УДК 343.3/.7

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ: СУЧАСНІ ВИКЛИКИ

Плетньов О. В.,
кандидат юридичних наук,
доцент спеціальної кафедри № 3
Інституту підготовки юридичних кадрів
для Служби безпеки України
Національного юридичного університету
імені Ярослава Мудрого,
м. Харків

Анотація: у статті розглянуто питання щодо визначення інформаційної безпеки держави предметом злочинного посягання в сучасних умовах розбудови інформаційного суспільства та зростання залежності усіх сфер життя людини та функціонування державних механізмів залежно від інформаційних фонових явищ. Проаналізовано сучасні виклики щодо забезпечення національної безпеки нашої держави від різного роду протиправних посягань в інформаційній сфері, в тому числі, що вчиняються з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, або з метою впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування. Зроблено висновок про соціальну обумовленість та наявність підстав і принципів криміналізації інформаційних посягань на відносини, що забезпечують суверенітет, територіальну цілісність та недоторканість, обороноздатність, державну безпеку країни, її конституційний лад.

Ключові слова: інформаційна безпека, національна безпека; комунікаційні технології.

Аннотация: в статье рассмотрены вопросы определения информационной безопасности государства предметом преступного посягательства в современных условиях переустройства информационного общества и роста зависимости всех сфер жизни человека и функционирования государственных механизмов в зависимости от информационных фоновых явлений. Проанализированы современные вызовы, связанные с обеспечением национальной безопасности нашего государства от разного рода противоправных посягательств в информационной сфере, в том числе, совершаемых с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта, международного осложнения, или с целью влияния на принятие решений или совершения либо несовершения действий органами государственной власти или органами местного самоуправления. Сделан вывод о социальной обусловленности и наличии оснований и принципов криминализации информационных посягательств на отношения, которые обеспечивают суверенитет, территориальную целостность и неприкосновенность, обороноспособность, государственную безопасность страны, ее конституционный строй.

Ключевые слова: информационная безопасность, национальная безопасность; коммуникационные технологии.

Annotation: in the article the questions of determination of informative safety of the state of criminal trespass an object are examined in the modern terms of reorganization of informative society and growth of dependence of all of spheres of life of man and functioning of state mechanisms depending on the informative base-line phenomena. Modern calls, related to providing of national safety of our state from the different sort of unlawfuls encroachments in an informative sphere, are analysed, including, accomplished with the purpose of public security breach, intimidation of population, provocation of military conflict, international complication, or with the purpose of influence on making a decision or feasance or omittance of actions public authorities or organs of local self-government. Drawn a conclusion about a social conditionality and presence of grounds and principles of criminalize of the informative trenching upon relations, which provide sovereignty, territorial integrity and inviolability, defence capacity, state security of country, its constitutional line-up.

Key words: informative safety, national safety; of communication technologies.

Становлення нашої країни як демократичної, соціально-правової держави, формування в Україні засад громадянського суспільства, розвиток міжнародного співробітництва безпосередньо пов'язані з належним дотриманням стану захищеності основ національної безпеки України: її суверенітету, конституційного ладу, територіальної цілісності та недоторканості, обороноздатності. Відповідно до ст. 17 Конституції України [10], захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу. Разом з тим, події останніх декількох років, активізація різного роду злочинних угруповань як в середині держави, так і за її межами, обумовлює необхідність поглиблення міжнародного співтовариства у цій сфері та вирішення цілої низки проблем кримінально-правової протидії зазначеним проявам, що можуть знаходити своє вираження й в інформаційній сфері.

Враховуючи серйозність і значне погіршення поточної ситуації, очевидно, що потреба кримінально-правового забезпечення охорони національної безпеки України в інформаційній сфері стала більш нагальною, ніж будь-коли. На виконання зазначених завдань вітчизняний законодавець ратифікував ряд міжнародно-правових документів, а також вніс чисельні зміни до Кримінального кодексу України [11] (далі – КК України). Зокрема, Законом України «Про ратифікацію Європейської конвенції про боротьбу з тероризмом» № 2990-III [13] ратифіковано Європейську конвенцію про боротьбу з тероризмом 1977 року [8], Законом України «Про ратифікацію Конвенції Ради Європи про запобігання

тероризму» № 54-V [14] ратифікована Конвенція Ради Європи про запобігання тероризму від 16 травня 2005 року [9], а 28 жовтня 2015 року Україна підписала Додатковий протокол до Конвенції Ради Європи про запобігання тероризму [16].

Водночас аналіз наведених законодавчих новел та публікацій, в яких наводяться доктринальні підходи до розв'язання проблематики кримінально-правової протидії посяганням щодо інформаційної безпеки нашої держави, свідчить про те, що сучасний стан Закону України про кримінальну відповідальність не відповідає повною мірою як положенням наведених міжнародно-правових документів, так і сьогоденним викликам, що стають перед нашою державою. Більш того, вони обумовили виникнення нових неузгодженостей та протиріч як між зазначеними нормами, так і з іншими положеннями кримінального закону України. Отже, положення закону про кримінальну відповідальність потребують ґрунтовних наукових досліджень, перегляду усталених у науці кримінального права поглядів та напрацювання практичних рекомендацій для правозастосовних органів з урахуванням як попереднього розвитку інститутів кримінального права, так і досвіду зарубіжних країн та новітніх світових демократичних стандартів щодо забезпечення інформаційної безпеки держави як складової національної безпеки України.

З другої половини XX – початку XXI століть відбувається трансформація суспільних відносин, що полягає у переорієнтації економічних і суспільних відносин з матеріальних цінностей на інформацію та знання, які стають сутністю нового типу суспільних відносин та є джерелом для усвідомлення змін, які відбуваються в політиці, економіці, соціумі, індивідуальній та суспільній свідомості. Інформаційне суспільство, як стадія розвитку суспільства з притаманними соціальній структурі кожного виду суспільства елементами, має глобальне значення як для філософії, економіки, політології, соціології, соціальної психології, так і безумовно для права нашої країни.

На сьогодні, інформаційне суспільство і його основні складові формують сучасний стан розвитку нашої держави, змінюють соціум, через свою ергономічність захоплюють все більше сфер життєдіяльності, життя людини охоплюється інформаційними потоками й повною мірою залежить від можливості здійснення комунікацій. Зважаючи на реалії впливу інформаційного суспільства на економіку та політику, забезпечення можливостей здійснення комунікацій з використанням сучасних інформаційно-комунікаційних технологій, щоденної модернізації та поширення засобів обміну інформацією, фактичної відсутності або суттєвої обмеженості можливості контролю над потоками інформації. Існування будь-якої країни за межами інформаційного поля стає неможливим.

Особливо звертає на себе увагу фактор незворотності процесу еволюції людства у напрямі інформаційного суспільства, за якого інформаційне наповнення охопить усі сфери життя та стане невід'ємною частиною для кожного члена цивілізованого суспільства. Вже зараз управління майже всіма галузями господарювання здійснюється за допомогою комунікаційних систем та найближчим часом такий спосіб управління поглине усі інші галузі життєдіяльності людини.

Як справедливо наголошує Н. А. Савінова, під впливом динаміки суспільних відносин у інформаційному суспільстві виникають нові види, форми і прояви суспільно небезпечних діянь, які раніше не могли існувати через відсутність технологій, з використанням яких вони реалізуються [19, с. 35]. На сьогодні є загальновизнаним, що інформаційна безпека, кібернетичний простір, інформація та інформаційно-комунікаційні технології потребують кримінально-правового забезпечення. При цьому, з одного боку, безпеку інформаційного простору, свідомості та спілкування, безпеку комунікації з усіма її складовими, а також безпеку знань, які й є основними ресурсами та цінностями інформаційного суспільства, необхідно розглядати як цінності, що потребують забезпечення їх охорони засобами кримінального права. З іншого боку, кібернетичний простір, інформація та інформаційно-комунікаційні технології можуть бути використані з метою вчинення суспільно небезпечних посягань на соціальні цінності без належного забезпечення охорони яких неможливе нормальне функціонування держави та відповідних її інститутів: суверенітету країни, її конституційного ладу, територіальної цінності та територіальної недоторканості, обороноздатності нашої держави, порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення тощо.

У контексті наведеного, особливо звертають на себе увагу нещодавні події навколо виборів Президента США. За словами колишнього Держсекретаря США Рекса Тіллерсона, Центральне розвідувальне управління дійшло до висновків, що хакерські атаки з боку Росії на офіційні установи США під час президентської кампанії були спрямовані безпосередньо на підтримку Дональда Трампа, який у підсумку і став Президентом [21]. Або нещодавній випадок із поширенням вірусу WannaCry, який особливо активно вражав комп'ютери державних установ, телекомунікаційних компаній, банків, стільникових операторів, лікарень, тобто установ, що в першу чергу забезпечують функціонування державного механізму будь-якої країни. Окремі організації навіть вимушені були на деякий час припинити свою діяльність. «Передбачуваний збиток, нанесений WannaCry за перші чотири дні, перевищив 1 млрд доларів США, якщо враховувати викликані цим масштабні простої крупних організацій у всьому світі», – заявив глава KnowBe4 Стью Сьюверман [6]. За даними цієї компанії, всього WannaCry уразив від 200 до 300 тисяч комп'ютерів у щонайменше 150 країнах світу. При цьому, експерти не виключають, що у майбутньому можуть відбуватися нові подібні атаки. І це тільки окремі випадки використання кібернетичного простору, інформації та інформаційно-комунікаційних технологій, що за своїм впливом на стан захищеності життєдіяльності людей значно перевищують передбачені на сьогодні КК України протиправні посягання на основи національної та громадської безпеки нашої держави.

Порівняно з такими загрозами, застосування зброї, вчинення вибуху, підпалу чи інших загальнонебезпечних дій, підстави кримінальної відповідальності за які на сьогодні встановлені в окремих нормах розділів I та IX Особливої частини КК України, на наш погляд, становлять значно менший ступень суспільної небезпеки. Актуалізує наведені підходи і питання визнання безпеки людини в Україні однією з найвищих соціальних цінностей (ч. 1 ст. 3 Конституції), а також визнання людини і громадянина, їх конституційних прав і свобод, інформаційного

середовища, конституційного ладу, суверенітету, територіальної цілісності та недоторканності об'єктами національної безпеки нашої держави (ст. 3 Закону України «Про основи національної безпеки» [12]).

Збільшення значення інформації, знань, інформаційно-комунікаційних технологій і комунікації, усвідомлення значення їх використання з метою впливу на свідомість та волю громадян, не може не вплинути на перегляд підходів правової і кримінально-правової політики та загальної оцінки їх не лише як цінностей, а і як до засобів вчинення посягань на основи національної безпеки нашої держави. Тому, з точки зору потреби криміналізації слід розглянути ті блоки суспільних відносин, які піддаються впливу злочинності, характерної для інформаційного суспільства. Трансформація злочинності в інформаційному просторі спостерігається з кожним роком все активніше. Саме тому, дослідження детермінації злочинності й динаміки збільшення суспільної небезпечності окремих суспільно небезпечних діянь під впливом розвитку інформаційних технологій є важливим напрямом досліджень соціальної обумовленості криміналізації. Як зазначає В. І. Борисов, основним напрямом вирішення соціальної обумовленості кримінально-правової заборони є визначення та дослідження чинників, що впливають на створення кримінального закону (КК, його інститутів, окремих кримінально-правових норм) та на їх ефективність [2, с. 7].

Як справедливо наголошує Н. А. Савінова, отримавши можливість використання сучасних інформаційно-комунікаційних технологій і можливості обігу інформації без обмежень часом, відстанню та кордонами, людство стало більш уразливим від злочинності, яка користуючись такими технологіями не обмежена відстанню до предмету посягання, не стримується кордонами [19, с. 172]. Такий розвиток обумовлює розвиток новітньої кібернетичної злочинності, спрямованої на відповідний предмет, який має нове вираження й не завжди є матеріальним [7, с. 1], і визначається як предмет об'єктивного світу, що створений за допомогою спеціальних методів та (або) засобів, фізично відсутній, але має зовнішнє представлення або може набути такого представлення за допомогою спеціальних методів та способів впливу [17, с. 106].

Такі раніше відомі суспільно-небезпечні діяння, що трансформувалися в інформаційний простір із реального у зв'язку з розвитком інформаційних технологій зберегли при цьому ознаки чільних злочинів. Це повною мірою стосується і можливості вчинення посягань, що характеризують як групу злочинів, передбачених Розділом I Особливої частини КК України (статті 109, 110, 110-2, 111, 113, 114, 114-1 КК України), так і окремих проявів суспільно небезпечної поведінки, підстави кримінальної відповідальності за які визначені у нормах Розділу IX Особливої частини КК України (статті 255, 256, 258, 258-1, 258-2, 258-2, 258-3, 258-4, 258-5, 259, 261 КК України).

Крім того, використання інформаційних технологій може засвідчувати і наявність ознак інших незакінчених злочинів, що відносяться до наведених груп посягань (статті 14 або 15 КК України), або вказувати на співучасть у вчиненні зазначених злочинів (частини 3, 4 або 5 ст. 27 КК України). Саме тому, варто звернути увагу на процес трансформації умовно кажучи «фізичної» злочинності в кібернетичну або інформаційну з метою усвідомлення сутності таких процесів та явищ та розроблення відповідного вектору удосконалення кримінально-правового механізму забезпечення охорони державних інституцій від таких інформаційних посягань. На нашу думку, саме прогалини або недосконаліть такого механізму на сьогодні обумовлюють у нашій державі спроби застосування інших публічно-правових механізмів забезпечити охорону інформаційної безпеки держави.

Так, відповідно до ст. 107 Конституції, Указом Президента України від 15 травня 2017 року № 133/2017 «Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)"» [15] в Україні було запроваджено блокування активів, обмеження торговельних операцій, повна або часткова заборона вчинення правочинів щодо цінних паперів, заборона передання технологій, прав на об'єкти права інтелектуальної власності, а також заборона Інтернет-провайдерам надання послуг з доступу до ресурсів сервісів ТОВ «Мэйл.РУ ГРУП», ТОВ «Вконтакте», ТОВ «Яндекс», АТ «Лабораторія Касперського», ТОВ «Доктор Веб», ТОВ «1С».

Як повідомила заступник начальника Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України Ю. Лапутіна, період підготовки до військового вторгнення супроводжувався активним застосуванням спецслужбами Російської Федерації спеціальних інформаційних та інформаційно-психологічних операцій проти України. Зокрема, шляхом створення, адміністрування, штучного нарощування відвідуваності антиукраїнських та проросійських груп в українському сегменті російських соціальних мереж «ВКонтакте» та «Одноклассники». В окремих випадках за грошове винагородження, що здійснювалося через сервіс «Яндекс.Деньги», здійснювали акції на шкоду територіальної цілісності, суверенітету та безпеки України [18]. Також неодноразово в засобах масової інформації зазначалося, що за допомогою програмних продуктів АТ «Лабораторія Касперського» та ТОВ «Доктор Веб» здійснюється збір інформації спецслужбами Російської Федерації [1]. На користь того, що заборона Інтернет-провайдерам надання послуг з доступу користувачам мережі до наведених ресурсів спрямована саме на захист інтересів держави у сфері інформаційної безпеки свідчить і рішення Вищого Адміністративного суду України під час розгляду позову М. Євстифеєва про визнання частково незаконним Указу Президента № 133/2017 щодо блокування російських інтеренет-ресурсів про залучення СБУ до розгляду як третьої сторони [20].

Слід зазначити, що така практика державно-правової протидії загрозам інформаційній безпеці держави є достатньо поширеною у світі та застосовується урядами багатьох країн. Так, влада Єгипту нещодавно за два тижні заблокувала щонайменше 62 сайта через наявність на них інформації, яка підтримує тероризм і екстремізм, зокрема сайт популярного катарського супутникового телеканалу «Al-Jazeera» [4]. Наприкінці минулого року і суд Російської Федерації визнав законним блокування соціальної мережі LinkedIn за позовом Роскомнагляду [5]. Крім того, представники ЄС та Північноатлантичного альянсу (НАТО) одноголосно наголосили на тому, що рішення про блокування російських сайтів в Україні було прийняте виходячи з інтересів національної інформаційної безпеки і наша держава стала об'єктом численних кібератак та дезінформаційних кампаній [3].

Таким чином, інформаційна безпека, як частина національної безпеки нашої держави, забезпечує саме існування України як суверенної, незалежної, демократичної, соціальної і правової держави (ст. 1 Конституції України). Важливість такого об'єкту кримінально-правової охорони визначає значною мірою засоби протидії загрозам національної безпеки – наявним та потенційно можливим явищам і чинникам, що створюють небезпеку життєво важливим національним інтересам України. Зважаючи на реалії впливу інформаційного суспільства на економіку та політику, забезпечення можливостей здійснення комунікацій з використанням сучасних інформаційно-комунікаційних технологій, щоденної модернізації та поширення засобів обміну інформацією, фактичної відсутності або суттєвої обмеженості можливості контролю над потоками та змістом інформації, на сьогодні існує нагальна потреба перегляду багатьох положень чинного закону про кримінальну відповідальність щодо визначення вичерпного або приблизного кола суспільно небезпечної поведінки та її сутності як складової підстав кримінальної відповідальності. Саме тому, з урахуванням сучасного стану та розвитку електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку існує необхідність відображення сучасних загроз національній безпеці України в кримінальному законодавстві нашої держави.

ЛІТЕРАТУРА

1. Антивирус Касперского является вирусом ФСБ, – военная разведка США [Електронний ресурс]. – Режим доступу: http://vlasti.net/news/234966 (дата звернення: 16.05.2017).
2. Борисов В. І. Соціальний аспект дослідження проблем кримінального права / Актуальні проблеми кримінального права та кримінології: матеріали всеукр. наук.-практ. конф. (м. Донецьк, 24.04.2009); Донецький юрид. ін-т ЛДУВС ім. Е. О. Дідоренка. Донецьк, 2009. С. 6–8.
3. В ЕС признали блокировку российских сайтов вопросом нацбезопасности [Електронний ресурс]. – Режим доступу: http://ru.espreso.tv/news/2017/05/19/v_es_pryznaly_blokyrovku_rossyyskykh_saytov_voprosom_nacbezopasnosty (дата звернення: 19.05.2017).
4. В Єгипті заблокували 62 сайта в рамках боротьби з екстремізмом [Електронний ресурс]. – Режим доступу: https://www.vectornews.net/news/society/27018-v-yegipt-zablokuvali-62-sayta-v-ramkah-borotbi-z-ekstremzmom.html (дата звернення: 19.05.2017).
5. В России заблокируют соцсеть LinkedIn [Електронний ресурс]. – Режим доступу: https://censor.net.ua/news/414435/v_rossii_zablokiruyut_sotsset_linkedin_sud_priznal_zakonnym_reshenie_roskomnadzora (дата звернення: 13.05.2017).
6. Вирус WannaCry: ущерб оценили в миллиард долларов [Електронний ресурс]. – Режим доступу: http://korrespondent.net/world/38554-vyrus-WannaCry-uscherb-otsenyly-v-myllyard-dollarov (дата звернення: 25.05.2017).
7. Голубєв В. Комп'ютерна злочинність // Юридичний вісник України. – 2002. – № 6. – С. 1, 4.
8. Європейська конвенція про боротьбу з тероризмом (ETS № 90) від 27.01.1977 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_331 (дата звернення: 10.05.2017).
9. Конвенція Ради Європи про запобігання тероризму від 16.05.2005 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_712 (дата звернення: 10.05.2017).
10. Конституція України: Закон від 28.06.1996 № 254к/96-ВР [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/254%D0%BA/96-%D0%B2%D1%80 (дата звернення: 20.05.2017).
11. Кримінальний кодекс України: Закон від 05.04.2001 № 2341–III [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/2341-14 (дата звернення: 15.05.2017).
12. Про основи національної безпеки України: Закон від 19.06.2003 № 964-IV [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/964-15 (дата звернення: 10.05.2017).
13. Про ратифікацію Європейської конвенції про боротьбу з тероризмом: Закон від 17.01.2002 № 2990-III [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2990-14 (дата звернення: 10.05.2017).
14. Про ратифікацію Конвенції Ради Європи про запобігання тероризму: Закон від 31.07.2006 № 54–V [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/54-16 (дата звернення: 10.05.2017).
15. Про рішення Ради національної безпеки і оборони України від 15.05.2017 № 133/2017 «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)»: Указ Президента України від 15.05.2017 № 133/2017 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/133/2017 (дата звернення: 20.05.2017).
16. Протокол, що вносить зміни до Європейської конвенції про боротьбу з тероризмом (ETS № 190) від 15.05.2003 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/994_173 (дата звернення: 10.05.2017).
17. Розенфельд Н. А. Віртуальний предмет злочинів, пов'язаних з порушенням авторського права і суміжних прав // Право України. – 2008. – № 5. – С. 105–108.
18. Российские спецслужбы использовали «ВКонтакте» и «Одноклассники» в период подготовки ко вторжению в Украину. – СБУ [Електронний ресурс]. – Режим доступу: https://censor.net.ua/news/443693/rossiyiskie_spetsslujby_ispolzovali_vkontakte_i_odnoklassniki_v_period_podgotovki_ko_vtorjeniyu_v_ukrainu (дата звернення: 14.05.2017).
19. Савнова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти: монографія. Київ: ТОВ «ДКС», 2011. – 342 с.
20. Судьи Высшего админсуда признали законной блокировку российских социальных сетей [Електронний ресурс]. – Режим доступу: https://www.vectornews.net/news/society/27018-v-yegipt-zablokuvali-62-sayta-v-ramkah-borotbi-z-ekstremzmom.html (дата звернення: 15.06.2017).
21. Тіллерсон: втручання Росії у вибори Президента США добре задокументовано [Електронний ресурс]. – Режим доступу: https://www.5.ua/svit/tillerson-vtruchannia-rosii-u-vybory-prezydenta-ssha-dobre-zadokumentovano-145387.html (дата звернення: 14.05.2017).