***УДК 351.86:007***

***Таволжанський Олексій Володимирович –***
*кандидат юридичних наук,*
*доцент кафедри кримінології та кримінально-виконавчого права*
*Національного юридичного університету імені Ярослава Мудрого*

***Oleksii V. Tavolzhanskyi –***
*candidate of juridical sciences,*
*assistant professor of department of criminology and penitentiary law Yaroslav Mudryi National Law University (77 Pushkinska Street, Kharkiv, 61024, Ukraine)*

# Інформаційна безпека України: стан правового забезпечення в контексті глобалізаційних процесів

*В статті розглянуто законодавче закріплення та вирішення питань інформаційної безпеки України. Наведено деякі проблеми нормотворчого процесу врегулювання запобігання кіберзлочинності. Проаналізовано актуальні питання системного підходу для захисту держави і суспільства в інформаційній сфері.*

***Ключові слова:*** *інформаційна безпека, кіберзлочин, кіберзлочинність, кібербезпека, кіберпростір, інформаційне законодавство.*

*В статье рассмотрено законодательное закрепление и решение вопросов информационной безопасности Украины. Приведены некоторые проблемы нормотворческого процесса урегулирования предотвращения киберпреступности. Проанализированы актуальные вопросы системного подхода для защиты государства и общества в информационной сфере.*

***Ключевые слова:*** *информационная безопасность, киберпреступность, киберпреступность, кибербезопасность, киберпространство, информационное законодательство.*

***O.V. Tavolzhanskyi Information Security of Ukraine: the State of Legal Security in the Context of Globalization Processes***

*The article deals with the legislative consolidation and resolution of the issues of information security of Ukraine. Some problems of normative process of cybercrime settlement are presented. The actual questions of a systematic approach to the protection of the state and society in the information sphere are analyzed.*

*The absence of a proper normative regulation of cybersecurity in Ukraine under hybrid cyber warfare significantly increases the risk of collapse of the national information security system and also questions the involvement of Ukrainian units in providing cyber security at the international level.*

*Information security aims at the protection of the sovereignty and territorial integrity of Ukraine, ensuring its economic security. Undoubtedly, these spheres of life are closely linked and the inadequate regulation in one sphere will inevitably lead to negative consequences in the other.*

*The emergence of a special legislative act on cybersecurity activates an integrated process for regulating cybersecurity as a separate important sector. In turn, considerable efforts of theorists and practitioners are required to improve the operating normative system.*

***Keywords:*** *information security, cybercrime, cybercrime, cyber security, cyberspace, information legislation.*

**Постановка проблеми.** Україна знаходиться на початку формування національного законодавства в сфері кібербезпеки. Безумовно дуже важливо саме зараз використовувати всі можливості, для того, щоб створити ефективні механізми інформаційного захисту.

Нормативно-правові акти з кіберзахисту мають різновекторний характер, не додержання принципів системності і послідовності, фактично створює віртуальний простір зручним для

кіберпосягань. У зв'язку з чим є нагальна потреба узгодження правових норм єдиним принципам, цілям і методам, можливо в подальшому з виокремленням окремої галузі права.

**Аналіз останніх досліджень та публікацій.** Протягом останніх декількох десятиліть, на теренах України, збільшується кількість публікацій стосовно розвитку теми поліпшення законодавчого врегулювання безпеки інформаційного простору. Серед робіт, безпосередньо спрямованих на вирішення питань інформаційної безпеки в цілому та проблематики нормотворчого аналізу у кіберсфері зокрема, можна відмітити публікації В. М. Бегми, В. П., І. Г. Луценко, Малінка, К. В. Рубеля, В.Ю. Степанова, А. І. Марущака, в яких проведено не лише аналіз різних джерел на предмет інформаційної безпеки, а й надане власне розуміння дефініцій, що впорядковують правовідносини інформаційної безпеки України. Значне місце тема нормативного врегулювання інформаційної безпеки, посідає і у деяких публікаціях таких вчених, як Сніцаренко П.М., Саричев Ю.О., Ткаченко В [1]. Крім цього, в Україні прийнято низку належних до сфери інформаційної безпеки загальнодержавних нормативно термінологічних стандартів та нормативних документів, які є актами прямої дії за певними напрямами інформаційної діяльності.

**Невирішені раніше проблеми.** Відсутність в Україні належного нормативного врегулювання кібербезпеки в умовах гібридної кібер війни значно підвищує ризики руйнування національної системи інформаційної безпеки, а також ставить під сумнів участь українських ланок у забезпеченні кібербезпеки на міжнародному рівнях. Як зазначають фахівці на сьогоднішній день в Україні відсутній єдиний центр координації роботи щодо законодавчого та нормативно-правового забезпечення ефективної системи кібербезпеки, яка би б базувалась на комплексному аналізі наявного стану в цій сфері, викликів, наявних та потенційних загроз, враховувала інтереси усіх зацікавлених осіб, інтегрувалась в європейську та глобальну міжнародну систему кібербезпеки, мала б достатнє фінансове, організаційне, технічне, кадрове забезпечення [2, с. 8].

**Метою статті є** виходячи із зазначеного, метою статті є розгляд і аналіз чинного законодавства України в сфері інформаційної безпеки, а також загальнотеоретичних передумов, необхідності його удосконалення з питань кібербезпеки держави.

**Виклад основного матеріалу.** Норми права щодо кібербезпеки Україні можна розділити за різними критеріями. Безумовно при встановленні правил на національному рівні мають бути враховані міжнародні договори, згода на обов'язковість яких надана Верховною Радою України але це питання окремого дослідження. Законодавство у кіберсфері можна розподілити за суб'єктом прийняття на ті що прийняті міжнародними інституціями і ті що створені національними право творцями. У цій роботі в першу чергу спробуємо більш докладно розглянути саме другу групу чинних на території України нормативно-правових документів.

Аналізуючи національне законодавство в сфері кіберзахисту його можна розподілити за ієрархією на такі групи нормативно-правових актів: Конституція України, норми Кримінального кодексу України, Закони України, постанови та рішення Кабінету Міністрів України, Укази Президента України, рішення інших суб'єктів діяльність яких безпосередньо пов'язана з інформаційною безпекою держави. Класифікація законодавства від основного закону країни до локальних актів передбачає цілісне і єдине розуміння об'єкту на який спрямоване врегулювання. Визначення специфічних методів досягнення поставлених цілей. Безумовне підпорядкування норм підзаконних актів нормам законів України в сфері захисту інформації.

Конституція України, відповідно до положень статті 17 найважливішою функцією держави визначає захист інформаційної безпеки. Окрім того Основний Закон України опосередковано покладає обов'язок щодо досягнення кібербезпеки і на суспільство, вказуючи, що інформаційна безпека є справою всього Українського народу. Фактично ця норма розділяє усі правовідносини пов'язані в сфері інформаційної безпеки на дві основні групи: публічну і приватну. В той же час ця теза несе спільну домовленість що існує в суспільстві с приводу забезпечення інформаційної безпеки у тому числі через добровільну відмову кожного члена суспільства від частини свобод і прав.

Інформаційна безпека знаходиться на одному щаблі з захистом суверенітету і

територіальної цілісності України, забезпеченням її економічної безпеки. Безумовно, що зазначені сфери життя тісно пов'язані і неналежне право регулювання в одній сфері з неминучістю призведе до негативних наслідків в іншій.

Окремо слід звернути увагу на норми приватності інформації, що знайшли свого закріплення в Конституції України. На думку деяких авторів відсутність чіткого розуміння того, чим власне є інформаційна безпека», призводить до того, що її предметна сфера штучно розширюється на дуже великий діапазон цілей: починаючи від іміджу держави, забезпечення інформаційних прав громадян і до боротьби з корупцією. Серед іншого до «інформаційної безпеки» відносять і ті її аспекти, які в західній науковій та юридичній практиці прийнято відносити саме до проблем кібербезпеки [3]. Хоча більш прийнятною є думка, що інформаційна безпека включає в себе не лише зовнішні загрози, а й внутрішні атаки, окрему групу яких складаються зловживання владними повноваженнями. Відповідно до політики інформаційної безпеки в Україні кожному гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо (стаття 31). Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України (стаття 32). Відповідно до Офіційного тлумачення положення частини першої статті 32 в Рішенні Конституційного Суду в аспекті конституційного подання положення частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України слід розуміти так: інформацією про особисте та сімейне життя особи є будь-які відомості та/або дані про відносини немайнового та майнового характеру, обставини, події, стосунки тощо, пов'язані з особою та членами її сім'ї, за винятком передбаченої законами інформації, що стосується здійснення особою, яка займає посаду, пов'язану з виконанням функцій держави або органів місцевого самоврядування, посадових або службових повноважень. Така інформація про особу є конфіденційною; збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди державою, органами місцевого самоврядування, юридичними або фізичними особами є втручанням в її особисте та сімейне життя. Таке втручання допускається виняткова у випадках, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.

За загальним правилом не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди. Виключенням може бути лише випадки, визначені законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Кожний громадянин має право знайомитися в органах державної влади, органах місцевого самоврядування, установах і організаціях з відомостями про себе, які не є державною або іншою захищеною законом таємницею. Кожному гарантується судовий захист права спростовувати недостовірну інформацію про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації.

Після введення в правовий обіг основним Законом країни терміну інформаційна безпека, у 1998 році з'явився інший термін — «інформаційний суверенітет». Його становлення, на законодавчому рівні, визнано одним із пріоритетних напрямків державної політики. Відповідно Закон України «Про Національну програму інформатизації» встановлено, що інформаційний суверенітет це — «здатність держави контролювати і регулювати потоки інформації з-поза меж держави з метою додержання законів України, прав і свобод громадян, гарантування національної безпеки держави» (ст. 1). Така дефініція породжує більше питань ніж відповідей, а інноваційному світі втрачає сенс, оскільки, широке тлумачення невизначеного поняття «інформаційних потоків», не окреслює зміст і основні ознаки явища, також, не зовсім нормативним виглядає словосполучення «інформацією з-поза меж держави», ну і звичайно знімається будь-яка

відповідальність за не належний «контроль і регулювання» на такі протиправні дії.

Ще до нормативного закріплення інформаційної безпеки держави в Конституції України, у 1994 розі Законом України «Про захист інформації в інформаційно-телекомунікаційних системах» було надано поняття захисту інформації в системі. Відповідно до зазначеного закону це діяльність, спрямована на запобігання несанкціонованість діям щодо інформації в системі. Згаданим Законом передбачено два варіанти захисту інформації, а саме:

криптографічний захист інформації — вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо; технічний захист інформації — вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації [4]. Відповідно до положень статті 13 (прикінцеві положення) цей Закон набирав чинності з 1 січня 2006 року. У 2006 році з'являється Закон України "Про Державну службу спеціального зв'язку та захисту інформації України" дія якого спрямована в першу чергу на захист інформації публічного сектору. Зокрема введено поняття протидія технічним розвідкам, що означає комплекс правових, організаційних та інженерно-технічних заходів, спрямованих на запобігання або ускладнення добування засобами технічної розвідки інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, про зразки озброєння, військову та спеціальну техніку, об'єкти оборонно-промислового комплексу, військові та інші об'єкти, діяльність державних органів, військових формувань, утворених відповідно до законів України, підприємств, установ і організацій в інтересах оборони і безпеки держави.

Відповідно до чинної редакції вказаного вище Закону основними завданнями Державної служби спеціального зв'язку та захисту інформації України є: формування та реалізація державної політики у сферах криптографічного та технічного захисту інформації, кіберзахисту, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах (далі - інформаційно-телекомунікаційні системи) і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціювання, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку; участь у формуванні та реалізації державної політики у сферах електронного документообігу (в частині захисту інформації державних органів та органів місцевого самоврядування), електронної ідентифікації (з використанням електронних довірчих послуг), електронних довірчих послуг (у частині встановлення вимог з безпеки та захисту інформації під час надання та використання електронних довірчих послуг, контролю за дотриманням вимог законодавства у сфері електронних довірчих послуг); забезпечення в установленому порядку та в межах компетенції діяльності суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом.

Поштовхом в забезпеченні інформаційної безпеки, але вже через призму кіберзагроз, – була ратифікована Верховною Радою України Конвенція про кіберзлочинність [5]. Цей поза державний регулятор вперше на міжнародному рівні закріпив основні вимог, щодо убезпечення віртуального, цифрового простору, проте зосереджений на протидії кримінальним посяганням (шахрайство, підроблення, поширення дитячої порнографії, порушення авторських прав тощо) з використанням комп'ютерної техніки та різноманітних мереж. Окрім того, в Конвенції нормативне визначення основної термінології (зокрема "кіберзлочин", "кіберзлочинець", "кіберзлочинність", тощо).

Наступним кроком у визначенні інформаційної безпеки країни було прийняття Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–

2015 роки» [6]. У ньому під інформаційною безпекою розуміється «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; несанкціонованість розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації». Включення оціночних термінів в норми права не завжди є доцільним, зокрема не має жодної необхідності вводити таку ознаку, як «негативний інформаційний вплив», як вказують деякі вчені це багато в чому розширює поле «інформаційної безпеки», що дозволяє постійно включати до нього нові елементи безпекової сфери, штучно роздмухуючи коло правовідносин, що вміщує це поняття.

На виконання положень зазначеного вище Закону України Кабінет Міністрів України прийняв Стратегію розвитку інформаційного суспільства в Україні, якою було визначено мету, базові принципи, стратегічні цілі розвитку інформаційного суспільства в Україні, завдання, спрямовані на їх досягнення, а також основні напрями, етапи і механізм реалізації цієї Стратегії з урахуванням сучасних тенденцій та особливостей розвитку України в перспективі до 2020 року. Також своїм розпорядженням від 15 серпня 2007 р. N 653-р Кабінет Міністрів України ввів в дію досить розгалужений план заходів з виконання завдань, передбачених Законом України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки". Але ці документи потребують окремого докладного вивчення.

9 травня 2018 року, введено в дію Закон України «Про основні засади забезпечення кібербезпеки України» [7]. Поява цього акту досить логічна і послідовна, ним визначено загальні правові та організаційні напрямки забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у віртуальному просторі, функції і обов'язки органів, підприємств, установ, організацій, у тому числі державної форми власності, осіб та громадян, форми координації їх діяльності, а також базові терміни у сфері інформаційної і кібербезпеки.

Вважаємо позитивною стороною появи цього акта, є покладення на Державна служба спеціального зв'язку та захисту інформації України обов'язок із забезпечення створення Національної телекомунікаційної мережі та Державного центру кіберзахисту, функціювання урядової команди реагування на комп'ютерні надзвичайні події CERT-UA для аналізу даних про кіберінциденти та для надання практичної допомоги щодо усунення їх наслідків. CERT-UA має розміщувати офіційні рекомендації щодо протидії кіберзагрозам та взаємодіяти з правоохоронцями по їх попередженню. Окрім того визначено основні об'єкти на які має бути спрямовані заходи з кіберзахисту. Такі об'єкти мають створити критичну інфраструктуру країни. Сформульовано принципи забезпечення кібербезпеки та національну систему кібербезпеки. Кординацію діяльності у сфері кібербезпеки здійснює Президент України через очолювану ним Раду національної безпеки та оборони. Поява спеціального законодавчого акту з приводу кібербезпеки активує комплексний процес регулювання кібербезпеки, як окремої важливої галузі. Наступним етапом має стати перелік об'єктів критичної інфраструктури від Кабміну (об'єкти, що мають життєво важливе значення для функціювання держави).

Загалом Закон розширив і доповнив положення Стратегії кібербезпеки України, затвердженої указом Президента України в 2016 році. Водночас, основним досягненням закону «Про основні засади забезпечення кібербезпеки України» є імплементація в правове поле визначень, що стосуються кібербезпеки, Кібератаки і кіберзахисту.

**Висновок.** Зараз на часі приведення нормативно-правових актів у відповідність до вимог Закону України "Про основні засади забезпечення кібербезпеки України". В той же час є й інші сторони які потребують уваги і додаткового опрацювання. Зокрема, Сніцаренко П.М., Саричев Ю.О.,; Ткаченко В.А. щодо національного законодавства в сфері інформаційної безпеки вказують на наявність методологічної помилки, наслідком якої стало введення в чинне інформаційне законодавство таких суперечливих актів: Стратегії кібербезпеки України, Доктрини інформаційної безпеки

України, а також Закону України "Про основні засади забезпечення кібербезпеки України". Суперечливість названих актів, на думку вказаних науковців полягає, по-перше, у відсутності їх підпорядкованості єдиній державній інформаційній політиці, яка в Україні, ще не визначена на законодавчому рівні, а отже не сформована, а по-друге, у слабкості термінологічної бази, як теоретичної основи сутності нормативних положень, викладених у цих документах. Особливо негативне враження викликає термінологічна база Закону України "Про основні засади забезпечення кібербезпеки України", яку слід визнати принципово недосконалою, що перешкоджає розглядати адекватно для практики значну кількість його положень. Це вимагає внесення, встановленим порядком, необхідних змін у термінологічну та, у відповідній інтерпретації, в змістовну частину цього закону – одного з найважливіших серед законодавчих актів щодо забезпечення інформаційної безпеки України [8]. З вказаною обґрунтованою критикою не можна не погодитись, але поява зазначених документів викликає наукову дискусію, що в подальшому можливо дозволить виправити допущені помилки.

**Список використаних джерел:**


1. Сніцаренко П. М. Актуальні передумови необхідності розвитку інформаційного законодавства України / П. М. Сніцаренко, Ю. О. Саричев, В. А. Ткаченко // Права, свободи і безпека людини в інформаційній сфері : матеріали наук.-практ. конф. / Упоряд. : В. М. Фурашев, С. Ю. Петряєв : Нац. техн. ун-т України «КПІ ім. Ігоря Сікорського». – 10 трав. 2018 р. – Київ : КПІ ім. Ігоря Сікорського, Вид-во «Політехніка», 2018. – С. 80-84.
2. Пропозиції ропозиції до політики щодо реформування до політики щодо реформування сфери кібербезпеки в Україні [Електронний ресурс]. – Режим доступу : http://parlament.org.ua/wp-content/uploads/2017/10/Policy-Paper_Kiberbezpeka.pdf.
3. Ширська В. С. Аспекти кібербезпеки України / В. С. Ширська // Кібербезпека в Україні: правові та організаційні питання : матеріали Всеукраїнської науково-практичної конференції (м. Одеса, 17 листопада 2017 р.). – Одеса: Одеський державний університет внутрішніх справ, 2017. – С. 58-60.
4. Про захист інформації в інформаційно-телекомунікаційних системах [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/show/en/80/94-%D0%B2%D1%80.
5. Конвенція про кіберзлочинність від 23 листопада 2001 року [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/show/994_575.
6. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/show/537?-16.
7. Про основні засади забезпечення кібербезпеки України : Закон України [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/show/2163-19.
8. Рішення Конституційного Суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України [Електронний ресурс]. – Режим доступу : http://zakon.rada.gov.ua/laws/show/v002p710-12#n51.


**References:**


1. P. M. Snitsarenko Aktualni peredumovy neobkhidnosti rozvytku informatsiinoho zakonodavstva Ukrainy / P. M. Snitsarenko, Yu. O. Sarychev, V. A. Tkachenko // Prava, svobody i bezpeka liudyny v informatsiinii sferi : materialy nauk.-prakt. konf. / Uporiad. : V. M. Furashev, S. Yu. Petriaiev : Nats. tekhn. un-t Ukrainy "KPI im. Ihoria Sikorskoho". – 10 trav. 2018 r. – Kyiv : KPI im. Ihoria Sikorskoho, Vyd-vo "Politekhnika", 2018. – Pp. 80-84.

2. Propozytsii ropozytsii do polityky shchodo reformuvannia do polityky shchodo reformuvannia sfery kiberbezpeky v Ukraini [Elektronnyi resurs]. – Rezhym dostupu : http://parlament.org.ua/wp-content/uploads/2017/10/Policy-Paper_Kiberbezpeka.pdf.

3. V. S. Shchyrska, Aspekty kiberbezpeky Ukrainy / V. S. Shchyrska // Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia : materialy Vseukrainskoi naukovo-praktychnoi konferentsii (m. Odesa, 17 lystopada 2017 r.). – Odesa: Odeskyi derzhavnyi universytet vnutrishnikh sprav, 2017. – S. 58-60.

4. Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh [Elektronnyi resurs]. – Rezhym dostupu : http://zakon.rada.gov.ua/laws/show/en/80/94-%D0%B2%D1%80.

5. Konventsiia pro kiberzlochynnist vid 23 lystopada 2001 roku [Elektronnyi resurs]. – Rezhym dostupu : http://zakon.rada.gov.ua/laws/show/994_575.

6. Pro Osnovni zasady rozvytku informatsiinoho suspilstva v Ukraini na 2007–2015 roky [Elektronnyi resurs]. – Rezhym dostupu : http://zakon.rada.gov.ua/laws/show/537?-16.

7. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy : Zakon Ukrainy [Elektronnyi resurs]. – Rezhym dostupu : http://zakon.rada.gov.ua/laws/show/2163-19.

8. Rishennia Konstytutsiinoho Sudu Ukrainy u spravi za konstytutsiinym podanniam Zhashkivskoi raionnoi rady Cherkaskoi oblasti shchodo ofitsiinoho tlumachennia polozhen chastyn pershoi, druhoi statti 32, chastyn druhoi, tretoi statti 34 Konstytutsii Ukrainy [Elektronnyi resurs]. – Rezhym dostupu : http://zakon.rada.gov.ua/laws/show/v002p710-12#n51.