11. Васильєв А., Пироженко О. До питання про криміналізацію публічного заперечення чи виправдання злочинів фашизму (ст. 436-1 КК України). Актуальні сучасні проблеми кримінального права та кримінології у світлі реформування кримінальної юстиції: матеріали конф. МВС України. Харків: Кримінологічна асоціація України, ХНУВС, 2014. С. 17–21

12. Письменський Є.О. Кримінально-правова охорона національної та історичної пам'яті: плутаний шлях законодавця. Вісник Асоціації кримінального права України. 2015. Випуск 1 (4). URL: http://nauka.nlu.edu.ua/wp-content/uploads/2015/07/4_16.pdf (дата звернення: 01.04.2018).

13. Козюбра М.І. Загальна теорія права: підручник. Київ, 2015. 392 с.

14. Рішення ЄСПЛ від 13 грудня 2001 року у справі «Церква Бессарабської Митрополії проти Молдови» (№ 45701/99). URL: http://search.ligazakon.ua/l_doc2.nsf/link1/SO2340.html (дата звернення: 01.04.2018).

15. Науково-практичний коментар Кримінального кодексу України / за заг. ред. О. Литвинова. Київ, 2016. 536 с.

16. Кримінальне право України: Особлива частина: підручник / Ю. Баулін, В. Борисов, В. Тютюгін та ін.; за ред. проф. В. Тація, В. Борисова, В. Тютюгіна. 5-те вид. перероб. і допов. Харків, 2015. 680 с.

17. Рішення ЄСПЛ від 21 жовтня 2014 року у справі «Мурат Вурал проти Туреччини» (№ 9540/07). URL: https://globalfreedomofexpression.columbia.edu/cases/vural-v-turkey (дата звернення: 01.04.2018).

18. Денисова Т.А. Кримінальне покарання: жорстокість чи необхідність? Держава та регіони. Серія «Право». 2001. № 1. С. 102–105.

БЕЗСУСІДНЯ Ю. В.,
аспірант кафедри кримінального права
(Національна академія внутрішніх справ України)

УДК 343.326

НЕОБХІДНІСТЬ ЗАКОНОДАВЧОЇ РЕГЛАМЕНТАЦІЇ ПРОТИДІЇ КІБЕРНЕТИЧНІЙ ВІЙНІ

У статті охарактеризовано кібервійну як одну з ключових проблем вітчизняного законодавства у сфері національної безпеки держави. Розглянуто протидію кібервійні як елемент кримінально-правового захисту національної безпеки України; запропоновано внесення змін до чинного законодавства.

Ключові слова: *кібервійна, національна безпека, інформаційна безпека, кібербезпека, інформаційна війна, кібертероризм, загроза національній безпеці, національні інтереси.*

В статье охарактеризована кибервойна как одна из ключевых проблем отечественного законодательства в сфере национальной безопасности государства. Рассмотрено противодействие кибернетической войне как элемент уголовно-правовой защиты национальной безопасности Украины; предложено внести изменения в действующее законодательство.

Ключевые слова: *кибервойна, национальная безопасность, информационная безопасность, кибербезопасность, информационная война, кибертерроризм, угроза национальной безопасности, национальные интересы.*

The article describes cyberwar as one of the key problems of the domestic legislation in the field of national security of the state. The opposition to cyberwar as an element of criminal law protection of Ukraine's national security is considered; proposed amendments to the current legislation.

Key words: *cyberwar, national security, information security, cybersecurity, information warfare, cyberterrorism, threat to national security, national interests.*

Вступ. Проблема кібервійни є новим видом загроз для національної безпеки України та потребує більш глибокого вивчення. Уведення в чинне законодавство кібервійни як суспільно-небезпечного явища є способом кримінально-правового захисту основ національної безпеки України.

Постановка завдання. Метою статті є обґрунтування законодавчої регламентації кібернетичної війни (кібервійни) як суспільно небезпечного явища, яке загрожує інтересам національної безпеки України.

Кібервійна є об'єктом дослідження таких науковців, як В. Каберник, О. Ларіна, В. Овчинський, С. Гриняєв, М. Ожеван, Д. Дубов, О. Мережко та інші. Проте кібервійна як суспільно небезпечне явище, яке посягає на національну безпеку України, не було предметом дослідження цих науковців.

Результати дослідження. Проблеми національної безпеки належать до найважливіших, найскладніших багатоаспектних та інтегральних явищ суспільного й політичного життя.

Законодавча регламентація – це встановлення в законодавчих актах положень, правил, норм поведінки, що регулюють певне коло суспільних відносин.

Кримінально-правовий захист – це певна система кримінально-правових способів, до яких варто включити кримінально-правові норми та методи кримінально-правової політики, за допомогою яких нормативність права переводиться в упорядкованість суспільних відносин.

Крім Кримінального кодексу України, інші джерела, в тому числі закони й підзаконні акти, що регулюють основи національної безпеки України, також є джерелами кримінального права, однак таке регулювання має фрагментарний характер. Правоположення, що містяться в них, починають діяти, якщо в законі про кримінальну відповідальність відсутні необхідні для цього приписи. Отже, норми, що містяться в цих джерелах, доповнюють норми Кримінального кодексу України. Багато підзаконних актів спрямовані на правильне застосування норм закону про кримінальну відповідальність.

Отже, кримінально-правовий захист певних суспільних відносин, у тому числі основ національної безпеки України, здійснюється як через закон про кримінальну відповідальність, так і фрагментарно іншими законами України, в тому числі й Законом України «Про основи національної безпеки України».

Так, у статті 1 Закону України «Про основи національної безпеки України» від 19.06.2003 надано поняття «національна безпека» – це захищеність життєво важливих інтересів людини та громадянина, суспільства й держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення реальних і потенційних загроз національним інтересам у різних сферах, запобігання реальним і потенційним загрозам національним інтересам у різних сферах і нейтралізація їх, у тому числі й у сфері інформаційної безпеки.

Інформаційна безпека – це стан захищеності життєво важливих інтересів особистості, суспільства й держави, за якого запобігається завдання шкоди через неповноту, невчасність і невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване поширення, використання та порушення цілісності, конфіденційності й доступності інформації.

У науковій і спеціальній літературі інформаційна безпека розглядається як елемент або підсистема національної безпеки. У Законі України «Про основи національної безпеки

України» визначено дев'ять основних напрямів державної політики національної безпеки в різних сферах життєдіяльності. До однієї з них належить інформаційна, що дає всі підстави стверджувати, що інформаційна безпека є вагомим складником національної безпеки. На думку Б. Кормич, інформаційний аспект національної безпеки є її невід'ємним компонентом, так само як інформаційна безпека не може існувати поза межами загальної національної безпеки, національна безпека не буде всеохопною в разі позбавлення своїх інформаційних векторів. Згідно із Законом України «Про національну програму інформатизації», інформаційна безпека є невід'ємною частиною політичного, економічного, оборонного та інших складників національної безпеки [1, с. 5].

Кібербезпека – це окремий випадок інформаційної безпеки, поява якого зумовлена використанням комп'ютерних систем і/або телекомунікаційних мереж, тобто кібербезпека – це інформаційна безпека в умовах використання комп'ютерних систем і/або телекомунікаційних мереж [2, с. 54].

Відповідно до статті 1 Закону України «Про основи національної безпеки України», загрози національній безпеці – наявні та потенційно можливі явища й чинники, що створюють небезпеку життєво важливим національним інтересам України;

Загрози кібернетичній безпеці держави спільномірні загрозам воєнного характеру. Забезпечення кібернетичної безпеки – один із найважливіших напрямів забезпечення національної безпеки будь-якої держави.

У сучасному суспільстві існує суспільно небезпечне явище, що містить реальну загрозу національній безпеці, яке називають «кібернетична війна».

Термін «кібервійна» не є усталеним. Науковцями пропонується широкий спектр визначень кібервійни.

О. Тонконогов уважає кібернетичну війну особливим видом війни нового типу, яка здійснюється з метою дезорганізації всіх рівнів управління силами та засобами супротивника й виражена в проведенні спеціальних технологічних операцій, спрямованих на психологічний тиск і руйнування чи використання у власних цілях інформаційно-технічних ресурсів соціумів та армій противника шляхом створення й контролю через кібернетичні (електронні) комунікаційні мережі (головним чином Інтернет) віртуальної реальності [3].

О. Запорожець трактує термін «кібервійна» як комплекс ретельно спланованих і скоординованих суб'єктами міжнародних відносин кібератак деструктивного характеру на (критичну) інформаційну інфраструктуру супротивника з метою послаблення позицій об'єкта впливу й досягнення політичних, економічних і військових цілей. Кібервійна передбачає масштабне вторгнення на «територію» супротивника, якою в цьому випадку є електронні системи й мережі об'єкта впливу; наявність певного стратегічного плану; використання насильницьких засобів у вигляді шкідливого програмного забезпечення; завдання значної шкоди цим системам (тобто певні руйнування та жертви) тощо. Кібервійна так само є продовження політики іншими засобами й використовується для здійснення впливу на волю та можливості прийняття рішень політичного й військового керівництва супротивника [4, с. 81].

Кібервійна має специфічні риси. У кібервійні передусім неможливо ідентифікувати «агресора», навіть коли причетність до кібератаки державних структур певних країн багатьом видається очевидною. До того ж географічним джерелом кібератаки є, як правило, зовсім не та держава, якій така атака може бути об'єктивно вигідною.

По-друге, характерною рисою кібервійни є прихованість впливу й відсутність видимих руйнувань. Ця особливість пов'язана, з одного боку, з основним принципом кібервійни – експлуатацією уразливостей інформаційної інфраструктури супротивника, а з іншого – з непомітністю дій шкідливих програм, які зазвичай не призводять до людських жертв. Як наслідок, надзвичайно важко виявити початок кібератаки (тобто момент вторгнення), застосувати превентивні заходи для запобігання таким атакам, а також адекватно оцінити рівень загрози й масштаб завданих збитків.

По-третє, кібервійна відрізняється надзвичайною швидкістю проведення атак, коли проміжок часу між початком «агресії» та її наслідками скорочується до мінімуму.

До того ж шкідливі програми мають здатність швидко «розмножуватись» копіями і практично безперешкодно поширюватись у різних напрямах.

По-четверте, для кіберзброї не мають значення кордони й відстань, а також відсутні технологічні, юридичні та інші перешкоди для проникнення в комп'ютерні системи й мережі супротивника та віддаленого управління його ресурсами. Як наслідок, кібератаки й кібервійни важко піддаються контролю з боку державних систем розвідки та безпеки.

Важливою особливістю кібервійни є також певна незавершеність або нескінченність, оскільки жоден з учасників протистояння не може напевно сказати, що супротивник припинив атаки. Крім того, кібервійна може проводитись як у мирний час, так і в період звичайної війни.

Тобто кібервійна – це комплекс спланованих дій деструктивного характеру однієї національної держави з проникнення в комп'ютери або мережі іншої національної держави з метою спричинення шкоди національним інтересам держави та для досягнення певних політичних, економічних або військових цілей.

Варто зазначити, що не всі шкідливі дії в кіберпросторі можна назвати кібервійною. Так, на думку Мартіна Лібікі, до кібервійни не можна зарахувати шпигунство (яке може передувати кібервійні), фізичні атаки на мережі, створення радіоперешкод для пошкодження каналів радіозв'язку, а також психологічні операції (навіть якщо кібератаки мають психологічний ефект).

На законодавчому рівні інформаційна безпека держави в інформаційній сфері регулюється Конституцією України, яка містить концептуальні положення національної безпеки України в усіх сферах її існування, а також Концепцією національної безпеки України, Доктриною інформаційної безпеки України, Законом України «Про основи національної безпеки України» й іншими нормативними актами. У чинних нормативних актах серед загроз кібернетичній безпеці України відсутнє таке явище, як «кібервійна».

У статті 7 Закону України «Про основи національної безпеки України» серед загроз національним інтересам і національній безпеці України в інформаційній сфері визначено комп'ютерну злочинність і комп'ютерний тероризм, проте жоден із цих термінів не має свого визначення.

Кібервійна хоча й тісно пов'язана з кібертероризмом (комп'ютерним тероризмом), однак не є тотожним поняттям.

Низка авторів під кібертероризмом розуміють сукупність протиправних дій, пов'язаних із посяганням на життя людей, погрозами насильства, деструктивними діями стосовно матеріальних об'єктів та об'єктивної інформації, а також іншими діями, що сприяють нагнітанню страху й напруженості в суспільстві з метою отримання переваг під час вирішення політичних, економічних і соціальних завдань.

Так, В. Голубєв під кібертероризмом розуміє умисну атаку на інформацію, що обробляється комп'ютером, комп'ютерну систему чи мережу, яка створює небезпеку для життя і здоров'я людей чи настання інших тяжких наслідків, якщо ці дії вчинені з метою порушення громадської безпеки, залякування населення чи провокації воєнного конфлікту [6, с. 81].

На думку Ю. Гаврилова та Л. Смирнова, сутність кібертероризму полягає в здійсненні протиправного впливу на інформаційні системи, здійсненого з метою створення небезпеки заподіяння шкоди життю, здоров'ю чи майну невизначеного кола осіб шляхом створення умов для аварій і катастроф техногенного характеру чи реальної загрози такої небезпеки [6, с. 81].

Підсумовуючи викладене, можемо констатувати, що під кібертероризмом (комп'ютерним тероризмом) варто розуміти навмисну, політично вмотивовану атаку на інформацію, яка обробляється комп'ютером, комп'ютерну систему та мережі, що створює небезпеку для життя чи здоров'я людей або настання інших тяжких наслідків, якщо такі дії вчинені з метою порушення громадської безпеки, залякування населення, провокації воєнного конфлікту [6, с. 81].

Різниця між кібертероризмом і кібервійною полягає в тому, що кібертероризм націлений на умисне створення обстановки страху та напруження серед мирного населення,

в тому числі спричинення фізичної шкоди абсолютно випадковим людям у зоні проведення терористичного акту, і не має чітко визначеної мети. Натомість кібервійна має визначену конкретну мету для досягнення агресором певних геополітичних цілей.

Іншою характерною особливістю кібертероризму є його відкритість, умови терориста широко оповіщуються. Кібервійна, навпаки, має таємний характер.

Важливими ознаками кібервійни є те, що сторонами її є держави, кібертероризм же здійснюється, як правило, недержавними суб'єктами [6, с. 326].

Згідно з пунктом 3.6 Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287/2015, до загроз інформаційній безпеці зараховано ведення інформаційної війни проти України. Цей нормативний акт не містить визначення інформаційної війни.

Однак інформаційна війна та кібервійна являють собою два різновиди воєн, що проводяться в мережевому електронному просторі, який охоплює не лише інтернет, а й закриті державні, воєнні, корпоративні і приватні мережі. Для кожного із цих двох типів воєн характерні свої інструменти, методи, стратегії, тактики, закономірності.

Головне завдання інформаційних воєн полягає в маніпулюванні масами. Мета такої маніпуляції найчастіше полягає в унесенні в суспільну та індивідуальну свідомість ворожих, шкідливих ідей і поглядів; дезорієнтації та дезінформації мас; послабленні певних переконань; залякуванні свого народу образом ворога; залякуванні супротивника своєю могутністю; забезпеченні ринку збуту для своєї економіки. Інформаційна війна – це війна, метою якої є зміна масової, групової й індивідуальної свідомості [5, с. 326].

Як зазначають ізраїльські дослідники, основна відмінність між інформаційною війною в кіберпросторі та кібервійною полягає в тому, що в першому випадку використовуються інформація та повідомлення, представлені в зрозумілому для звичайних людей вигляді, а в другому випадку використовується мова комп'ютерів, зрозуміла лише інженерам та експертам з інформаційних технологій [4, с. 81].

По-друге, інформаційна війна в мережі Інтернет проводиться відкрито й передбачає безпосередній психологічний вплив на масову аудиторію. Кібернетична війна, навпаки, ведеться приховано, її безпосередня мета – пошкодження кібернетичних мереж і систем, завдання таким шляхом шкоди інтересам держави.

На підставі проведеного аналізу можемо сказати, що кібервійну не можна ототожнювати з кібернетичним тероризмом та інформаційною війною.

Щодо впливу кібернетичної війни на спричинення шкоди інтересам національної безпеки України, то із цього приводу існують різні думки.

Відповідно до ст. 1 Закону України «Про основи національної безпеки України», національні інтереси – життєво важливі матеріальні, інтелектуальні й духовні цінності Українського народу як носія суверенітету і єдиного джерела влади в Україні, визначальні потреби суспільства й держави, реалізація яких гарантує державний суверенітет України та її прогресивний розвиток.

Науковці мають різні думки щодо суспільної небезпечності впливу кібернетичної війни на національні інтереси держави.

На думку Мартіна Лібікі, попри потенційний масштаб і серйозність наслідків, кібервійна має досить обмежені можливості в досягненні політичних, економічних і військових цілей. За допомогою кібервійни неможливо роззброїти супротивника, окупувати його територію або змінити політичний режим у країні, кібервійна може слугувати лише засобом здійснення психологічного тиску на ворога, а також може на певний час завадити йому використовувати свої інформаційні системи та мережі належним чином [4, с. 82].

О. Запорожець підтримує позицію Мартіна Лібікі й уважає, що масовані кібератаки спричиняють лише тимчасові, локалізовані проблеми в політичній, економічній або інших сферах життєдіяльності країн – об'єктів впливу. Подібні атаки є скоріше способом попередження та психологічного тиску на іншу країну. За масштабом впливу й наслідками їх можна зарахувати до оперативно-тактичного рівня, а не стратегічного. На думку О. За-

порожця, на сучасному етапі навряд чи можна говорити про повномасштабні кібервійни. Однак не виключено, що в майбутньому технологічно розвинуті країни зможуть вивести кібератаки на стратегічний рівень, подібний за рівнем організованості, комплексності, масштабності й наслідками до традиційної війни [4, с. 82].

Протилежної думки дотримується А. Капто, який указує, що кібервійна – один із нових видів війни, заснований на сучасних технологіях, це не самостійний вид протиборства, кібервійна завжди є складовою частиною інформаційної війни, загалом є елементом повномасштабної воєнної кампанії. Кібервійна не існує поза традиційною війною. Вона передбачає порушення діяльності чи повне виведення з ладу систем управління державою і збройними силами за рахунок впливу на комп'ютерні мережі, в результаті чого державні та воєнні інститути можуть опинитися повністю виведеними з ладу [7, с. 617].

А. Капто зазначає, що кібервійна – це вища ступінь кіберконфлікту між державами, під час якого кібератаки є складовими частинами воєнної операції. Кібервійні передують спочатку кібератака, а потім кіберконфлікт, у який утягуються дві чи більше держав або політичних груп, коли ворожі кібератаки провокують у відповідь аналогічні дії.

Отже, кібервійна являє собою суспільно небезпечне явище, яке може завдати шкоди національній безпеці України в різних її сферах.

Кібервійна може бути характеристикою об'єктивної сторони низки злочинів проти основ національної безпеки України, що містяться в розділі I Особливої частини Кримінального кодексу України, в тому числі передбачених статтею 109 («Дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади»); статтею 110 («Посягання на територіальну цілісність і недоторканність України»); статтею 113 («Диверсія»); статтею 114 («Шпигунство»); статтею 114-1 («Перешкоджання законній діяльності Збройних Сил України та інших військових формувань»).

Як уже згадувалось, у чинних нормативних актах відсутнє визначення такого явища, як «кібервійна». Вищевказаний недолік законодавства не дає змоги використовувати цей термін з метою характеристики об'єктивної сторони та способу вчинення злочинів проти основ національної безпеки України.

Висновки. Кримінально-правовий захист основ національної безпеки України здійснюється із застосуванням фрагментарно законодавства у сфері національної безпеки, в тому числі Закону України «Про основи національної безпеки України». В останньому Законі надано як поняття національної безпеки, так й інші терміни, які характеризують національну безпеку України. Однак у термінології цього Закону відсутнє поняття «кібернетична війна». Визначення такого явища як суспільно небезпечного дасть змогу використовувати цей термін у галузі кримінального права в тому числі з метою характеристики об'єктивної сторони низки злочинів проти основ національної безпеки України. З такою метою автор пропонує внести відповідні зміни в чинне законодавство у сфері національної безпеки:

- статтю 1 «Визначення термінів» Закону України «Про основи національної безпеки України» доповнити терміном «кібернетична війна»;
- статтю 7 Закону України «Про основи національної безпеки України» доповнити положенням, що кібернетична війна є загрозою національній безпеці України в інформаційній сфері.

Список використаних джерел:

1. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: навчальний посібник. Київ: Кондор, 2004. 384 с.

2. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». Правова інформатика. 2014. Вип. 2 (42). С. 54–62.

3. Тонконогов А.В. Кибернетическая безопасность: понятие и сущность феномена. Аналитический интернет-портал «Отрасли права». 30.05.2015. URL: http://отрасли-права.рф/article/7472.

4. Запорожець О.Ю. Кібервійна: концептуальний вимір. Актуальні проблеми міжнародних відносин. 2014. Вип. 121. Частина І. С. 81–89.

5. Паршин С.А. Современные американские подходы к проблеме кибертерроризма. Вестник Московского университета. Серия 25 «Международные отношения и мировая политика». Москва, 2011. № 3. С. 81–105.

6. Шпига П.С., Рудник Р.М. Основні технології та закономірності інформаційної війни. Проблеми міжнародних відносин. 2014. Вип. 8. С. 326–339.

7. Капто А.С. Кибервойна: генезис и доктринальные очертания. Вестник Российской академии наук. 2013. Том 83. № 7. С. 616–625.

ДАН Г. В.,
ад'юнкт кафедри кримінології та кримінально-виконавчого права
(Національна академія внутрішніх справ)

УДК 343.85 (477)

ІСТОРІЯ РОЗВИТКУ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ЗАПОБІГАННЯ ВИКОРИСТАННЯ МАЛОЛІТНЬОЇ ДИТИНИ ДЛЯ ЗАНЯТТЯ ЖЕБРАЦТВОМ

У статті проведено комплексний історико-правовий аналіз становлення та розвитку кримінально-правового забезпечення запобігання використанню малолітньої дитини як жебрака. Автором проведено історичний аналіз захисту дітей від заняття жебрацтвом нормами вітчизняних та закордонних галузей права, що дозволило виявити стійку тенденцію нехтування правами дітей із найдавніших часів до кінця XIX – початку XX ст.

Ключові слова: *дитина, жебрацтво, запобігання, історико-правовий аналіз, злочинність, кримінальна відповідальність.*

В статье проведен комплексный историко-правовой анализ становления и развития уголовно-правового обеспечения предотвращения использования малолетнего ребенка для занятия попрошайничеством. Автор провел исторический анализ защиты детей от занятия попрошайничеством нормами отечественных и зарубежных отраслей права, что позволило выявить устойчивую тенденцию пренебрежения правами детей с древнейших времен до конца XIX – начала XX в.

Ключевые слова: *ребенок, попрошайничество, предотвращение, историко-правовой анализ, преступность, уголовная ответственность.*

The article provides a comprehensive historical and legal analysis of the formation and development of criminal-legal provision for the prevention of the use of a young child for begging. The author carried out a historical analysis of the protection of children from begging with the norms of domestic and foreign branches of law, which revealed a steady tendency to neglect children's rights from ancient times to the end of the nineteenth and early twentieth centuries.

Key words: *child, begging, prevention, historical-legal analysis, crime, criminal liability.*