сфері засобів масової інформації, розпалює в Україні, зокрема в Криму міжнаціональну ворожнечу, закликає до повалення законної української влади, розчленування незалежної і соборної України.

Склалася ситуація, коли на території Російської Федерації он-лайн медіа ресурси України (теле- та радіоканали, а також різноманітні Інтернет-ЗМІ, що поширюють достовірну інформацію про події в Україні) заблоковані для користувачів зони Російської Федерації у зв`язку з тим, що інформація, яка надається, суперечать ідеології Кремля.

Для громадян Російської Федерації блокування медіа ресурсів, що висвітлюють правдиві новини з України, відбувається за IP-адресами, доменами, окремими сторінками. Новинні веб-сайти України було також заблоковано.

Також у мережі Інтернет майже відсутні українські російськомовні новинні канали. Це стосується майже всіх видів контенту. Наприклад, Україна представлена в мережі Інтернет приблизно 100 радіостанціями, з яких новинних немає. Інтернет-ресурси України, що надають час від часу новинну інформацію, як правило, видають її виключно на українській мові, що заздалегідь робить їх неприйнятними для російськомовних слухачів. У той же час у мережі Інтернет існує більш ніж 500 радіостанцій Російської Федерації, з яких біля 50 новинних, що цілодобово поширюють спотворену інформацію про ситуацію в Україні та в Криму.

Так, на думку відомого громадського діяча Червака Б.О., ми не використовуємо ще один потужний ресурс – закордонні ЗМІ, через які теж можна доносити світу правду про Україну. Нинішні українські керівники володіють англійською мовою, тому вони повинні скликати прес-конференції, “круглі столи” за участі іноземних представників ЗМІ, коментувати події в Україні. Якщо голоси українського прем’єра, депутатів почують на CNN, BBC, інших провідних каналах, це теж реальна протидія тій інформаційній інвазії, яка ведеться з боку Російської Федерації.

Російська пропаганда щодо України велася ще за часів Радянського Союзу. Коли Україна стала незалежною державою, вона оголосила свободу слова і плюралізму ЗМІ. Але виникли інші проблеми – власники допускали плюралізм, однаке їх канали виконували певні замовлення, тобто ми не формувався власний інформаційний простір, який би захищав інтереси української нації. Нині, коли країна опинилася у небезпеці, сталося диво. Ми стали свідками консолідації суспільства навколо захисту своєї держави, в тому числі в інформаційному просторі. Фонд Разумкова недавно провів соціологічне дослідження, за яким 97 % громадян України сказали, що це їх батьківщина, а 87 % вважають себе патріотами України.

Рішенням Ради національної безпеки і оборони України ”Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України” від 28.04.14 р., уведеним в дію Указом Президента України від 01.05.14 р. № 449, Кабінету Міністрів України, зокрема, передбачено:

– розробити і внести на розгляд Верховної Ради України законопроекти про внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав,

передбачивши, зокрема, визначення механізму протидії негативному інформаційно-психологічному впливу, в тому числі шляхом заборони ретрансляції телевізійних каналів, а також щодо запровадження для іноземних засобів масової інформації системи інформування та захисту журналістів, які працюють у місцях збройних конфліктів, вчинення терористичних актів, при ліквідації небезпечних злочинних груп;

– розробити за участю Національного інституту стратегічних досліджень, Служби безпеки України, представників громадянського суспільства та подати на розгляд РНБО проект Стратегії розвитку інформаційного простору України, в якому, зокрема, визначити мету, завдання, структуру та режим функціонування національної системи забезпечення інформаційної безпеки держави;

– розробити за участю Національного інституту стратегічних досліджень, Служби безпеки України, інших державних органів і науково-дослідних установ та подати на розгляд Ради національної безпеки і оборони України проект нової редакції Доктрини інформаційної безпеки України.

У зв’язку з цим, виникла необхідність у підготовці:

–проекту Закону України “Про внесення змін до деяких законів України щодо протидії інформаційній агресії іноземних держав”;

–проекту Указу Президента України “Про затвердження Стратегії розвитку інформаційного простору України”;

–проекту Указу Президента України “Про Доктрину інформаційної безпеки України”.

Для громадського обговорення вказані проекти нормативно-правових актів розміщено у рубриці “Законопроектна діяльність” офіційного веб-сайту Держкомтелерадіо України.

Тому, саме сьогодні кожен має унікальну можливість долучитися до підготовки вказаних нормативно-правових актів.

На часі підготовка та прийняття Закону України “Про засади інформаційної безпеки України”, яким буде визначено основні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства і держави в інформаційній сфері, та організації забезпечення інформаційної безпеки в умовах формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору.

28 травня 2014 р. у Верховній Раді України зареєстровано проект Закону України “Про засади інформаційної безпеки України” (реєстр. № 4949), внесений народними депутатами України Стойком І.М., Кузьмуком О.І., Сиротюком Ю.М.

Вказаним законопроектом передбачається визначити основні засади державної політики, спрямованої на захист життєво важливих інтересів людини і громадянина, суспільства і держави в інформаційній сфері, та організації забезпечення інформаційної безпеки в умовах формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору.

З цією метою проектом Закону України пропонується визначити: основні принципи забезпечення інформаційної безпеки України; життєво важливі інтереси України в інформаційній сфері; реальні та потенційні загрози інформаційній безпеці України; пріоритети державної політики у сфері інформаційної безпеки; основні напрями діяльності держави у сфері забезпечення інформаційної безпеки; об’єкти інформаційної безпеки і суб’єктів забезпечення інформаційної безпеки та їх основні функції; статус, порядок створення, засади діяльності та повноваження спеціально уповноваженого центрального органу виконавчої влади з питань інформаційної безпеки; питання координації і контролю за діяльністю суб’єктів забезпечення інформаційної безпеки; засади міжнародного співробітництва у сфері інформаційної безпеки; відповідальність за правопорушення в інформаційній сфері, а також прикінцеві положення.

Вважаємо, що за результатами розгляду у першому читанні зазначений законопроект може бути прийнятий за основу. На нашу думку, зазначене вище підлягає врахуванню під час законотворчої діяльності, що в подальшому сприятиме вдосконаленню інформаційного законодавства та відповідному забезпеченню державної інформаційної політики.

~~~~~~~~~~~~ * * * ~~~~~~~~~~~~
~~~~~~~~~~~~

ТЕХНОЛОГІЇ ВИЯВЛЕННЯ ОЗНАК ІНФОРМАЦІЙНОЇ ВІЙНИ В ПОТОКАХ ІНТЕРНЕТ-НОВИН

Панченко В., *кандидат технічних наук, с.н.с.*
Полевий В., *кандидат технічних наук, с.н.с.*

Новинний простір (множина інформаційних повідомлень інформаційних агентств, ЗМІ, Інтернет-видань, офіційних сайтів державних установ, Інтернет-ресурсів політичних, громадських та ін. організацій) є проекцією подій реального світу. Окрім відомостей про події реального світу, новинний простір містить повідомлення, спрямовані на маніпулювання суспільною свідомістю, аналітичні оцінки подій тощо. Оцінювання загроз національній безпеці здійснюється шляхом аналізу подій та прогнозування їх наслідків із використанням попереднього досвіду. Це дає підстави зробити припущення, що новинний простір як проекція подій містить індикатори загроз національній безпеці. Зокрема, заходи інформаційного впливу (інформаційні акції, операції, війни), які передбачають вплив інформації на масову, суспільну, індивідуальну свідомість, як правило, мають своє відображення в інформаційному просторі, представленому потоками новин. З огляду на динаміку та обсяги потоків новин, на сьогодні одним з ефективних шляхів виявлення ознак інформаційної війни є застосування технології контент-моніторингу. Найбільш ґрунтовні дослідження у цьому напрямку проводились д.т.н. Д. Ланде, яким за результатами ретроспективного аналізу потоків Інтернет-новин були виявлені певні закономірності проведення інформаційних операцій. Разом з тим, подальшого уточнення та удосконалення потребують методи оперативного аналізу потоків Інтернет-новин в інтересах виявлення ознак інформаційного впливу.

У 2006 році під час дослідження інформаційного відображення подій щодо блокування “місцевим населенням” у Феодосії спільних військових навчань Україна-НАТО “Сі Бриз-2006” авторами було сформовано перелік тем, які використовувались у вітчизняному інформаційному просторі з метою маніпулювання суспільною свідомістю: федералізм (сепаратизм), статус Криму, Чорноморський флот РФ, міжконфесійна ворожнеча, міжнаціональна ворожнеча, расизм, статус російської мови, масові протести, військово-політичне співробітництво України з НАТО, інтеграція в ЄС, утиски демократії, протистояння гілок влади, неефективність правоохоронних органів, торгівля зброєю, енергозалежність України, фінансово-економічна криза, соціальна справедливість, меншовартість України. Такі теми ми назвали “критичними”, оскільки вони викликають резонанс, і є предметом постійних дискусій та конфліктів в українському суспільстві. Виявилось, що на фоні “феодосійського конфлікту” в інформаційному просторі були збурені теми федералізму (сепаратизму), статусу Криму, підстав для перебування Чорноморського флоту РФ на території Криму, статусу російської мови. За результатами проведеного тоді дослідження було доведено, що з боку РФ проводилася спеціальна інформаційна операція, стратегічною метою якої був подальший розкол України за мовно-етнічною ознакою.

Метою даного дослідження є пошук додаткових параметрів контент-моніторингу, які можуть бути використані з метою виявлення ознак інформаційної війни. З цією метою нами вивчалася динаміка часових рядів, які характеризують зазначені вище “критичні” теми в умовах дій РФ щодо анексії Криму за період з 1 листопада 2013 року по 15 травня 2014 року; проводилась експериментальна перевірка гіпотези про доцільність застосування розроблених нами індикаторів маніпулятивності, впроваджених у системі контент-моніторингу WisdomWell (http://wwell.com.ua), для виявлення ознак інформаційної війни.

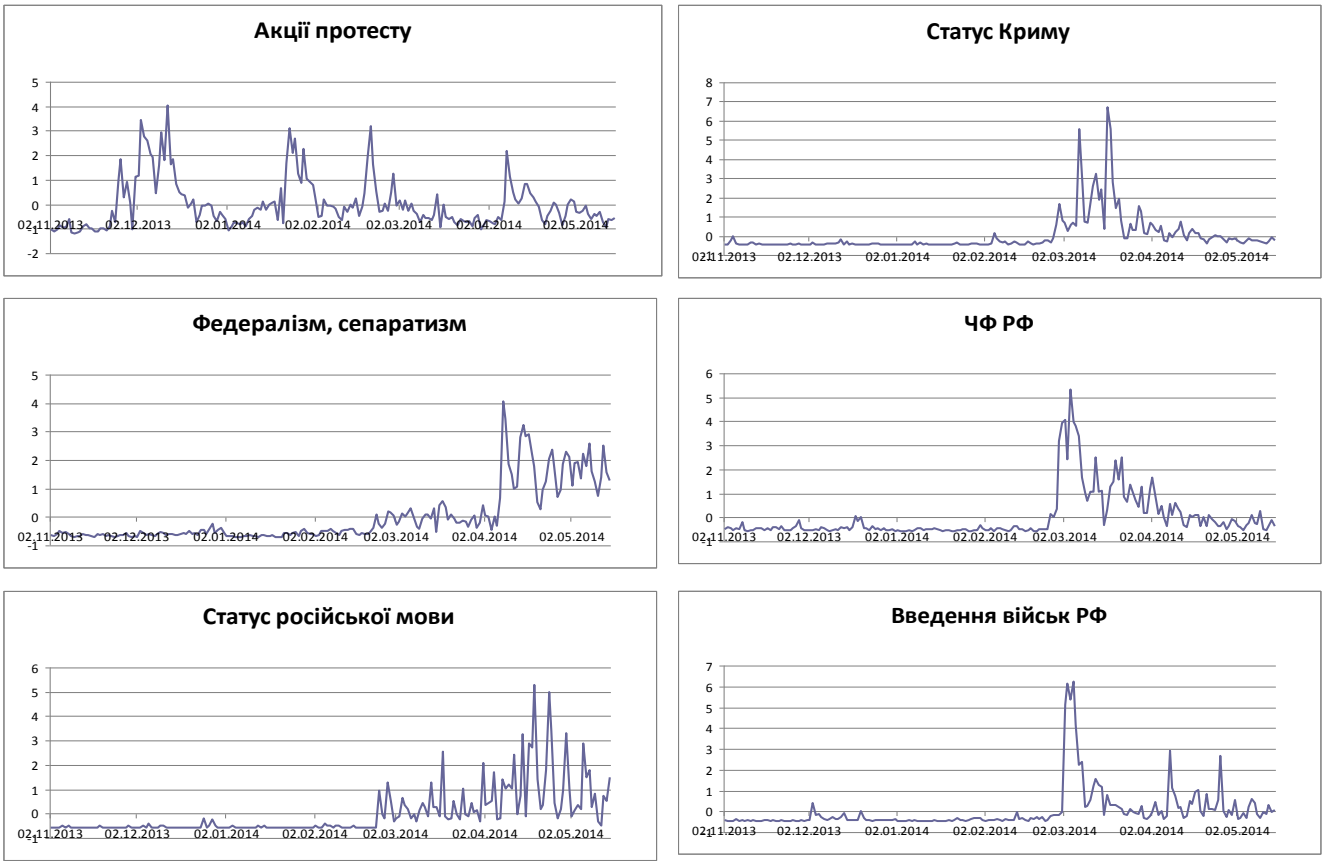
На рис. 1 відображено нормалізовані криві кількості повідомлень по заданих темах. Завдяки нормалізації відображено: 1) найбільш яскраві “сплески” тем, не характерні для їх звичайної активності в інформаційному просторі; 2) різні теми в одній шкалі, що надає можливість їх порівнювати.

Загалом графіки досить точно характеризують події, які відбулися, що свідчить про адекватність побудованих лінгвістичних фільтрів, за якими відбираються повідомлення

відповідно до заданих тем. Зокрема, на графіку “Акції протесту” бачимо Україну, охоплену протестами протягом півріччя, з основними збуреннями, які відповідають протестам 1 грудня 2013 року, подіям на Грушевського, розстрілу Майдану, захопленням адмінбудівель на Донеччині та Луганщині. У травні 2014 року акції протесту трансформувалися в терористичні акти, про що свідчить “затухання” цієї кривої протягом кінця квітня-початку травня на фоні того, що тема “Федералізм, сепаратизм” зберігає свою активність.

Звертає на себе увагу той факт, що Закон України “Про засади державної мовної політики” скасовано 23 лютого 2014 року, 4 березня оголошено про ветування цього рішення, а найбільш бурхливе обговорення мовного питання, як свідчить аналіз кривої “Статус російської мови”, відбувається 19 квітня. Отже, має місце невідповідність реальних подій щодо проблеми визначення статусу російської мови їх інформаційному супроводженню. Форма зазначеної кривої (синусоїда із постійною амплітудою і періодом) свідчить про штучне роздмухування цієї теми в інформаційному просторі, тобто її знову використовують з метою маніпулювання.

Порівняння кривих, які відповідають темам “Статус Криму”, “ЧФ РФ”, “Введення військ РФ” дає підстави зробити висновок про їх корельованість. Такий же зв’язок було помічено під час аналізу подій 2006 року. Отже, дії РФ щодо анексії Криму є ретельно спланованою довготривалою спецопераційю, а не спонтанним рішенням.



© WisdomWell

Рис. 1. Динаміка “критичних” тем в умовах дій РФ щодо анексії Криму

З метою розробки індикаторів маніпулятивності авторами за результатами опрацювання низки наукових праць у сфері лінгвістики, психології, соціології, політології та безпекознавства було узагальнено певні ознаки інформаційної війни:

1. Поширення фейкових (неправдивих) новин.

2. Інформаційна ізоляція або запровадження цензури на інформацію, яка потрапляє до суб’єкта впливу; блокування каналів супротивника.

3. Подання інформації у форматі “жовтої преси”, а не інформування.

4. Першоджерелом інформації є відомі пропагандистські рупори супротивника: підконтрольні інформагенства, посадові особи (експерти, радники), “жовті” ЗМІ та Інтернет-сайти.

5. Невідповідність часу публікації повідомлень про подію реальним термінам її перебігу.

6. Дискредитація дій супротивника, використання синонімів з потрібним контекстом, формування: “війна” – “миротворча операція”, “блокада” – “ембарго”, “антитерористична операція” – “каральна операція”.

7. Провокування суспільно-політичної конфронтації (протиставлення жителів Західної України Східній, протиставлення Криму материковій Україні) та міжетнічних конфліктів;

8. Залякування, підтримання стану тривожності, нагнітання ситуації шляхом поширення інформації про загрозу військового вторгнення, введення військ.

З цього переліку було виділено ті ознаки, які можуть бути описані лінгвістичними конструкціями та відображатися у потоках новин. Для виявлення таких ознак розроблено алгоритм, що ґрунтується на умовній ймовірності Байеса. Інтегральну характеристику, яка визначається для кожного повідомлення потоку новин за цим алгоритмом, ми назвали індикатором маніпулятивності.

На рис. 2 (який представлено на екрані) відображена динаміка часового ряду, що характеризує тему “Введення військ РФ” (побудовано за допомогою системи контент-моніторингу WisdomWell): загальна кількість повідомлень на цю тему, кількість повідомлень з ознаками маніпулювання, кількість повідомлень з негативним/позитивним контекстом. Повідомлення цієї теми, як правило, містять ознаки маніпулювання та негативний контекст, що свідчить про:

- адекватність запропонованих авторами індикаторів маніпулятивності;
- застосування з боку РФ однієї із технологій інформаційного впливу, що полягає у залякуванні, намаганні викликати почуття страху.

Висновки. Потоки Інтернет-новин є джерелом ознак інформаційної війни. Технології та засоби контент-моніторингу надають можливість одержувати з потоків Інтернет-новин метадані, які свідчать про проведення інформаційної війни. Зокрема, в процесі оперативного аналізу такими ознаками можуть бути:

- активізація “критичних” тем;
- поява повідомлень, що несуть контекст залякування, провокування суспільно-політичної конфронтації, спрямовані на дискредитацію супротивника;
- зростання кількості повідомлень з ознаками маніпулювання.

Виявлені за результатами контент-моніторингу ознаки інформаційної війни є основою для формулювання аналітичних висновків, спрямованих на прогнозування подальшого розвитку подій та організації оперативного реагування відповідних органів державної влади України.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~

СТРАТЕГІЧНІ ЦІЛІ ТА ЗАДАЧІ ІНФОРМАЦІЙНОЇ БОРОТЬБИ

Косогов О.М., *кандидат військових наук, с.н.с.*

Аналіз досліджень з військової тематики дозволяє зробити висновок, що у військовій справі настає новий етап розвитку: ефективність сучасних засобів ураження все більше визначається не стільки вогневою могутністю, скільки ступенем інформаційного забезпечення. Інформатизація збройних сил стала пріоритетною задачею військово-технічної політики економічно розвинених держав. У змісті військових дій все більше зростає значення інформаційного протиборства. Перевага у ступені поінформованості стає неодмінною умовою перемоги в війні, що переконливо доводить досвід збройних конфліктів і локальних війн сучасності.

Сучасні дослідники традиційно дотримуються гіпотези, що інформаційна війна ніким не оголошувалася і ніколи не припинялася, ведеться потай і не знає кордонів, ні в просторі, ні в часу. Інформаційна боротьба є об'єктивно існуючою тенденцією розвитку сучасного суспільства.
~~~~~~~~~~~~~~

А відповідно, форми і способи збройної боротьби призвели до появи таких нових наукових категорій, як “інформаційна боротьба”, “засоби інформаційної боротьби”, “інформаційна зброя”.

Вироблення замислу і прийняття організаційно-управлінських рішень у системах управління військами (силами) здійснюється на основі інформаційного зведення про поточну ситуацію і його співставлення з гіпотетичними або еталонними описами. В ергономічних системах, до яких відносяться автоматизовані системи управління (АСУ) військового призначення, це зведення включає в себе частини, що формалізуються і не формалізуються.

В обчислювальних системах частина, яка формалізується, представлена інформаційними ресурсами, компонентами яких є дані і знання. Знання представляються в декларативній або процедурній формах.

Процедурні знання визначають спосіб обробки даних і декларативних знань, направлених на вироблення обґрунтованих рішень. Вони втілені в конкретних програмних алгоритмах обробки інформації і управління, які дозволяють вирішувати задачі впливу на поведінку противника у двох напрямках.

1. Цілеспрямовано формувати дезінформацію таким чином, щоб примусити противника приймати бажані для дезінформатора рішення.

2. Впливати на функціонування систем управління противника з метою руйнування окремих частин програм, їхні модифікації, створення умов, що ускладнюють їхнє функціонування. Такий вплив може бути здійснений шляхом впливу існуючих програмних вірусів, логічних бомб тощо.

Це дозволяє сформулювати основний принцип боротьби на інформаційному рівні: цілеспрямований комплексний вплив на інформаційні ресурси противника. Останнє підтверджує правомірність прийнятої методології дослідження, що розглядає військово-інформаційну безпеку як складову інформаційної безпеки.

Такий методологічний підхід не суперечить сучасним досягненням кібернетики, що розглядають інформацію як зв'язок у будь-яких інформаційних системах, визначаючих їхню цілісність, тривалість і ефективність функціонування.

Загальною стратегічною метою інформаційної боротьби є забезпечення переваги у вирішенні задач, що ставляться, однією із сторін за рахунок досягнення переваги над протиборствуючою стороною на інформаційному рівні.

Частковими стратегічними цілями інформаційної боротьби є:

– формування інформаційного простору, який би забезпечував безпеку природи, людини, соціальної (національної) групи, суспільства від проявів різного роду факторів ризику;

– оптимізація взаємовідносин різних соціальних спільнот, створення єдиного безпечного інформаційного простору в Україні, Європі та світі;

– освіченість суспільства в галузі інформаційної безпеки;

– піклування про наявність достатніх і захищених інформаційних ресурсів і інформаційних потоків для підтримання життєдіяльності та життєздатності, стійкого функціонування і розвитку суспільства і держави;

– підтримка постійної готовності до адекватних дій в інформаційному протиборстві, ким би воно не було нав’язане.

Для досягнення стратегічних цілей вирішуються наступні стратегічні завдання:

– прогнозування можливих негативних інформаційних дій, спрямованих проти екології, людини, суспільства, держави;

– виявлення причинно-наслідкових зв’язків фактора ризику і наслідків реалізації для суспільства і держави;

– прогнозування основних напрямків розвитку інформатизації в цілях безпеки людини, суспільства; держави;

– визначення співвідношення інформаційної діяльності, інформатизації та безпеки людини, суспільства і держави;

– вироблення механізмів протидії інформаційним небезпекам і загрозам, негативним інформаційним діям на індивідуальну та суспільну свідомість та психику людини;

– забезпечення фізичної безпеки і сталого функціонування об’єктів інформаційних ресурсів;

– обмеження доступу до інформації, яка складає державну, воєнну, науково-технічну і комерційну таємницю.

Інформаційній боротьбі притаманні наступні основні закономірності:

– використання загальних, об'єктивно існуючих фізичних полів для інформаційного забезпечення функціонування систем і засобів озброєння і військової техніки;

– збільшення масштабів інформаційного зіткнення, систем управління і значного скорочення часу на проведення отримання, аналізу і розподілу інформації;

– зменшення вільних фрагментів частотного діапазону і збільшення його енергетичної завантаженості;

– одночасне використання великої кількості функціонально об’єднаних засобів, побудованих на різноманітних фізичних принципах;

– комплексне застосування різнорідних систем і засобів згідно єдиного замислу і плану в складі єдиної системи управління.

Висновки сучасних дослідників дозволяють очікувати в майбутньому збільшення кількості точок взаємного інформаційного впливу протиборствуючими сторонами; зростання обсягу змістовної інформації, зменшення часу на її обробку і темпу її поновлення; використання доступної для обох сторін інформації про окремі об’єкти (цілі), або їхньої великої сукупності, в якості вхідної при плануванні воєнних дій і реалізації задумів.

Досягнута однією із сторін інформаційна перевага може бути реалізована в часі оцінки стану сил протиборствуючих сторін, що випереджає і впливає на її інформаційні ресурси різноманітними засобами з метою ускладнити прийняття адекватного реальній обстановці рішення і управління військами (силами).

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~

ПРАВОВІ ГАРАНТІЇ ЗАХИЩЕНОСТІ ЛЮДИНИ В ПРОЦЕСІ ІНФОРМАЦІЙНОГО ПРОТИБОРСТВА

Тихоміров О.О., *кандидат юридичних наук*

Очевидно, що проблема гарантування у правовій сфері має глибокий комплексний характер. У контексті інформаційного протиборства, в якості юридичних гарантій, можна розглядати певну частину гарантій реалізації прав і свобод людини у процесі інформаційного обміну, поширення соціально значущої інформації, яка визначає прийняття людиною певних рішень. До них належить, загалом, виважене законодавство і спеціальні юридичні засоби й процедури, зокрема юридична відповідальність, правосуддя тощо. Проте ці гарантії стають реальними лише за умов наявності ідеологічного і культурного фундаменту правового життя суспільства, який забезпечує належне сприйняття і дієвість правових механізмів.

Для України наразі, з державницьких позицій, актуальним є захист індивідів, передусім, як громадян, оскільки в процесі наявних інформаційних впливів люди залишаються людьми зі своїми природними потребами та інтересами, але при цьому, як громадяни, змінюють свій світогляд та власні політичні уподобання, на основі чого корегують власну громадянську позицію. У залежності від спрямування і результативності інформаційних впливів вона, зокрема, може стати такою:

- активною державницькою (конструктивною, орієнтованою на захист держави, її розвиток і удосконалення);
- активною антидержавницькою (деструктивною до існуючого конституційного ладу);
- пасивно-спостерігальною (безучасною взагалі, або в тій чи іншій ситуації).

Превалювання двох останніх призводить до «втрати» державою частини своїх громадян, а в гіршому випадку і з частиною території, що виражається, передусім, через втрату
~~~~~~~~~~~~~

самоіндентифікації частини населення саме як громадян цієї держави. Про це можуть свідчити такі факти, як: невизнання конституційного ладу, територіальної цілісності, зневага до державної символіки, перешкоджання діяльності щодо забезпечення державної безпеки тощо. Вони не сумісні з конституційним статусом громадянина України і є, по суті, відмовою від своїх конституційних прав, свобод і обов’язків, тобто, де-факто відмовою від громадянства.

Для реалізації такого сценарію нема необхідності в деструктивному впливі на психіку індивіда з певними фатальними для нього як людської істоти наслідками. Достатньо дезорієнтувати людину в політико-правовому просторі, що зробить її громадянську позицію вразливою перед агітаційними впливами певного спрямування.

Саме те, що дозволить людині протистояти такому впливу, використавши наявні правові засоби, і є реальними фундаментальними правовими гарантіями її захищеності. Очевидно що вони ґрунтуються на тому компоненті свідомості людини, який відображає правову дійсність, тобто на правосвідомості.

Хоча в питаннях інформаційного захисту панацеї бути не може, зважаючи на індивідуальність кожної людини, але високий рівень правосвідомості і правової культури дає значні переваги щодо адекватного сприйняття ситуації у правовому вимірі (правової реальності) і певним чином дозволяє:

- оцінювати правову позицію і правові можливості суб’єктів інформаційного впливу;
- визначати правові перспективи їх пропозицій, ідей, закликів;
- прогнозувати правові наслідки реалізації намірів суб’єктів інформаційного впливу, зокрема їх оцінки на державному і міжнародному рівні.

Крім того маніпулювати правосвідомістю значно важче, оскільки вона ґрунтується на достатньо сталих у своїй основі формально-визначених правилах поведінки, традиціях, принципах, притаманних тій чи іншій правовій системі. Тим більше важко маніпулювати правосвідомість, якщо вона є активною, орієнтованою на самостійне ініціативне пізнання правової реальності.

Звичайно, формування правосвідомості і правової культури – це не першочергові заходи зі швидким ефектом, а далекоглядна, консолідована, щоденна, системна, кропітка діяльність, якою сьогодні в Україні не можна нехтувати, оскільки вона є рушійною силою механізмів реалізації прав, свобод та обов’язків людини і громадянина, забезпечення транспарентності й гуманізації владного апарату, підвищення ефективності правоохоронної та судової системи тощо.

Отже, розвиток правової освіти і правового виховання населення з метою підвищення рівня правосвідомості і правової культури має стати одним з пріоритетних напрямів закладення фундаменту майбутнього української державності.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~

ПРАВОВЕ МОДЕЛЮВАННЯ ЯК УНІВЕРСАЛЬНИЙ ЗАСІБ ПОПЕРЕДЖЕННЯ ТА ПРОТИДІЇ ІНФОРМАЦІЙНИМ ВІЙНАМ

Юдкова К.В., викладач кафедри інформаційного права та права інтелектуальної власності
Національного технічного університету України “КПІ”

Оцінюючи сучасний стан процесу забезпечення інформаційної безпеки як процес безперервного застосування заходів, що забезпечують відносну захищеність об’єктів, так і стан захищеності інформації, необхідно звернути увагу на ті способи і засоби, якими оперують суб’єкти інформаційної безпеки.

З-поміж числа існуючих заходів і методів необхідно розглянути метод інформаційного та соціально-правового моделювання.
~~~~~~~~~~~~~

Загрози інформаційній безпеці, як то: загрози “тріаді захисту” інформації, стану захищеності інформації. А також, суб’єктивізуючи об’єкти направленості таких загроз, можна виділити окремий об’єкт – свідомість як абстракція.

Під “тріадою захисту” інформації розуміється такий стан захищеності інформації, коли можливим є збереження її основних характеристик:

- конфіденційність – стан інформації, при якому доступ до неї здійснюють тільки суб'єкти, що мають на неї право;
- цілісність – уникнення несанкціонованої модифікації інформації;
- доступність – уникнення тимчасового або постійного приховування інформації від користувачів, що отримали права доступу.

Таким чином, інформаційні загрози, що посягають на вказаний вище стан руйнують (пошкоджують, змінюють первісний стан, унеможливлюють подальше розповсюдження/ використання за цілями призначення тощо) або безпосередньо саму інформацію, або організаційні зв’язки відносин, пов’язаних з оборотом, використанням, зберіганням, розповсюдженням інформації.

Сьогодні існує явище негативного впливу інформації, інформаційних ресурсів безпосередньо на свідомість об’єкта впливу. Такий вплив набув більшою мірою публіцистичного визначення – інформаційна війна. Іноді в певних джерелах можна зустріти термін “інформаційне протиборство” (information warfare) – суперництво соціальних систем в інформаційно-психологічній сфері з приводу впливу на ті чи інші сфери соціальних відносин і встановлення контролю над джерелами стратегічних ресурсів, у результаті якого одні учасники суперництва отримують переваги, необхідні їм для подальшого розвитку, а інші їх втрачають. Термін “information warfare” був запозичений із словообігу військових США.

Аналізуючи комплексний, синтетичний, міжгалузевий метод пізнання об’єктивної дійсності, необхідним є звернення до предметних досліджень різних галузей наук, таких як: політологія, політтехнології, психологія мас, полемологія. Жодна із галузей не містить дефініції поняття “інформаційна війна”, “інформаційне протиборство”. Таким чином, для цілей використання терміну в рамках дослідження методу правового моделювання прийнято рішення використовувати термінологічне позначення таких негативних впливів: деструктивний інформаційний вплив.

Визначаючи об’єкти деструктивного інформаційного впливу, можна погодитися із думкою спеціалістів Університету національної оборони США, що ними є:

- особа, власне людська свідомість;
- суспільство (як цілісний детермінований організм), самосвідомість на макрорівнях;
- держава.

Метод правового моделювання використовується найчастіше саме в тих випадках, коли проведення експериментів з реальними об’єктами є неможливим або потребує значних ресурсовитрат. Таким чином, метод правового моделювання залишається найбільш універсальним способом попередження та протидії деструктивному інформаційному впливу.

Результатом використання методу інформаційного та соціально-правового моделювання є побудова діючої моделі. Тип та загальна характеристика моделі залежить від набору ресурсів, використовуваних в процесі її побудови, а також цілей її побудови: мережеві моделі, індивідуум-орієнтовані моделі, експертні моделі тощо. Крім того, процес забезпечення інформаційної безпеки передбачає як структурне, так і функціональне моделювання.

Структурне моделювання доцільно використовувати при проектуванні та прогнозуванні складу і зв’язків між елементами системи та підсистем.

Функціональне моделювання – це процес моделювання функцій виконуваних об’єктом (інформаційної системою), шляхом створення описового структурованого графічного зображення, що демонструє предмет, спосіб і відповідального виконавця в рамках функціонування об’єкта та об’єктів, що зв’язують ці функції, з урахуванням наявної інформації.

Загальна правова модель інформаційної безпеки враховує як організаційно-правові способи захисту інформації, так і слугує платформою для визначення можливих негативних наслідків.

Поняття моделі інформаційної безпеки: кількісно-якісний опис можливого варіанту забезпечення її системи, з обов’язковим визначенням цілей, оцінкою рівня інформаційного імунітету (в залежності від типу ранжування), можливих загроз, а також розробкою правових механізмів захищеності об’єкта (інформаційної системи) та його здатності до самозахисту від цих загроз. Таким чином, використання моделі інформаційної безпеки забезпечує підтримку діяльності суб’єктів інформаційної безпеки в рамках превентивного підходу.

Фрагментарність нормативної бази, відсутність єдності поглядів спеціалістів щодо понятійно-категоріального апарату, створює всі умови для неможливості застосування комплексного підходу до забезпечення інформаційної безпеки. Рудиментарність законодавчих положень як національного, так і міжнародного права є достатнім обґрунтуванням розробки низки нормативно-правових та нормативних актів для врегулювання суспільних відносин у сфері інформаційної безпеки. У рамках вирішення вказаної проблеми доцільним є розробка Методики визначення загроз інформаційної безпеки, розрахунку рівня інформаційного імунітету на виконання Указу Президента України “Про доктрину інформаційної безпеки України”.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~

НЕОБХІДНІСТЬ ПРАВОВОГО РЕГУЛЮВАННЯ ВІДНОСИН У СФЕРІ ІНТЕРНЕТ

Адамюк Д.І., старший науковий співробітник НДІ правового забезпечення інноваційного розвитку НАПрНУ

Для правильної відповіді на питання про необхідність правового регулювання відносин у сфері Інтернет, насамперед, треба зосередити увагу на юридичній його природі. Інтернет, будучи всесвітньою комп’ютерною мережею, не є яким-небудь єдиним інститутом. У жодній країні світу не існує організаційної структури, що виступає як одноосібний власник даної комп’ютерної мережі.

Будь-який об’єкт як частина навколишнього світу існує самостійно, незалежно від наявності або відсутності діючих відносно нього правових норм. З іншого боку, об’єктами права можна вважати лише ті об'єкти, які окрім свого природного або культурного буття знаходять також і буття правове, тобто наділяються відповідним правовим статусом і підкорюються правовому впливу.

Відносно Інтернету неможливо виділити ознаки, що звичайно характеризують його як юридичну особу – він не має організаційної єдності, не інкорпорований у жодній з країн світу й не створений як міжнародна організація. Інтернет не має власного відособленого майна, тому що використовувані в ньому матеріальні й інформаційні ресурси належать на праві власності, володіння або користування різним суб’єктам. Не здатний Інтернет мати будь-які самостійні права й нести обов’язки, тому що за кожним виникаючим у роботі Інтернет правовідношенням пов’язаний конкретний правоздатний суб’єкт.

Таким чином, можна зробити висновок про те, що правові відносини породжує не Інтернет як комп’ютерна мережа, а самі суб’єкти, які цим або іншим способом пов’язані з цією мережею. Об’єктом регулювання є відносини операторів і користувачів Інтернету, як між собою, так і у відносинах з іншими особами й державними органами у зв’язку з передачею інформації й наданням послуг.

Слід додати, що на сьогодні будь-якого загальноприйнятого правового визначення поняття Інтернет відсутнє. В основному всі існуючі визначення пов’язані з його технічними характеристиками.

Інтернет у буквальному сенсі з англійської означає взаємопов’язану мережу. Дійсно Інтернет являє собою глобальну комп’ютерну мережу, що включає мільйони комп’ютерів по всьому світі. На нашу думку, Інтернет – це комплексний об’єкт правого регулювання, що
~~~~~~~~~~~~~

поєднує різноманітні суспільні відносини в єдину соціально-технічну систему, створену в процесі розвитку глобальної комп’ютерної мережі й призначеної для здійснення масової інформації й комунікації.

Спеціальні правові норми, що регулюють функціонування Інтернету, вже створюються у рамках національного права. Вони також повинні бути об’єктом уваги держав з гармонізації таких норм за допомогою міжнародних договорів та інших джерел міжнародного права.

Відсутність правових норм може служити ознакою, що вказують на необхідність урегулювання того або іншого питання міжнародно-правовими засобами. Проте сам по собі даний факт не може бути єдиним приводом для початку процесу розробки таких норм. Головним показником може служити лише правова анархія, що загрожує суспільним інтересам.

З іншого боку, будь-яка дія припускає наявність політичної волі, без якої яка-небудь ініціатива зі зближення правових систем приречена на невдачу. Приміром, даремно очікувати гармонізації правових систем відносно свободи вираження думок в Інтернеті через існуючі серйозні розбіжності в національних концепціях щодо цього питання.

Вибір засобів для гармонізації права досить широкий, приміром, це можуть бути прийняття як міжнародних договорів, так і розробка типових (модельних) законів. Практика прийняття типових (модельних) законів особливо добре підходить у сфері електронної торгівлі, зокрема, електронно-цифрового підпису, що вже було зроблено в рамках ЮНСІТРАЛ.

У доктрині також наявні думки прихильників створення для Інтернету власних специфічних методів регулювання, що опираються, при цьому, на ті об'єктивні особливості кіберпростору, які відрізняють його від реального фізичного простору.

Позитивною стороною такого підходу є те, що при ньому користувачі не повинні замислюватися, які національні законодавчі й інші нормативно-правові акти будуть застосовуватися до їхньої діяльності. Значення буде мати тільки перехід кордону кіберпростору. Причому, користувачі Інтернету не повинні одержувати ніяких переваг у порівнянні з аналогічною діяльністю в реальному фізичному світі тільки тому, що діяльність здійснюється у віртуальному світі – кіберпросторі.

Багато правових проблем, що виникають у зв'язку із використанням мережі Інтернет, можуть бути вирішені шляхом признання кіберпростору як особливого простору для цілей правового регулювання з використанням функціонального принципу.

Принцип територіальності створює багато проблем у глобальній інформаційній інфраструктурі, тому що законодавство держав, у яких може з’являтися одна і та сама інформація, може значно відрізнятися. Сприймаючи кіберпростір як окремий простір, можна не тільки розв'язати проблему колізії законів про юрисдикцію, але й розбудовувати нові доктрини, які враховували б особливі специфічні характеристики кіберпростору.

На даний момент Інтернет являє собою найцікавіший приклад того, наскільки вдало й ефективно може розбудовуватися настільки складна технічна система фактично за відсутності формального правого регулювання.

Нерегульовані правом соціальні відносини в мережі розбудовуються незалежно від спроб здійснити контроль над ними – нормативне регулювання відстає від життєвих реалій. Втім, така ситуація спостерігалася майже завжди – спочатку з'являлася економічна або соціальна основа для регулювання, а вже потім виникала потреба в регулюванні виниклих соціальних відносин, і, нарешті, з’являлися й регулюючі правові механізми.

У цей час дискусії ведуться не навколо того, чи повинні держави брати участь у регулюванні Інтернету, а про те, яким чином вони повинні бути залучені у цей процес.

Занадто жорстке регулювання з боку держави може змусити системних операторів та інших постачальників послуг у сфері всесвітньої мережі змінити своє місце знаходження, тим самим виключивши відповідні території з нової світової економічної системи інформаційного суспільства. У цій ситуації владні структури скоріше за все визнають, що в них не вистачає сил і можливостей контролювати всі сфери Інтернету, і, отже, нема необхідності регулювати ті операції, які не справляють істотного негативного впливу на суспільство.

Для ефективного функціонування такої схеми необхідний міцний зв'язок між державною

владою й Інтернет-співтовариством для того, щоб держава могла вчасно зрозуміти, коли і які дії в кіберпросторі створюють загрозу для громадян і держави.

З того, що Інтернет за своєю природою є всесвітнім феноменом, випливає, що процес гармонізації законодавства у відповідних сферах повинен проходити на всесвітньому рівні. Процесам гармонізації права у сфері Інтернет є і певний супротив. У якості аргументу супротивники використовують прагнення залишити мережу без міжнародного регулювання й зберегти її статус-кво. Прихильники саморегулювання відстоюють точку зору про те, що держава повинна залишити всі спроби врегулювати Інтернет. Крім того, вони заявляють про те, що на користь саморегуляції говорить технологічна природа об’єкта регулювання, його постійний розвиток і вдосконалювання. Крім того, ними наводяться аргументи про те, що тільки самі автори регулювання здатні оцінити ризики, що криються в тому або іншому рішенні, і що більш важливо, оцінити доцільність і ефективність санкцій.

Дійсно, саморегулювання – достатньо ефективний, і поки що майже єдиний спосіб регулювання відносин у глобальній мережі. Але ефективне саморегулювання припускає наявність певних правил, прийнятих на основі загальної згоди учасниками того або іншого співтовариства, соціальної групи, колективу. Механізми контролю над дотриманням таких правил також розробляються й застосовуються учасниками співтовариства без залучення яких-небудь методів впливу “ззовні”. Такі механізми, втім, можуть бути досить дієвими, стосовно порушників норм самоврядування.

Таким чином, необхідність правового регулювання відносин, які виникають при використанні глобальної мережі, стає неминучою. У цей час зароджується й формується Інтернет-право, що регулює суспільні відносини, які виникають під час обміну інформацією в глобальній мережі Інтернет, за допомогою публічно-правових і приватно-правових засобів, а усвідомлення державами обмеженості своїх можливостей у застосуванні національного права має призвести не до відмови від будь-якого регулювання у цій сфері, а, навпаки, до вироблення нових підходів, що враховують специфічну природу Інтернету.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~

ПРАВОВЕ РЕГУЛЮВАННЯ СУСПІЛЬНИХ ВІДНОСИН, ПОВ’ЯЗАНИХ ІЗ ВИКОРИСТАННЯМ МЕРЕЖІ ІНТЕРНЕТ

Битяк О.Ю., *кандидат юридичних наук, с.н.с.*

Для вирішення питань правового регулювання відносин, пов’язаних із використанням Інтернету, необхідно розглянути зміст та особливості тих суспільних відносин, які виникають, розвиваються та припиняються у зв’язку із застосуванням послуг мережі Інтернет. Слід звернути увагу, що правові відносини, які виникають у цій сфері, регулюються як нормами публічного, так і нормами приватного права, тобто нормами різних галузей права.

У Законі України “Про телекомунікації” дано визначення поняття Інтернету – це всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами. Закон визначає засади захисту прав споживачів та контролю за ринком телекомунікацій з боку держави. Однак його метою є не лише контроль владних структур за ринком комунікацій, а й забезпечення надання споживачам телекомунікаційних послуг достатнього асортименту, обсягу та якості шляхом обмеженого регулювання ринкових відносин для сприяння ефективному функціонуванню відкритого і справедливого конкурентного ринку, захисту прав споживачів.

Слід зазначити важливість визначення системи тих правовідносин стосовно використання мережі Інтернет, які можуть визначатися, як вбачається, на державному рівні та регулюватися національним законодавством. Це можуть бути відносини між державою і власниками (операторами) Інтернету, зокрема: регулювання державою, її органами, інформації, яка може бути надана в Інтернет; визначення інформації, яка не підлягає розголошенню; захист
~~~~~~~~~~~~~

інформації; фіскальні відносини при використанні електронної комерції; дотримання норм суспільної моралі; Інтернет як форма оповіщення суспільства про діяльність органів влади та ін.

Серед основних принципів діяльності у сфері телекомунікацій є: доступ споживачів до загальнодоступних телекомунікаційних послуг, які необхідні їм для задоволення власних потреб, участі в політичному, економічному та громадському житті; взаємодія та взаємопов’язаність телекомунікаційних мереж для забезпечення зв’язку між споживачами всіх рівнів; забезпечення сталості телекомунікаційних мереж і управління цими мережами з урахуванням їх технологічних особливостей на основі єдиних стандартів, норм та правил; державна підтримка розвитку вітчизняного виробництва технічних засобів телекомунікацій; впровадження світових досягнень у сфері телекомунікацій, залучення, використання вітчизняних та іноземних матеріальних і фінансових ресурсів, новітніх технологій, управлінського досвіду.

Органами управління у сфері телекомунікацій є Кабінет Міністрів України, центральний орган виконавчої влади в галузі зв’язку, інші органи відповідно до Закону України “Про телекомунікації”. Кабінет Міністрів України забезпечує проведення державної політики у сфері телекомунікацій, рівні умови розвитку всіх форм власності у сфері телекомунікацій, спрямовує і координує діяльність міністерств, інших центральних органів виконавчої влади у сфері телекомунікацій. Центральний орган виконавчої влади розробляє пропозиції щодо державної політики у сфері телекомунікацій і реалізує її у межах своїх повноважень; розробляє проекти законів, інших нормативно-правових актів; впроваджує технічну політику у сфері надання телекомунікаційних послуг, стандартизації, підтвердження відповідності стандартам технічних засобів телекомунікацій та інше.

Органом державного регулювання у сфері телекомунікацій є Національна комісія, що здійснює державне регулювання у сфері зв’язку та інформатизації, до повноважень якої відноситься: внесення пропозицій до органів державної влади щодо проектів законів та інших нормативно-правових актів, стандартів у сфері телекомунікацій; видання нормативних актів з питань, що належать до компетенції національної комісії, що здійснює державне регулювання у сфері зв’язку та інформатизації та контролює їх видання; забезпечення державного нагляду за додержанням суб'єктами ринку законодавства про телекомунікації; здійснення ліцензування та реєстрації у сфері надання телекомунікаційних послуг; встановлення Правил здійснення діяльності у сфері телекомунікацій та інші.

Умовами застосування технічних засобів телекомунікацій є їх відповідність стандартам і технічним регламентам. Технічні засоби телекомунікацій повинні мати виданий у встановленому законодавством порядку документ про підтвердження відповідності вимогам нормативних документів у сфері телекомунікацій.

Розвиток та вдосконалення телекомунікаційних мереж загального користування України здійснюється відповідно до Концепції розвитку телекомунікацій України із застосуванням новітніх технологій у сфері телекомунікацій, які відповідають міжнародним стандартам, з урахуванням технологічної цілісності всіх мереж та засобів телекомунікацій, підвищення ефективності та сталості функціонування. Головною метою Концепції розвитку телекомунікацій України є гармонійний та динамічний розвиток телекомунікаційних мереж на всій території країни, насамперед у регіонах з недостатнім рівнем насиченості місцевих мереж загального користування.

На думку автора, необхідно визначити рівень правових (законодавчих) актів (закони, укази Президента, постанови Кабінету Міністрів України, акти Центрального органу з питань телекомунікацій), якими можуть регулюватися певні відносини, пов’язані з використанням мережі Інтернет. Безумовно лише законами мають регулюватися всі відносини, пов’язані з правами і свободами людини, їх забезпеченням і охороною.

Актуальним залишається питання правового регулювання якості послуг, які надаються споживачам. Однією із головних проблем є визначення правового порядку встановлення технічних параметрів показників якості доступу до мережі Інтернет для кожного окремого споживача та правове регулювання процедур їх контролю.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

ДО ПИТАННЯ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ПРАВОВОГО МЕХАНІЗМУ ЗАХИСТУ ПРАВ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ У МЕРЕЖІ ІНТЕРНЕТ

Атаманова Ю.Є., *доктор юридичних наук, доцент*

Проблема захисту авторських прав у найбільш вираженій формі виявляється протягом останнього десятиріччя у сфері Інтернет, що зумовлено, перш за все, у простоті та швидкості розміщення інформації у всесвітній мережі, у відсутності необхідності обов’язкової авторизації при вчиненні таких дій, відкритості та доступності користування електронними ресурсами необмеженим фактично колом осіб. Такі переваги інформаційних технологій мають у той же час відповідно до принципу діалектичного розвитку й зворотній бік – у відкритому стані інформація та об’єкти права інтелектуальної власності потрапляють до мережі Інтернет без згоди й навіть поза межами обізнаності автора, чим порушуються не тільки права автора на отримання винагороди за свою інтелектуальну працю, а і його особисті немайнові права, перш за все, право вимагати визнання свого авторства шляхом зазначення належним чином власного імені на творі і його примірниках і за будь-якого публічного використання твору. Отже, при однозначній привабливості саме Інтернет-мережа стає віртуальним ринком обороту і збуту продукції із порушенням виключних прав авторів та інших правоволодільців.

Вітчизняне законодавство не визначає особливостей регулювання та захисту авторських прав у мережі Інтернет, факт чого стає підставою для поширення норм ст. 50 Закону України (далі – ЗУ) “Про авторське право і суміжні права” щодо встановлення тих дій, які визнаються порушенням авторського права та суміжних прав.

Питанням перспективних способів захисту від таких порушень стурбовані багато науковців, учених, юристів. Зокрема Т. Кудрицька і Ю. Чижова справедливо зазначають, що специфіка правового захисту прав полягає у тому, що об'єкти інтелектуальної власності використовуються в мережі, переважно, як вміст веб-сайтів і як розпізнавальна частина доменних імен. Так, якщо в доменних іменах використовуються торгові марки та фірмові найменування, меншою мірою – географічні позначення, то для наповнення веб-сайту може бути використано практично все, насамперед, літературні та художні твори, аудіовізуальні та музичні твори, фотографічні твори, бази даних, комп'ютерні програми.

Сьогодні до найбільш застосовних механізмів захисту прав інтелектуальної власності в мережі Інтернет належать: захист прав у судовому порядку, в адміністративно-правовому порядку, а також самозахист прав. Але досвід намагання отримати захист прав інтелектуальної власності, порушених у мережі Інтернет, у судових органах виявив такі проблеми, як відсутність належного законодавчого регулювання відносин, що складаються із застосуванням засобів електронного та цифрового зв’язку, на національному рівні; можливість доступу до мережі з будь-якого місця; складність визначення порушника, який дійсно вчинив порушення, та доведення його вини; неможливість представлення належних та допустимих доказів, що зумовлена електронною формою листування та укладеннях угод.

Ці та інші факти засвідчують необхідність проведення істотних змін у правовому механізмі захисту прав інтелектуальної власності, порушених у мережі Інтернет. По-перше, слід ставити питання про відповідальність власника веб-сайту за наявність матеріалів на ньому, які порушують права інтелектуальної власності, що належать іншій особі. Сьогодні її застосування за відсутності законодавчої підстави може базуватися на положеннях договору між провайдером та власником електронного ресурсу.

Такий підхід зараз сприйнятий і судовою практикою, за яким у зв’язку зі складністю встановлення безпосередньо винної особи за порушення авторських прав у мережі відповідає або споживач телекомунікаційних послуг, який поширив неправомірний контент, або власник веб-сайту, що є більш частим випадком. У п. 12 Постанови Пленуму Верховного Суду України “Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи” від 27.02.09 р. № 1, у якому зазначено, якщо автор поширеної інформації невідомий, а також коли інформація є анонімною і доступ до сайта – вільним, належним

відповідачем буде власник сайту, на якому розміщений інформаційний матеріал, оскільки саме він створив технологічну можливість та умови для поширення недостовірної інформації. Незважаючи на те, що зазначена правова позиція стосується практики розгляду справ про захист честі та гідності фізичної, а також ділової репутації фізичної та юридичної особи, дана концепція широко застосовується в справах про порушення авторських прав в Інтернеті.

Фактично за таких умов складається презумпція вини власника сайту, який створює умови для розміщення інформації на ньому, встановлює вимоги по завантаженню та безпосередньо контролює цей процес, що пропонується закріпити й на законодавчому рівні. Але вимога до нього має полягати лише щодо видалення інформації, що порушує права правовласника виключних прав. І лише у випадку його обізнаності у вчиненні такого порушення на належному йому сайті та неприйняття жодних заходів для його припинення, можна ставити питання про їх кваліфікацію як вчинення дій, що створюють загрозу порушення авторського права і (або) суміжних прав, що, зокрема, передбачено, підп. “д” ч. 1 ст. 50 ЗУ “Про авторське право і суміжні права”.

Другий рівень правового механізму захисту прав інтелектуальної власності, порушених у мережі Інтернет, стосується відповідальності провайдера. Слід відзначити, що у міжнародній практиці склався так званий “горизонтальний підхід” до відповідальності ISP-провайдерів, який полягає у тому, що такі суб’єкти несуть відповідальність тільки в тому випадку, якщо існує технічна можливість запобігти передачі матеріалу, що порушує виключні права інтелектуальної власності третіх осіб, провайдер знає про існування такого матеріалу, а також усвідомлює, що він є порушником прав, або мав можливість розуміти, що він порушує права.

Наступний – третій – рівень правового механізму захисту виключних прав на об’єкти інтелектуальної власності, порушених у мережі Інтернет, полягає у введенні “альтернативного підходу”, за яким відбувається видалення веб-сайту, зміст якого порушує виключні права інтелектуальної власності третіх осіб, або блокування доступу до нього шляхом звернення правоволодільця відповідно до пошукової системи або провайдера. Такий механізм запроваджений та функціонує, зокрема, у пошуковій системі Google, правда, небагато українських пересічних користувачів обізнаний про нього. А згідно з законом Франції щодо регулювання діяльності у файлообмінних мережах (закон HADOPI) активну участь у припиненні порушення авторських прав покладається на провайдера. У випадку, коли останній викрив користувача у скачуванні й розповсюджуванні захищеного авторським правом контенту, він направляє йому лист електронною поштою. Відсутність реагування порушника на таке попередження є підставою для направлення йому другого повідомлення рекомендованим листом. Якщо ці попередження не зупинили порушника, провайдер відключає йому Інтернет на тримісячний строк. Крім того його заносять у чорний список, і він не зможе змінити провайдера.

Таким чином, підвищення рівня дотримання виключних прав інтелектуальної власності в мережі Інтернеті вимагає побудови багаторівневого правого механізму гарантування їхнього дотримання та захисту з відповідним реагуванням як законодавства на такі вимоги часу, так і всіх учасників відносин, що виникають у віртуальному просторі, мінімум на локальному та договірному рівнях.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~

ТРЕНДОВІ ПРОПОЗИЦІЇ МІЖНАРОДНО-ПРАВОВОГО РЕГУЛЮВАННЯ ВІДНОСИН В МЕРЕЖІ ІНТЕРНЕТ

Ващенко А.В., старший лаборант
НДІ правового забезпечення інноваційного розвитку НАПрН України

У 2014 році міжнародне співтовариство святкує 25-ту річницю створення Інтернету. Зокрема, з привітального виступу 12 березня “батька-засновника” Інтернету Тімоті Джона Бернерса-Лібув закладений початок нового витка розвитку правового регулювання відносин в Інтернет-сфері: сер Бернерс-Лі запропонував створити і запровадити в дію Велику Хартію
~~~~~~~~~~~~~

Інтернету (anonlineMagnaCarta за назвою “TheGuardian”) або Білль про права користувачів мережі, який встановить веб-принципи відкритості, конфіденційності (англ. “privacy”) та нейтралітету – так би мовити, конституційні основи поведінки в Інтернеті. Джон Бернерс-Лі наголошує, що нові правила потрібні, щоб захистити “відкриту, нейтральну” систему. Так, принцип відкритості означає надання вільного, безперешкодного доступу до Інтернет, конфіденційності – збереження конфіденційної інформації, охоронюваної законом, під час розміщення та передачі контенту, а засада мережевого нейтралітету передбачає рівноцінне ставлення провайдерів до цільового призначення, класів додатків (програм) тощо.

Таку пропозицію від творця Інтернету варто вважати “зеленим світлом” для створення нової моделі правового регулювання відносин у мережі Інтернет та підвищенням рівня актуальності правових досліджень даної сфери. Ми підтримуємо заклик сера Бернерса-Лі та вважаємо за необхідне прийняти подібну Велику Хартію Інтернету як універсальний фундаментальний міжнародно-правовий акт.

Також слід відзначити у другому десятилітті XXI століття особливу суспільно-правову активність у напрямку нового розуміння прав людини, пов’язаних з Інтернетом. Зокрема, за останні роки низка міжнародних установ прийняли резолюції та інші акти з питань розвитку правового закріплення прав у сфері Інтернет. Так, 3 червня 2011 року ООН прийняла резолюцію, якою визнала доступ до Інтернету одним з базових, фундаментальних прав людини, вважаючи відключення певних регіонів від всесвітньої мережі з червня 2011 року порушенням прав людини. Хоча прийнята ця резолюція була, в тому числі, і з підстав політичного характеру, коли в Сирії було відключено доступ до Інтернету під час зіткнень між урядом та опозицією, прийняття цієї резолюції стало і важливим юридичним кроком.

Наступним кроком 5 липня 2012 року Рада ООН з прав людини на спеціальному засіданні 47 країн-членів прийняла резолюцію про право на свободу слова в Інтернет-мережі. Подала проект Швеція, а підтримали цей документ країни-союзники США, а також Куба та Китай, хоча вони перед голосуванням стримано коментували проект. Міністр закордонних справ Швеції Карл Більдт назвав голосування по резолюції “перемогою для Інтернету”: “Ми не можемо визнати, що зміст Інтернету повинен бути обмежений чи ним можна маніпулювати залежно від мінливих пристрастей політичних лідерів. Тільки шляхом забезпечення доступу до відкритої та глобальної мережі Інтернет буде здійснюватися справжній розвиток”.

Європейська правова система оновлює тлумачення свободи слова: 9 жовтня 2012 року була прийнята Резолюція ПАРЄ № 1877 (2012), направлена на захист свободи слова та інформації в Інтернеті. Зокрема, Парламентська Асамблея зазначила, що зараз свобода слова реалізується через ЗМІ, Інтернет, у тому числі он-лайн-ЗМІ та засоби мобільного зв’язку, отже, на всі ці сфери необхідно розповсюдити рівноцінний захист свободи слова. Також як вид обмеження свободи слова Асамблея засудила надто широке застосування законів про наклеп і образи, тероризм і національну безпеку, коли це обмежує право людей на розкриття інформації, що становить суспільний інтерес. У резолюції акцентується увага на можливих обмеженнях: будь-яка пропаганда війни і всякий виступ на користь національної, расової чи релігійної ненависті, що являє собою підбурювання до дискримінації, ворожнечі або насильства, повинні бути заборонені законом. Резолюція нагадує, що ст. 10 Європейської Конвенції зобов'язує органи державної влади не лише не обмежувати свободу слова та інформації, а й забезпечити, щоб приватний сектор не загрожував цій фундаментальній свободі. А зробити це можливо національними засобами захисту конституційних свобод людини і громадянина на вибір держави.

До того ж, судова практика міжнародних судових установ продовжує тенденцію розширення тлумачення питань свободи слова, свободи вираження думки, в тому числі в Інтернет-мережі. Зокрема, було винесено рішення Європейського суду з прав людини у справі “Ахмед Юлдірім проти Туреччини” (заява № 3111/10), яким визнано порушення ст. 10 Європейської Конвенції про захист прав людини та основоположних свобод (свобода вираження поглядів) у блокуванні сайту, що спричинило як побічний наслідок блокування доступу до всього домену і всіх сайтів, які мали на ньому хостинг. Також були зазначені цим рішенням пробіли національного законодавства: національне право не передбачає жодної гарантії для

запобігання тому, аби захід з блокування, спрямований на конкретний сайт, не використовувався як засіб загального блокування. Рішення містить аргументацію розширеного тлумачення свободи вираження поглядів, в тому числі поширюючи захист цієї статті на Інтернет-середовище та встановлюючи необхідність визнати право на безперешкодний доступ до Інтернету.

Таким чином, останнім часом пожвавилися спроби різних міжнародних установ врегулювати лише окремі, в основному публічно-правові, аспекти питання правового регулювання відносин у мережі Інтернет, виявлені в певних спорах, суспільно-політичних протистояннях тощо. З одного боку, це демонструє природний процес становлення правового регулювання, а з іншого – прогалини, недосконалість існуючого регулювання правом цього кола відносин.

На нашу думку, для гармонійного врегулювання Інтернет-відносин у світі необхідно чітко визначити певну сферу міжнародно-правового регулювання таких відносин, а інші достатньо вагомі повноваження віднести на розсуд парламентів та урядів держав. Зокрема, доцільно на міжнародному рівні визначити загальні, основоположні права, наприклад, особисті немайнові права на доступ до Інтернету як джерела інформації, так і середовища для вчинення юридичних фактів, право на вільне вираження поглядів в онлайн-мережі, а також межі втручання держави у здійснення таких прав, наприклад, обмеження, встановлені ст.ст. 10 та 15 Конвенції про захист прав людини та основоположних свобод, а також ч. 3 ст. 19 Міжнародного пакту про громадянські та політичні права. Також треба закріпити на рівні міжнародного права веб-принципи на зразок засад відкритості, нейтралітету та конфіденційності з обов’язковим чітким розкриттям змісту таких засад у розумінні міжнародної спільноти.

До компетенції національного законодавця доцільно відносити ширше коло, проте більш конкретних повноважень, наприклад, встановлення переліку складу кіберзлочинів (проступків), адміністративних, цивільних та інших правопорушень та санкцій за їх вчинення, інституційні повноваження по створенню та визначенню функціональної компетенції спеціалізованих наглядових органів у Інтернет-сфері, правове регулювання здійснення електронної комерційної діяльності та чіткі обмеження щодо розміщення контенту, забороненого законом, правові засоби гарантування доступу до мережі Інтернет тощо.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~

ОСОБЛИВОСТІ ПРАВОВОГО СТАТУСУ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ

Давидюк О.М., *кандидат юридичних наук*

Сучасний стан розвитку технологій призводить до бурхливого розвитку систем дистанційного обміну різноманітною інформацією. Особливості її правової природи вимагають створення адекватного правового регулювання правового статусу вказаного об’єкта дослідження, закріплення особливостей обігу та введення додаткових засобів захисту суб’єктивних прав її володільців.

Особливості правового статусу інформації в мережі Інтернет в Україні майже не визначені положеннями чинного законодавства. Так, Цивільний кодекс України, Закон України “Про інформацію”, визначають останню як – будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді.

Як вбачається із наведеного визначення, відомості які наведені в мережі Інтернет мають той же правовий статус, що і закріплені в інших джерелах – наприклад у друкованих засобах масової інформації. При цьому, чинне законодавство України жодним чином не враховує особливостей електронної форми, способів передачі, відкритості доступу, майже безмежних потенційних можливостей щодо копіювання, відтворення, розмноження такої інформації за допомогою сучасних засобів комп’ютерної техніки, не фіксує додаткових засобів захисту власників такої інформації, а існуючі механізми захисту взагалі не визначають відомості в електронному вигляді як належні та допустимі докази.
~~~~~~~~~~~~~

Аналогічна ситуація в українському законодавстві із поняттям самої системи Інтернет. Законом України “Про телекомунікації” та положеннями Постанови Кабінеті Міністрів України “Про затвердження Правил надання та отримання телекомунікаційних послуг” від 09.08.05 р. № 720 визначено, що система Інтернет – це всесвітня інформаційна система загального доступу, яка логічно зв'язана глобальним адресним простором та базується на Інтернет-протоколі, визначеному міжнародними стандартами. Чинними нормативно-правовими актами також надано тлумачення поняттю інформаційних систем загального доступу, як сукупності телекомунікаційних мереж та засобів для накопичення, обробки, зберігання та передавання даних. Іншими словами система Інтернет це сукупність телекомунікаційних мереж, засобів для накопичення, обробки, зберігання та передавання даних, ідентифікованих адресними (доменними) іменами, що встановлені міжнародними стандартами.

Таким чином, законодавець в Україні звів систему Інтернет лише до сукупності телекомунікаційних мереж, засобів обробки, збереження та передачі даних, практично ігноруючи при цьому цілий комплекс суспільних відносин, що нею опосередковані.

Вже із наведених понять випливає одне із найголовніших протиріч, що негативно відзначається на розвитку всіх інформаційних відносин в нашій державі. Мова йде про те, що поняття “інформація” розкривається через поняття “відомості” або через поняття “дані”, зміст яких чинним законодавством України не визначено. Таким чином, номінально поняття інформації в нашій країні є, але реальний його зміст визначити неможливо.

Проблематика правового статусу інформації, особливостей її передачі та розповсюдження активно розроблюється вченими протягом останнього часу. В багатьох наукових працях визначається та детально досліджується поняття системи Інтернет, правового статусу його користувачів, інших учасників суспільних відносин у сфері передачі інформації та/або відомостей та/або даних за допомогою телекомунікаційних засобів їх передачі, накопичення та обробки. Проте, при цьому жоден із авторів не пропонує конкретних шляхів вдосконалення правового регулювання всіх перелічених відносин.

На нашу думку, найбільш доцільним є прийняття окремого нормативно-правового документа на рівні не нижче Закону України, в якому слід закріпити цілий ряд додаткових визначальних понять, що в кінцевому своєму результаті допоможуть створити дієву систему захисту та приватноправового контролю учасників системи Інтернет за потоками інформації, яка нею переміщується. Оптимальною “робочою” назвою для такого нормативно-правового акта є Закон України “Про правовий статус телекомунікаційної мережі Інтернет в Україні”.

На нашу думку, даним документом необхідно закріпити:

- поняття відомостей та даних, що передаються вказаною мережею, тим самим деталізувавши поняття інформації;
- способи передачі шляхом відкритого розповсюдження та передачі конкретно індивідуалізованому споживачу;
- наслідки відкритого розповсюдження інформації, які пов’язати із правовим регулюванням об’єктів права інтелектуальної власності;
- наслідки передачі такої інформації від власника до індивідуалізованого споживача;
- поняття та правові наслідки транзитного розповсюдження інформації (“репосту”) користувачем, який не є її володільцем чи первісним джерелом розповсюдження;
- можливі форми договірної співпраці між фізичними особами, фізичними особами-підприємцями та юридичними особами, що будуть опосередковані через мережу Інтернет;
- правовий статус користувачів системи Інтернет, їх відповідальність за неправомірне використання телекомунікаційних джерел, правові наслідки зберігання, розповсюдження та подальшого використання інформації, відомостей, даних, отриманих за її допомогою;
- механізми захисту персональних даних користувачів отримуваних учасниками суспільних відносин, пов’язаних із використанням мережі Інтернет;
- відповідальність учасників відносин, опосередкованих мережею Інтернет, за несанкціоноване розповсюдження персональних даних користувачів цієї мережі;

- спеціальні додаткові механізми ідентифікації користувачів системи Інтернет із закріпленням додаткових зобов’язань для суб’єктів господарювання, що надають такі послуги, із їх додаткового захисту;

- всі інші питання, що виникають між учасниками відносин, опосередкованих мережею Інтернет.

Перераховані напрямки вдосконалення правового забезпечення функціонування мережі Інтернет в Україні є дискусійними. Будь-які дії в напрямку додаткової ідентифікації учасників відносин цієї системи сприймаються суспільством виключно як один із способів обмеження існуючих конституційних прав та свобод людини і громадянина, що гарантовані основним законом нашої держави. Через надзвичайно вразливу громадську реакцію на такого роду дії основоположним завданням законодавця при розробці відповідних заходів має стати закріплення оптимальної системи державного регулювання відносин, які виникають у ході збирання, розміщення, передачі та використання інформації в мережі Інтернет.

На нашу думку, зазначена мета може бути досягнута лише шляхом масштабного реформування вітчизняного законодавства, системи органів державної влади, процедурних та процесуальних способів і механізмів захисту прав і законних інтересів учасників суспільних відносин, опосередкованих мережею Інтернет, яке має бути проведене із врахуванням головного принципу – оптимальності поєднання персональної свободи користувача цієї мережі та дієвих засобів захисту інтересів держави і суспільства.

На наше переконання, тільки у разі досягнення зазначеної мети в нашій країні можна буде говорити про фіксацію правового статусу інформації в мережі Інтернет та забезпечувати її дієвий захист на належному і відповідному рівнях.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~

СТРУКТУРА ІНТЕРНЕТ-ПРАВОВІДНОСИН У КОНТЕКСТІ ВИЗНАЧЕННЯ П РАВОВОГО СТАТУСУ І РЕЖИМУ ЇЇ ЕЛЕМЕНТІВ

Єфремова К.В., *кандидат юридичних наук*

Для України проблема правового регулювання доступу та поширення інформації за допомогою мережі Інтернет є надзвичайно актуальною з огляду на процес визначення шляхів інтеграції до світового інформаційного суспільства.

Будь-яку інформацію, з якою користувач може ознайомитись у мережі Інтернет, прийнято називати “контент”, тобто будь-яке інформаційно змістовне наповнення інформаційного ресурсу. Таким чином, Інтернет-відносини виникають між власником контенту і користувачем інформації (споживачем) з приводу розміщення будь-якої інформації у глобальній мережі.

Суспільні відносини як відносини між людьми з приводу тих чи інших соціальних благ складаються з кількох елементів: суб'єктів, між якими складаються певні відносини (учасників відносин); об'єктів, тобто, тих соціальних благ, з приводу яких виникають суспільні відносини; і змісту відносин, тобто прав та обов’язків, які визначають поведінку конкретних людей, індивідів.

Щодо структури Інтернет-правовідносин, то крім класичних складових (суб’єкт, об’єкт і зміст) слід віднести й особливі притаманні лише цим відносинам елементи такі, як сама мережа Інтернет, завдяки якій суб’єкти і вступають у специфічні відносини щодо об’єкту у вигляді контенту, а також поведінка суб’єктів відносин (дія, бездіяльність) при користуванні мережею Інтернет та поза нею (наприклад, набуття виключних майнових прав на сайт/контент/IP-адресу/ доменне ім’я, купівля продаж інформаційних об’єктів, тиражування і поширення їх та інші дії).

Інтернет може займати двояке місце в структурі суспільних відносин: виступати засобом зв’язку суб’єктів або об’єктом суспільних відносин у випадку відносин, які складаються з приводу користування мережею Інтернет.

На думку М.С. Дашян, Інтернет не є фізичним об’єктом, що має матеріальні характеристики. Це самостійний діючий набір протоколів передачі даних (правила, які
~~~~~~~~~~~~~

наслідують комп’ютери і програми при обміні інформацією) прийнятий багатьма телекомунікаційними мережами.

Суб’єктний склад відносин, пов’язаних із використанням мережі Інтернет, доволі часто також виявляється складним. Це зумовлено тим, що користувач входить у мережу завдяки діяльності самостійної особи, що надає такі Інтернет-послуги – провайдера, доменне ім'я реєструється самостійною третьою особою – реєстратором, до того ж самостійним суб'єктом є і власник самої адреси сайту, який може не бути власником самого сайту.

Основними учасниками правовідносин, які виникають, змінюються та припиняються у зв’язку з функціонуванням мережі Інтернет, є: володільці інформації, розміщеної за допомогою мережі і власники інформаційних ресурсів в Інтернет, інформаційні посередники (провайдери), користувачі.

До специфіки структурних елементів Інтернет-відносин в частині суб'єкта можна віднести:

- складність ідентифікації учасників правовідносин у мережі;
- неможливість чіткого визначення дієздатності особи-учасника відносин;
- велика кількість наявних віртуальних організацій;
- використання програм-роботів, які надають можливість вступати у відносини автоматично;
- неможливість визначити місцезнаходження сторін (суб’єктів), що обумовлює можливі проблеми з вибором права, яке необхідно застосовувати, а також з реальним виконанням обов’язків;
- залежність відносин між безпосереднім власником інформації і її споживачем (користувачем) від відносин з провайдером Інтернет-послуг;
- електронний характер документообігу в мережі, що обумовлює необхідність застосування суб’єктами спеціального програмного і матеріально-технічного забезпечення.

Однією із прогалин законодавства сьогодення є відсутність обов’язку особи, яка має намір створити веб-сайт, надати свої персональні дані (як для фізичних, так і для юридичних осіб) для ідентифікації її як власника цього сайту. Звісно, що у мережі вже розроблений ряд заходів для ідентифікації таких осіб за допомогою сервісу “whois”, що використовується для направлення запитів з приводу отримання інформації про реєстрацію доменного імені до фактичного делегування веб-адреси клієнту, але це не вирішує проблему ідентифікації, тому що, як зазначалося раніше, власником доменного імені і власником інформації, розташованій на веб-сайті, можуть виступати різні особи.

Також слід звернути увагу на складність застосування територіальних критеріїв, яка полягає у тому, що суб’єкт, який здійснює комерційну діяльність в Інтернеті, може не мати ні торгового приміщення, ні офісу, ні складу, ні персоналу, і єдиними його ознаками, які зможуть виступати ідентифікаторами його територіальної належності, будуть адреси Інтернет-сайту та веб-сервера, що є ознаками провайдерів першого рівня: ua, ru тощо. Але можлива ситуація, коли певний веб-ресурс знаходиться у доменній зоні “ru”, що робить умовну прив’язку до території Російської Федерації, а сам сервер, що обслуговує цей ресурс, розташований в Україні, тим самим породжуючи проблему територіальної ідентифікації суб’єкта правовідносин.

Таким чином, Інтернет-правовідносини існують у віртуальному просторі, але залежні від наявних кордонів та особливостей національних законодавств суб’єктів таких відносин, від особливостей правового режиму доступу до інформації.

У процесі становлення і розвитку інформаційного суспільства залишаються нерозв’язаною низка питань щодо визначення правового статусу учасників Інтернет-відносин, одноманітних підходів до їх розуміння і практики вирішення спорів щодо них, визначення правового режиму об’єкту відносин – контенту, закріплення на законодавчому рівні змісту відносин, а саме прав, обов’язків і відповідальності суб’єктів і учасників, які виникають при створенні інформаційних об’єктів і під час їх обігу у мережі Інтернет.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

ЗАГАЛЬНА ХАРАКТЕРИСТИКА ВЕБ-САЙТУ ЯК ОБ’ЄКТА ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

Новиков Є.А., молодший науковий співробітник
НДІ правового забезпечення інноваційного розвитку НАПрН України

На сьогоднішній день майже кожна друга людина не може уявити свого життя без користування всесвітньою мережею Інтернет. Ні для кого не секрет, що “світова павутина” настільки завоювала прихильність людей у всіх країнах світу, не є винятком і українці. Вона стала одним з найголовніших засобів розповсюдження інформації науково-пізнавального, ділового, рекламного та розважального характеру. Кількість інформації, яка зберігається в мережі, є незліченною, адже щодня її стає все більше і більше, з’являється все більше сайтів, на яких вона розміщується. На ряду з цим виникає проблема захисту прав на досягнення власних творчих зусиль, набуває все більшої актуальності та необхідності її висвітлення для широких верств населення, і не лише для тих, хто наповнює мережу інформацією, а й для тих, хто нею користується. Наряду з цим виникає необхідність захисту такої інформації, зокрема від посягань тих користувачів мережі, які віддають перевагу не самостійному створенню сайтів та їх наповненню, а “позичанню” інформації з сайтів інших осіб. Користувачі “світової павутини” часто стикаються з певними проблемами, які виникають внаслідок того, що майже вся розміщена інформація підпадає під захист авторського права. До такої інформації відносяться новини, програмне забезпечення, оповідання, сценарії, графіки, картинки. Практично все в Інтернеті захищається, підпадає під захист законодавства про авторське право.

Інформація яка знаходиться в мережі Інтернет, розміщується на сторінках веб-сайтів. Веб-сайт – сукупність веб-сторінок, доступних у мережі Інтернет, які в свою чергу об’єднуються як за змістом, так і навігаційно. Сайт може розміщуватися як на одному, так і на кількох серверах. Законодавець не закріплює такого поняття як веб-сайт. Теж саме стосується визначення веб-сайта як об’єкта інтелектуальної власності в законах України, в сфері інтелектуальної власності та Цивільного кодексу України. Визначення веб-сайту можна зустріти тільки у Наказі Державного комітету інформаційної політики, телебачення і радіомовлення України, Державного комітету зв’язку та інформатизації України “Про затвердження Порядку інформаційного наповнення та технічного забезпечення Єдиного веб-порталу органів виконавчої влади та Порядку функціонування веб-сайтів органів виконавчої влади” від 25.11.02 р. № 327/225, згідно з яким: “веб-сайт – сукупність програмних та апаратних засобів з унікальною адресою у мережі Інтернет разом з інформаційними ресурсами, що перебувають у розпорядженні певного суб’єкта і забезпечують доступ юридичних та фізичних осіб до цих інформаційних ресурсів та інші інформаційні послуги через мережу Інтернет”. Серед науковців існує дві думки стосовно того як розглядати веб-сайт у сфері інтелектуальної власності. Перша точка зору полягає в тому, що веб-сайт розглядається як об’єкт інтелектуальної власності, в цілому як єдине ціле. Друга позиція базується на тому, що веб-сайт складається з елементів, які підлягають правовій охороні та їх реєстрації, як окремих об’єктів інтелектуальної власності (торговельних марок, об’єктів авторського права). Існує ще одна точка зору, яка заснована на тому, що сайт може бути об’єктом авторського права в цілому, однак як складений твір.

Якщо брати до уваги кожну з цих точок зору, необхідно відмітити, що усі складові елементи сайту успішно охороняються законодавством про інтелектуальну власність від будь-якого використання та несанкціонованого копіювання. Адже веб-сайт є поєднанням трьох об’єктів інтелектуальної власності: комп’ютерної програми, бази даних і промислового зразка.

Створення будь-якого сайту пов’язане з розробкою нового інтелектуального продукту. Кожен хто займається створенням такого продукту бажає захистити свої права на результат своєї роботи. Як правило одним з видів захисту об’єктів інтелектуальної власності є патентування (реєстрація винаходів, корисних моделей, промислових зразків, товарних знаків), яке вважається найбільш надійною формою охорони, однак головними мінусами даного способу захисту прав є тривала процедура реєстрації, додаткові матеріальні витрати і обмежений термін. Отже ця форма

повинна застосовуватися до тих об’єктів, які становлять основну цінність і втрата прав на які може реально відбитися на діяльності компанії. До таких об’єктів слід відносити доменні імена, логотипи, що реєструються як товарні знаки, а також основні ідеї з організації сайту, які реалізовані в програмному забезпеченні.

Якщо у користувача виникає бажання скопіювати інформацію, розміщену на веб-сайті, то для початку необхідно звернути увагу на повідомлення про авторське право, яке зазвичай розміщується на самій сторінці. Повідомлення повинно чітко вказувати на те, чи можна копіювати зі сторінки веб-сайту матеріал і вставляти його в інші документи, чи існує можливість завантажити матеріали з мережі, а також роздрукувати його. Існують такі випадки, коли повідомлення про авторське право відсутнє, або ж якщо операція з копіювання, яку ви збираєтесь здійснити, не передбачена повідомленням про авторське право, в цьому разі необхідно одержати спеціальний дозвіл. Для цього ви можете скористатися електронною поштою й відіслати запит розробнику Інтернет-сторінки, з тим питанням, яке цікавить вас.

Підводячи підсумки дослідження, слід зазначити про доволі низьке правове регулювання відносини у сфері Інтернету, зокрема в сфері інтелектуальної власності. Для подолання прогалин у законодавстві України необхідне створення системи підзаконних актів, які б регулювали конкретні сфери відносин. Також необхідно враховувати при розробці нормативної бази зарубіжний досвід тих країн, які досягли значних успіхів у даній сфері.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~

ДО ПИТАННЯ ПРАВОВОЇ ОХОРОНИ ДОМЕННИХ ІМЕН

Волощенко О.М., молодший науковий співробітник
лабораторії проблем правового забезпечення
реалізації інноваційних проектів НДІ ПЗІР

В результаті узагальнення існуючої судової практики стосовно спорів про незаконність реєстрації та використання доменного імені простежується тенденція, що саме доменні імена стають одними із спірних об’єктів, і такими, що посягають на незаконне використання торговельних марок, географічних зазначень та знаків для послуг.

На підтвердження попереднього твердження наведемо приклад з практики щодо розгляду судової справи на предмет вирішення спору з питань неправомірного використання прав на доменне ім’я. ТОВ “Одноклассники” звернулось до Арбітражного суду м. Москви з позовом до ТОВ “Видавництво “Ексмо”. Позовні вимоги було вмотивовано тим, що ТОВ “Видавництво “Ексмо” розмістило у вихідних даних своєї книги “Одноклassники” доменне ім’я позивача //www.odnoklassniki.ru. Однак, Федеральний арбітражний суд Московського округу відхилив доводи позивача про те, що //www.odnoklassniki.ru є засобом індивідуалізації, а також про те, що ТОВ “Одноклассники” володіє майновими правами на зареєстроване за ним в установленому порядку доменне ім’я //www.odnoklassniki.ru, вказавши, що ст. 1225 Цивільного кодексу Російської Федерації установлено вичерпний та такий, що не підлягає розширенню, перелік об'єктів інтелектуальної діяльності.

Слід зауважити і той факт, що перелік результатів інтелектуальної діяльності та засобів індивідуалізації, який вказано у зазначеній статті ЦК РФ, значно відрізняється від об’єктів, які відносяться до інтелектуальної власності відповідно до міжнародного права. Тобто, зазначене рішення викликає певного роду сумнів стосовно займаної позиції на предмет відповідності міжнародним стандартам сфери права інтелектуальної власності.

Характерно, що стосовно цього питання вітчизняна судова практика не займає таку жорстку позицію. Так, Постановою Пленуму Вищого Господарського суду України “Про деякі питання практики вирішення спорів, пов’язаних із захистом прав інтелектуальної власності” від 17.10.12 р. зазначено, що у вирішенні відповідних спорів про оспорювання правомірності розміщення на сайті об’єктів інтелектуальної власності тотожних іншим об’єктам, права на які
~~~~~~~~~~~~~~

належать іншим особам, суд повинен встановити, чи перебуває веб-сайт та розміщена на ньому інформація в розпорядженні особи, якій пред’явлено позовні вимоги, а також чим підтверджується факт порушення нею авторського права та/або суміжних прав. Дані щодо власника веб-сайту можуть бути витребувані відповідно до положень пункту 4 статті 65, статті 38 ГПК у адміністратора системи реєстрації та обліку доменних імен і адрес українського сегменту мережі Інтернет.

Така позиція вказує на доменне ім’я як на засіб індивідуалізації відповідного суб’єкта у віртуальному просторі, що допомагає відстежувати належність прав на той чи інший домен та полегшує процедуру ідентифікації правопорушників. Необхідно мати на увазі також, що публічний доступ до конфіденційних даних про фізичних осіб, що містяться в записах ідентифікатора власників домену, є закритим. Тому в разі необхідності доступу до таких даних позивач вправі звернутися до господарського суду з клопотанням про їх витребування відповідно до статті 38, пункту 4 статті 65 ГПК.

Зазначені тезиси стосовно закритого доступу до списків ідентифікатора власників доменних імен та спеціальної процедури доступу до таких даних дають зрозуміти позицію вітчизняної судової практики як такої, що схильна до визнання доменного імені як об’єкта інтелектуальної власності, що володіє рядом особливостей, становить цінність у доказовому матеріалі та потребує, відповідно, правової охорони.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~

DOS-АТАКА: ПРАВОВАЯ ЗАЩИТА ОТ ЦИФРОВОГО ВМЕШАТЕЛЬСТВА

Лымаренко С.А., курсант 5 курса ИПЮК для СБУ
НЮУ имени Ярослава Мудрого

Каждому из нас важно, чтобы доступ к необходимому сайту был беспрепятственным, а обработка запроса осуществлялась как можно быстрее. Максимально качественный результат за минимальное время – основное требование каждого пользователя. Но иногда возникают случаи, когда вполне простой запрос на доступ к сайту обрабатывается достаточно медленно, что в некотором смысле вызывает определенные неудобства. Тогда возникает вопрос, в чем причина, ведь скорость входящего и исходящего трафика высокая, а скорость обработки низкая. Возможно, в этом случае сайт подвержен DoS-атаке. Проанализируем понятие DoS-атаки и соответствующие методы защиты.

DoS-атака (атака типа “отказ в обслуживании”, от англ. Denial of Service) – атака на вычислительную систему (обычно совершенная хакерами) с целью довести её до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён. Если атака выполняется одновременно с большого числа компьютеров, говорят о DDoS-атаке (от англ. Distributed Denial of Service, распределённая атака типа “отказ в обслуживании”). Такая атака проводится в том случае, если требуется вызвать отказ в обслуживании хорошо защищенной крупной компании или правительственной организации. Первым делом злоумышленник сканирует крупную сеть с помощью специально подготовленных сценариев, которые выявляют потенциально слабые узлы. Выбранные узлы подвергаются нападению, и злоумышленник получает на них права администратора. На захваченные узлы устанавливаются троянские программы, которые работают в фоновом режиме. Теперь эти компьютеры называются компьютерами-зомби, их пользователи даже не подозревают, что являются потенциальными участниками DDoS-атаки. Далее злоумышленник отправляет определенные команды захваченным компьютерам и те, в свою очередь осуществляют мощную DoS-атаку на целевой компьютер. В некоторых случаях к фактической DDoS-атаке приводит непреднамеренное действие, например, размещение на популярном Интернет-ресурсе ссылки на сайт, размещённый на не очень производительном сервере (слэшдот-эффект). Большой наплыв
~~~~~~~~~~~~~

пользователей приводит к превышению допустимой нагрузки на сервер и, следовательно, отказу в обслуживании части из них.

Для защиты от сетевых атак применяется ряд фильтров, подключенных к интернет-каналу с большой пропускной способностью. Фильтры действуют таким образом, что последовательно анализируют проходящий трафик, выявляя нестандартную сетевую активность и ошибки. В число анализируемых шаблонов нестандартного трафика входят все известные на сегодняшний день методы атак, в том числе реализуемые и при помощи распределенных бот-сетей.

24 сентября 2013 года состоялась новая DDoS-атака мощностью 100 Гбит/с, которая продолжалась девять часов, сообщает компания Incapsula. При этом она не назвала URL сайта своего клиента, жертвы атаки.

Отличительная особенность указанной DDoS-атаки – атакующие вовсе не использовали резольверы. Получается, что это первая в истории атака подобной силы без умножения запросов, и что у кого-то из пользователей есть в наличии каналы суммарной пропускной способности 100 Гбит/с! Если бы они использовали умножение запросов, то могли бы увеличить трафик в десятки раз.

С технической точки зрения возможность борьбы с DoS-атаками существует и фактически используется. Недостаточно урегулированным остается вопрос о наступлении негативных правовых санкций для лиц, осуществляющих эти атаки.

Представляется возможным предложение на уровне закона наделить Интернет-провайдеров административными функциями, позволяющими при обнаружении DoS-атак, прекращать использование трафика, а также блокировать работу компьютеров-зомби. Для эффективной работы этих мероприятий необходима разработка технических норм и стандартов, позволяющих по ряду критериев определить наличие DoS-атаки и обосновать необходимость применения административных мер к нарушителям, с подробным описанием применяемых фильтров по защите от дальнейших негативных последствий и прочее.

Также необходим действительно быстрый механизм взаимодействия Интернет-провайдеров и органов государственной власти, поскольку в случае совершения атак времени для длительных бюрократических процедур нет. А вред, принесенный такими действиями, может достигать миллиардов долларов. В случае существенного нарушения необходимо зафиксировать сам факт такой DoS-атаки, поскольку в дальнейшем необходимо формирование доказательной базы. На сегодня не существует единой системы для борьбы с DoS-атаками, а каждый сервер фактически остается один на один с нарушителем. Существование системы групповой защиты позволит в короткие сроки определить наличие атак, выявить их источник, прекратить атаки, ликвидировать последствия и с помощью административных мер призвать нарушителя к ответственности.

В итоге появляется еще один субъект защиты – государство в лице уполномоченных органов, чтобы примененные меры правового принуждения не подвергались критике в смысле их законности и во избежание злоупотреблениям со стороны субъектов частного права.

~~~~~~~~~~~~ * * * ~~~~~~~~~~~~

ПРАВОВА ОХОРОНА КОМП’ЮТЕРНОЇ ПРОГРАМИ ЯК ОБ’ЄКТА ІНФОРМАЦІЙНИХ ВІДНОСИН

Водорєзова С.Р., здобувач наукового ступеня,
Національний юридичний університет імені Ярослава Мудрого

При наданні інформаційних послуг основною проблемою стає захищеність інтересів прав володільців об’єктів інтелектуальної власності, які є об’єктом інформаційних послуг, у тому числі певних інформаційних систем та їх складових – комп’ютерних програм. Інформаційна система як об’єкт правової охорони розглядається на підставі вже відомих правовій практиці
~~~~~~~~~~~~

складових цього поняття, таких як інформація, програмне забезпечення ЕОМ, бази даних, операційні та експертні системи.

У Законі України “Про авторське право і суміжні права” комп’ютерна програма визначається як набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи у будь-якому іншому вигляді, виражених у формі, придатній для зчитування комп’ютером, які приводять його у дію для досягнення певної мети або результату, а базу даних – як сукупність творів, даних або будь-якої іншої незалежної інформації у довільній формі, в тому числі – електронній, підбір і розташування складових частин якої та її упорядкування є результатом творчої праці, і складові частини якої є доступними індивідуально і можуть бути знайдені за допомогою спеціальної пошукової системи на основі електронних засобів (комп’ютера) чи інших засобів.

Згідно зі ст. 18 Закону України “Про авторське право і суміжні права” комп’ютерні програми охороняються як літературні твори. Така охорона поширюється на комп’ютерні програми незалежно від способу чи форми їх вираження.

На нашу думку, така позиція вітчизняного законодавця має свої як позитивні, так і негативні риси. Головною позитивною рисою такого виду захисту є наступне: права автора виникають з моменту створення комп’ютерної програми (бази даних), будуть діяти протягом усього життя автора, та 70 років після його смерті, хоча користь від такого тривалого терміну дії незначна, тому що ринок програмного забезпечення стрімко розвивається, і на ринок швидко виходять нові версії програм.

З іншого боку, недоліком вказаного виду захисту є те, що авторське право захищає саму програму у формі вихідного тексту або об’єктного коду, а зміст (як процес, засіб) – авторським правом не охороняється. Отже, охороняється авторське вираження ідеї в конкретній матеріальній формі, а це означає, що при захисті комп’ютерної програми має значення код, а не ідея, концепція, принципи, алгоритми.

На сьогодні вже непоодинокими є пропозиції про встановлення поряд з авторським правом патентної системи охорони для комп’ютерних програм. Хоча, нерозповсюдження норм патентного права на комп’ютерні програми та бази даних мотивується тим, що процес патентування є тривалим і дорогим, крім того жорстким критеріям патентоспроможності може відповідати лише певна частина комп’ютерної програми. Для проходження експертизи в патентному відомстві потрібна ретельна підготовка заявочної документації. З моменту подання документації до видачі патенту в середньому минає два-три роки. Тільки після успішного проходження експертизи заявці на патент надається охорона.

Маючи технічну сутність, комп’ютерна програма спрямована, як правило, на рішення якогось технічного завдання та задовольняє технічні потреби, виступає засобом виробництва. Тому стає питання про доцільність запровадження миттєвої, комбінованої процедури реєстрації прав на комп’ютерні програми та бази даних, з метою подальшого захисту та спрощення використання в господарській діяльності.

Для введення так званого комбінованого механізму захисту прав доцільно було б розглянути окремі елементи комп’ютерної програми:

- алгоритм (так звана “вісь” програми), його можна визначити як набір структурних блоків, до яких не входять загальновідомі математичні формули, методи, розрахунки, які не несуть в собі ознак наукового відкриття. Алгоритм реалізує функціональність, для такого елементу може бути використаний аналогічний механізму захисту винаходу;

- інтерфейс – дизайн, зовнішній вигляд. Саме інтерфейс визначає зовнішній вигляд програми, з яким користувач має справу в процесі використання програми. Виходячи з вказаного, інтерфейс підпадає під правову охорону як промисловий зразок. Законодавець в п. 2 ст. 5 Закону України “Про охорону прав на промислові зразки” визначає що об’єктом промислового зразка може бути форма, малюнок чи розфарбування або їх поєднання, які визначають зовнішній вигляд промислового виробу і призначені для задоволення естетичних та ергономічних потреб.

- код програми (варіант виконання, текст програми), який за своєю сутністю є твором в галузі науки, доцільно залишити під захистом авторського права.

Але з введенням такого комбінованого механізму захисту окремим проблемним питанням стає процедура реєстрації прав на вказані об’єкти. Як зазначалося вище, на сьогодні сама процедура реєстрації прав є досить тривалою та коштовною, тому доцільно було б введення кваліфікаційно-формальної експертизи на відповідність таким критеріям, як новизна, винахідницький рівень, промислова придатність, наявність технічного вкладу. Після проведення експертизи буде виноситись рішення про видачу державного документа (патент або свідоцтво), або про відмову в реєстрації заявленого об’єкта.

З урахуванням вище вказаного можна дійти висновку, що модель правової охорони такого об’єкту інформаційних відносин як комп’ютерна програма необхідно будувати, враховуючи як і її природу, так і особливості. На нашу думку, запровадження комплексного захисту забезпечить спрощення використання даного об’єкту в господарській діяльності.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~

СОЦІАЛЬНІ МЕРЕЖІ – ЗАГРОЗА ІНФОРМАЦІЙНІЙ БЕЗПЕЦІ ДЕРЖАВИ

Артюх В.Ю., курсант 4 курсу ІПЮК для СБУ
НЮУ імені Ярослава Мудрого

Третє тисячоліття диктує правила життя, яких особа повинна дотримуватися, щоб відчувати себе частиною соціуму та бути в центрі подій. Однією з таких умов в сучасному світі є використання соціальних мереж. Це явище стало настільки звичним та буденним для нас, що ми навіть не замислюємося про ті потенційні загрози, які можуть виникнути внаслідок такої звичної діяльності. Як свідчить статистика, на сьогодні близько 81 % Інтернет-користувачів є учасниками соціальних мереж. Україна увійшла у п’ятірку країн, Інтернет-користувачі яких найактивніше відвідують соціальні мережі. Тому забезпечення безпеки особи та держави в цій загальній мережі спілкування є одним з важливих питань порядку денного нашої держати та міжнародного товариства.

Ні для кого не секрет, що соціальні мережі можуть використовуватися для збору інформації про особу – від її смаків та вподобань до членів сім’ї та друзів, створювати згубний маніпуляційний вплив на суспільство та державу в цілому. Тобто вони постали потужною “інформаційною зброєю”, якою можна оперувати для реалізації злочинних мотивів. Відповідно, втручання держави є необхідним для підтримання нормального рівня безпеки користувачів та держави. Реєстрація на соціальних сайтах має природу цивільно-правового договору, у якому користувач добровільно погоджується на всі умови, що, на жаль, створені для захисту інтересів, насамперед, адміністрації цих сайтів. Тобто до відповідальності фактично притягнути нікого, адже користувач добровільно погоджується на всі негативні наслідки використання його особистої інформації адміністрацією сайта та будь-яких третіх осіб. Тому для врегулювання питання, щоб убезпечити користувачів, необхідно покласти більшу кількість обов’язків на адміністрації сайтів. Після врегулювання відповідних правових питань потрібно буде забезпечити нормальний механізм реалізації цих норм права. Для цього вбачаємо доцільним, наприклад, поповнити положеннями КУпАП та КК України відповідними статтями для притягнення потенційних порушників до відповідальності. Але поряд з цим також доцільно буде здійснити відповідні реформи у судовій системі шляхом виділення окремого судового провадження в адміністративному судочинстві та перепрофілювання, відповідно, суддівського корпусу для успішного відправлення судочинства. Підґрунтям врегулювання цього питання з правової точки зору має стати формування та використання усіма адміністраціями соціальних мереж типових положень користування соціальними ресурсами, затвердивши їх як обов’язкові для можливості надавати послуги такого виду. Тоді суб’єкти надання відповідних послуг будуть змушені якісно виконувати свої обов’язки. Поряд з нормативним врегулюванням для реалізації та контролю за виконанням необхідно наділити відповідними обов’язками компетентні правоохоронні органи, провівши належні реформи шляхом створення та забезпечення нормального функціонування вже існуючих відділів у правоохоронних органах України.
~~~~~~~~~~~~~

Соціальні мережі функціонують у мережі Інтернет, яка є всесвітнім ресурсом, відповідно, забезпечувати інформаційну безпеку особи потрібно на міжнародному рівні у тісній співпраці з адміністрацією цих сайтів. При цьому необхідно діяти демократичним шляхом, не порушуючи основоположних прав та свобод людини та громадянина. Пріоритет при вирішенні цієї проблеми потрібно зробити на превентивних методах діяльності, адже використовуючи різноманітні імперативні методи правового регулювання, можемо зіткнутися з проблемою обмежень низки конституційних прав громадян, що є недопустимим в демократичних державах, які взяли курс на гуманізацію. Тому можна виділити такі основні шляхи вирішення проблеми врегулювання діяльності соціальних мереж:

- удосконалення міжнародного та національного законодавства;
- створення належного механізму реалізації та захисту прав користувачів;
- реорганізація та розподіл повноважень між уповноваженими органами;
- механізми прийняття рішень та розмежування повноважень;
- сприяння процесам самоорганізації;
- активне інформування суспільства про потенційну небезпеку;
- правові механізми притягнення до відповідальності порушників;
- використання методу моніторингу шляхом “контролю та перехоплення”;
- примусові заходи (закриття чи обмеження доступу до серверів).

Звичайно, все це потребує залучення фахівців різних галузей науки та значних економічних витрат нашої держави, але затрати на забезпечення національної безпеки в кінцевому результаті завжди будуть повернуті. За неофіційною інформацією для підтримки нормальної роботи соціальних мереж потрібно близько 15 млн. грн. за місяць, для України – це значна сума, але цілком виправдана, якщо проаналізувати, яку кількість збитків ми можемо отримати, ігноруючи вищеназвані проблеми. Комплексне забезпечення виконання вказаних пропозицій може забезпечити національну безпеку держави, у контексті використання соціальних мереж, практично у всіх проблемних напрямках, від інформаційної безпеки особи до забезпечення національної безпеки держави в цілому. Однозначно, нововведення, що були запропоновані в даній роботі, можуть викликати зауваження та є дискусійними. Але дискусія виступає необхідним джерелом нових ідей та шляхом їх вдосконалення.

~~~~~~~~~~~~ * * * ~~~~~~~~~~~~

ПРОБЛЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ПРО ПАЦІЄНТА В ЗМІ

Калініченко А.І., старший науковий співробітник
НДІ правового забезпечення інноваційного розвитку НАПрН України

На адресу медичних закладів надходять різноманітні запити, зокрема адвокатські запити, запити органів або осіб, які згідно з чинним законодавством України не завжди мають право на отримання інформації про самого пацієнта, факт його звернення за медичною допомогою та відомості про його лікування. У свою чергу, медичні працівники, не маючи достатніх правових знань, не завжди можуть правильно зорієнтуватись, на які запити, що надійшли, потрібно надавати відомості, а в яких випадках слід обмежити надання тої інформації, що становить лікарську таємницю. У результаті цього медичні заклади відповідають на запити з наданням повної інформації про пацієнта, зазвичай не усвідомлюючи, що порушують вимоги закону щодо розголошення відомостей, які становлять лікарську таємницю. Відповідно до Клятви лікаря, що затверджена Указом Президента України від 15.06.92 р. № 349, кожен лікар зобов’язується зберігати лікарську таємницю, не використовувати її на шкоду людині.

З огляду на недосконаліть та несистемність чинного законодавства, що регулює сферу охорони здоров’я, у тому числі питання збереження лікарської таємниці, не кожен лікар достеменно знає, які саме відомості є об’єктом лікарської таємниці, не говорячи про обізнаність у процедурі й нюансах розголошення такої інформації.
~~~~~~~~~~~~

Складність збереження інформації про пацієнта, що становить лікарську таємницю, полягає в тому, що в чинному законодавстві України відсутній єдиний нормативний акт, який би повністю регулював дане питання. Лікарська таємниця регулюється низкою нормативно-правових актів. Право на лікарську таємницю випливає з положення, закріпленого статтею 32 Конституції України від 28.06.96 р. № 254к/96-ВР, про те, що ніхто не може зазнавати втручання в його особисте і сімейне життя.

Законодавство України не містить вичерпного переліку відомостей, які утворюють зміст категорії “лікарська таємниця”. Аналізуючи наведену нормативно-правову базу, можна дійти висновку, що об’єкт лікарської таємниці становить наступна інформація: факт звернення за медичною допомогою; стан здоров’я пацієнта; хвороба та діагноз; огляд та його результати; методи лікування; інтимна і сімейна сторони життя; інші відомості, одержані при медичному обстеженні.

Важливо зауважити, що суб’єктами збереження лікарської таємниці є не тільки безпосередньо лікуючий лікар, а й молодший медичний персонал (санітари, няньки), адміністративний персонал лікувально-профілактичної установи (працівники кадрових, юридичних, фінансових, господарських служб тощо), посадові особи органів управління охорони здоров’я, співробітники судових і правоохоронних органів, яким інформація, що становить лікарську таємницю, стала відомою через виконанання професійних обов’язків.

Відсутність положення про підстави, за яких розголошення лікарської таємниці без згоди особи було б законним, є суттєвою прогалиною української правової бази та породжує труднощі при вирішенні “медичних справ” і створює проблеми при застосуванні законодавства. Доречно було б систематизувати та чітко закріпити у законодавстві підстави, за яких медична таємниця може бути розголошена без згоди особи чи її законних представників.

Щодо надання відомостей засобам масової інформації можна зазначити наступне. Відповідно до частин першої, другої статті 32 Основного Закону України: “Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України; не допускається 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 прав людини”. Згідно з частиною 2 статті 11 Закону України “Про інформацію” від 02.10.92 р. № 2657-XII дані про стан здоров’я фізичної особи належать до конфіденційної інформації. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом (ч. 2 ст. 21вищезазначеного Закону). Розпорядники інформації, які володіють конфіденційною інформацією, можуть поширювати її лише за згодою осіб, які обмежили доступ до інформації, а за відсутності такої згоди – лише в інтересах національної безпеки, економічного добробуту та прав людини (ч. 2 ст. 7 Закону України “Про доступ до публічної інформації” від 13.01.11 р. № 2939-VI).

Таким чином, лише фізична особа, якої стосується конфіденційна інформація, (пацієнт) відповідно до конституційного та законодавчого регулювання права особи на збирання, зберігання, використання та поширення конфіденційної інформації має право вільно, на власний розсуд визначати порядок ознайомлення з нею інших осіб, держави та органів місцевого самоврядування, а також право на збереження її у таємниці.

З іншого боку, згідно з частинами першою, другою статті 34 Конституції України: “Кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань; кожен має право вільно збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб – на свій вибір”.

Однією з гарантій реалізації конституційних прав на вільне збирання, зберігання, використання і поширення інформації є законодавче закріплення права кожного на доступ до інформації, яке згідно зі статтею 5 Закону України “Про доступ до публічної інформації” забезпечується систематичним та оперативним оприлюдненням інформації в офіційних друкованих виданнях, на офіційних веб-сайтах у мережі Інтернет, на інформаційних стендах та будь-яким іншим способом, а також шляхом надання інформації на запити.

Положення частини першої статті 32 та частини третьої статті 34 Конституції України перебувають у системному взаємозв’язку і передбачають як недопустимість порушення права людини на недоторканність особистого та сімейного життя, так і реалізацію особою права на вільне збирання, зберігання, використання і поширення інформації.

Положення частини другої статті 32 Конституції України передбачають вичерпні підстави можливого правомірного втручання в особисте та сімейне життя особи. Такими підставами є: згода особи на збирання, зберігання, використання та поширення конфіденційної інформації стосовно неї, а також, у разі відсутності такої згоди, випадки, визначені законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Даючи офіційне тлумачення положень частин першої, другої статті 32 Конституції України у системному зв’язку з частиною другою статті 34 цієї Конституції, Конституційний Суд України дійшов висновку, що збирання, зберігання, використання та поширення державою, органами місцевого самоврядування, юридичними або фізичними особами конфіденційної інформації про особу без її згоди є втручанням в її особисте та сімейне життя, яке допускається виняткова у визначених законом випадках і лише в інтересах національної безпеки, економічного добробуту та прав людини (Рішення Конституційного Суду України від 20.01.12 р. № 2-рп/2012).

Таким чином, надання відомостей, які становлять лікарську таємницю, ЗМІ можливе у наступних випадках: (1) згода пацієнта і (2) у разі відсутності такої згоди, випадки, визначені законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

Окремо слід вказати, що якщо мова йде про зйомку в загальнодоступному місці, передбачатиметься, що зафіксована інформація відноситься до загальнодоступної. Те ж саме можна сказати і про ситуації, коли приблизний діагноз є відомим із зовнішнього вигляду хворого, наприклад, зламану і загіпсовану кінцівку може побачити будь-хто. Зйомка всередині палат, де хворі проводять досить тривалий час, може порушувати і таємницю особистого життя, тому перед тим, як знімати, слід отримати дозвіл від усіх хворих палати або від тих з них, хто потраплять до кадру.

Медичному персоналу перед тим, як відповідати на будь-які запити, доцільно отримати фахову консультацію юриста, щоб переконатися у правомірності своїх дій, адже розголошення відомостей, що становлять лікарську таємницю, тягне за собою дисциплінарну, цивільно-правову, адміністративну або кримінальну відповідальність згідно з законодавством України. За умови правильного реагування на такі запити, з точки зору законодавства, ризик розголошення лікарської таємниці, як правило, зводиться до мінімуму.

Оскільки в чинному законодавстві України відсутній єдиний нормативний акт, який би повністю регулював питання збереження лікарської таємниці та враховуючи відсутність положення про підстави, за яких розголошення лікарської таємниці без згоди особи було б законним, доцільно розробити локальний нормативний акт (у межах лікувально-профілактичного закладу), в якому передбачити відповідно до чинного законодавства випадки надання відомостей, які становлять лікарську таємницю, правила поводження сторонніх осіб, у тому числі представників засобів масової інформації, в загальнодоступних місцях та в палатах на території відповідного закладу, та проінструктувати персонал.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ПЕРЕДАЧІ ТА ЗБЕРЕЖЕННЯ ІНФОРМАЦІЇ ПРИ ЗАСТОСУВАННІ ТЕЛЕМЕДИЧНИХ ТЕХНОЛОГІЙ

Воронина І.С., науковий співробітник
НДІ правового забезпечення інноваційного розвитку НАПрН України

В умовах реформування системи охорони здоров’я України стратегічно важливим є забезпечення взаємодії лікувально-профілактичних закладів різного рівня зі спеціалізованими закладами охорони здоров’я шляхом дистанційного надання висококваліфікованої медичної
~~~~~~~~~~~~~~

допомоги громадянам із залученням сучасних інформаційно-телекомунікаційних технологій та використанням інтелектуального потенціалу кращих науковців країни і світу.

Термін “телемедицина” з’явився у 1970-х роках та розшифровувався як “лікування на відстані”, тобто використання інформаційно-комунікаційних технологій з метою поліпшення результатів лікування пацієнтів шляхом розширення їх доступу до медичної інформації. Відповідно до уніфікованого визначення, прийнятого ВООЗ: “телемедицина – це надання послуг охорони здоров’я в умовах, коли відстань є критичним фактором, працівниками сфери охорони здоров’я, які використовують інформаційно-комунікаційні технології для обміну необхідною інформацією з метою діагностики, лікування і профілактики захворювань та травм, проведення досліджень і оцінок, а також для безперервної освіти медичних працівників в інтересах покращення здоров’я населення і розвитку місцевих громад”.

Можна виділити наступні характерні ознаки телемедицини:

1. Використання різних видів інформаційно-комунікаційних технологій.

2. Метою телемедицини є надання клінічної підтримки та покращення стану здоров’я населення.

3. Транскордонний характер, оскільки за допомогою телемедицини встановлюється зв’язок між користувачами, які фізично знаходяться у різних географічних точках.

Деякі автори розрізняють поняття “телемедицина” та “телемедична охорона здоров’я”, оскільки у першому випадку розглядається надання послуг тільки лікарями, а у другому випадку мається на увазі надання послуг всіма працівниками галузі охорони здоров’я, в тому числі медичними сестрами, клінічними провізорами та іншими кваліфікованими спеціалістами галузі.

Виділяють 2 види телемедицини, в залежності від строків передачі інформації, характеру взаємодії між учасниками та сфери застосування:

1) асинхронна телемедицина – використовуються попередньо записані дані між двома чи більшою кількістю осіб у різний час (приклад – пацієнт або медичний працівник направляє лікарю-експерту електронною поштою опис медичної події, після чого лікар-експерт надсилає назад свій експертний висновок з приводу діагнозу і рекомендованого курсу лікування);

2) синхронна телемедицина відбувається у реальному часі та потребує одночасної присутності всіх осіб, що приймають участь у процесі під час інтерактивного обміну інформацією (приклад – проведення відеоконференцій).

В обох типах телемедицини, синхронній та асинхронній, форми передачі інформації можуть бути різними: текст, відео- чи аудіозображення.

Законодавче оформлення телемедицини в Україні було розпочато наказом Міністерства охорони здоров’я “Про впровадження телемедицини в закладах охорони здоров’я” від 26.03.10 р. № 261, яким затверджені Примірне положення про взаємодію телемедичних центрів та закладів охорони здоров’я і Примірне положення про телемедичний центр (кабінет) закладу охорони здоров’я.

Вказаним нормативно-правовим актом врегульовані питання взаємодії телемедичних центрів та закладів охорони здоров’я, а також затверджене примірне положення про телемедичний центр (кабінет) закладу охорони здоров’я, із визначенням завдань, функцій, прав та обов’язків телемедичного центру, порядок його створення та ліквідації.

19.11.2010 р. Україною була підписана Угода про співробітництво держав-учасниць СНД щодо створення сумісних національних телемедичних систем СНД. Окремі положення, що стосуються безпосередньо інформаційної складової телемедичних послуг, закріплені у нормативно-правових актах з питань інформатизації та захисту персональних даних.

Для того щоб отримати послуги із телемедицини, споживач повинен мати спеціальне обладнання – комп’ютер, під’єднаний до Інтернет-мережі, веб-камеру та додаткові аксесуари – для повноцінного спілкування з постачальником таких послуг в особі лікаря. За відсутності такого обладнання надання телемедичних послуг технічно неможливе.

Однією з головних правових проблем використання телемедичних технологій та мережі Інтернет є проблема відповідальності за зміст та достовірність інформації, розміщеній на сайтах, та за використання телемедичних консультацій. Також актуальним є питання відсутності державної цільової програми розвитку телемедичних технологій в Україні.

Крім цього, потрібно забезпечити безпечну передачу інформації, консультацій для лікаря і пацієнта, в тому числі вирішити питання з переліком обладнання, що використовується та визначити вимоги до технічних параметрів.

Розвиток відносин у сфері телемедичних технологій у світі відбувається не тільки на рівні державного регулювання, але й на рівні суспільного саморегулювання. У США медичними організаціями було створено Коаліцію охорони здоров’я у мережі Інтернет. Метою створення цієї структури є забезпечення якості медичних ресурсів у мережі Інтернет, що досягається шляхом надання достовірної та перевіреної інформації споживачам та професіоналам у галузі охорони здоров’я, саморегулювання через створення етичних норм та інше.

У травні 2000 року Коаліцією охорони здоров’я у мережі Інтернет опубліковано Кодекс етики телемедицини. (eHealth Code of Ethics). Зазначеним Кодексом врегульовано надання споживачам відомостей стосовно власників медичного сайту, спонсорів сайту, цілей та завдань сайту; розмежування рекламних та освітніх матеріалів; відносини по забезпеченню конфіденційності персональних даних споживачів телемедичних послуг; зворотній зв’язок із власниками ресурсу; інформування споживачів про обмежені можливості телемедицини та інше.

Користувач телемедичного ресурсу має бути попереджений про можливість збору персональних даних під час користування ресурсом та вирішити питання про їх надання.

Поняття “телемедична послуга” та “телемедичні технології надання медичної допомоги і передачі медичної інформації з використанням інформаційно-комунікаційних технологій” не тотожні. Відмінність полягає у тому, що нові технології застосовуються у межах існуючої структури організації медичної допомоги населенню, що регулюється діючим законодавством. З іншого боку, у процесі розвитку технологій з’являється можливість надання нових медичних послуг, не передбачених в існуючій нормативній базі.

Права пацієнта забезпечуються можливістю надання телемедичної послуги та обрання місця звернення за телемедичною консультацією. Суб’єкт телемедичної послуги має бути захищений від неякісної, неповної та недостовірної інформації, яка шкодить здоров’ю. Інформована згода пацієнта дійсна тільки у тому випадку, коли пацієнт отримав всю необхідну інформацію і пояснення у попередній розмові, що не може бути замінена формальним підписанням згоди затвердженого зразка. Інформована згода пацієнта повинна містити опис способу передачі його даних, перелік та обсяг даних, що передаються. Пацієнт має бути проінформований щодо ризиків, таких як незаконний доступ до даних пацієнта та їх подальша безконтрольна передача, неспівпадіння малюнків та висновків, переривання процесу передачі даних з технічних причин, перерва у супутниковій трансляції; додаткових витратах на телемедичну консультацію та інше. У разі виникнення ситуації, загрозливої для життя та здоров’я пацієнта, що не може підписати інформовану згоду, професіонали у галузі охорони здоров’я приймають самостійне рішення на підставі можливої згоди пацієнта, після ретельного розгляду позитивних чи негативних наслідків.

Конфіденційність є базовим аспектом телемедицини, оскільки інформація про пацієнта передається на великі відстані й у комунікаційних мережах загального користування. Загальноприйнятним стає використання електронно-цифрового підпису, що забезпечує всі ключові ознаки конфіденційності: секретність, посвідчення оригінальності документу чи підпису, цілісність і відповідальність за результат. Обов’язковість використання відповідних засобів захисту інформації у сфері охорони здоров’я дозволить створювати нові системи послуг, наприклад, електронна історія хвороби чи електронні банки даних медичної інформації, що фіксується протягом всього життя пацієнта.

Використання переданої при наданні телемедичних послуг інформації засновано на праві пацієнта на інформаційне самовизначення. Зберігання, обробка та передача інформації, що стосується особи пацієнта, заборонені до моменту надання згоди безпосередньо пацієнтом чи дозволено діючим законодавством. Мають бути застосовані всі передбачені технічні й організаційні засоби для перешкоджання неправомірному використанню даних пацієнта.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~

ПРАВО СПОЖИВАЧІВ НА БЕЗПЕКУ ТОВАРІВ В ІНТЕРНЕТ-ТОРГІВЛІ

Кузьміна М.М., *кандидат юридичних наук*

Споживачі під час придбання, замовлення або використання продукції, яка реалізується на території України, для задоволення своїх особистих потреб мають право на безпеку.

Під безпекою продукції Закон України “Про захист прав споживачів” від 12.05.91 р. розуміє відсутність будь-якого ризику для життя, здоров’я, майна споживача і навколишнього природного середовища при звичайних умовах використання, зберігання, транспортування, виготовлення й утилізації продукції. Загальні положення безпеки продукції передбачені Директивою 2001/95/ЄС від 03.12.01 р. щодо загальної безпеки продукції – “безпечною” визнається продукція, що за звичайних чи розумно передбачуваних умов не несе жодного ризику або мінімальний ризик, що співвідноситься з використанням продукції та вважається допустимим за умови додержання високого рівня захисту здоров’я й безпеки людини. Поняття дефініції “безпека” включає: 1) властивості продукції, у тому числі її склад, пакування, умови збірки, установки та догляду; 2) дослідження наслідків спільного використання цієї продукції з іншою, а також категорій споживачів, що можуть наражати себе на небезпеку при її використанні (люди похилого віку, діти); 3) зовнішнє оформлення продукції, що передбачає інформування споживачів щодо попередніх пунктів та будь-які вказівки щодо використання чи знищення.

Стандартизація, підтвердження відповідності, в тому числі сертифікація, є засобами забезпечення безпеки та якості продукції. Так, продукція, на яку в державних стандартах та в інших нормативно-технічних документах є вимоги щодо безпеки для здоров’я і життя населення, підлягає обов’язковій сертифікації. У документах на товари, що підлягають обов’язковій сертифікації (наприклад, мийні засоби, велосипеди, коляски дитячі, посуд з чорних та кольорових металів, фарфору, фаянсу, спиртні напої, дитяче харчування), повинні зазначатися реєстраційні номери сертифіката відповідності чи свідоцтва про визнання відповідності та/або декларації про відповідність, якщо це встановлено технічним регламентом.

Крім цього, відповідно до ст. 14 Закону України “Про захист прав споживачів”, створюючи новий (модернізований) товар, розробник повинен подати технічну документацію відповідному органу для проведення державної експертизи на його відповідність вимогам щодо безпеки для життя, здоров’я і майна споживачів, а також навколишнього природного середовища. Виробник (виконавець) зобов’язаний інформувати споживача про можливий ризик і про безпечне використання продукції за допомогою прийнятих загальновідомих у міжнародній практиці позначень.

Щодо безпеки харчових продуктів, відповідно до Закону України “Про безпечність та якість харчових продуктів”, то це відсутність токсичної, канцерогенної, мутагенної, алергенної або іншої несприятливої для організму людини дії харчових продуктів при їхньому споживанні в загальноприйнятих кількостях, межі яких встановлені Міністерством охорони здоров’я України.

Для забезпечення безпечності харчових продуктів, вироблених в Україні, забороняється: використання харчових добавок, ароматизаторів та допоміжних матеріалів для переробки, дієтичних добавок, які не зареєстровані для використання в Україні; використання допоміжних засобів і матеріалів для виробництва та обігу, які не дозволені для прямого контакту з харчовими продуктами; використання допоміжних засобів і матеріалів для виробництва та обігу, які за своєю природою та складом можуть передавати забруднюючі речовини харчовим продуктам; використання харчових продуктів як інгредієнтів для виробництва, включаючи сільськогосподарську продукцію, якщо вони містять небезпечні фактори на рівнях, що перевищують обов’язкові параметри безпечності.

Виробники, що здійснюють діяльність з виробництва харчових продуктів, підконтрольних санітарній службі, зобов’язані погодити технологію виробництва з центральним органом виконавчої влади у сфері охорони здоров’я. Виробники, що здійснюють діяльність з виробництва харчових продуктів, підконтрольних ветеринарній службі, зобов'язані погодити технологію виробництва з центральним органом виконавчої влади у сфері аграрної політики.

Виробник, імпортер або продавець, який вводить новий харчовий продукт в обіг в Україні (далі – заявник), подає заяву на проведення державної санітарно-епідеміологічної експертизи до центрального органу виконавчої влади у сфері охорони здоров’я. Висновки державної санітарно-епідеміологічної експертизи повинні містити рішення про те, чи допускається новий харчовий продукт в обіг, умови дозволу та, якщо це необхідно: умови використання харчового продукту; призначення харчового продукту та його специфікацію; всі особливі вимоги до етикетування.

До товарів, продукції, сировини, що імпортуються в Україну, застосовуються вимоги щодо їх безпеки для здоров’я і життя людини, а також до процедур контролю, експертиз, надання дозволів, встановлення санітарно-епідеміологічних нормативів, регламентів аналогічно тим вимогам, що застосовуються до відповідних товарів, продукції, сировини, які вироблені в Україні.

Таким чином, законодавцем встановлене визначення безпеки продукції як відсутність ризику (можливості виникнення негативного впливу та вірогідні масштаби його наслідків протягом певного періоду часу), в складі, пакуванні, умовах збірки, установки та догляду. Відповідно до європейських норм у визначенні “безпечна продукція” важливо вказати наслідки спільного використання цієї продукції з іншою, а також категорії споживачів, що можуть наражати себе на небезпеку при її використанні, інформування споживачів щодо попередніх пунктів та будь-які вказівки щодо використання чи знищення. Можна виділити такі види безпеки (або небезпеки) продукції: санітарно-епідеміологічна, біологічна, радіаційна, екологічна тощо.

Продукція має відповідати вимогам безпеки**:** 1) для життя, здоров’я і майна споживачів. Проводиться санітарно-епідеміологічна експертиза на відповідність технічної документації та готової продукції санітарним нормам. Необхідний спеціальний дозвіл для роботи з радіоактивними речовинами. 2) для навколишнього природного середовища. Проводиться екологічна експертиза на відповідність екологічним стандартам та нормам документації при створенні продукції та її впровадження. Видається дозвіл на створення штамів мікроорганізмів та біологічно активних речовин.

Законодавство України передбачає заходи щодо забезпечення безпеки продукції: спрямовані на недопущення надходження в обіг товарів, що можуть заподіяти шкоду, а також щодо запобігання нанесення шкоди товарами, що вже реалізуються споживачам. Через недосконаліть законодавства ці заходи не застосовуються повною мірою до регулювання торгівлі товарами через мережу Інтернет. Тому, купуючи товари в Інтернеті, споживач дуже часто: а) може купити небезпечний товар; б) ускладнює для себе механізм відшкодування заподіяної шкоди через суд. Має бути розроблено спеціальний закон “Про електронну комерцію”, який би врегулював всі питання, пов’язані з торгівлею в мережі Інтернет, і передусім встановити механізм захисту прав споживачів. Необхідно врегулювати діяльність Інтернет-магазинів як суб’єктів господарювання, впровадити прозорий алгоритм доведення того, що товар небезпечний (неякісний), у тому числі забезпечення проведення судової експертизи при доказуванні недоліків придбаного товару.

~~~~~~~~~~~~ * * * ~~~~~~~~~~~~

ІНФОРМАЦІЙНА ПОСЛУГА ЯК ОБ’ЄКТ ПРАВОВІДНОШЕННЯ І ПРЕДМЕТ ДОГОВОРУ

Борисов І.В., молодший науковий співробітник
Науково-дослідного інституту правового забезпечення
інноваційного розвитку НАПрН України

Ефективний розвиток сучасного суспільства неможливо уявити без інформаційної складової. Практично будь-яка сфера діяльності суб’єктів господарювання певним чином пов’язана з інформацією щодо тих чи інших явищ, подій, фактів. Публічний та приватний інформаційний інтерес учасників майнового обороту забезпечується за допомогою закріплення в
~~~~~~~~~~~~

правових нормах права на отримання ними інформації. Звідси інформаційними слід визнавати правовідносини, в яких уповноваженому суб’єкту належить право отримати від зобов’язаної особи при настанні визначених законом або договором умов інформацію з тих чи інших питань, що в подальшому дасть можливість цій особі визначитись з лінією своєї поведінки.

Підставою для виникнення інформаційних правовідношень може слугувати як закон, так і договір. Разом із тим проблема правового регулювання інформаційних відносин, складовою яких є надання інформаційних послуг, на сьогодні все ще залишається поза увагою законодавця. Так, ЦК України не ідентифікує послуги, які можуть виступати предметом договору про надання послуг. Щодо спеціального законодавства, то й на його рівні врегулювання договорів на надання інформаційних послуг майже відсутнє, а тому при укладенні договорів в інформаційній сфері, як правило, сторони опираються на подібні правовідносини надання послуг, застосовуючи аналогію закону, що свідчить про прогалини у законодавстві.

З’ясовуючи доцільність і необхідність закріплення на рівні законодавства договору про надання інформаційних послуг як пойменованого, перш за все, з’ясуємо, що ж представляє собою послуга в інформаційній сфері в контексті того, що й інформація, і послуга визнаються самостійними об’єктами цивільних прав, і як впливає поєднання термінів “інформація” і “послуга” в єдине словосполучення “інформаційна послуга” на суть її як послуги?

Інформація (від лат. – “informatio” – роз’яснення, викладання, ознайомлення) – це відомості (знання) про оточуючий світ і ті процеси, які в ньому відбуваються, повідомлення щодо положення справ; відомості про певні події, факти, діяльність тощо.

У доктрині права усталеним є підхід до інформації як блага особливого роду, що нерозривно пов’язане з життям, з його виникненням і закінченням, що проявляється як особисте немайнове благо, як результат впливу на людину й інших суб’єктів та об’єктів права, як результат інтелектуальної творчої діяльності й як відомості про осіб, події та явища, предмети, об’єкти і процеси незалежно від форми їхнього представлення. Цей підхід знайшов своє втілення і на рівні закону. Зокрема Закон України “Про інформацію” (далі – Закон) під інформацією розуміє документовані або публічно оголошені відомості про події та явища, що відбуваються в суспільстві, державі та навколишньому природному середовищі

Таким чином, і вчені, і законодавець оперують поняттям інформації в прагматичному аспекті. Ми ж поділяємо точку зору тих вчених, зокрема В.В. Гришиної, які наполягають на тому, що інформацію слід вважати способом отримання відомостей, засобом й інструментом їх передачі. Звідси й інформаційна послуга – це здійснювані на користь замовника дії іншої сторони правовідношення щодо створення або перетворення інформації, яка не охороняється як результат інтелектуальної діяльності, і передача її замовнику з метою задоволення його інформаційних потреб.

При аналізі обороту інформації, яка виступає особливим об’єктом цивільних прав, якому притаманні такі ознаки: нематеріальний характер, непоживність, оскільки з нею можна лише ознайомлюватися, пізнавати її; можливість багаторазового використання, переважна об’єктивізація у разі включення у правовий оборот, суб’єктивний характер, збереження у суб’єкта, який її передає, здатність до відтворення, копіювання, збереження, перетворення і накопичення, виникає проблема невідчужуваності останньої у звичайному сенсі цього слова, оскільки виробник не позбавляється інформації при її передачі або обміні. У результаті відчуження інформація зберігається у виробника, переходячи з індивідуального володіння до суспільного. Засобом відчуження інформації виступає право. У результаті реалізації інформації виробник зберігає її в своїй пам’яті або розтиражованому вигляді, але, у випадку її повного продажу разом з усіма правами на використання, не має можливості її повторної реалізації. Отже, відчуженню підлягає тільки товарна форма інформаційного продукту і тільки у випадку продажу всіх прав на нього. Останній аргумент дуже важливий і допомагає, на наш погляд, з’ясувати сутність інформації як особливого об’єкта майнового обороту, що і призводить до необхідності впровадження різних правових механізмів договорів, що опосередковують передачу такого об’єкта.

Особливість інформації, яка може бути предметом договору на надання послуг, полягає насамперед у тому, що вона, як благо нематеріальне, не може ототожнюватися зі своїм

матеріальним носієм і потребує особливого правового режиму. Ця інформація повинна мати цінність, оскільки замовник згоден заплатити тільки за надання необхідної йому інформації. Якщо останній звертається за цією послугою до третьої особи, це означає, що сам він вільно отримати відомості, які його цікавлять, не має змоги, а звідси цю інформацію не можна вважати загальнодоступною. Для того щоб знайти у нескінченних інформаційних потоках ті дані, що замовлені, виконавець за договором повинен мати спеціальні знання, які дали б йому змогу знайти необхідну інформацію та обробити її так, щоб зробити доступною для розуміння замовника. А це свідчить про те, що інформація в процесі виконання договору набуває іншого вигляду через застосування до її обробки професіональних навиків виконавця.

Щодо послуги, то на сьогодні усталеною є точка зору, що для неї характерні такі ознаки: відсутність матеріалізованого результату; надання її особисто послугодавцем; невідчутність; одночасність надання і споживання; неможливість зберігання. Ми ж погоджуємося з тими правниками, які вважають, що послуги у порівнянні з об’єктами матеріального світу не існують самі по собі, не є самодостатніми. Вони існують тільки у сфері зобов’язального права, бо послуга – це та дія виконавця (послугодавця), заради якої виникає зобов’язання з її надання. А тому послуга – об’єкт зобов’язальних правовідносин, який є правомірною дією виконавця, спрямовану на досягнення певного результату не матеріалізованого характеру, обмежену в часі, і споживання якої, як правило, відбувається в момент її надання

Але чи можна вважати, що всі ознаки послуги характерні для інформаційної послуги? Вважаємо що ні. Адже, якщо інформація не споживається і з нею можна лише ознайомлюватися, то логічно припустити, що і споживання наданої інформаційної послуги в момент її отримання замовником теж не відбувається.

На відміну від інших послуг, яким притаманна спільна ознака – результату їх надання передує виконання певних дій, а тому продається не результат цих дій (ефект, правові наслідки), а сама дія, що призвела до цього, за договором на надання інформаційних послуг така послуга безпосередньо не споживається замовником у процесі вчинення виконавцем дій з пошуку, перетворенню (обробки), зберіганню інформації, а тому він оплачує результат цих дій, а не дії, що призвели до цього.

Інформаційна послуга – це такий спосіб задоволення інформаційних потреб замовника, що включає не тільки дії виконавця з пошуку, збирання, зберігання, обробки, систематизації інформації і передачі її замовнику, а також і здійснення самим замовником координації діяльності виконавця в процесі отримання ним потрібної для замовника інформації.

Підбиваючи підсумок вищевикладеному, вважаємо, що ознаки, які притаманні інформації, дають можливість виділити спеціальний тип договору – договір на надання інформаційних послуг, предметом якого виступає отриманий замовником корисний ефект від здійснення виконавцем певних дій (пошук інформації, її обробка тощо). При цьому корисний ефект має немайновий характер, що втілений у конкретних відомостях певної галузі знань, які становлять інтерес для замовника. Отримані замовником відомості мають бути цінними, носити ексклюзивний характер і не можуть бути загальнодоступними.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~

ПРАВОВЕ РЕГУЛЮВАННЯ БЕЗПЕКИ ПРОВЕДЕННЯ РОЗРАХУНКІВ

Глібко С.В., *кандидат юридичних наук, доцент*

Питання правового регулювання забезпечення інтересів клієнтів банків при проведенні розрахунків, як правило, пов’язується з відображенням у правовій формі маркетингових заходів банківських установ, використанням розробок програмних продуктів інших суб’єктів, які обов’язкові для застосування у зв’язку з участю банків у платіжних системах. У цих реаліях інтереси клієнтів є похідними, оскільки останні вимушені користуватися запропонованими послугами банків, і, знаходячись в нерівному економічному становищі, клієнти власними силами
~~~~~~~~~~~~~

або участю в переговорному процесі при укладанні правочинів з банками не спроможні змінити або посилити свою захищеність певними технічними або програмними засобами. При таких умовах стає питання про захист публічних інтересів, що полягають у стабільності проведення платежів, і на реалізацію яких спрямовані функції уповноважених державних органів, насамперед Національного банку України (далі – НБУ). Так, серед найближчих до відмічених завдань функцій НБУ відповідно до п. 7 ч. 1 ст. 7 Закону України “Про Національний банк України” є визначення напрямів розвитку сучасних електронних банківських технологій, створює та забезпечує безперервне, надійне та ефективне функціонування, розвиток створених НБУ платіжних та облікових систем, контролює створення платіжних інструментів, систем автоматизації банківської діяльності та засобів захисту банківської інформації.

При проведенні переказу коштів фізичними особами основні пріоритети та переваги, які відмічаються в сучасній банківській діяльності, при відсутності чіткої правової форми або не відповідають правовим інститутам, або приводять до порушень інтересів клієнтів банків. Такими (невичерпний перелік) новими або допрацьованими банківськими продуктами, банківськими новаціями на практиці вважаються, наприклад, наступні:

1) інновації в Інтернет-банкінгу, як правило, пов'язуються з дизайном, додатковими функціями, швидкістю операцій;

2) однією з переваг онлайн-банкінгу є реєстрація в онлайні без ідентифікації, випуск електронних грошей, проведення “кредитних” операцій;

3) застосування технології NFC (Near Field Communication), яка є технологією бездротового високочастотного зв’язку малого радіусу дії, при якій розрахунки відбуваються з мобільного пристрою, в якому міститься образ банківської пластикової картки. Зазначимо, що на цей час відсутній правовий механізм розподілу відповідальності стосовно переказів за допомогою цього програмного продукту;

4) проведення переказу коштів у сучасних платіжних системах електронних грошей без відкриття рахунку, а тільки шляхом прив’язки до номера телефону або поштової адреси;

5) відмова від електронного цифрового підпису для прискорення переказу коштів за рахунок програмного забезпечення.

Наведені новації умовно можливо поділяти на такі, що в певній мірі не відповідають вимогам законодавства, та на такі, що не порушують законодавства, але призводять до появи додаткових “технічних” загроз у формі крадіжки інформації, несанкціонованого доступу до рахунку та ін. Більшість із них є ризиками та загрозами, що призводять до правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, які передбачені в Конвенції про кіберзлочинність 2001 р., ратифікованій Україною 7 вересня 2005 р.

Правовими засобами усунення таких недоліків можуть бути наступні:

– Введення заборони на відкриття рахунків без належної ідентифікації клієнта, що одночасно є правовим засобом сталих цивільних та господарських відносин і попередньою умовою для введення механізму захисту доступу до інформації на рахунку та проведення переказу коштів. Такий засіб відповідає заходам належної перевірки клієнта та збереження даних, які є рекомендацією 10 з Міжнародних стандартів з протидії відмиванню доходів та фінансуванню тероризму і розповсюдженню зброї масового знищення FATF 2012 р., згідно з якими фінансовим установам мало бути заборонено відкривати анонімні рахунки або рахунки на явно фіктивні імена.

– Використання електронних цифрових підписів, дозволить ідентифікувати клієнта банку та розподілити на підставі договору розподіл ризиків при реалізації певних загроз, що призвели до втрати коштів.

– Застосування при проведенні розрахунків фізичними особами за межами комерційного та господарського обігу, як мінім, визнаних міжнародних стандартів PSIDSS, з поступовим переходом до стандартів 3-D Secure, MasterCard SecureCode. Обов'язковість застосування подібних стандартів надання послуг слід передбачити в законодавстві України про платіжні системи.

– Встановлення вимог щодо введення обов’язкової сертифікації НБУ програмно-технічних засобів платіжних організацій та операторів послуг платіжної інфраструктури (клірингова установа, процесингова установа та інші особи, уповноважені надавати окремі види послуг у платіжній системі або здійснювати операційні, інформаційні та інші технологічні функції щодо переказу коштів). Крім того, названі господарські організації, які позиціонуються не як учасники платіжних систем, а як суб’єкти господарювання, що надають послуги фізичним особам тільки для пересилання їх вимог до платіжних організацій, мають узаконити свою діяльність для надання, фактично, фінансових послуг. Тим більше, законодавство передбачає всі підстави для внесення в реєстр тих учасників, які надають послуги, пов’язані з переказом коштів.

– Забезпечення ведення реєстру платіжних систем, систем розрахунків, учасників цих систем та операторів послуг платіжної інфраструктури, що віднесено до функцій НБУ відповідно до п. 28 ч. 1 ст. 7 Закону України “Про Національний банк України”. Але у відповідному реєстрі на сайті НБУ відсутні оператори послуг платіжної інфраструктури. Їх внесення у відповідний реєстр буде відповідати принципу внесення в реєстр усіх фінансових установ та підкреслить виконання функцій держави при реалізації грошово-кредитної політики. Таке регулювання буде відповідати також наведеним стандартам FATF, а саме рекомендації 14, яка передбачає необхідність вживання заходів країнами для забезпечення того, щоб фізичні чи юридичні особи, які надають послуги з переказу коштів або цінностей, мали ліцензію, або були зареєстрованими та були об’єктом ефективної системи моніторингу. Також, додатково, необхідно визначитися з переліком операторів послуг платіжної інфраструктури, які повинні бути враховані в переліку суб’єктів первинного фінансового моніторингу згідно зі ст. 5 Закону України “Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, або фінансуванню тероризму”.

~~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~~

ДЕЯКІ АСПЕКТИ ПРАВОВОГО ЗАХИСТУ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ ТА КОМЕРЦІЙНОЇ ТАЄМНИЦІ

Мозальова М.В., *кандидат юридичних наук*

Кожний суб’єкт господарювання знайомий з явищем конкурування на ринку однакових або схожих робіт та послуг. На разі, погіршення економічних умов у країні відобразилось на більшості верств населення, що призвело до зниження рівня платоспроможності широкого пласту споживачів. Це дзеркально відобразилось на підприємницькій діяльності, де встановились ще жорсткіші правила існування на ринку між конкуруючими підприємцями.

Процес зайняття підприємницькою діяльністю завжди має певну унікальну складову, що є основою для реалізації комерційної мети. Сюди можна відносити найрізноманітнішу інформацію – від специфічного технологічного процесу виробництва продукції до маркетингових досліджень, не стандартних рекламних заходів та напрацьованої клієнтської бази. Досвід суб’єктів господарювання, втілений в унікальну інформацію, може бути захищений за допомогою правових механізмів різними шляхами. Підприємець може зареєструвати торгову марку, запатентувати власний процес виробництва, промисловий зразок або захистити свої права на конфіденційну інформацію, уклавши угоду про нерозголошення комерційної таємниці, зробивши відповідні застереження у контракті, звернутись до суду з вимогою про компенсацію шкоди, завданої внаслідок розголошення інформації, віднесеної до конфіденційної або комерційної таємниці.

Так, Закон України “Про захист від недобросовісної конкуренції” від 07.06.96 р. відносить до протиправних дій: неправомірне збирання комерційної таємниці, розголошення комерційної таємниці, схилення до розголошення комерційної таємниці, неправомірне використання комерційної таємниці.
~~~~~~~~~~~~~~

Стаття 164^3 Кодексу України про адміністративні правопорушення встановлює відповідальність за отримання, використання, розголошення комерційної таємниці, а також іншої конфіденційної інформації з метою заподіяння шкоди діловій репутації або майну іншого підприємця.

Відповідно виокремлюється два різновиди інформації: комерційна таємниця та конфіденційна інформація. Їх співвідношення можна охарактеризувати як загальне до складової частини, де конфіденційна інформація являє собою загальне поняття – інформації з обмеженим доступом для широкого загалу про діяльність суб’єкта господарювання, а комерційна таємниця – це частка цього поняття, що стосується внутрішнього процесу виробництва та продажу товарів, специфіки надання послуг.

Але на практиці ці поняття зазвичай не розрізняються. Суб’єкти господарювання на власний розсуд відносять ту чи іншу інформацію до такої, що має обмежений доступ, часто змішуючи ці поняття. Проте, узагальнивши коло суб’єктів, що контактують з інформацією підприємців, можна виокремити дві основні групи – контрагенти та працівники. За ознакою споживачів інформації можна здійснити розмежування інформації.

Договірні відносини полягають, як правило, у закріпленні прав та обов’язків сторін щодо виконання умов договору. Укладений договір є, скоріше, наслідком реалізації підприємницької діяльності. Під час укладення контракту сторони як правило мають доступ до інформації, що не виходить за межі умов договору. Відповідно контракт має містити положення, що обмежують доступ до інформації, викладеної в договорі, осіб, які не є сторонами за цим договором.

У практиці укладання договорів поширеним є наступне формулювання: “цей договір і вся інформація, яка пов’язана з ним, вважається конфіденційною інформацією. Сторони зобов'язується не розкривати конфіденційну інформацію третім особам протягом строку дії договору, а також протягом трьох років після його припинення”. Строк у три роки заздалегідь обумовлений особливостями позовної давності на порушення податкового законодавства. Але одразу слід зазначити, що дане договірне застереження не позбавляє органи податкової інспекції права на витребування від контрагентів інформації про угоду, включаючи всі документи бухгалтерського обліку.

Включаючи до договору положення про конфіденційну інформацію, сторони надають собі можливість звернутись до суду з вимогою про відшкодування шкоди, завданої розголошенням умов контракту. Здебільшого це може стосуватись компенсації упущеної вигоди від угод, що могли бути укладені, але укладені не були в результаті розголошення такої інформації.

На відміну від конфіденційної інформації, що може бути захищена лише за умови визначення у договірних відносинах, комерційна таємниця захищається з боку законодавства нормами кримінального, адміністративного та трудового права. Визнання комерційної таємниці об’єктом інтелектуальної власності надає можливість захисту такої інформації в межах цивільного та господарського судового процесу.

Відповідно, комерційна таємниця, хоч і входить до кола конфіденційної інформації, проте захищається законодавцем більш жорсткими заходами. Зважаючи на значну різницю відповідальності за розголошення цих двох видів інформації, слід чітко визначити інформацію, що входить до комерційної таємниці. Стаття 36 Господарського кодексу України надає можливість віднести до комерційної таємниці відомості, пов’язані з виробництвом, технологією, управлінням, фінансовою та іншою діяльністю суб’єкта господарювання, що не є державною таємницею, розголошення яких може завдати шкоди інтересам суб’єкта господарювання. Проте затвердження чіткого переліку комерційної таємниці залишається на розсуд самого суб’єкта господарювання.

На практиці до комерційної таємниці, окрім опису самої технології виробництва, як правило, відноситься: рівень заробітної плати всіх робітників; дані про постачальників і покупців; інформація про переговори; маркетингові дослідження; дані про розрахунок відпускних цін; розміри знижок; калькуляція витрат виробництва підприємства; структури цін; рівень прибутку; плани розвитку підприємства та його інвестицій; організаційна структура

підприємства; характер виробництва; організація праці на підприємстві; відомості, що розкривають планові та фактичні показники фінансового плану; майновий стан; обороти; банківські операції; відомості про фінансові операції; банківські зв’язки; специфіка міжнародних розрахунків із закордонними фірмами; планові та звітні дані по валютних операціях; стан банківських рахунків підприємства; рівень виручки; рівень доходів.

Виходячи із наведеного вище критерію розмежування інформації, працівник, що знаходиться у трудових відносинах із роботодавцем як правило є саме тією особою, що в силу своїх службових обов’язків має доступ до комерційної таємниці. Відповідно працівник має бути ознайомлений з переліком інформації, що відноситься до комерційної таємниці та має отримати чіткі установки, які дії свідчать про розголошення комерційної таємниці. Наприклад, працівник зобов’язується не передавати (усним, письмовим іншими способами) третім особам та не розголошувати публічно відомості, що, відповідно до затвердженого роботодавцем переліку, становлять комерційну таємницю без письмової згоди на те уповноваженої особи.

Проте в процесі виконання своєї трудової функції працівники не рідко проходять спеціальне навчання, що здійснюється на базі напрацьованого досвіду суб’єкта господарювання. У результаті робітник отримує певні навички, які після припинення трудових відносин із роботодавцем можуть використовуватись колишнім робітником для зайняття самостійною підприємницькою діяльністю. Виникає ситуація коли роботодавець, намагаючись запобігти поширенню конкуренції на ринку, вдається до поширення комерційної таємниці на отримані навички робітника та навіть зобов’язує колишнього працівника не займатись аналогічним видом діяльності протягом певного строку після звільнення. Це, звісно, є неправомірним обмеженням прав людини та не може входити до комерційної таємниці підприємства.

~~~~~~~~~~~~ * * * ~~~~~~~~~~~~

ПРАВОВІ ПИТАННЯ СТВОРЕННЯ СИСТЕМИ ІНФОРМАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ОПТОВИХ РИНКІВ СІЛЬСЬКОГОСПОДАРСЬКОЇ ПРОДУКЦІЇ

Уркевич В.Ю., *доктор юридичних наук, професор*

Однією з важливих інституцій аграрного ринку України, що забезпечує організацію збуту виробленої сільськогосподарської продукції, є оптові ринки сільськогосподарської продукції, мережа яких у даний час створюється в Україні.

На сьогодні свідоцтва оптових ринків сільськогосподарської продукції видано 11-ом юридичним особам, а загалом протягом найближчих декількох років такі ринки планують створити у кожній області України. Зважаючи на актуальність характеристики правових питань створення та функціонування названих оптових ринків, у даній доповіді зупинимося на правових аспектах створення системи інформаційного забезпечення діяльності оптових ринків сільськогосподарської продукції.

Статтею 1 Закону України “Про оптові ринки сільськогосподарської продукції” від 25.06.09 р. № 1561-VI (далі – Закон) визначено, що оптовий ринок сільськогосподарської продукції – це юридична особа, предметом діяльності якої є надання послуг, що забезпечують здійснення оптової торгівлі сільськогосподарською продукцією, і якій в установленому порядку надано статус такого оптового ринку. Зрозуміло, що названий суб’єкт виступає організатором при укладенні відповідних договорів купівлі-продажу оптових партій сільськогосподарської продукції. У зазначених договорах серед іншого обов’язково зазначаються такі їх істотні умови, як кількість сільськогосподарської продукції, що реалізується, та її ціна. Укладення таких договорів на оптових ринках без налагодженої системи інформаційного забезпечення є просто неможливим.

З приводу формування системи інформаційного забезпечення діяльності оптових ринків сільськогосподарської продукції названий Закон містить окремі приписи, вміщені у його ст. 15, згідно яких система створюється з метою постійного і повного забезпечення оптових ринків
~~~~~~~~~~~~

сільськогосподарської продукції та операторів таких ринків інформацією про кон’юнктуру ринку відповідної продукції, тобто про наявні пропозиції та попит на аграрну продукцію та рівень цін на неї. З цією метою у структурі центрального органу виконавчої влади, що реалізує державну аграрну політику, політику у сфері сільського господарства (тобто Міністерства аграрної політики та продовольства України), створюється система інформаційного забезпечення діяльності оптових ринків сільськогосподарської продукції.

З метою наповнення названої інформаційної системи, на оптові ринки сільськогосподарської продукції покладається обов’язок надавати названому Міністерству у визначених ним порядку та обсягах інформацію про кон’юнктуру відповідного ринку сільськогосподарської продукції. Вважаємо, що йдеться про інформацію як про фактично укладені протягом певного проміжку часу договори оптової купівлі-продажу сільськогосподарської продукції, так і про наявну пропозицію такої продукції.

Формування названої інформаційної системи має важливе значення для організації функціонування усього аграрного ринку. Адже на її показники, що відображають рівень гуртових цін на окремі види сільськогосподарської продукції, можуть орієнтуватися не лише її виробники, а й закупівельні та переробні підприємства, а також її кінцеві споживачі. Зважаючи на це, Закон містить припис, що відомості системи інформаційного забезпечення діяльності оптових ринків сільськогосподарської продукції є відкритими, що забезпечується їх систематичною публікацією в офіційних друкованих та електронних виданнях (бюлетенях, збірниках), поширенням засобами масової інформації, в тому числі в мережі Інтернет на веб-сайті Міністерства аграрної політики та продовольства України, а також безпосереднім їх наданням заінтересованим органам та особам.

Важливим в аспекті створення та функціонування системи інформаційного забезпечення діяльності оптових ринків сільськогосподарської продукції є те, що відповідальним за це є Міністерство аграрної політики та продовольства України, а створюється та підтримується розглядувана інформаційна система за рахунок коштів Державного бюджету України. Такі приписи законодавства фактично можна розглядати як одну з форм державної підтримки створення та функціонування оптових ринків сільськогосподарської продукції.

З метою реалізації розглянутих положень, ст. 15 названого Закону прямо встановлює, що Міністерство аграрної політики та продовольства України має затвердити Положення про систему інформаційного забезпечення діяльності оптових ринків сільськогосподарської продукції, яке, незважаючи на набрання Законом чинності ще 1 січня 2010 року, до цього часу так і не затверджене.

Викладене дозволяє підсумувати, що формування та належне функціонування системи інформаційного забезпечення діяльності оптових ринків сільськогосподарської продукції має важливе значення для функціонування національного ринку аграрної продукції. Потребує невідкладного затвердження Міністерством аграрної політики та продовольства України Положення про систему інформаційного забезпечення діяльності оптових ринків сільськогосподарської продукції.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~

ПРАВО НА ІНФОРМАЦІЮ В АКЦІОНЕРНИХ ВІДНОСИНАХ: ПРОБЛЕМИ РЕАЛІЗАЦІЇ ТА ЗАХИСТУ

Вінник О.М., *доктор юридичних наук, професор, чл.- кор. НАПрН України*

Інформаційні війни – поширене явище в сучасному світі, що має місце на всіх рівнях – від міжнародного (інформаційна війна Російської Федерації проти України на забезпечення напівприхованої агресії, в результаті якої було окуповано Крим та тероризується Схід України) до локального. Прикладом останнього є корпоративні конфлікти, що виникають в акціонерних
~~~~~~~~~~~~~

товариствах (АТ) з приводу не лише майна та можливості контролювати АТ, а й такого важливого ресурсу, як інформація. І хоча небезпека подібних конфліктів зазвичай менша, ніж міжнародних – як політичних, так і економічних, проте і вони можуть набувати характеру транснаціональних (зокрема, в холдинговій групі акціонерних товариств, розташованих на території різних держав, що стає досить поширеним явищем в сучасному світі).

В корпоративних відносинах, що виникають в акціонерних товариствах між безпосередніми їх учасниками (товариством, його засновниками та акціонерами, органами управління та контролю АТ) та опосередкованими учасниками (потенційні учасники АТ, що планують придбати його акції або уклали договір на придбання додаткових акцій, кредитори товариства, уповноважені органи держави, саморегулівні організації) стосовно корпоративних благ (майна товариства, управління його справами, інформації товариства) важливу роль відіграє право на отримання відповідної інформації, без володіння якою досить проблематично впливати на вирішення будь-яких питань, пов’язаних із зазначеними благами.

Можливість доступу до інформації забезпечується закріпленням в законі та/або статуті чи інших локальних документах АТ права на її отримання за вищезазначеними учасниками акціонерних відносин, кореспондуючих обов’язків інших учасників цих відносин щодо надання відповідної інформації, відповідальністю за порушення таких прав чи невиконання обов’язків. Разом з тим, законодавець часом непослідовно регулює інформаційні відносини стосовно акціонерних товариств. Так, згідно із ст. 12 Закону України “Про акціонерні товариства” засновники акціонерного товариства (далі – АТ) несуть солідарну відповідальність за пов'язаними з його заснуванням зобов’язаннями, що виникли до його державної реєстрації. При цьому інформація про такі зобов’язання товариства має бути відображена у його статуті. Останнє відповідає за пов'язаними з його заснуванням зобов’язаннями засновників тільки у разі схвалення їх дій загальними зборами акціонерів, які мають бути проведені протягом шести місяців після державної реєстрації товариства.

Закріплюючи ці положення, законодавець уникає питання про наслідки невідображення в статуті товариства вищезгаданої інформації, хоча це може мати наслідки для товариства, його акціонерів/потенційних акціонерів та/або кредиторів. Так, після державної реєстрації АТ склад його акціонерів може істотно змінитися (адже законодавець не зобов’язує засновників бути держателем акцій протягом певного строку, як це було передбачено для відкритих акціонерних товариств ч. 1 ст. 30 Закону України “Про господарські товариства”). Потенційні акціонери та нові акціонери повинні володіти інформацією про угоди засновників (як схвалені товариством, так і не схвалені), адже це може позначитися на їх можливостях щодо реалізації права на отримання дивідендів (схвалення угод засновників на значні суми може вплинути на фінансовий стан АТ, якщо такі угоди виявилися збитковими). Новим акціонерам можливість отримання інформації про угоди засновників необхідна, оскільки їм доведеться брати участь у прийнятті рішення про схвалення таких угод і, відповідно, про відповідальність товариства за схваленими угодами засновників, що може позначитися на платоспроможності АТ. Тому, з метою захисту інтересів акціонерів, що не брали участь у заснуванні товариства, доцільно закріпити правові механізми, що забезпечують їх захист у разі відсутності в статуті відомостей про угоди засновників або викривлення таких відомостей. Це може бути норма про солідарну відповідальність засновників за їх зобов’язаннями, що виникли в процесі заснування акціонерного товариства і були схвалені загальними зборами, проте не відображені в статуті товариства.

Разом з тим, можливі випадки ігнорування закріпленого Законом України “”Про акціонерні товариства” обов’язку надання інформації цим не обмежується, що потребує окремого дослідження.

Однак, навіть розглянутий випадок свідчить про важливість інформації для реалізації акціонерами їх корпоративних прав (насамперед, класичних щодо участі в розподілі прибутку, в управління товариством, розподілі його майна у разі ліквідації), у зв’язку з чим доцільно право на інформацію закріпити як одне з основних корпоративних прав, скорегувавши відповідним чином положення актів законодавства, що закріплюють ці права: Господарського кодексу України (ст. 167), Закону України “Про акціонерні товариства” (п. 8 ст. 2).

Не варто ігнорувати і досвід США: прагматичне ставлення до підприємницьких корпорацій (аналог АТ), для яких притаманні суто ринкові засади управління, віддзеркалені в принципі голосування на загальних зборах “одна акція – один голос”, компенсується закріпленням за акціонерами (в т.ч. міноритарними) низки додаткових прав, серед яких – право на подання похідних (в інтересах АТ) позовів (статті 7.40-7.47). Це дозволяє акціонерам, які не мають реальних можливостей впливати на прийняття рішення на загальних зборах, захищати АТ, а відтак – і свої інтереси у разі завдання шкоди товариству контролюючими акціонерами та пов’язаними з ними особами, які мають вирішальний вплив на прийняття рішень органами АТ (в т.ч. щодо захисту своїх інтересів у разі завдання шкоди чи загрози її завдання в результаті укладення угод на значні суми, з елементами заінтересованості тощо).

Український законодавець, прийнявши в 2008 р. Закон України “Про акціонерні товариства”, закріпив один випадок наявності у акціонерів права на подання похідних позовів – у разі порушення порядку вчинення правочинів, щодо яких має місце заінтересованість (ч. 2 ст. 72), проте в 2011 р. необґрунтовано скасував ці положення (ст. 55), що відповідає інтересам лише крупних акціонерів.

Відтак, доцільно закріпити в Законі України “Про акціонерні товариства” низку заходів, спрямованих на реалізацію акціонерами права на інформацію, в т.ч. : (1) включити до основних корпоративних прав право на інформацію; (2) передбачити негативні наслідки для учасників корпоративних відносин у разі невиконання ними обов’язків щодо надання, фіксації у статуті, інших документах АТ передбаченої законом інформації (на зразок вище запропонованих); (3) відновити право акціонерів на подання похідних позовів, передбачивши можливість їх подання не лише у разі порушення порядку вчинення правочинів, щодо яких має місце заінтересованість, а й у разі порушення встановленого законом та статутом АТ порядку надання акціонерам необхідної інформації при прийнятті товариством юридично значущих рішень, якщо їх реалізація завдала шкоди товариству.

~~~~~~~~~~~~ * * * ~~~~~~~~~~~~

МІЖНАРОДНО-ПРАВОВА ОЦІНКА ЗАБОРОНИ РЕТРАНСЛЯЦІЇ РОСІЙСЬКИХ ТЕЛЕРАДІОМОВНИХ КАНАЛІВ НА ТЕРИТОРІЇ УКРАЇНИ

Пазюк А.В., *кандидат юридичних наук*

Агресія по відношенню до України з боку Російської Федерації, яка розпочалась задовго до схвалення 1 березня 2014 року Радою Федерації Федеральних Зборів звернення Президента РФ В.В. Путіна про введення “обмеженого військового контингенту” збройних сил Росії на територію України, супроводжувалась потужним інформаційним супроводом. Російські телеканали супутникового мовлення, що ретранслювались у багатоканальних телемережах на території України, поширювали програми з аудіовізуальною інформацією, яка була спрямована на підрив конституційного ладу в Україні.

Національна рада України з питань телебачення і радіомовлення у березні 2014 року звернулась із позовною заявою до дистриб’ютора російських програм – товариства з обмеженою відповідальністю “Торсат” щодо тимчасового припинення ретрансляції в багатоканальних телемережах іноземних програм: “Первый канал. Всемирная сеть” (ОАО “Первый канал”), “РТР-Планета”, “Российский Информационный канал “Россия-24” (“Всероссийская государственная телевизионная и радиовещательная компания”), “НТВ Мир” (ОАО “Телекомпания НТВ”).

Ухвалою Окружного адміністративного суду міста Києва від 25 березня 2014 р. було задоволено клопотання Національної ради з питань телебачення та радіомовлення про вжиття заходів забезпечення адміністративного позову – дистриб’ютора та провайдерів програмних послуг суд зобов’язав тимчасово припинити ретрансляцію в багатоканальних телемережах на території України вищезазначених іноземних програм до вирішення справи по суті.
~~~~~~~~~~~~

У зв’язку з тим, що Україна є учасницею Міжнародного пакту про громадянські та політичні права (стаття 19), Конвенції Ради Європи про захист прав людини та основних свобод (стаття 10), а також Європейської конвенції про транскордонне телебачення (стаття 4), що передбачають свободу вираження незалежно від кордонів, актуальним є надання оцінки відповідності прийнятого судом процесуального рішення міжнародно-правовим зобов’язанням України.

Заборона інформаційної агресії випливає із загального міжнародно-правового принципу незастосування сили і погрози силою. Згідно з пунктом 4 статті 2 Статуту ООН – “всі Члени Організації Об’єднаних Націй утримуються в їхніх міжнародних відносинах від загрози силою або її застосування як проти територіальної недоторканності або політичної незалежності будь-якої держави, так і яким-небудь іншим чином, несумісним з цілями Об’єднаних Націй”. На 29-й сесії Генеральної Асамблеї ООН була прийнята резолюція 3314 від 14.12.74 р., в якій дається визначення агресії: “Агресією є застосування збройної сили державою проти суверенітету, територіальної недоторканності або політичної незалежності іншої держави, або яким-небудь іншим чином, несумісним із Статутом ООН, як це зазначено в цьому визначенні”.

Стаття 20 Міжнародного пакту про громадянські і політичні права покладає на держави обов’язок заборонити пропаганду війни, виступи на користь національної, расової чи релігійної ненависті, що являє собою підбурювання до дискримінації, ворожнечі або насильства. Вміщені в цій нормі приписи є позитивними зобов’язаннями держави по відношенню до міжнародного співтовариства в цілому, що виключає можливість застосування будь-яких винятків.

У Зауваженнях загального порядку № 11, прийнятих Комітетом ООН з прав людини в 1983 році, наголошується, що заборона, що згадується в пункті 1 статті 20 Пакту, “поширюється на всі види пропаганди, здійснюваної з метою погрози або акту агресії або порушення миру всупереч Статуту організації Об’єднаних Націй”.

Врегулювання на міжнародно-правовому рівні питань свободи інформації в радянській доктрині міжнародного права розглядалося як викликане “безпосереднім, органічним зв’язком з головною проблемою сучасності – завданням підтримки миру і безпеки народів”. Ця теза знайшла своє втілення в ініційованих СРСР Резолюції 110 (II) другої сесії Генеральної Асамблеї ООН “Заходи, які повинні були застосовані проти пропаганди та підпалювачів нової війни” від 3 листопада 1947 року та Резолюції 127 (II) “Хибна або спотворена інформація” від 15 листопада 1947 року. Зокрема, у першій із зазначених Резолюцій, Генеральна Асамблея засудила будь-яку форму пропаганди, що має за мету або що може створити або посилити загрозу миру.

У Декларації про посилення ефективності принципу відмови від загрози силою або її застосування в міжнародних відносинах, ухваленій в Резолюції 42/22 Генеральної Асамблеї від 18 листопада 1987 року, вказується, що з метою дотримання принципу незастосування сили та загрози силою “у відповідності з цілями і принципами Організації Об’єднаних Націй держави зобов’язані утримуватися від пропаганди агресивних війн”.

Втручання Російською Федерацією у внутрішні справи України шляхом поширення закликів до зміни територіального устрою нашої держави порушує у загальній формі принцип невтручання у справи, що входять у внутрішню компетенцію держав, зафіксований у п. 7 статті 2 Статуту ООН. Свою конкретизацію цей принцип отримав у Декларації про принципи міжнародного права 1970 р., Декларації ООН щодо неприпустимість втручання у внутрішні справи держав, про захист їх незалежності і суверенітету 1965 року, Заключному акті НБСЄ 1975 р.

У Декларації 1965 року вказується, що “пряме втручання, підривні дії і всі форми непрямого втручання суперечать цим принципам і становлять, отже, порушення Статуту Організації Об’єднаних Націй”. Заборона підбурювання до порушення правопорядку та війни проти іншої держави шляхом використання радіомовлення є не лише правом, а й міжнародними зобов’язанням Російської Федерації та України.

Міжнародна конвенція про використання радіомовлення в інтересах миру 1936 року, яка вступила в силу для СРСР 4 квітня 1983 року, передбачає обов’язок держав забороняти і негайно припиняти на своїх територіях передачу будь-яких програм, які, на шкоду доброму міжнародному взаєморозумінню, за своїм характером спрямовані на підбурювання населення будь-якої території до дій, несумісних з внутрішнім порядком або безпекою будь-якої території

держави (стаття 1). Держави зобов’язались забезпечити, щоб передачі зі станцій, що знаходяться на їхніх територіях, не становили підбурювання до війни проти іншої держави або до дій, що можуть до неї привести (стаття 2).

Відповідно до статті 9 Конституції України Міжнародна конвенція про використання радіомовлення в інтересах миру є частиною національного законодавства України. А отже застосування обмежень свободи вираження шляхом заборони ретрансляції програм передбачено національним законодавством у розумінні ч. 2 статті 10 ЄКПЛ.

Застосування обмежень (заборони) щодо передачі програм, які несуть загрозу національним інтересам України, територіальній цілісності, безпеці і добробуту громадян, є міжнародно-правовим зобов’язанням України у сфері захисту прав і свобод людини. Відповідно до Загальної декларації прав людини, проголошеної Генеральною Асамблеєю ООН 10 грудня 1948 року, при здійсненні своїх прав і свобод кожна людина повинна зазнавати тільки таких обмежень, які встановлені законом виключно з метою забезпечення належного визнання і поваги прав і свобод інших та забезпечення справедливих вимог моралі, громадського порядку і загального добробуту в демократичному суспільстві (стаття 29).

Відповідно до статті 1 Європейської Конвенції про захист прав людини та основоположних свобод від 4 листопада 1950 року, Україна як її учасниця гарантує кожному, хто перебуває під її юрисдикцією, права і свободи, передбачені Конвенцією. Стаття 10 Конвенції гарантує кожному право на свободу вираження поглядів. Це право включає свободу дотримуватися своїх поглядів, одержувати і передавати інформацію та ідеї без втручання органів державної влади і незалежно від кордонів. Проте здійснення цих свобод, оскільки воно пов’язане з обов’язками і відповідальністю, може підлягати таким формальностям, умовам, обмеженням або санкціям, що встановлені законом і є необхідними в демократичному суспільстві в інтересах національної безпеки, територіальної цілісності або громадської безпеки, для запобігання заворушенням чи злочинам, для охорони здоров’я чи моралі, для захисту репутації чи прав інших осіб, для запобігання розголошенню конфіденційної інформації або для підтримання авторитету і безсторонності суду.

Європейський суд з прав людини у своїй практиці підтвердив певну свободу держав при вирішення питання про необхідність обмеження права на свободу вираження поглядів. Проте необхідність обмеження мусить бути переконливо обґрунтована нагальною потребою і бути передбачена національним законодавством.

Враховуючи обставини невідворотної загрози національним інтересам України внаслідок рутинного і постійного поширення російськими телерадіомовними каналами пропаганди, спрямованої на розпалювання війни, існувала нагальна потреба у забороні ретрансляції цих каналів на території України на підставі положень Міжнародної конвенції про використання радіомовлення в інтересах миру 1936 року.

Проте чи є достатніми правові підґрунтя для обмежень трансляції програм за законодавством України? В обґрунтування прийнятого процесуального рішення суд навів посилання на положення статті 3 Закону України “Про інформацію”, якою визначено, що основними напрямами державної інформаційної політики є, зокрема, забезпечення рівних можливостей щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації, забезпечення інформаційної безпеки України. Відповідно до статті 28 Закону України “Про інформацію” інформація не може бути використана для закликів до повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості, розпалювання міжетнічної, расової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини.

Також суд застосував статтю 42 Закону України “Про телебачення та радіомовлення”, відповідно до якої ретрансляція телерадіопрограм та передач, зміст яких відповідає вимогам Європейської конвенції про транскордонне телебачення, на території України не обмежується. Суб’єкт господарювання, який перебуває під юрисдикцією України, має на меті здійснювати ретрансляцію і отримав на це дозвіл від правовласника (виробника), який не підпадає під юрисдикцію країни, що входить до Європейського Союзу, або країни, яка ратифікувала

Європейську конвенцію про транскордонне телебачення, зобов’язаний адаптувати зміст призначених для ретрансляції програм до вимог законодавства України.

Відповідно до статті 4 Європейської конвенції про транскордонне телебачення, ратифікованої із заявою та застереженням Законом України від 17.12.08 р. № 687-VI (687-17), сторони забезпечують свободу самовираження й інформації відповідно до статті 10 Конвенції про захист прав людини і основоположних свобод, гарантують свободу прийому й не обмежують ретрансляцію на своїх територіях програмних послуг, які відповідають умовам цієї Конвенції.

Посилався суд також на статті 59 і 72 Закону України “Про телебачення і радіомовлення”, якими передбачається, що телерадіоорганізації зобов’язані дотримуватись Законів України та вимог ліцензії, а у разі порушення законодавства про телебачення і радіомовлення юридичними або фізичними особами Національна рада звертається до суду для усунення цих порушень у визначеному законодавством порядку та в її повноваження входить подання до суду справи про анулювання ліцензії на мовлення».

Проте чинне законодавство України не передбачає такого механізму захисту як тимчасова заборона на ретрансляцію програм за позовом Національної ради з питань телебачення і радіомовлення. А отже для дотримання вимог частини 2 статті 10 Європейської Конвенції про захист прав людини і основоположних свобод щодо наявності відповідних положень національного законодавства, якими визначаються підстави та порядок застосування обмежень свободи вираження, Україні слід прийняти відповідні зміни до законодавства.

Крайнім інструментом для реагування на інформаційну агресію можуть бути заходи, які передбачені в статті 15 Європейської Конвенції про захист прав людини та основоположних свобод. Під час війни або іншої суспільної небезпеки, яка загрожує життю нації, Україна може вживати заходів, що відступають від її зобов’язань за цією Конвенцією, виключно в тих межах, яких вимагає гострота становища, і за умови, що такі заходи не суперечать іншим її зобов’язанням згідно з міжнародним правом. Україна може відступити від своїх зобов’язань, крім тих, що містяться у ч. 2 статті 15 (стаття 10 не згадується), але при цьому зобов’язана поінформувати Генерального секретаря Ради Європи про вжиті нею заходи і причини їх вжиття. Вона також повинна повідомити Генерального секретаря Ради Європи про час, коли такі заходи перестали застосовуватися, а положення Конвенції знову застосовуються повною мірою.

Сподіваємось, що до таких кроків як відступ від зобов’язань за Конвенцією про захист прав людини та основоположних свобод Україна не вдасться, а для забезпечення національних інтересів в інформаційній сфері будуть запровадженні ефективні механізми інформаційного спротиву. Саме на це спрямоване й рішення Ради національної безпеки та оборони “Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України” від 28.04.14 р., уведене в дію Указом Президента України від 01.05.14 р. № 449/2014.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~

РЕАКЦІЯ РОЗВАЖАЛЬНОГО КОМПОНЕНТУ УКРАЇНСЬКОЇ ПРЕСИ НА ДЕЗІНФОРМАЦІЮ РОСІЙСЬКИХ ЗМК

Михайлюта О.О., аспірант кафедри історії журналістики
Інституту журналістики КНУ імені Тараса Шевченка

Дезінформація, яку ретранслювали російські мовники останні місяці про події в Україні, спричинила резонанс в українському суспільстві. У соціальних мережах активно тиражуються вдалі дотепні зображення і вислови на складні події сьогодення, зокрема реагує суспільство і мас-медіа на інформаційну війну Росії. Зараз в Інтернеті з’явилось безліч анекдотів, карикатур на гострі соціальні теми, гумор спирається на події сьогодення. На телебаченні це випуски студії “95 квартал” “Вечірній квартал”, “Казкова Русь”, фотожаби в соціальних мережах та на порталах, зокрема ряд зображень із сайтів “Буквоїда”, “Цензор.Нет”, “ТвІ”, “ТСН”, “Обозреватель”, “Главред”, “Gazeta.ua”. Активізацією і актуальною необхідність сатири на
~~~~~~~~~~~~~

теперішній момент можна пояснити також і те, що редакція газети “Газета по-українськи”, журналу “Країна” і сайт “Gazeta.ua” проводять перший міжнародний конкурс карикатур “Майдан”. Громадське об’єднання “Телекритика” проводить конкурс журналістських матеріалів про інформаційні війни. “Телекритика” готує спеціальний приз за кращий демотиватор, графічний колаж (“фотожаба”) або інфографіку.

На сьогодні тимчасово заборонена ретрансляція на території України чотирьох російських каналів – “Первый канал. Всемирная сеть”, “РТР-Планета”, “Россия-24”, “НТВ-Мир”. Втім, українська аудиторія має доступ до російських ЗМІ завдяки Інтернету (до прикладу сайт російського агентства РИА-новости можна переглядати і в Україні). Національна рада з питань телебачення і радіомовлення подала на розгляд суду понад 40 сторінок цитат – витягів із програм, в яких, за узагальненнями фахівців регулятора, містилися заклики до національної ворожнечі, порушення територіальної цілісності України, перекручення наявної інформації, маніпуляції свідомістю громадян. Варто проаналізувати, як інформаційна агресія Росії відобразилась у пресі, зокрема в її розважальному компоненті.

Згідно з твердженням теоретика соціальних комунікацій З. Партико, мета інформаційної війни – створити хибну, фіктивну реальність. Вона створена в Росії, там, де немає альтернативних джерел інформації, також в Криму та на Сході України, де озброєні бойовики вимкнули українське мовлення. Як зазначає науковець З. Партико, під час проведення інформаційної війни населення не відчуває, що його піддають інформаційній атаці. Проте населення відчуває дискомфорт, оскільки від нього вимагають зміни світогляду й певних дій . Жителі України ж розуміють і усвідомлюють, що повідомлення російських ЗМІ стосовно подій в Україні часто неправдиві чи недостовірні. Свою обурення українці висловлюють у соціальних мережах, реагує на інформаційну агресію й аналітична преса, яка окрім статей на політичні і соціальні теми, містить розважальний компонент (карикатури, анекдоти). Крім того, військова агресія та брехня також відображена у гуморі і сатирі. Зокрема, на сайті “Українського тижня” регулярно розміщуються фотожаби та карикатури, останні на тему військової агресії Росії – 20 зображень (за 3 березня 2014 р.) . Найпопулярнішим різновидом зображальної сатири на сьогодні є так звана фотожаба – це графічна карикатура, шарж; сленгова назва різновиду фотомонтажу, переробки зображення за допомогою растрового або векторного графічного редактора із застосуванням спецефектів комп’ютерного дизайну. Рідше сленгове “жаба” використовується як вираз недовіри по відношення до змісту поста або коментаря, в тому числі не графічного, а текстового. Ці жанри є похідними від традиційної карикатури.

Дослідниця історії української преси О. Хобта влучно зазначає, що “розквіт карикатури був закономірним явищем у час війни та революції, адже вона – найдієвіший засіб боротьби”.

Сміхова реакція на складні події виконує важливу функцію у соціальних комунікаціях, особливо в нестабільний час. Зокрема, науковці визначили афективно-комунікативну функцію. Вона належить до емоційної сфери особистості, визначає її ставлення до явищ навколишнього світу. Весь спектр людських емоцій виникає і розвивається в процесі спілкування людей. Потреба у спілкуванні часто виникає у зв’язку з необхідністю змінити свій емоційний стан. У процесі спілкування людей може змінитися інтенсивність емоційних станів партнерів: відбувається зближення цих станів, або їх поляризація, взаємне посилення або ослаблення. Людина в спілкуванні може емоційно розрядитися або, навпаки, підсилити емоційну напруженість.

Отже, порушення правил інформування суспільства російськими мас-медіа не лишилось не поміченим. На вищому державному рівні вжито заходів стосовно мовників, які порушують українське законодавство, відреагувало на дезінформацію і суспільство (варто констатувати, що це та частина, яка упродовж тривалого часу мала доступ до українських джерел інформації). Мас-медіа публікують, окрім аналітичних статей на тему інформаційної війни, ще й розважальні матеріали (фотожаби, карикатури, анекдоти). Розважальний компонент виконує важливу в нестабільний час функцію – висміювання і засудження інформаційного ворога, має на меті змінити інтенсивні емоційні стани – тривоги, страху на позитивні завдяки засобам гумору та сатири.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~