УДК 351.746:007(477)

Демиденко В. О. – кандидат юридичних наук, доцент, професор кафедри конституційного права та прав людини Національної академії внутрішніх справ, м. Київ
ORCID 0000-0001-6771-0080

Принципи застосування органами місцевого самоврядування законодавства України у сфері кібербезпеки

Констатовано, що масштабні кібератаки проти України, які відбулися протягом останніх років, засвідчують неготовність державного апарату, органів місцевого самоврядування, правоохоронних органів, медіа, приватного сектору до протидії цим кіберзагрозам і мінімізації їх негативних наслідків.

Доведено доцільність дотримання певних принципів органами місцевого самоврядування та іншими суб'єктами, наділеними державно-владними повноваженнями, під час застосовування законодавства України у сфері забезпечення кібербезпеки, що сприятиме ефективності захисту національного кіберпростору. Аргументовано, що, згідно із Законом України «Про основні засади забезпечення кібербезпеки України», до таких принципів належить потреба в регулюванні, відповідно до якого рішення (заходи) суб'єктів владних повноважень мають бути необхідними та мінімально достатніми для досягнення мети й завдань забезпечення кібербезпеки нашої держави.

Окреслено також принципи об'єктивності та правової визначеності, прозорості, забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, послуг із захисту інформації, кіберзахисту, зокрема прав щодо невтручання в приватне життя та захисту персональних даних.

Попри те, що хоча правозастосовні акти органів місцевого самоврядування у сфері забезпечення кібербезпеки мають переважно персоніфікований характер, не розраховані на багаторазове використання, загальний конституційний принцип дії цих актів у часі збережено. Доведено, що принципи застосування законодавства у сфері кібербезпеки та прийняття суб'єктами владних повноважень рішень у цій сфері є рівнозначними, їх застосовують з метою безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства й держави.

Ключові слова: органи місцевого самоврядування; принципи; кібербезпека; кіберзагроза; правозастосовні акти; національне законодавство.

Постановка проблеми. Протягом останніх п'яти років ми стали свідками низки масштабних кібератак проти України. Остання масова кібератака 2017 року, здійснена за допомогою

модифікованої версії вірусу Wannacry – Petya.A, яскраво засвідчила неготовність державного апарату, органів місцевого самоврядування, правоохоронних органів, медіа, приватного сектору до протидії таким кіберзагрозам і мінімізації їх негативних наслідків.

Від неї постраждали органи державної влади (Кабінет Міністрів України, МВС України, Міністерство інфраструктури України, Київська міська державна адміністрація, департамент кіберполіції тощо), органи місцевого самоврядування (сервісні системи Київської та Львівської міських рад), великі стратегічні підприємства, зокрема критичної інфраструктури (наприклад, аеропорт «Бориспіль», ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця), медіакомпанії (телеканали «Інтер», «СТБ», «ICTV», «24 канал», різні інтернет-видання) тощо. Фінансові збитки становлять декілька мільярдів гривень.

Згідно з прогнозами ІТ-фахівців, щорічно кількість таких кібератак буде збільшуватися, причому вони будуть глобальнішими. Останнє зумовлено з-поміж іншого виявом агресії Росії проти України, невід'ємним й особливо небезпечним елементом якої є кібератаки.

Вищезазначене дає змогу констатувати, що перед Україною нині постало нагальне завдання щодо формування системної, комплексної державної політики у сфері забезпечення кібербезпеки, яка міститиме низку адаптованих до сучасних реальних і потенційних викликів правових, організаційних, фінансово-економічних, технічних, науково-експертних та інших заходів. Це, власне, й зумовлює мету підготовки пропонованої статті. Дослідження передбачає ґрунтовний аналіз особливостей реалізації законодавства України у сфері кібербезпеки, зокрема визначальних засад і принципів його застосування органами місцевого самоврядування.

Виклад основного матеріалу. Першими кроками в Україні щодо формування правового поля протидії кібератакам були Стратегія кібербезпеки України [1], Стратегія національної безпеки України [2], Основні засади забезпечення кібербезпеки України [3] тощо.

Водночас для забезпечення ефективної реалізації зазначених стратегічних документів, протидії реальним і потенційним кіберінцидентам нині вкрай бракує належного науково-експертного супроводження цих процесів. Проблемною залишається сфера

науково-теоретичного забезпечення кібербезпеки органами місцевого самоврядування України.

Відповідно до ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII, органи місцевого самоврядування є одним із суб'єктів забезпечення кібербезпеки в Україні. Безперечно, важлива роль у цьому належить Кабінету Міністрів України, Національному координаційному центру кібербезпеки, Міністерству оборони України, Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національній поліції України та іншим державним інституціям.

Попри широкий спектр суб'єктів забезпечення кібербезпеки в Україні, посилену увагу слід приділяти захисту кіберпростору у сфері функціонування органів місцевого самоврядування, оскільки вони становлять найбільший пласт суспільних відносин, пов'язаних із реалізацією їхньої компетенції в різних сферах забезпечення життєдіяльності. Крім цього, значущість захищеності життєво важливих інтересів людини та громадянина, суспільства й держави під час використання кіберпростору у сфері функціонування органів місцевого самоврядування буде лише зростати, що зумовлено, передусім поступовою децентралізацією публічної влади, прагненням до зміцнення фінансових засад територіальних громад тощо.

Важливою передумовою підвищення ефективності захисту національного кіберпростору є застосування органами місцевого самоврядування (як, власне, й іншими суб'єктами з державно-владними повноваженнями) вітчизняного законодавства у сфері забезпечення кібербезпеки з дотриманням певних чітких принципів.

Зокрема, ідеться про Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII, де закріплено потребу в мінімально необхідному регулюванні. Згідно із цим принципом, рішення (заходи) суб'єктів владних повноважень мають бути необхідними та мінімально достатніми для досягнення мети й завдань із забезпечення кібербезпеки України.

Цей принцип передбачає, що правозастосовна діяльність суб'єктів владних повноважень повинна органічно поєднувати два аспекти. Так, з одного боку, регулювання суспільних відносин щодо забезпечення кібербезпеки в Україні суб'єктами владних повноважень передбачає мінімальне втручання в цю

сферу. Воно не повинно бути бюрократизованим, надмірно регульованим. Адже активне втручання органів публічної влади, їх посадових і службових осіб у цю сферу призведе до певного обмеження прав і свобод людей щодо вільної комунікації через функціонування сумісних (з'єднаних) комунікаційних систем і забезпечення електронних комунікацій із використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Це негативно позначиться на можливостях громадянського суспільства щодо протидії корупції, громадянського контролю за законністю й ефективністю діяльності органів публічної влади, реалізації принципу народовладдя, а також перешкоджатиме активному залученню громадян до управління державою та вирішення питань місцевого значення, унеможливить формування глобального інтерактивного ринку ідей, досліджень та інновацій тощо. Таким чином, може виникнути ситуація, за якої елементарні відносини не витримають тиску нагромаджених зверху норм і приписів, що, зрештою, призведе до збоїв у роботі – від ігнорування до цілковитого заперечення [3].

З іншого боку, як органи місцевого самоврядування, так й інші суб'єкти з державно-владними повноваженнями мають здійснювати регулювання суспільних відносин щодо забезпечення кібербезпеки в Україні тією мірою, яка однозначно забезпечить формування ефективної національної системи кібербезпеки, тобто сукупності політичних, соціальних, економічних та інформаційних відносин одночасно з організаційно-адміністративними й техніко-технологічними заходами шляхом комплексного підходу в тісній взаємодії державного, муніципального та приватного секторів і громадянського суспільства.

Важливим принципом застосування законодавства у сфері забезпечення кібербезпеки є об'єктивність і правова визначеність, максимально можливе застосування національного та міжнародного права щодо повноважень й обов'язків державних органів, органів місцевого самоврядування, підприємств, установ, організацій, громадян у сфері кібербезпеки.

Застосовуючи законодавство України у сфері забезпечення кібербезпеки, органи місцевого самоврядування повинні максимально точно й усебічно аналізувати події та дії суб'єктів правовідносин щодо електронних комунікацій, захисту муніципальних інформаційних ресурсів, інформації тощо, ураховуючи їхню багатогранність і суперечливість, позитивні

та негативні аспекти, на підставі цього приймати правове легітимне рішення. Прийняття такого рішення має відповідати положенням національного та міжнародного права.

Під час застосування правових норм національного та міжнародного права може постати питання щодо співвідношення юридичної сили вітчизняних і міжнародних нормативно-правових актів із забезпечення кібербезпеки. Варто наголосити, що в системі нормативно-правових актів України в зазначеній сфері найвищу юридичну силу має Конституція України та конституційні закони, зокрема щодо міжнародних договорів різних видів і суб'єктного складу. Якщо співвідносити юридичну силу національних нормативно-правових актів (за винятком актів Конституційного Суду України) та міжнародних договорів у сфері кібербезпеки, пріоритет належить саме міжнародним договорам, про що йдеться в ч. 2 ст. 19 Закону України «Про міжнародні договори» [4].

Крім цього, зазначене правозастосовне рішення органів місцевого самоврядування має бути чітким та однозначним.

У контексті вивчення проблематики дослідження варто звернутися до змісту доповіді Європейської комісії «За демократію через право» (Венеціанської комісії) щодо верховенства права, затвердженої на 86-му пленарному засіданні (м. Венеція, 25–26 березня 2011 року), у якій було зазначено, що однією зі складових верховенства права є правова визначеність. Вона вимагає, щоб правові норми були чіткими й точними, забезпечували постійну прогнозованість ситуацій правовідносин [5].

Наступним принципом застосування законодавства у сфері кібербезпеки органами місцевого самоврядування й суб'єктами з державно-владними повноваженнями є забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій, послуг із захисту інформації, кіберзахисту, зокрема прав щодо невтручання в приватне життя та захисту персональних даних.

Практичне втілення наведених вище тез дає змогу дійти таких висновків: а) фраза «прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій», використана в Законі України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII, є узагальненим поняттям і передбачає можливості користувачів

комунікаційних систем та/або споживачів послуг електронних комунікацій, які конкретизовано в Конституції України, законах і підзаконних актах України через такі юридичні категорії, як «права», «свободи» та «законні інтереси» користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій; б) положення «захист прав» користувачів містить такі структурні елементи, як відновлення порушеного правомірного стану та притягнення винних до юридичної відповідальності.

Водночас у межах забезпечення захисту прав користувачів комунікаційних систем та/або споживачів послуг електронних комунікацій законодавець акцентує увагу на невтручанні в приватне життя й захисті персональних даних. Гарантування поваги до приватного життя та захисту персональних даних є вимогою як національного, так і міжнародного законодавства.

Так, ст. 31 Конституції України гарантує кожному таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції, зокрема в разі використання електронних комунікаційних систем. Проте це конституційне право не є абсолютним і може бути обмежене судом у передбачених законом випадках з метою запобігання злочинові чи з'ясування істини під час кримінального провадження, якщо в інший спосіб одержати інформацію неможливо.

Водночас у ст. 32 Основного Закону України встановлено, що ніхто не може зазнавати втручань у його особисте й сімейне життя, крім випадків, передбачених Конституцією. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [6].

Згідно з рішенням Конституційного Суду України в 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 від 20 січня 2012 року № 2-рп/2012, 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 обіймає 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 є можливим лише за умов, передбачених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [7].

На захист основоположних прав і свобод людини та громадянина, зокрема права на невтручання в особисте життя, у зв'язку з обробкою персональних даних спрямований Закон України «Про захист персональних даних» від 1 червня 2010 року № 2297-VI. Відповідно до нього, персональні дані – це відомості чи сукупність відомостей про фізичну особу, яку ідентифіковано або може бути конкретно ідентифіковано [8].

Повагу до приватного та сімейного життя закріплено і в ст. 8 Конвенції про захист прав людини і основоположних свобод [9]. У цьому контексті особливий інтерес становить практика Європейського суду з прав людини.

Зокрема, Суд зауважує, що поняття «приватне життя» є досить широким, а отже, не підлягає однозначному тлумаченню. Воно охоплює фізичну та психічну цілісність людини (рішення в справі «X. і Y. проти Нідерландів» від 26 березня 1985 року). Іноді воно може містити окремі аспекти її фізичного та соціального «я» (рішення в справі «Мікулич проти Хорватії» від 7 лютого 2002 року). Такі аспекти життя людини, як, наприклад, гендерна ідентифікація, ім'я та сексуальна орієнтація, статеве життя, визнано елементами її особистого життя (наприклад, рішення в справі «B. проти Франції» від 25 березня 1992 року, рішення в справі «Бурґгартц проти Швейцарії» від 22 лютого 1994 року, рішення в справі «Даджен проти Сполученого Королівства» від 22 жовтня 1991 року) [10, с. 26].

Слід зауважити, що одним із важливих принципів застосування законодавства у сфері кібербезпеки є принцип прозорості, згідно з яким рішення (заходи) органів місцевого самоврядування мають бути належно обґрунтовані та повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування).

Реалізація цього принципу в правозастосовній діяльності органів місцевого самоврядування є вагомим чинником демократизації муніципальної влади та розвитку громадянського суспільства, беззаперечною умовою забезпечення дієвості громадянського контролю за законністю й ефективністю роботи органів публічної влади у сфері забезпечення кібербезпеки, сприяє залученню громадян до вирішення питань кіберзахисту як на державному, так і на муніципальному рівнях. Водночас прозорість прийняття рішень суб'єктами владних повноважень у сфері електронних комунікацій сприяє досягненню інформаційної стабільності та безпеки, посилює ефективність протидії кібератакам, підвищує рівень довіри громадян до влади.

Принцип прозорості в правозастосовній діяльності органів місцевого самоврядування має бути непорушним не лише на етапі прийняття кінцевого правозастосовного акта, а й на стадії підготовки проекту рішення, вивчення об'єктивних обставин конкретної життєвої ситуації, що потребує реагування цих органів, їх посадових і службових осіб у сфері забезпечення кібербезпеки.

Максимальне залучення громадськості до підготовки та прийняття відповідних соціально орієнтованих управлінських рішень значною мірою впливає на рівень довіри до управлінської діяльності, пов'язаної з електронними комунікаційними системами, поінформованості про цю діяльність органів державної влади та місцевого самоврядування.

Реалізація принципу прозорості суттєво активізує участь громадян та їх об'єднань у прийнятті рішень, унеможливлюючи громадський контроль за їх виконанням. Це, відповідно, оптимізує механізм протидії таким негативним явищам, як кібератаки, кібершпигунство, кіберзлочини, кібертероризм тощо.

Правове підґрунтя участі громадян та їх об'єднань на стадії підготовки рішень суб'єктами, наділеними державно-владними повноваженнями, у сфері забезпечення кібербезпеки становлять закони України «Про звернення громадян» від 2 жовтня 1996 року № 393/96-ВР, «Про інформацію» від 2 жовтня 1992 року № 2657-XII, «Про доступ до публічної інформації» від 13 січня 2011 року № 2939-VI, «Про місцеве самоврядування в Україні» від 21 травня 1997 року № 280/97-ВР, Постанова Кабінету Міністрів України «Про забезпечення участі

громадськості у формуванні та реалізації державної політики» від 3 листопада 2010 року № 996 [11] тощо. Концептуальні засади та заходи розвитку електронної демократії в Україні визначені розпорядженням Кабінету Міністрів України «Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації» від 8 листопада 2017 року № 797-р [12].

Крім цього, Законом України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII встановлено, що рішення (заходи) суб'єктів владних повноважень у сфері забезпечення кіберзахисту мають бути повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування).

Закріплення цих положень зумовлено конституційною гарантією забезпечення реалізації прав і свобод людини, передбаченою ст. 57 Основного Закону. Відповідно до неї, кожен має право знати свої права й обов'язки. Закони та інші нормативно-правові акти, що визначають права й обов'язки громадян, мають бути доведені до відома населення в законодавчо визначеному порядку. Закони та інші нормативно-правові акти, що визначають права й обов'язки громадян, не доведені до відома населення у відповідному порядку, є нечинними [6].

Висновки. Отже, попри те, що правозастосовні акти органів місцевого самоврядування у сфері забезпечення кібербезпеки здебільшого не є нормативно-правовими (адже мають персоніфікований характер і не передбачають багаторазового використання), загальний конституційний принцип їхньої дії збережено в часі. Вони мають бути повідомлені суб'єктам, яких вони стосуються, до набрання ними чинності (їх застосування).

У статті висвітлено не всі принципи застосування законодавства України органами місцевого самоврядування та іншими суб'єктами з державно-владними повноваженнями в межах забезпечення кібербезпеки України. Водночас усі ці принципи є рівнозначними та мають на меті досягнення безпечного функціонування кіберпростору, використання його в інтересах особи, суспільства й держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс] : Указ Президента України від 15 берез. 2016 р. № 96/2016. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/96/2016. – Назва з екрана.

2. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» [Електронний ресурс] : Указ Президента України від 26 трав. 2015 р. № 287/2015. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/287/2015. – Назва з екрана.

3. Про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Закон України від 5 жовт. 2017 р. № 2163-VIII. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2163-19. – Назва з екрана.

4. Про міжнародні договори України [Електронний ресурс] : Закон України від 29 черв. 2004 р. № 1906-IV. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1906-15. – Назва з екрана.

5. Report on the rule of law – Adopted by the Venice Commission at its 86th plenary session (Venice, 25–26 March 2011) [Electronic resource]. – Access mode: http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2011)003rev-e. – Title from the screen.

6. Конституція України [Електронний ресурс] : Закон України від 28 черв. 1996 р. № 254к/96-ВР. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80. – Назва з екрана.

7. 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] : рішення Конституційного Суду України від 20 січ. 2012 р. № 2-рп/2012. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/v002p710-12. – Назва з екрана.

8. Про захист персональних даних [Електронний ресурс] : Закон України від 1 черв. 2010 р. № 2297-VI. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2297-17. – Назва з екрана.

9. Конвенція про захист прав людини і основоположних свобод [Електронний ресурс] : міжнар. док. від 4 листоп. 1950 р. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/995_004. – Назва з екрана.

10. Стаття 8 Конвенції про захист прав людини і основоположних свобод: стандарти застосування при здійсненні правосуддя / [Н. Ахтирська, В. Філатов, Т. Фулей та ін.]. – Київ : Істина, 2011. – 200 с.

11. Про забезпечення участі громадськості у формуванні та реалізації державної політики [Електронний ресурс] : Постанова Кабінету Міністрів України від 3 листоп. 2010 р. № 996. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/996-2010-%D0%BF. – Назва з екрана.

12. Про схвалення Концепції розвитку електронної демократії в Україні та плану заходів щодо її реалізації [Електронний ресурс] : розпорядження Кабінету Міністрів України від 8 листоп. 2017 р. № 797-р. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/797-2017-%D1%80. – Назва з екрана.

REFERENCES

1. Ukaz Prezydenta Ukrainy "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 27 sichnia 2016 roku "Pro Stratehiiu kiberbezpeky Ukrainy": vid 15 berez. 2016 r. No. 96/2016 [Decree of the President of Ukraine "On the decision of the Council of National Security and Defense of Ukraine dated January 27, 2016 "On the Strategy of Cybersecurity of Ukraine" from March 15, 2016, No. 96/2016]. (n.d.). *zakon2.rada.gov.ua.* Retrieved from http://zakon2.rada.gov.ua/laws/show/96/2016 [in Ukrainian].

2. Ukaz Prezydenta Ukrainy "Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 6 travnia 2015 roku "Pro Stratehiiu natsionalnoi bezpeky Ukrainy": vid 26 trav. 2015 r. No. 287/2015 [Decree of the President of Ukraine "On the decision of the National Security and Defense Council of Ukraine dated May 6, 2015 "On the Strategy of National Security of Ukraine" from May 26, 2015, No. 287/2015]. (n.d.). *zakon2.rada.gov.ua.* Retrieved from http://zakon2.rada.gov.ua/laws/show/287/2015 [in Ukrainian].

3. Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy": vid 5 zhovt. 2017 r. No. 2163-VIII [Law of Ukraine "On the Basic Principles of Cybersecurity Protection of Ukraine" from October 5, 2017, No. 2163-VIII]. (n.d.). *zakon3.rada.gov.ua.* Retrieved from http://zakon3.rada.gov.ua/laws/show/2163-19 [in Ukrainian].

4. Zakon Ukrainy "Pro mizhnarodni dohovory Ukrainy": vid 29 cherv. 2004 r. No. 1906-IV [Law of Ukraine "On international treaties of Ukraine" from June 29, 2004, No. 1906-IV]. (n.d.). *zakon2.rada.gov.ua.* Retrieved from http://zakon2.rada.gov.ua/laws/show/1906-15 [in Ukrainian].

5. *Report on the rule of law - Adopted by the Venice Commission at its 86th plenary session (Venice, 25-26 March 2011).* Retrieved from http://www.venice.coe.int/webforms/documents/?pdf=CDL-AD(2011)003rev-e.

6. Konstytutsiia Ukrainy: vid 28 cherv. 1996 r. No. 254k/96-VR [Constitution of Ukraine from June 28, 1996, No. 254k/96-VR]. (n.d.). *zakon5.rada.gov.ua.* Retrieved from http://zakon5.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 [in Ukrainian].

7. 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": vid 20 sich. 2012 r. No. 2-pn/2012 [Decision of the Constitutional Court of Ukraine "In the case of the constitutional petition of the Zhashkiv regional council of the Cherkasy region concerning the official interpretation of the provisions of parts one, two, Article 32, parts two and three of Article 34 of the Constitution of Ukraine" from January 20, 2012, No. 2-pn/2012]. (n.d.). *zakon3.rada.gov.ua.* Retrieved from http://zakon3.rada.gov.ua/laws/show/v002p710-12 [in Ukrainian].

8. Zakon Ukrainy "Pro zakhyst personalnykh danykh": vid 1 cherv. 2010 r. No. 2297-VI [Law of Ukraine "On Protection of Personal Data" from June 1, 2010, No. 2297-VI]. (n.d.). *zakon3.rada.gov.ua.* Retrieved from http://zakon3.rada.gov.ua/laws/show/2297-17 [in Ukrainian].

9. Mizhnarodnyi dokument "Konventsiia pro zakhyst prav liudyny i osnovopolozhnykh svobod": vid 4 lystop. 1950 r. [International document "Convention for the Protection of Human Rights and Fundamental Freedoms" from November 4, 1950]. (n.d.). *zakon5.rada.gov.ua.* Retrieved from http://zakon5.rada.gov.ua/laws/show/995_004 [in Ukrainian].

10. Akhtyrska, N., Filatov, V., & Fulei, T. (et al.). (2011). *Stattia 8 Konventsii pro zakhyst prav liudyny i osnovopolozhnykh svobod: standarty zastosuvannia pry zdiisnenni pravosuddia [Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms: standards of application in the administration of justice].* Kyiv: Istyna [in Ukrainian].

11. Postanova Kabinetu Ministriv Ukrainy "Pro zabezpechennia uchasti hromadskosti u formuvanni ta realizatsii derzhavnoi polityky": vid 3 lystop. 2010 r. No. 996 [Resolution of the Cabinet of Ministers of Ukraine "On Ensuring Public Participation in the Formation and Implementation of State Policies" from November 3, 2010, No. 996]. (n.d.). *zakon3.rada.gov.ua.* Retrieved from http://zakon3.rada.gov.ua/laws/show/996-2010-%D0%BF [in Ukrainian].

12. Rozporiadzhennia Kabinetu Ministriv Ukrainy "Pro skhvalennia Kontseptsii rozvytku elektronnoi demokratii v Ukraini ta planu zakhodiv shchodo yii realizatsii": vid 8 lystop. 2017 r. No. 797-p [Order of the Cabinet of Ministers of Ukraine "On Approval of the Concept for the Development of Electronic Democracy in Ukraine and Action Plan for its Implementation" from November 8, 2017, No. 797-p]. (n.d.). *zakon5.rada.gov.ua.* Retrieved from http://zakon5.rada.gov.ua/laws/show/797-2017-%D1%80 [in Ukrainian].

Стаття надійшла до редколегії 25.04.2018

Demydenko V. *– Ph.D in Law, Associate Professor, Professor of the Department of Constitutional Law and Human Rights of the National Academy of Internal Affairs, Kyiv, Ukraine*

ORCID 0000-0001-6771-0080

The Principles of Application of Legislation by Local Government in the Field of Cybersecurity

Large-scale cyberattacks against Ukraine in recent years demonstrating the unpreparedness of the State apparatus, local governments, law enforcement, media, the private sector to counter this focused and minimize their negative consequences.

In order to enhance the effectiveness of the national protection of cyberspace is important to local governments, and other entities with state-government powers applied legislation in the field of cyber security in compliance with certain clear principles. To them, the law of Ukraine about basic principles of ensuring cybersecurity Ukraine 2017 year includes the need for minimum required regulation, according to which decisions (measures) of the subjects of powers must be necessary and minimally sufficient for achievement of the goals and tasks of ensuring cybersecurity Ukraine.

Among other principles – fairness and legal certainty, transparency, ensuring the protection of the rights of users of communication systems and/or users of services of electronic communications and/or services on information security, cyber defence, including rights non-interference in private life and protection of personal data.

Although the acts of application of local self-government bodies in the field of ensure cybersecurity mainly have the personified, is not designed for repeated use, and a general constitutional principle of these acts in time. They must be notified to the subjects to which they apply before they enter into force (their application). The principles of application of legislation in the field of cybersecurity and subjects of power solutions in this field, without the benefits of any of them in order to secure the functioning of cyberspace and its use in the interests of the person society and the State.

Keywords: authority and local self-government; principles; cybersecurity; cyberthreat; enforcement acts; national legislation.