Определено, что свобода и творчество имеют диалектическаю связь в их единстве как целое и часть. Соотношение свободы и свободы творчества сводится к аналогии положительного и отрицательного аспектов свободы. Соотношение свободы творчества и права на свободу творчества выражается в том, что свобода творчества является понятием более широким чем право на свободу творчества.

***Ключевые слова**: право, свобода, творчество, свобода творчества, право на свободу творчества*

Opolska N. The Legal Dimension of the Freedom Creativity.

The article analyzes the theoretically-legal basics of the freedom creativity. This article reveals the legal dimension of the freedom creativity on the analysis principle of the basic freedom, law and creativity concepts. This article determinants the correlation of the dyads, such as "freedom – creativity freedom", "creativity – freedom", "right – freedom" and "right to the creativity freedom – creativity freedom".

The article defined that the freedom as well as the creativity has a dialectical connection in the unity of as an integral whole so and a separate part. The relation between the freedom and the creativity freedom is reduced to the analogy of the positive and negative aspects of freedom. The relations between the creativity freedom and the right to the freedom of creation are expressed in the aspect that the creativity freedom is a wider notion than the right for the freedom creativity.

***Keywords:** right, freedom, creativity, the freedom creativity, the right for the freedom creativity*

АДМІНІСТРАТИВНЕ ТА ІНФОРМАЦІЙНЕ ПРАВО

УДК 004.056.5:343.326

Довгань О. Д.
доктор юридичних наук, с.н.с.,
перший заступник директора з наукової роботи
Науково-дослідного інституту інформатики і права
Національної академії правових наук України

Доронін І. М.
кандидат юридичних наук, доцент,
завідувач наукової лабораторії права
національної безпеки та військового права
Науково-дослідного інституту інформатики і права
Національної академії правових наук України

РОЗВИТОК ЗАКОНОДАВСТВА У СФЕРІ КІБЕРБЕЗПЕКИ: ІНФОРМАЦІЙНО-ПРАВОВЕ ДОСЛІДЖЕННЯ

У статті досліджуються проблеми пов'язанні з формуванням правової основи у сфері кібербезпеки. Акцентується увага на доцільність формування відповідного масиву нормативно-правових актів, що складатимуть безпосереднє законодавство у сфері забезпечення кібербезпеки.

***Ключові слова**: кібербезпека, забезпечення кібербезпеки, кіберпростір, кіберзагрози, кіберінциденти, кібервійна, кіберзахист, правова регламентація у сфері кібербезпеки, законодавство у сфері кібербезпеки.*

Питання необхідності створення цілісної та узгодженої системи забезпечення інформаційного суверенітету, управління ризиками і можливостями новітніх викликів у інформаційній сфері, розбудови власних спроможностей надійних та достовірних державних комунікацій та створення тісної взаємодії між органами влади, формування інфраструктури національного інформаційного простору з метою створення умов для його інтегрування у світовий інформаційний простір, налагодження комунікаційного процесу між органами влади та споживачами інформації та інше в сучасних умовах залишаються актуальними, а питання кібербезпеки, у т.ч. її правового регулювання, у нашій державі має надзвичайно велике значення.

Дослідженню різнобічних аспектів кібернетичної безпеки присвячені праці значної кількості вітчизняних та зарубіжних науковців. Проте, незважаючи на значний рівень наукового осмислення проблем кібернетичної безпеки, в сучасних умовах стрімкого розвитку інформаційних технологій, засобів та способів ведення інформаційних війн нагальними є питання удосконалення її забезпечення, правового регулювання у цій сфері, що й обумовлює актуальність наукової статті.

Метою статті є визначення стану розвитку законодавства у сфері кібербезпеки, яке буде сформовано на відповідному масиві нормативно-правових актів.

Після ухвалення 20 грудня 2002 року Генеральною асамблею ООН резолюції 57/239 "Елементи для створення глобальної культури кібербезпеки" [1] термін "кібербезпека" почав активно використовуватись у вітчизняній правовій термінології. До цього поняття кібербезпеки у понятійному апараті нормативно-правових актів не використовувалось і в основному сприймалось як технічний термін у контексті заходів технічного захисту інформації.

Для імплементації положень резолюції ООН більш детально проаналізуємо її зміст. Зокрема, Генеральна асамблея ООН констатувала, що стрімкий розвиток інформаційної технології означає зміну підходів державних органів, організацій та індивідуальних користувачів до питання кібербезпеки. Звичайно, що комп'ютерна злочинність виникла одночасно із розповсюдженням комп'ютерних мереж, тому протидія комп'ютерній злочинності (та кіберзлочинності) було предметом міжнародного співробітництва, починаючи з 1990-х років [2]. Але питання забезпечення кібербезпеки вийшло далеко за межі діяльності правоохоронних органів із протидії злочинності, оскільки загрози у цій сфері не обмежуються лише злочинною діяльністю. У термінології, яку використовує ООН, мова йде про глобальну культуру кібербезпеки, для визначення якої, було визначено дев'ять взаємопов'язаних елементів:

– *обізнаність* (тобто учасники повинні бути обізнані щодо необхідності безпеки інформаційних систем та мереж, а також про те, що саме вони можуть здійснити для підвищення безпеки);

– *відповідальність* (учасники відповідають за безпеку мереж відповідно до власної ролі);

– *реагування* (учасники мають вживати своєчасних та спільних заходів щодо попередження інцидентів, які стосуються безпеки, їх виявленню та реагуванню, у тому числі обмінюватись інформацією і вводити процедури, які передбачають оперативне та ефективні співробітництво з попередження, виявлення та реагування таки

інцидентів);

– *етика* (врахування законних інтересів інших);

– *демократія* (безпека повинна забезпечуватись таким чином, щоб це відповідало демократичним цінностям, включаючи свободу обміну думками та ідеями, вільний потік інформації, конфіденційність інформації, належний захист приватної інформації; відкритість та гласність);

– *оцінка ризиків* (учасники повинні здійснювати періодичну оцінку ризиків з метою виявлення загроз та факторів уразливості, мати належні технології та інструменти контролю для цього з урахуванням значущості інформації, яка захищається);

– *проектування та впровадження засобів забезпечення безпеки*;

– *переоцінка* (належні та своєчасні заходи з внесення змін в політику, практику забезпечення безпеки з врахуванням нових та зміни існуючих загроз).

На 58-й сесії Генеральної асамблеї ООН 23 грудня 2003 року в розвиток раніше ухвалених положень було прийнято резолюцію 58/199 "Створення глобальної культури кіберпростору і захист найважливіших інформаційних інфраструктур" з додатком "Елементи для захисту найважливіших інформаційних інфраструктур" [3]. Останній містить вимоги до систем забезпечення кібербезпеки у напряму захисту найважливіших інформаційних інфраструктур.

Чергова резолюція "Створення глобальної культури кібербезпеки та оцінка національних зусиль по захисту найважливіших інформаційних інфраструктур" [4], мала за мету оцінити ефективність заходів, що вживались на виконання раніше ухвалених резолюцій Генеральної асамблеї. При цьому було застосовано метод проведення самооцінки на підставі доданого документу – "Інструменту національної самооцінки національних зусиль по захисту найважливіших інформаційних інфраструктур". Окрім цього, технічні питання заходів із забезпечення кібербезпеки були викладені у Глобальній програмі кібербезпеки Міжнародного союзу електрозв'язку 2007 року [5].

В Україні правова регламентація питань ужиття заходів з кібербезпеки (окрім деяких суто кримінально-правових аспектів) в основному було зумовлено вимогами євроатлантичної інтеграції держави і випливало з доктрин, стратегій та настанов НАТО і Євросоюзу. Як зазначалося вище, питання забезпечення кібербезпеки далеко не вичерпані кримінально-правовими аспектами, тому доцільно проаналізувати стан регламентації цих питань на рівні документів стратегічного планування у сфері національної безпеки України.

Відповідно до ст. 2 Закону України "Про основи національної безпеки України" [6] цільові настанови та керівні принципи воєнного будівництва, а також напрями діяльності органів державної влади в конкретній обстановці з метою своєчасного виявлення, відвернення і нейтралізації реальних і потенційних загроз національним інтересам України визначаються Стратегією національної безпеки України і Воєнною доктриною України. Ці документи є, обов'язковими для виконання і основою для розробки конкретних програм за складовими державної політики національної безпеки.

Але слід зазначити, що положення цього Закону оминули питання регламентації забезпечення кібербезпеки. Серед загроз національній безпеці України у сфері

інформаційної безпеки ст. 7 Закону було визначено комп'ютерну злочинність та комп'ютерний тероризм.

У подальшому у п. 2.8 Стратегії національної безпеки, затвердженої Указом Президента України від 12 лютого 2007 року № 105 [7], стан безпеки інформаційно-комп'ютерних систем в галузі державного управління фінансової і банківської сфери, енергетики транспорту, внутрішніх та міжнародних комунікацій охарактеризовано як такий, що *"наближається до критичного"*. Такий висновок зроблено не тільки із врахуванням їх вразливості перед проявами комп'ютерної злочинності, а й виходячи із усього спектра питань підтримання зазначених систем у належному технічному стані, що дає змогу адекватно та ефективно виконувати поставлені завдання.

Окрім цього, у п. 4.1 зазначеної Стратегії з метою реалізації державної політики було визнано за необхідне розробку та впровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих з відповідними європейськими стандартами, у тому числі згідно з вимогами Конвенції про кіберзлочинність. Варто зазначити, що запропонований у першій редакції Стратегії національної безпеки підхід, який з одного боку передбачав пріоритет державного впливу на рівні національних стандартів та технічних регламентів, а з іншого – зумовлював вжиття заходів правового регулювання відповідно до вимог міжнародно-правових актів, взятих на себе міжнародних зобов'язань та вимог гармонізації законодавства до європейських стандартів, був цілком адекватним тодішній обстановці та повністю відповідав елементам для створення глобальної культури кібербезпеки, визначеним резолюцією Генеральної асамблеї ООН.

У подальшому Указом Президента України від 8 червня 2012 року № 389 було затверджено нову редакцію Стратегії національної безпеки України "Україна у світі, що змінюється" [8]. Характеризуючи у документі безпекове середовище, серед чинників впливу на національну безпеку було визначено і нездатність держави протистояти викликам, пов'язаним із застосуванням інформаційних технологій в умовах глобалізації, насамперед кіберзагрозам. При цьому на той час залишалась без змін і редакція ст. 8 Закону України "Про основи національної безпеки України", яка серед загроз в інформаційній сфері визначала такі: *"прояви обмеження свободи слова та доступу громадян до інформації; поширення засобами масової інформації культу насильства, жорстокості, порнографії; комп'ютерна злочинність та комп'ютерний тероризм; розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави; намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації"*.

Отже, визначені на рівні документу стратегічного планування новітні виклики та загрози фактично не було імплементовано на рівні спеціального законодавчого акту, що регламентує основи національної безпеки, оскільки комп'ютерна злочинність та комп'ютерний тероризм далеко не повністю охоплюють такі загрози.

Серед завдань забезпечення інформаційної безпеки, окрім визначених у першій редакції Стратегії, додатково також було зазначено наступні: *"стимулювання впровадження новітніх інформаційних технологій і виробництва конкурентоспроможного*

національного інформаційного продукту, зокрема сучасних засобів і систем захисту інформаційних ресурсів; забезпечення безпеки інформаційно-телекомунікаційних систем, що функціонують в інтересах управління державою, забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки, систем управління об'єктами критичної інфраструктури; створення національної системи кібербезпеки". Отже, мова йшла про низку реальних заходів організаційного характеру, у тому числі і створення національних систем управління у цій сфері.

У сучасних умовах фактичної гібридної війни, яка ведеться проти України в активній фазі з весни 2014 року, питання забезпечення кібербезпеки має надзвичайно важливе значення.

Слід зазначити, що у такій гібридній війні значне місце мають бойові дії у кіберпросторі. Мова йде про "кібератаки", які вочевидь здійснювались та підтримувались іноземними державами, і за своєю суттю мали характер агресії. Можна стверджувати, що застосування існуючих категорій війни до таких дій відбулось після так званих "естонських кіберінцидентів" 09.05.2007.

"Естонськими кіберінцидентами" називають масштабні дії, сплановані та скоординовані з Росії, стосовно державних органів та об'єктів інфраструктури Естонії, які відбувались у кіберпросторі і полягали у нанесенні шкоди зазначеним об'єктам [9]. "Естонські кіберінциденти" були першими такими діями і за своїми наслідками призвели до збитків для інфраструктури держави, хоча і в менших масштабах ніж кібератаки проти України 2015–2017 років. Але реагування на зазначені інциденти з боку НАТО відбувалось в декількох сферах, однією з яких була сфера застосування положень міжнародного права, а саме права війни, до кібервійни, яка відбувається у кіберпросторі, інші стосувались реформування системи протидії загрозам воєнного характеру і кіберпросторі та технічне удосконалення існуючих систем кіберзахисту [10].

Питання забезпечення кібербезпеки виділені у чинній редакції Стратегії національної безпеки України [11]. Зокрема, серед загроз інформаційній безпеці визначено: *"ведення інформаційної війни проти України; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства"*. Перша з окреслених загроз констатує факт наявності інформаційної війни проти нашої держави як продовження бойових дій специфічними методами. Друга визначає умови, за яких методи інформаційної війни, що застосовуються противником, досягають поставлених ним цілей.

Загрозами кібербезпеці і безпеці інформаційних ресурсів згідно з положеннями Стратегії є: *"уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак;фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом"*. Це говорить про обмеженість характеристики загроз кібербезпеці, а фактично її зведено лише до проведення кібератак щодо державних інформаційних ресурсів та застарілості системи охорони інформації з обмеженим доступом, хоча дещо застаріла система зберігання інформації з обмеженим доступом переважно на паперових носіях інформації робить таку систему досить стійкою з точки зору загроз саме у сфері кібербезпеки. З іншого боку визначення Стратегією як окремої загрози ведення інформаційної війни проти України розширило поле, що характеризує загрози у кіберпросторі.

У подальшому основні напрями державної політики забезпечення саме кібербезпеки було окреслено у Стратегії кібербезпеки України [12]. Метою якої є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Як показує аналіз пріоритетів та напрямів державної політики щодо забезпечення кібербезпеки, що визначені у розділі 4 Стратегії кібербезпеки, переважна більшість з них стосуються організаційних заходів, які є взаємопов'язаними і повинні складати відповідну систему забезпечення кібербезпеки. Що стосується заходів правового регулювання питань забезпечення кібербезпеки, то Стратегією визнано за доцільне проведення гармонізації вітчизняного законодавства у відповідність до вимог НАТО та ЄС, комплексне вдосконалення правової основи кіберзахисту об'єктів критичної інфраструктури, подальшого розвитку кримінально-правової охорони суспільних відносин у цій сфері, боротьбу з кіберзлочинністю.

Ужиття заходів, визначених чинними Стратегією національної безпеки України та Стратегією кібербезпеки, зумовило зміни у чинному законодавстві, насамперед з метою подальшого унормування суспільних відносин, пов'язаних з реалізацією таких функцій держави, як оборона та забезпечення державної безпеки.

На розвиток цього було ухвалено низку доктринальних документів і підзаконних нормативно-правових актів, серед яких Концепція розвитку сектору безпеки і оборони України, затверджена Указом Президента України від 14 березня 2016 року № 92, Стратегічний оборонний бюлетень, уведений в дію Указом Президента України від 6 червня 2016 року № 240, Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 7 червня 2016 року № 242, Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, затверджений постановою Кабінету Міністрів України від 23 серпня 2016 року № 563 та низка інших.

Як показує аналіз зазначених актів, переважна більшість з них встановлює загальні засади державної політики і визначає окремі підходи до унормування питань забезпечення кібербезпеки. Водночас, деякі заходи та стратегічні підходи не повною мірою базуються на науковому підґрунті, що неодмінно призведе до виникнення спірних питань стосовно правової регламентації.

Окремо слід згадати спеціальний законодавчий акт з питань кібербезпеки – "Про основні засади забезпечення кібербезпеки України" від 5 жовтня 2017 року, що досить тривалий час розглядався Верховною Радою України і був неоднозначно сприйнятий суспільством та бізнес-спільнотою. Згідно п. 1 його Прикінцевих та перехідних положень Закон набуває чинності через 6 місяців після його опублікування. Офіційне опублікування тексту законодавчого акту відбулось у газеті "Голос України" 9 листопада 2017 року, тому він набирає чинності 9 травня 2018 року – рівно через 11 років після "естонських кіберінцидентів".

Як визначено у його преамбулі, цей Закон *"визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки"* [13].

Отже згідно задекларованих у преамбулі положень законом фактично встановлюються можливість та засади регулювання за допомогою норм вітчизняного права у кіберпросторі з метою забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, а також національних інтересів України.

Частина 1 стаття 2 Закону містить виключення щодо його дії. Зокрема, Закон не поширюється на: *"відносини та послуги, пов'язані із змістом інформації, що обробляється (передається, зберігається) в комунікаційних та/або в технологічних системах; діяльність, пов'язану із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення; соціальні мережі, приватні електронні інформаційні ресурси в мережі Інтернет (включаючи блог-платформи, відеохостинги, інші веб-ресурси), якщо такі інформаційні ресурси не містять інформацію, необхідність захисту якої встановлена законом, відносини та послуги, пов'язані з функціонуванням таких мереж і ресурсів; комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій (електронними мережами загального користування), не підключені до мережі Інтернет та/або інших глобальних мереж передачі даних (крім технологічних систем)"* [14].

Зазначені правові дефініції потребуватимуть у майбутньому роз'яснень і не виключено, що вимагатимуть подальших змін у чинному законодавстві. Аналіз приписів, що містяться у пунктах 1 та 4 частини 1 статті 2 дозволяє зробити висновок про їх тотожність у багатьох аспектах. Узагальнюючи приписи, можливо зробити висновок, що дія Закону не розповсюджуватиметься на внутрішні (локальні) комп'ютерні мережі, що не взаємодіють (не підключені) до глобальних комп'ютерних мереж. Обмеження щодо інформації, яка становить державну таємницю, діятимуть відповідно до приписів актів спеціального законодавства у цій сфері. Водночас, відносини, що складаються при використанні соціальних мереж, а також "приватних" інформаційних електронних ресурсів *(хоча, судячи з усього мова йде про недержавні ресурси)* не регламентуються Законом "Про основні засади забезпечення кібербезпеки в Україні" за певних умов – відсутності інформації, необхідність захисту якої встановлено законом. Зазначене положення викликатиме певні труднощі оскільки приписи чинної редакції Закону України "Про інформацію" [15] (ст. 10) визначає *дев'ять* видів інформації і цей перелік не є вичерпним. Згідно ст. 11 цього ж Закону обмеження встановлені щодо інформації про фізичну особу (персональні дані), а щодо інших визначено наявність особливостей правового режиму щодо кожного виду, який встановлюватиметься законодавчими актами. Щодо обмеженості доступу до інформації, то відповідно до ст. 21 Закону "Про інформацію" встановлено 3 види інформації з обмеженим доступом – конфіденційна, таємна та службова. Конфіденційною при цьому вважається інформація про фізичну особу, а також інформація доступ до якої обмежено фізичною чи юридичною особою за умови неналежності цієї інформації до публічної. Таким чином, визначення належності чи неналежності функціонування тих чи інших "приватних" електронних ресурсів та соціальних мереж до сфери дії Закону "Про основні засади забезпечення кібербезпеки України" є складним питанням, що потребуватиме додаткових роз'яснень.

Закон встановлює перелік об'єктів кібербезпеки та кіберзахисту. Під

кібербезпекою розуміється *"захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі"*, а під кіберзахистом – *"сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем"* (пункти 5 та 7 частини 1 статті 1 Закону). Таким чином деякі об'єкти можуть бути одночасно об'єктами і кібербезпеки, і кіберзахисту.

Зокрема, об'єктами кібербезпеки є: *"конституційні права і свободи людини і громадянина;суспільство, сталий розвиток інформаційного суспільства та цифрового комунікативного середовища; держава, її конституційний лад, суверенітет, територіальна цілісність і недоторканність; національні інтереси в усіх сферах життєдіяльності особи, суспільства та держави; об'єкти критичної інфраструктури"*.

Останній з об'єктів кібербезпеки (як об'єкт критичної інформаційної інфраструктури) є одночасно і об'єктом кіберзахисту. Законодавець до їх числа відносить зокрема: *"комунікаційні системи всіх форм власності, в яких обробляються національні інформаційні ресурси та/або які використовуються в інтересах органів державної влади, органів місцевого самоврядування, правоохоронних органів та військових формувань, утворених відповідно до закону; об'єкти критичної інформаційної інфраструктури;комунікаційні системи, які використовуються для задоволення суспільних потреб та/або реалізації правовідносин у сферах електронного урядування, електронних державних послуг, електронної комерції, електронного документообігу"* [16].

Зазначений перелік є вичерпним хоча і зумовлює необхідність у додаткових роз'ясненнях. Зокрема, встановлено, що перелік об'єктів критичної інформаційної інфраструктури визначає Кабінет Міністрів України та Національний банк України. З об'єктами критичної інфраструктури ситуація не така однозначна. Зокрема, згідно порядку [17] такий перелік затверджується Кабінетом Міністрів України на підставі погоджених з СБУ пропозицій державних органів, що подаються до Адміністрації Держспецзв'язку України. Чинне законодавство також містить дещо неузгоджені терміни, оскільки за буквальним тлумаченням приписів нормативно-правових актів одночасно Кабінет Міністрів України вестиме переліки об'єктів критичної інфраструктури, об'єктів критичної інформаційної інфраструктури та інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави.

Питання визначення таких об'єктів на жаль попри на очевидну важливість для забезпечення національної безпеки дещо розпорошується у сучасних умовах, оскільки у літературі та деяких нормативно-правових документах вживаються терміни щодо об'єктів критичної інфраструктури у різних сферах, а переліки таких об'єктів по суті несформовані.

Окрім цього виникатиме питання і щодо суб'єктів, підстав та порядку прийняття рішень стосовно належності конкретних комунікаційних систем до об'єктів

кіберзахисту в розумінні Закону України "Про основні засади забезпечення кібербезпеки України". Тим більше, що ужиття терміну "комунікаційна система" не спирається на законодавчу дефініцію.

Не дивлячись на огріхи, прийняття цього Закону дозволяє впровадити комплексний підхід під егідою держави і у тісному співробітництві з приватним сектором і громадянським суспільством та створює умови для забезпечення кіберзахисту критично важливих інфраструктурних об'єктів України.

Крім цього, у Законі йдеться про так звану "державно-приватну взаємодію" у сфері кібербезпеки. Документ зобов'язує держустанови, підприємства і навіть окремих громадян сприяти органам держбезпеки, повідомляючи, наприклад, про кіберзагрози.

Важливим у цьому законі є й те, що він запроваджує відповідальність, у тому числі кримінальну, за злочини, вчинені саме в кіберпросторі. І як раніше згадували у Законі також тлумачаться самі поняття "кібербезпеки", "кіберзахисту" та "кіберзлочинності", які вже понад десятиліття використовують у юридичній практиці, у тому числі у зв'язку із вчиненими в мережі злочинами, але які досі не були ніде закріплені в документах.

Більшість експертів загалом схвально відгукуються про його ухвалення – як базового документу, хоча у ньому й є ціла низка недопрацювань. Водночас на нашу думку, ще зарано говорити про ефективність цього закону для підвищення рівня кібербезпеки.

Поки не будуть сформовані суб'єкти, які безпосередньо займатимуться оперативним реагуванням на кіберінциденти, поки в цих суб'єктів не буде належної технічної бази та висококваліфікованих спеціалістів, що в свою чергу потребує належного фінансування, – всі заявлені в законопроекті положення так і залишаться на папері. Тепер справа за урядом, суб'єктами забезпечення кібербезпеки, які мають розробити вимоги до захисту критичних інфраструктур, нові стандарти і методики та забезпечити контроль за ефективністю кіберзахисту.

Підсумовуючи стан розвитку вітчизняного законодавства у сфері забезпечення кібербезпеки можливо прийти до наступних основних висновків.

Розвиток вітчизняного законодавства у сфері забезпечення кібербезпеки відбувався поступово із врахуванням документів міжнародно-правового характеру у розрізі резолюцій Генеральної асамблеї ООН щодо культури кібербезпеки у сучасних умовах. Стан та ступінь загроз у кіберпросторі зумовили реагування держави у документах стратегічного характеру у сфері національної безпеки і оборони України. Агресія проти України у 2014 році, що відбувалась з активним використанням бойових дій проти нашої держави у кіберпросторі, а також посилення загальносвітових загроз кібербезпеці зумовили формування спеціального законодавства. Найбільш активно зазначений процес відбувався останні два роки. 8 травня 2018 року набуває чинності Закон України "Про основні засади забезпечення кібербезпеки України" від 5 жовтня 2017 року. Цей Закон є комплексним спеціальним законодавчим актом у сфері забезпечення кібербезпеки. Попри деякі неоднозначні формулювання у тексті законодавчого акту і можливі питання з його практичним застосуванням, слід зазначити, що період формування національного законодавства у сфері кібербезпеки розпочатий, а основний акт спеціального законодавства, що започатковує відповідну систему законодавства, ухвалений. У подальшому буде сформований відповідний

масив нормативно-правових актів, що складатимуть безпосереднє законодавство у сфері забезпечення кібербезпеки. Одночасно буде відбуватись процес узгодження положень нового законодавства кібербезпеки з нормами права, насамперед у галузі кримінального, адміністративного, цивільного права.

В и к о р и с т а н і д ж е р е л а :

1. Резолюция Генеральной Ассамблеи ООН 57/329, принятая на 78 пленарном заседании 57-й сессии. 20 декабря 2002 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N02/555/24/PDF/N0255524.pdf?OpenElement (дата звернення: 27.11.2017).
2. *Волеводз А. Г.* Противодействие компьютерным преступлениям. Правовые основы международного сотрудничества / А. Г. Волеводз. – М. : Юрлитинформ, 2002. – 496 с. – С. 9-11.
3. Резолюция Генеральной Ассамблеи ООН 58/199, принятая на 78 пленарном заседании 58-й сессии. 23 декабря 2003 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N03/506/54/PDF/N0350654.pdf?OpenElement (дата звернення: 27.11.2017).
4. Резолюция Генеральной Ассамблеи ООН 64/211, принятая на 66 пленарном заседании 64-й сессии. 21 декабря 2009 года URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N09/474/51/PDF/N0947451.pdf?OpenElement (дата звернення: 27.11.2017).
5. Global Cybersecurity Agenda (GCA). 17.09.2007 URL : https://www.itu.int/ITU-D/cyb/events/2007/Geneva/docs/kitaw-global-cybersecurity-agenda-geneva-17-sept-07.pdf (дата звернення: 27.11.2017).
6. Про основи національної безпеки України : Закон України від 19.06.2003 р. № 964-IV: Дата оновлення 30.11.2017. URL: http://zakon3.rada.gov.ua/laws/main/964-15 (дата звернення: 03.12.2017).
7. Стратегія національної безпеки України: затв. Указом Президента України від 12.02.2007 № 105. Офіційний вісник України. 2007. 23.02.2007. № 11. – С. 7. Ст. 389.
8. Про рішення Ради національної безпеки і оборони України від 8 червня 2012 року "Про нову редакцію Стратегії національної безпеки України": Указ Президента України від 08.06.2012 № 389. Офіційний вісник України. 2012. 22.06.2012. № 45. С. 104. Ст. 1749.
9. *Czosseck C., Ottis R, Taliharm A-M.* Estonia after 2007 Cyber Attacks: Legal, Strategic and Organizational Changes in Cyber Security// Proceedings of the 10th European Conference on Information Warfare and Security: 10th European Conference on Information Warfare and Security, Tallinn, 7-8 July 2011. Ed. Ottis, R. Reading, UK: Academic Publishing Limited, P. 57–64.
10. *Ilves L., Evans T., Ciluffo F., Nadeau A.* European Union and NATO Global Cybersecurity Challenges. URL: http://cco.ndu.edu/LinkClick.aspx?fileticket=HVj82hUX7_s%3D&portalid=96 (дата звернення: 03.12.2017).
11. Стратегія національної безпеки України: затв. Указом Президента України від 26.05.2015 № 287. Офіційний вісник України. 09.06.2015. № 43. С. 14. Ст. 1353.
12. Стратегія кібербезпеки України: затв. Указом Президента України від 15.03.2016 № 96. Офіційний вісник України. 29.03.2017. № 23. С. 69. Ст. 899.
13. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19. (дата звернення: 03.12.2017).
14. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19. (дата звернення: 03.12.2017).
15. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. Дата оновлення 01.01.2017. URL: http: //zakon3.rada.gov.ua/laws/main/2657-12 (дата звернення: 03.12.2017).
16. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 р. № 2163-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2163-19. (дата звернення: 03.12.2017).
17. Порядок формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави: затв. Постановою Кабінету Міністрів України від 23.08.2016 № 563. Урядовий кур'єр. 08.09.2016. № 168.

Довгань А. Д., Доронин И. М. Развитие законодательства в сфере кибербезопасности: информационно-правовое исследование.

В статье исследуются проблемы связанные с формированием правовой базы в сфере кибербезопасности. Акцентируется внимание на целесообразность формирования соответствующего массива нормативно-правовых актов, которые будут составлять непосредственное законодательство в сфере обеспечения кибербезопасности.

***Ключевые слова**: кибербезопасность, обеспечение кибербезопасности, киберпространство, киберугрозы, киберинциденты, кибервойна, киберзащита, правовая регламентация в сфере кибербезопасности, законодательство в сфере кибербезопасности.*

Dovgan O., Doronin I. Development of cybersecurity legislation: information and legal research.

The article researched problems of formations and development of cyber security legislation. The authors propose to form a complex of legislation on cybersecurity adequate to modern threats.

***Keywords:** cybersecurity, cyber threats, cyber space, cyber incidents, cyber war, cyber protection, cybersecurity legislation.*

УДК 342.9(477):35.083.8

Морозова О. О.
кандидат політичних наук, доцент,
доцент кафедри правознавства
Національного педагогічного університету
імені М. П. Драгоманова

ПРАВОВА ОХОРОНА ДЕРЖАВНОЇ ТАЄМНИЦІ В УКРАЇНІ

В Україні створено і діє національна система охорони державної таємниці. Діючим законодавством визначено правовий статус державної таємниці і перелік відомостей, що відноситься до цього виду інформації з обмеженим доступом, визначено організацію охорони державної таємниці, розподілені повноваження усіх органів, що забезпечують охорону цього найважливішого виду інформації, встановлено відповідальність за розголошення відповідної інформації.

***Ключові слова**: державна таємниця, інформація з обмеженим доступом, правова охорона державної таємниці.*

В травні 1993 року з метою реалізації державної політики національної безпеки України у сфері охорони державної таємниці було створено спеціально уповноважений центральний орган державної виконавчої влади – Державний комітет з питань державних секретів України (Держкомсекретів України). На Держкомсекретів України були покладені такі завдання: – участь у формуванні та реалізації проведення державної політики з охорони державної таємниці у сферах оборони, економіки, зовнішніх відносин, державної безпеки та охорони правопорядку; – організація, координація та контроль режимно-секретної діяльності державних органів, органів місцевого та регіонального самоврядування, підприємств, установ, організацій, незалежно від форми власності.

Однією з головних складових реалізації державної політики у сфері охорони державної таємниці було створення відповідної нормативно-правової бази. Фахівцями Держкомсекретів України було, безпосередньо, розроблено та забезпечено введення в дію цілої низки загальнодержавних нормативно-правових актів, зокрема: Закону