УДК 32.019.51:323.28:323.2(477)

БІЛАН І.А., науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України.
ORCID: https://orcid.org/0000-0003-1237-1565.

КІБЕРТЕРОРИЗМ: ІНФОРМАЦІЙНО-ПРАВОВИЙ АСПЕКТ

Анотація. *У статті висвітлені інформаційно-правові аспекти кібертероризму. На підставі аналізу підходів, вироблених зарубіжними і вітчизняними вченими, визначено суттєві ознаки кібертероризму, критерії його відмежування від суміжних понять. Аналізуються кіберінциденти та основні цілі кібертерористів у кіберпросторі України. Міститься правовий аналіз як нормативних актів України у сфері інформаційної безпеки, так і міжнародно-правових актів у цій сфері. Проаналізовано новації в законодавстві окремих зарубіжних країн у сфері боротьби з кібертероризмом. Запропоновано авторське визначення кібертероризму. На базі аналізу зарубіжного досвіду у сфері боротьби з тероризмом пропонуються зміни до Закону України "Про боротьбу з тероризмом", а також законодавства про кримінальну відповідальність за акти кібертероризму.*

Ключові слова*: тероризм, кібертероризм, кіберпростір, інформаційні технології, інформаційне насильство, кримінальна відповідальність.*

Summary*. The article covers the informational and legal aspects of cyberterrorism. On the basis of the analysis of approaches developed by foreign and domestic scientists, essential signs of cyberterrorism. Cyber incidents and the main goals of cyber terrorists in Ukrainian cyberspace are analyzed. It contains a legal analysis of both regulatory acts of Ukraine in the field of information security and international legal acts in this area. Innovations in the legislation of certain foreign countries in the field of combating cyberterrorism are analyzed. The author's definition of cyberterrorism as a type of terrorist activity, which is carried out using cyberattacks in cyberspace, is proposed. Based on the analysis of foreign experience in the field of combating terrorism, amendments are proposed to the Law of Ukraine "On Combating Terrorism", as well as to the legislation on criminal liability for acts of cyberterrorism.*

Keywords*: terrorism, cyberterrorism, cyberspace, information technologies, information violence, criminal liability.*

Постановка проблеми. Кібертероризм є серйозною загрозою для світової спільноти поряд з ядерною, бактеріологічною і хімічною зброєю. Світовий досвід свідчить про безперечну уразливість будь-якої держави, тим більше, що кібертероризм не має державних кордонів; кібертерорист здатний рівною мірою загрожувати інформаційним системам, розташованим практично в будь-якій точці земної кулі шляхом використання спеціального програмного забезпечення, призначеного для несанкціонованого проникнення в комп'ютерні мережі та організації віддаленої кібератаки на інформаційні ресурси жертви [1, с. 42-43]. Очевидно, що актуальність цієї загрози буде зростати і надалі в ході розвитку і поширення інформаційно-телекомунікаційних технологій.

Рівень загрози кібертероризму проти України стрімко зростає в умовах неприкритої агресії рф проти України з лютого 2022 року. Особливо помітне зростання кількості кіберінцидентів і кібератак на державні інформаційні ресурси та об'єкти

критичної інфраструктури України з боку російських хакерів. Від початку повномасштабної війни (і станом на середину листопада 2022 року) на українську енергетику було здійснено понад 1,2 млн. кібератак [2].

Результати аналізу наукових публікацій. Теоретичні аспекти протидії кібертероризму досліджували Лабенко Л.В. [3], Бураєва Л.А. [4], Банк Р.О. [5], Діордіца І.В. [6], Пилипчук В.Г., Дзьобань О.П. [7] та ін.

Особливості кібертероризму як одного із способів інформаційної війни висвітлені у працях Почепцова Г.Г. [8], Коршунова В.О. [9], Леонова Б.Д. [10], Рижова І.М. [11], Яцик Т.П. [12] та ін.

Істотний внесок у дослідження кібертероризму як засобу введення інформаційної війни в умовах глобалізації та розвитку кіберпростору здійснили зарубіжні вчені, серед яких можна виділити роботи Д. Белла [13], Е. Тоффлера [14], Б. Хофмана [15], А. Шміда [16] та ін.

Проте серед науковців і практичних фахівців у сфері інформаційних технологій немає єдиних підходів до визначення поняття "кібертероризм", його суттєвих ознак. Існують також розбіжності поглядів щодо форм і різновидів такого тероризму.

Метою статті є удосконалення на базі аналізу вітчизняного і зарубіжного досвіду у сфері інформаційної безпеки визначення кібертероризму, а також внесення пропозицій з встановлення кримінальної відповідальності за його суспільно небезпечні прояви.

Виклад основного матеріалу. Закон України "Про боротьбу з тероризмом" не містить визначення терміну "кібертероризм". Цей Закон згадує поняття "технологічний тероризм", під яким слід розуміти кримінальні правопорушення, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров'я людей речовин, засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру (ст. 1) [17]. Наведене визначення охоплює різні різновиди тероризму і не збігається з дефініцією кібертероризму, який, виходячи з наведеного визначення, вбачається одним з проявів технологічного тероризму.

Закон України "Про основні засади забезпечення кібербезпеки України" визначає кібертероризм як терористичну діяльність, що здійснюється в кіберпросторі або з його використанням (ст. 1) [18]. Проте, ст. 1 Закону України "Про боротьбу з тероризмом" не згадує такий прояв терористичної діяльності у кіберпросторі.

Стратегія інформаційної безпеки [19] визначає основні напрями забезпечення інформаційної безпеки України. Серед них згадується протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів (Стратегічна ціль 1).

Стратегія національної безпеки України [20] основним завданням розвитку системи кібербезпеки визначає гарантування кіберстійкості та кібербезпеки національної інформаційної інфраструктури (п. 52), а серед пріоритетних завдань правоохоронних, спеціальних, розвідувальних та інших державних органів виділяє активну та ефективну протидію розвідувально-підривній діяльності, спеціальним інформаційним операціям та

кібератакам. У Стратегії згадується інформаційна “зброя”, яку застосовує рф для поширення міжнародного тероризму у кіберпросторі [10, с. 73-74].

Міжнародний тероризм, зокрема в кіберпросторі, згадує також Стратегія забезпечення державної безпеки (затверджена Указом Президента України від 16 лютого 2022 року № 56) [21]. Ця Стратегія одним з об’єктів забезпечення державної безпеки називає кібербезпеку.

Забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки України, реалізація якої здійснюватиметься шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі. З цією метою Указом Президента України від 26 серпня 2021 року № 447/2021 затверджено Стратегію кібербезпеки України [22].

У цій Стратегії зазначається, що російська федерація залишається одним з основних джерел загроз національній та міжнародній кібербезпеці, активно реалізує концепцію інформаційного протиборства, базовану на поєднанні деструктивних дій у кіберпросторі та інформаційно-психологічних операцій, механізми якої активно застосовуються у гібридній війні проти України. Така деструктивна активність створює реальну загрозу вчинення актів кібертероризму та кібердиверсій стосовно національної інформаційної інфраструктури [22].

Глобального масштабу набуває використання кіберпростору терористичними організаціями. У Розділі 1 Стратегії кібербезпеки України зазначається, що пріоритетними цілями кібертероризму залишаються об’єкти атомної енергетики, електро- та водопостачання, сфери електронних комунікацій, фінансової та банківської сфери, авіа- та залізничного транспорту, сховищ стратегічних видів сировини, хімічні й біологічні об’єкти тощо [22]. Кіберінциденти здійснюються через інформаційно-телекомунікаційні системи, які необхідні для повсякденного життя людей, функціонування структур економіки, органів державної влади.

Аналіз нормативно-правових актів у сфері боротьби з тероризмом свідчить про те, що кібертероризм розглядається як одне з основних джерел загроз національній та міжнародній кібербезпеці, а його визначення на рівні закону згадує кіберпростір як сферу застосування терористичної діяльності.

Зауважимо, що визначення кібертероризму не містять міжнародні правові акти, серед яких виділяються Конвенція Ради Європи про запобігання тероризму (2005 р.), Конвенція про кіберзлочинність (2001 р.). Наслідком ратифікації остатнньої став Закон України “Про внесення змін до Кримінального та Кримінально-процесуального кодексів України” від 23 грудня 2004 року, відповідно до якого в Розділі 16 “Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку” викладені у новій редакції статті 361, 362, 363 Кримінального кодексу та встановлена відповідальність за статтями 361-1, 361-2 та 363-1 цього Кодексу [23, с. 256].

Аналіз різних підходів, викладених у зазначених актах, дає підстави для висновку, що кібертероризм є частиною або, за твердженням деяких науковців, ідентичним поняттям щодо інформаційного тероризму [5, с. 112]. Деякі дослідники вважають, що кібертероризм є видовим, а інформаційний тероризм – родовим поняттям одного негативного явища – тероризму [6]. Більшість вчених вважає, що інформаційний тероризм як явище за змістом охоплює прояви кібертероризму.

На доктринальному рівні це поняття досліджувалося як вченими, так і практичними фахівцями у сфері інформаційних технологій. На думку зарубіжних дослідників, кібетероризм є різновидом кібератак на комп’ютерні системи.

Центр стратегічних і міжнародних досліджень визначає кібертероризм як використання комп'ютерних мережевих інструментів для припинення функціонування критичних об'єктів національної інфраструктури (зокрема, енергетичних, транспортних, урядових), або для примусу або залякування уряду або цивільного населення [24].

З точки зору американського професора У. Тафойа, кібертероризмом є залякування суспільства шляхом використання високих технологій для досягнення політичних, релігійних чи ідеологічних цілей, а також дії, які призводять до відключення, виведення з ладу об'єктів критичної інфраструктури або знищення інформації [25].

Визначення кібертероризму міститься й в роботах вітчизняних вчених.

На думку Діордіци І.В., термін "кібертероризм" є синтезом понять "кібербезпековий простір" та "тероризм" [6]. Для кібертероризму характерним є використання комп'ютера як інструмента злочину та існування Інтернету як міжнародного інформаційного простору, в якому перебуває об'єкт злочину [6].

Пилипчук В.Г. та Дзьобань О.П. вважають, що кібертероризм – це навмисна, політично вмотивована атака на об'єкти інформаційного простору, що створює небезпеку для життя та/або здоров'я людей або настання інших тяжких наслідків, якщо такі дії були здійснені з метою порушення державної чи громадської безпеки, залякування населення, провокації військового конфлікту чи загроза вчинення таких дій [4].

Схожого підходу дотримується В.В. Топчій, на думку якого під кібертероризмом слід розуміти навмисну мотивовану атаку на інформацію, що обробляється комп'ютером, комп'ютерну систему або мережу, яка пов'язана з небезпекою для життя і здоров'я людей або настанням інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокування військового конфлікту [26].

Залежно від злочинної мети та використання інструментів (засобів) її досягнення від кібертероризму слід відрізняти медіа-тероризм, під яким розуміють зловживання інформаційними системами, мережами, та їхніми компонентами для здійснення терористичної діяльності (пропаганда та поширення ідеології тероризму, сприяння вчиненню теракту). Засобами здійснення медіа-тероризму є друковані ЗМІ, мережі ефірних й кабельних мас-медіа, Інтернет, електронна пошта, спам тощо [5, с. 114].

Основною ознакою кібертероризму є кібератаки, які здійснюються у кіберпросторі. Відповідно до Закону України "Про основні засади забезпечення кібербезпеки України" під кібератакою слід розуміти спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [18].

Об'єктами таких атак є інформація, програми, комп'ютери, локальні та глобальні мережі. З-поміж властивостей інформаційного насильства виділяється: несиловий, ідеальний характер, вихід за межі фізичних закономірностей; не лінійність; порушення закону збереження речовини й енергії, кумулятивний характер, можливість бурхливого зростання інформації; широке розповсюдження; можливість ідеального клонування; нелокалізованість у часі; опосередкований характер і прихованість впливу; віртуальний

характер впливу; можливість фіксування; селективність; легкість доступу, злому інформаційних систем [27].

Україна зазнає кібератак різної потужності, починаючи ще з 2014 року.

Однією із наймасштабніших за наслідками була кібератака з поширення вірусу NotPetya, який 27 червня 2017 р. атакував численні комп'ютерні системи українських державних і комерційних установ. За підрахунками спеціалістів Microsoft та ESET, кібератака зачепила щонайменше 65 країн. Встановлено, що першою й основною (якщо не єдиною) метою кібератаки була саме Україна. За попередніми підрахунками, у результаті атаки на території України станом на 7 липня 2017 р. було виведено з ладу до 10 % приватних, урядових і корпоративних комп'ютерів [28].

Ще до повномасштабного вторгнення рф в лютому 2022 року експерти з кібербезпеки прогнозували збільшення проявів кібертероризму в Україні. З початку неприкритої агресії рф Україна стала об'єктом чисельних кібератак, які охопили державні установи, приватні організації та громадян. У 2022 році рф втричі збільшила кількість таких атак на Україну[29].

Однак, якщо раніше вони були спрямовані здебільшого на військові цілі, то в умовах війни суспільно небезпечні хакери спрямовані на критичну інфраструктуру, яка зазнає кібератак [29].

Збільшення кібератак на критичну інфраструктуру України викликає занепокоєння у країн ЄС та НАТО, які теж можуть стати об'єктами кібератак. Світова тенденція сучасності – кожна країна динамічно працює над інституційними засадами протидії кібертероризму, навіть в певних випадках у форматі створення кібервійськ [30, с. 148].

В даному контексті доречно розглянути досвід окремих зарубіжних країн – союзників України у сфері боротьби з кібертероризмом.

Так, кримінальне законодавство Франції значно розширило межі відповідальності за злочинні прояви тероризму в кіберпросторі. У КК Франції у 2016 р. було криміналізоване створення сайтів терористичної спрямованості за межами Франції. У гл. 25 кн. 4 КПК Франції визначено особливу процедуру, що застосовується до справ організованої злочинності, у т.ч. тероризму, зміст якої полягає, зокрема, у встановленні спеціальних складів судів і оперативно-розшукових команд.

Парламент Франції також затвердив положення про створення паризького суду, що спеціалізуватиметься на боротьбі з кіберзлочинністю [31].

КК ФРН не містить визначення тероризму. У КК ФРН передбачено посилену відповідальність за злочини, що вчиняються організованими об'єднаннями. До них слід віднести такі: створення злочинних об'єднань (ст. 129), створення терористичних об'єднань (ст. 129-а), тяжкі випадки торгівлі людьми (ст. 181), геноцид (ст. 220-а), викрадення людини (ст. 234), насильницьке переміщення громадян за межі країни (ст. 234-а). До проявів терористичної діяльності у ФРН, зокрема, відносять: заподіяння шкоди територіальній цілісності, порушення зовнішньої чи внутрішньої безпеки держави; порушення конституційних засад; заподіяння шкоди військам НАТО, розміщеним на території ФРН.

Федеральним законом передбачено створення спільних файлів поліції та розвідувальних служб щодо осіб, підозрюваних у здійсненні терористичної діяльності. Мова йде про створення так званих "файлів антитерору", в рамках яких відбувається обмін інформацією між правоохоронними органами та службами ФРН [32, с. 35].

Закон ФРН від 25 грудня 2008 р. розширив повноваження кримінальної поліції щодо впровадження спеціальних програм у комп'ютери осіб, підозрюваних у причетності до діяльності терористичних організацій [33]. Цей Закон мав профілактичну мету: відстеження терористів-одинаків.

24 червня 2016 р. в ФРН прийнято Закон "Про заходи з протидії тероризму", яким передбачається: запровадження більш жорстких правил реєстрації власників передплаченого зв'язку; організація автоматизованого обміну даними між національними спецслужбами та правоохоронними органами, а також із спецслужбами іноземних держав; збільшення термінів зберігання відповідної інформації; зменшення з 16 до 14 років мінімального віку громадян, за якими дозволено здійснювати стеження [34].

Також у 2016 р. внесено зміни до Закону ФРН "Про Федеральну розвідувальну службу" (BND), якими розширюються її повноваження. Зокрема, передбачено надання права щодо зняття інформації з телекомунікаційних каналів на території ФРН, у т.ч. й прослуховування громадян країни (до цього BND не мала повноважень здійснювати такі заходи на території країни), зберігати інформацію про користувачів Інтернету та передавати її до партнерських спецслужб [34].

Норми про відповідальність за кібертероризм містить федеральне законодавство США. Відповідно до положень Патріотичного закону США 2001 р. федеральне кримінальне законодавство розрізняє поняття *"*кібертероризм". Так, згідно зі ст. 814 цього Закону, положення якої доповнюють § 1030 "Шахрайство та пов'язана з ним діяльність щодо комп'ютерів" Розділ 18 Зведеного закону США, поняття "кібертероризм" охоплює різні кваліфіковані форми хакерства (в тому числі й ті, що спричиняють матеріальні збитки на суму, яка становить $5 тис. і більше), заподіяння шкоди захищеним комп'ютерним мережам громадян, юридичних осіб та урядових установ, включаючи шкоду медичному обладнанню, "фізичну шкоду якій-небудь особі", "загрозу громадському здоров'ю та безпеці", "шкоду, що завдана комп'ютерній системі, яку використовує урядова установа для відправлення правосуддя, організації національної оборони чи забезпечення національної безпеки" (покаранням за це є штраф та/або тюремне ув'язнення на строк до 20 років) [32, с. 371]. Отже, у США (на рівні федерації) введено поняття "кібертероризм", а також встановлено кримінальну відповідальність за його злочинні прояви.

Викладене свідчить про необхідність удосконалення на законодавчому рівні поняття "кібертероризм", а також встановлення кримінальної відповідальності за вчинення терористичного акту з використанням кібертероризму. До речі, стаття 7.2.4. проекту КК України передбачає відповідальність за терористичний акт, згідно з якою винною визнається, зокрема, особа, яка з метою залякати населення або дестабілізувати діяльність органу державної влади, органу місцевого самоврядування, міжнародної організації, представництва іноземної держави чи юридичної особи, або примусити їх вчинити яку-небудь дію чи утриматися від її вчинення: захопила, утримувала, знищила або пошкодила об'єкт критичної інфраструктури чи його устаткування, необхідне для функціонування цього об'єкта, або порушила його належне функціонування; незаконно втрутилася в роботу інформаційної (автоматизованої), електронної комунікаційної, інформаційно-комунікаційної системи, електронної комунікаційної мережі [33].

Висновки.

Аналіз викладених підходів свідчить про те, що основою кібертероризму є кібератаки, які вчинюються у кіберпросторі або з його використанням. Ці атаки спрямовані на залякування населення або дестабілізацію діяльності органу державної влади, органу місцевого самоврядування, міжнародної організації, представництва іноземної держави чи юридичної особи з метою примусити їх вчинити яку-небудь дію чи утриматися від її вчинення.

Під кібертероризмом слід розуміти терористичну діяльність, яка здійснюється із застосуванням кібератак у кіберпросторі або з його використанням. Таку діяльність

доцільно визначити в ст. 1 Закону України “Про боротьбу з тероризмом”, а серед ознак терористичного акту (ст. 258 КК України) слід передбачити його вчинення у формі кібертероризму. Одним із варіантів вирішення порушеного питання є доповнення частини 2 ст. 258 КК України після слів “групою осіб” словами “або вчинені шляхом кібератаки”. Заходи з протидії кібертероризму доцільно передбачити в Концепції боротьби з тероризмом в Україні та Плані заходів з її реалізації.

Вважаємо, що реалізація запропонованих змін сприятиме боротьбі з проявами кібертероризму в Україні.

Використана література

1. Мазуров В.А. Кибертерроризм: понятие, проблемы противодействия: доклады ТУСУРа, 2010. № 1(21). Ч. 1. С.41-45.

2. Російські хакери посилюють кібератаки на цивільні цілі, щоб тероризувати українців. – (Посадовець АНБ). URL: https://lb.ua/society/2023/01/12/542313_rosiyski_hakeri_posilyuyut.html

4. Лабенко Л.В. Інформаційний тероризм: поняття та ознаки. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/3439/%D0%9B%D0%B0%D0%B1%D0%B5%D0%BD%D0%BA%D0%BE.pdf?sequence=1&isAllowed=y (дата звернення: 04.02.2021).

4. Бураева Л.А. Информационный терроризм как угроза национальной безопасности российской федерации. URL: https://cyberleninka.ru/article/n/informatsionnyy-terrorizm-kak-ugroza-natsionalnoy-bezopasnosti-rossiyskoy-federatsii/viewer

5. Банк Р.О. Інформаційний тероризм як загроза національній безпеці України: теоретико-правовий аспект. *Інформація і право.* № 1(16)/2016. С. 110-116.

6. Діордіца І.В. Поняття та зміст кібертероризму. URL: https://goal-int.org/ponyattya-ta-zmist-kiberterorizmu

7. Пилипчук В.Г., Дзьобань О.П. Теоретичні та державно-правові аспекти протидії інформаційному тероризму в умовах глобалізації. *Стратегічні пріоритети*. 2011. № 4. С. 12-17.

8. Почепцов Г.Г. Информационные войны. – (Серия: Образовательная библиотека); москва: Рефл-бук, 2001. 576 с.

9. Коршунов В.О. Політичний тероризм: інформаційні методи боротьби: автореф. дис. …канд. політ. наук: спец. 23.00.02. Дніпропетровськ, 2008. 18 с.

10. Леонов Б.Д. Тероризм: інформаційно-правовий вимір. *Інформація і право*. № 2(37)/2021. С. 72-79.

11. Рижов І.М., Строгий В.І. Концептуальні засади соціально-інформаційних технологій упередження кризових явищ соцілального характеру (на прикладі моніторингу тероризму). *Науковий вісник Львівського державного університету внутрішніх справ*. *Серія юридична.* 2014. № 3. С. 219-228.

12. Яцик Т.П. Особливості інформаційного тероризму як одного із способів інформаційної війни. *Науковий вісник Національного університету ДПС України (економіка, право)*. 2014. № 2(65). С. 55-60.

13. Livingstone M.H. International terrorism in the contemporary World. Westport (Conn.). 1978.

14. Тоффлер Э., Тоффлер Х. Война и антивойна: Что такое война и как с ней бороться. Как выжить на рассвете XXI века; москва: АСТ: Транзиткнига, 2005. 412 с.

15. Хоффман Б. Терроризм – взгляд изнутри ; пер. с анг. Е. Сажина; москва: Ультра. Культура, 2003. 252 с.

16. Шмид А. Статистика терроризма: задачи определения тенденций в глобальном масштабе. *Форум по проблемам преступности и общества*. Т. 4. 2004. № 1, 2. С. 51-71.

17. Про боротьбу з тероризмом: Закон України від 20.03.03 р. № 638-IV. *Відомості Верховної Ради України*. 2003. № 25. Ст. 180. URL: https://zakon.rada.gov.ua/laws/show/638-15#Text

18. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.17 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

19. Про рішення Ради національної безпеки і оборони України від 15 жовтня 2021 року "Про Стратегію інформаційної безпеки": Указ Президента України від 28.12.21 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/685/2021#n2

20. Стратегія національної безпеки України: Указ Президента України від 14.09.20 р. № 392. URL: https://zakon.rada.gov.ua/laws/show/392/2020#Text

21. Стратегія державної безпеки: Указ Президента України від 16.02.22 р. № 56/2022. URL: https://zakon.rada.gov.ua/laws/show/56/2022#n5

22. Стратегія кібербезпеки безпеки України: Указ Президента України від 26.08.21 р. № 447/2021. URL: https://www.president.gov.ua/documents/4472021-40013

23. Макаренко Є.А., Рижиков М.М., Ожеван М.А. Міжнародні інформаційна безпека: сучасні виклики та загрози. Київ: Центр вільної преси, 2006. 916 с.

24. James A. Lewis Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. URL: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/02 1101_risks_of_cyberterror.pdf

25. Tafoya W.L. Cyber Terror. *FBI Law Enforcement Bulletin.* 2011. URL: http://www.fbi.gov/stats-services/publications/law-enforcementbulletin/november-2011/cyber-terror

26. Топчій В.В. Кібертероризм в Україні: поняття та запобігання кримінально-правовими та кримінологічними засобами. URL: http://www.lj.kherson.ua/2015/pravo06/part_3/16.pdf

27. Дзьобань О.П. Насильство інформаційне. Енциклопедія соціогуманітарної інформології. Київ: Видавничий дім "Гельветика", 2020. Т. 1. С. 151-155.

28. Інформаційна безпека та кібербезпека держави: аналітична доповідь до Щорічного послання Президента України до Верховної Ради України "Про внутрішнє та зовнішнє становище України в 2017 році". Київ: Національний інститут стратегічних досліджень, 2017. С. 47-56.

29. Victor Zhora. State Service of Special Communications and Information Protection of Ukraine. Russia's Cyber Tactics: Lessons Learned. 2022. URL: https://cip.gov.ua/en/news/russia-s-cyber-tactics-lessons-learned-in-2022-ssscip-analytical-report-on-the-year-of-russia-s-full-scale-cyberwar-against-ukraine

30. Білан І.А. Особливості застосування шкідливого програмного забезпечення спецслужбами країни-агресора. *Інформація і право*. № 2(45)/2023. С.139-152.

31. Франція посилала боротьбу з тероризмом. URL: https://www.ukrinform.ua/rubric-world/1995413-francia-posilila-borotbu-z-terorizmom.html

32. Романовский Г.Б. Противодействие терроризму в Германии: законодательные новеллы. *Наука. Общество. Государство.* – (Электронный научный журнал), 2019. Т. 7. № 4 (28). С. 33-39. URL: http://esj.pnzgu.ru ISSN 2307-9525

33. Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das Bundes kriminalamt / dejure.org. URL: https://dejure.org/BGBl/2008/BGBl._I_S._3083

34. Іноземний досвід протидії тероризму: висновки для України: аналітична записка. URL: https://niss.gov.ua/doslidzhennya/nacionalna-bezpeka/inozemniy-dosvid-protidii-terorizmu-visnovki-dlya-ukraini

35. Савченко А.В. Порівняльний аналіз кримінального законодавства України та федерального кримінального законодавства США: дис. …док-ра юрид. наук. 12.00.08. Київ: Акад. МВС України 2007. 614 с.

36. Проект Кримінального кодексу України за станом на 22 трав. 2023 року). URL: https://ewcriminalcode.org.ua/upload/media/2023/05/22/kontrolnyj-tekst-proektu-kk-22-05-2023.pdf

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