Тетяна БОРИСЕНКО
викладач кафедри адміністративного права, процесу та адміністративної діяльності Дніпропетровського державного університету внутрішніх справ (м. Дніпро, Україна)

РОЛЬ ІНФОРМАЦІНОЇ БЕЗПЕКИ В УМОВАХ РОЗВИТКУ ІНФОРМАТИЗАЦІЇ ТА ГЛОБАЛІЗАЦІЇ

Сьогодні світ перебуває на новому етапі свого розвитку – інформаційному. Недарма сучасну епоху називають «ерою інформації» або «інформаційним суспільством», що характеризується домінуючою роллю інформації та знань, створенням глобального інформаційного простору, в якому завдяки високорозвинутим інформаційно-комунікативним мережам і технологіям забезпечуватиметься стале економічне та соціальне зростання, вільний доступ до світових інформаційних ресурсів. За цих умов надзвичайної актуальності набуває проблема впровадження дієвої системи державного управління в процесі переходу до високотехнологічного інформаційного суспільства [1, с. 2].

У сучасному світі інформаційна безпека в умовах глобального інформаційного суспільства відіграє провідну роль. Суцільна інформатизація всіх сфер життя суспільства, зокрема сфери забезпечення безпеки особи, суспільства, економіки і фінансів, державної інфраструктури ставить питання про комплексний підхід до проблеми інформаційної безпеки.

Україна як і абсолютна більшість країн світу все більше включається в процес глобалізації. Забезпечення міжнародної безпеки стає однією з глобальних загальнолюдських проблем. З огляду на зростаючу взаємозалежність світу в ядерну епоху, розуміння безпеки як винятково військово-стратегічної проблеми відходить у минуле. Зростає значення інформаційної, політичної та економічної безпеки як складових елементів національної безпеки, які безпосередньо пов’язані з глобалізацією [2, с. 22].

Процеси глобалізації торкаються дедалі нових сфер діяльності. Інформаційна сфера стає не тільки найважливішою сферою міжнародної співпраці, а й об’єктом суперництва. Проблеми у сфері інформаційних відносин, формування інформаційних ресурсів і користування ними загострюються внаслідок політичного й економічного протиборства держав [1, с. 2].

Входження будь-якої країни в процес глобалізації неминуче супроводжується як позитивними надбаннями, відкриттям нових можливостей, так і загрозами національній безпеці. Це, насамперед, втрата національної ідентичності та культури малочисельних народів, порушення авторських прав на інтелектуальну та промислову власність, прояви міжнародної злочинності та тероризму, зростання корупції, збільшення масштабів нелегальної міграції, торгівлі людьми, протиправного обігу зброї та наркотичних речовин, злочини в інформаційних мережах [2, с. 22].

Визнання проблем інформаційної безпеки на міжнародному рівні обумовлюється такими чинниками глобалізації:

1) більшості розвинутих країн проводиться дослідження і розроблення нової інформаційної зброї, що дозволяє здійснювати безпосередній контроль над інформаційними ресурсами потенційного супротивника, а в необхідних випадках впливати на них;

2) кардинально змінилася оцінка доктрини інформаційної безпеки в цілому і позиції більшості країн світу, які усвідомили потенціал інформаційної загрози і необхідність створення відповідного міжнародного механізму для контролю інформаційного протиборства [3, с. 39].

У сучасній науковій літературі глобальна безпека характеризується як захищеність системи взаємовідносин усієї світової спільноти від загроз дестабілізації ситуації, криз, збройних конфліктів і війн. Міжнародна безпека заснована на дотриманні всіма країнами загальновизнаних норм і принципів міжнародного права, що не допускають вирішення суперечливих та конфліктних питань за допомогою сили або загрози застосування сили [2, с. 23].

Слід визнати, що національна безпека конкретної держави та реалізація нею національних інтересів у сучасних умовах значною мірою залежать від міри захищеності та реалізації національних інтересів держав-сусідів, отримання колективних гарантій безпеки,

членства у військово-політичних та економічних блоках, тобто від глобальної та міжнародної безпеки.

На сучасному етапі світового розвитку інформація є фактором, що здатний призвести до широкомасштабних аварій, воєнних конфліктів, дезорганізації державного управління. Одним із головних пріоритетів України є прагнення побудувати орієнтоване на інтереси людей, відкрите для всіх і спрямоване на розвиток інформаційне суспільство, в якому кожен міг би створювати і накопичувати інформацію та знання, мати до них вільний доступ, користуватися і обмінюватися ними [4, с. 14].

З позицій системного аналізу інформаційної безпеки України можна виділити чотири групи інформаційно-технологічних небезпек. До першої групи відносять появу інформаційної зброї, здатної впливати на психіку людей та інформаційно-технологічну інфраструктуру держави. Діяльність окремих людей стає керованою під впливом фармакологічних та психотропних засобів, комп'ютерних банків даних та інформації.

Друга група небезпек пов'язана з використанням досягнень сучасних інформаційних технологій – махінації з банківськими операціями, комп'ютерне хуліганство, незаконне копіювання технологічних рішень.

Третя група загроз проявляється у тотальному контролі за життям, настроями, планами громадян, роботою державних установ, за населенням країни у цілому з використанням комп'ютерних систем.

Четверта група небезпек полягає у використанні інформаційних технологій у політичній боротьбі. З цим пов'язане політичне заангажування ЗМІ, чорний PR під час проведення виборчих кампаній, зосередженість інформаційних видань в руках кількох власників, відсутність незалежних ЗМІ [5, с. 93-94].

Все це свідчить про початок ери воєн «сьомого покоління» – інформаційних воєн. Це війни з використанням маніпуляцій індивідуальною та масовою свідомістю, нейролінгвістичним програмуванням, діяльність проти системи управління суперника, кібернетична, економічна боротьба, боротьба з використанням хакерів, власне військова боротьба з використанням високоточної керованої зброї, переваг свого геополітичного та геоекономічного становища, здобутків операції проти волі нації та національних культур («політика подвійних стандартів», маніпулятивна пропаганда, «переписування історії», метод «ставлення опонента в становище сторони, що виправдовується») тощо, «PR»-заходів. Інформаційна війна – це є найвищий ступінь інформаційного протиборства, спрямований на розв'язання суспільно-політичних, ідеологічних, а також національних, територіальних та інших конфліктів між державами, народами, націями, соціальними групами шляхом широкомасштабної реалізації засобів і методів інформаційного насильства (інформаційної зброї) [6, с. 99].

Інформаційні війни сучасності є ознакою високого розвитку суспільств й належать до несилових способів розв'язання конфліктів. У міжнародній політиці фактично виникло нове явище – можливість досягнення політичних цілей, зміни легітимних урядів та політичного, економічного, духовного підкорення народів і країн без застосування військової сили. Інформаційна війна – це дії з метою досягнення інформаційної переваги шляхом застосування заходів для експлуатації, підриву, знищення, дестабілізації і руйнування інформаційного потенціалу противника і його функцій [7, с. 266].

Ще одним новим явищем у світовому інформаційному просторі поряд із політичним тероризмом став інформаційний тероризм, або кібертероризм, що включає цілеспрямовані дії окремих суб'єктів або їхніх груп із дезорганізації роботи автоматизованих інформаційних систем і мереж зв'язку [8, с. 62].

Метою "інформаційних терористів" є порушення суспільної безпеки, залякування населення або здійснення впливу на прийняття рішень органами державної влади, а також деструкція інформаційних систем, які створюють сприятливі умови для вчинення нових актів тероризму.

У підсумку варто зазначити, що глобалізаційні процеси у світі є історично обумовленим та закономірним наслідком розвитку світової спільноти. Однак із процесами глобалізації пов'язана низка загроз національній безпеці та інформаційній безпеці, в тому числі України. Так, загрозами інформаційній безпеці міжнародного значення є інформаційний тероризм, комп'ютерна злочинність, інформаційні війні, використання інформаційної зброї, маніпулювання громадською думкою тощо. Для нейтралізації та запобігання загрозам інформаційній безпеці України слід на державному рівні послідовно розробляти та вдосконалювати нормативно-правову базу, підвищувати науковий потенціал

у галузі інформатизації, телекомунікації та зв'язку, вдосконалювати систему захисту вітчизняної інформаційної інфраструктури. Необхідно також удосконалювати форми і способи активної протидії інформаційно-психологічним операціям, спрямованим на послаблення обороноздатності країни, моделей превентивного інформаційного впливу, захисту інформаційного суверенітету [2, с. 27].

Захищаючи свої інформаційні інтереси, кожна держава має дбати про свою інформаційну безпеку. Цього ж вимагає і зміцнення української державності. Збалансована державна інформаційна політика України формується як складова частина її соціально-економічної політики, виходячи з пріоритетності національних інтересів та загроз національній безпеці країни. Із правової точки зору вона ґрунтується на засадах правової демократичної держави і впроваджується шляхом розробки та реалізації відповідних національних доктрин, стратегій, концепцій та програм згідно з чинним законодавством. В Україні назріла об'єктивна потреба у державно-правовому регулюванні науково-технологічної та інформаційної діяльності, що відповідала б реаліям сучасного світу та рівню розвитку інформаційних технологій, нормам міжнародного права, але водночас ефективно захищала б власні українські національні інтереси. [9, с.68]

1. Крюков О. І. Інформаційна безпека держави в умовах глобалізації. *Державне будівництво.* 2007. № 2. URL : http://nbuv.gov.ua/UJRN/DeBu_2007_2_12/
2. Косілова О. І. Інформаційна безпека України в умовах глобалізації. *Правова інформатика.* 2010. № 3. С. 22-28.
3. БорисоваЛ. В., В. В. Тулупов Інформаційна безпека як визначальний компонент національної безпеки України ресурс. Право і Безпека. 2013. № 1. С. 39-42.
4. Марущак А. І. Інформаційне право: регулювання інформаційної діяльності : навч. посібник. Київ : Видавничий дім "Скіф", 2008. 344 с.
5. Нижник Н. Р., Ситник Г. П., Білоус В. Т. Національна безпека України: методологічні аспекти, стан і тенденції розвитку : навч. посібник ; за заг. ред. П. В. Мельника. Ірпінь, 2000. 304 с
6. Ліпкан В. А., Максименко Ю. Є. Інформаційна безпека України в умовах Євроінтеграції: навч. посібник. Київ : КНТ, 2006. 279 с.
7. Кормич Б. А. Інформаційна безпека: організаційно-правові основи : навч. посібник. Київ : Кондор, 2008. 384 с.
8. Юдін О., Богуш В. Інформаційна безпека держави : навч. посібник. Харків : Консум, 2005. 574 с.
9. Боднар І.Р. Інформаційна безпека як основа національної безпеки. *Mechanism of Economic Regulation*. 2014. № 1. С. 68-75. URL : http://nbuv.gov.ua/UJRN/Mre_2014_1_8/

Катерина МІТУСОВА
викладач кафедри цивільного права
та процесу Дніпропетровського
державного університету внутрішніх
справ (м. Дніпро, Україна)

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ

Кожного дня світ відчуває прогресуючих зміни у технологіях шляхом впровадження цифрової модернізації, які з кожним роком відбуваються у ще більших швидкості та масштабах, ніж минулого року.

Так, все більших обертів в Україні набуває впровадження оцифрування суспільства, що отримало свою назву як «діджиталізація». Так звана діджиталізація суспільства безпосередньо стосується й оцифрування персональних даних громадян, зокрема: паспортних даних, податкових, транспортних, даних про освіту, про стан здоров'я та, в умовах карантинних обмежень, наявність курсу вакцинації. Отже, цифрові технології приходять на зміну звичним (паперовим) носіям інформації.

Так, Концепцією розвитку цифрової економіки та суспільства України на 2018-2020 роки, схваленою розпорядженням Кабінету Міністрів України від 17.01.2018 № 67-р, було визначено основні цілі цифрового розвитку, а саме: прискорення економічного зростання та залучення інвестицій; трансформація секторів економіки в конкурентоспроможні та ефективні; технологічна та цифрова модернізація промисловості та створення