ВИСНОВОК
ГРОМАДСЬКОЇ АНТИКОРУПЦІЙНОЇ ЕКСПЕРТИЗИ

Назва законопроекту	Про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері
Номер і дата реєстрації	6688 від 12.07.2018 р.
Автор законопроекту	Народні депутати України Вінник І.Ю., Тимчук Д.Б., Чорновол Т.М.
Веб-адреса картки законопроекту на сервері ВРУ	http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62236
Головний комітет ВРУ	Комітет з питань національної безпеки і оборони
Етапи проходження законопроекту	Включено до порядку денного (21.06.2018)
Корупційна небезпечність проекту (за 5-бальною шкалою)	5
Суспільна важливість проекту (за 5-бальною шкалою)	4
Висновок та рекомендації	**Законопроект слід відхилити.**

Задекларована суть законопроекту

Створення дієвих механізмів, спрямованих на оперативне виявлення, реагування, попередження, запобігання, нейтралізацію кіберзагроз, кібератак та кіберзлочинів, ліквідацію їх наслідків та відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Корупціогенні фактори та їхні наслідки

Абз. 6 ст. 7, ч. 2 ст. 8 Закону «Про основи національної безпеки України» – корупціогенні вади законодавчої техніки

Пропонується внести зміни до статей 7, 8 Закону «Про основи національної безпеки України». Водночас, цей Закон втратив чинність на підставі п. 3 Прикінцевих та перехідних положень Закону «Про національну безпеку України» (№ 2469-VIII від 21.06.2018).

Ч. 1 ст. 1 Закону «Про боротьбу з тероризмом» – незрозумілий зміст положення

Пропонується змінити визначення терміну «технологічний тероризм», аби відповідними злочинами вважались ті, що вчиняються із терористичною метою із використанням суміс-них комунікаційних систем із застосуванням мережі Інтернет; створюють умови для аварій і катастроф техногенного характеру та/або спрямовані на порушення громадської безпеки, залякування населення, провокації воєнного конфлікту, міжнародного ускладнення, на здійснення впливу на прийняття рішень чи вчинення або невчинення дій органами державної влади чи органами місцевого самоврядування, службовими особами цих органів, об'єднаннями громадян, юридичними особами, або привернення уваги громадськості до певних політичних, релігійних чи інших поглядів винного (терориста).

Враховуючи визначення терміну «тероризм» (відповідно до цього визначення, тероризмом вважається, зокрема, суспільно небезпечна діяльність, яка полягає у свідомому, цілеспрямованому застосуванні *насильства* шляхом залякування населення та органів влади), у посадо-

вих осіб правоохоронних органів з'являється можливість неоднозначно трактувати це положення і використовувати його з метою тимчасового блокування інформаційних ресурсів відповідно до положень кримінального процесуального закону.

П. 20-2 ч. 1 ст. 18; п. 18-3 ч. 1 ст. 39 Закону «Про телекомунікації»; ч. 1 ст. 213-7 КПК України – надмірна свобода підзаконної нормотворчості

Зазначені положення визначають, що Кабінет Міністрів України встановлює порядок, за яким оператори телекомунікацій зобов'язані здійснювати обмеження (блокування) доступу до інформаційних ресурсів, та за яким національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації спільно зі Службою безпеки України та ДССЗЗІ організовує виконання рішень щодо тимчасового обмеження (блокування) доступу до визначених інформаційних ресурсів.

П. 20-2 ч. 1 ст. 18 Закону «Про телекомунікації» наділяє національну комісію, що здійснює державне регулювання у сфері зв'язку та телекомунікацій, повноваженнями із організації у порядку, встановленому Кабінетом Міністрів України, виконання операторами (провайдерами) телекомунікацій рішень про блокування (обмеження) доступу до інформаційного ресурсу (сервісу).

У п. 18-3 ч. 1 ст. 39 Закону «Про телекомунікації» передбачено, що оператори телекомунікації зобов'язані в порядку, встановленому Кабінетом Міністрів України, тимчасово або на визначений час блокувати (обмежувати) доступ до визначеного інформаційного ресурсу. Схоже за змістом положення міститься у ч. 1 ст. 213-7 КПК України, відповідно до якої виконання ухвали слідчого судді про тимчасове блокування (обмеження) доступу до інформаційного ресурсу організовується в порядку, встановленому Кабінетом Міністрів України. Регулювання цього питання на рівні підзаконних нормативних актів через закритість процесу підготовки підзаконних НПА та їх прийняття створює додаткові ризики, а істотні умови порядку блокування (обмеження) доступу до інформаційних систем у законопроекті не визначені.

Абз. 1 ч. 4-1 ст. 39 Закону «Про телекомунікації» – широта дискреційних повноважень, надмірна свобода підзаконної нормотворчості, дискримінація

У ч. 4-1 ст. 39 Закону «Про телекомунікації» визначається, що суб'єкти господарювання, які використовують міжнародні канали електрозв'язку, зобов'язані за власні кошти закуповувати та встановлювати технічні засоби, які необхідні для блокування (обмеження) доступу до інформаційних ресурсів та які відповідають технічним вимогам, визначеним Адміністрацією Державної служби спеціального зв'язку та захисту інформації України за погодженням зі Службою безпеки України. Посадові особи ДССЗЗІ та СБУ отримують достатньо широкі дискреційні повноваження при визначенні на власний розсуд технічних вимог до обладнання, котре мають встановити провайдери.

Крім того, вимога встановлювати відповідне обладнання за рахунок власних коштів суб'єкта господарювання є дискримінаційною за своїм змістом: вона є надмірним обтяженням і покладає на суб'єктів господарювання необхідність витратити значну кількість часу та фінансових ресурсів для придбання і впровадження відповідних технічних засобів задля забезпечення блокування (обмеження) доступу до інформаційного ресурсу. Фактично йдеться про обмеження права власності, як воно визначене у ст. 41 Конституції України, оскільки суб'єкти господарювання, які використовують міжнародні канали електрозв'язку, будуть обмежені в праві користуватися і розпоряджатися своєю власністю (зазначених каналів), при цьому без попереднього і повного відшкодування їхньої вартості.

На практиці реалізувати запропоновані норми щодо наявності технічних засобів для обмеження (блокування) доступу на визначені інформаційні ресурси можливо лише з використанням апаратно-програмних комплексів DPI (системи глибокого аналізу трафіку). У світі існує обмежена кількість компаній, які є виробниками такого обладнання і програмного забезпечення. За даними ЗМІ та учасників ринку телекомунікацій, вже укладений договір із конкретним постачальником комплексу DPI і ним, ймовірно, стала компанія Allot[1].

Ч. 3 ст. 75 Закону «Про телекомунікації» – незрозумілий зміст положення

[1] Див.: https://www.epravda.com.ua/publications/2018/07/10/638560/

Незрозумілим є зміст положень про: доведення до відома в інший спосіб рішення національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, про накладення штрафу; одержання рішення про накладення штрафу суб'єктом господарювання.

Так, не є зрозумілим, що вважатиметься *доведенням до відома* суб'єкта господарювання рішення про накладення штрафу, а також, що означає *одержання* рішення. Наприклад, чи вважатиметься *одержанням* рішення, якщо його було *доведено до відома в інший спосіб*, крім надсилання поштою чи вручення під розписку, у т.ч. публікацією на веб-сайті національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації? Що у такому разі свідчитиме про ознайомленість суб'єкта господарювання із відповідним рішенням? Відповідно, з'являється можливість для отримання (надання) неправомірної вигоди при визначенні того, чи було належним чином *доведено до відома* суб'єкта господарювання рішення про накладення штрафу або при визначенні дати, коли рішення про накладення штрафу було *одержано* суб'єктом господарювання.

Ст. 96-13 КК України – незрозумілий зміст положення, колізія

Запропоновано здійснювати за рішенням суду блокування визначеного інформаційного ресурсу (сервісу) та видалення з нього інформації у разі, якщо через цей ресурс (сервіс) поширювалась інформація, з використанням якої вчиняються тяжкі або особливо тяжкі злочини.

Із цього формулювання випливає можливість по-різному трактувати, чи був вчинений тяжкий або особливо тяжкий злочин з використанням інформації, розміщеної на певному інформаційному ресурсі. Наприклад, якщо певна особа вчинила злочин, передбачений ч. 3 ст. 187 КК України (грабіж, поєднаний із проникненням у житло потерпілого), при цьому потерпілий є суб'єктом декларування відповідно до ст. 45 Закону «Про запобігання корупції» та оприлюднив достовірні відомості у своїй декларації, зокрема, щодо наявності значного обсягу готівкових коштів, то із відповідним положенням КК України у суду з'являється можливість прийняти рішення про блокування доступу до конкретної декларації чи до усього реєстру декларацій загалом, адже виходить, що особа вчинила тяжкий злочин з використанням інформації, яка наявна на зазначеному інформаційному ресурсі.

Іншою проблемою є колізія, яка виникає із КПК України. Абз. 2 ст. 96-13 КК України визначає, що блокування визначеного інформаційного ресурсу (сервісу) в інформаційно-телекомунікаційних мережах (системах) застосовується судом у порядку, встановленому КПК України. Однак, КПК України визначає порядок здійснення кримінального провадження, у той час як КК України визначає, які суспільно небезпечні діяння є злочинами та які покарання застосовуються до осіб, що їх вчинили. Тобто, запропоновані положення ст. 96-13 КК України є санкцією, яка може застосовуватись за наявності визначених підстав.

Ч. 3 ст. 213-1 КПК України – широта дискреційних повноважень

Пропонується, що у виняткових невідкладних випадках, пов'язаних із врятуванням життя людей та запобіганням вчиненню тяжкого або особливо тяжкого злочину, за постановою прокурора або за постановою слідчого, погодженою з прокурором, на строк не більше 48 годин може застосовуватись тимчасове блокування (обмеження) доступу до інформаційних ресурсів до постановлення ухвали слідчого судді, суду. У такому випадку невідкладно після початку дії тимчасового блокування прокурор, слідчий за погодженням з прокурором мають звернутись із відповідним клопотанням до слідчого судді, суду.

Це положення наділяє невиправдано широкими дискреційними повноваженнями прокурорів, слідчих, які можуть на власний розсуд тлумачити: а) винятковість та б) невідкладність випадків, в) наявність потреби врятування життя людей, г) наявність можливості вчинення тяжкого або особливо тяжкого злочину із використанням відповідного інформаційного ресурсу, – та застосовувати цей захід принаймні на 48 годин. Існує ризик того, що цим положенням зможуть зловживати з метою отримання неправомірної вигоди за прийняття того чи іншого рішення прокурора, слідчого.

Частини 1, 2 ст. 213-3 КПК України – незрозумілий зміст положення, прогалина в нормах матеріального права, широта дискреційних повноважень

Пропонується зобов'язати прокурора, слідчого одночасно зі зверненням із клопотанням про застосування тимчасового обмеження (блокування) доступу до інформаційного ресурсу направляти власнику (розпоряднику або адміністратору) попередження про протиправність поширення інформації, яку містить інформаційний ресурс, та про необхідність застосування

відповідного заходу забезпечення кримінального провадження. Водночас, попередження має надсилатися лише у разі, якщо на відповідному інформаційному ресурсі (сервісі) розміщено контактні дані його власника (розпорядника або адміністратора).

Чинне законодавство не містить визначення термінів розпорядника або адміністратора інформаційного ресурсу (сервісу), тому виникає можливість їх множинного тлумачення. У тих випадках, коли інформаційні ресурси (сервіси) будуть належати суб'єктам владних повноважень або іншим суб'єктам, визначеним у ст. 13 Закону «Про доступ до публічної інформації», існує можливість використовувати аналогію права із визначенням розпорядника публічної інформації, яке міститься у ст. 12 вищезгаданого Закону. Але варто дати визначення розпорядника та адміністратора інформаційного ресурсу, аби уникнути дискреції правоохоронців при їх тлумаченні. В іншому разі, у прокурора, слідчого виникає дискреція, яка виражається у визначенні на власний розсуд, чи зазначені на інформаційному ресурсі контакти певної особи (фізичної або юридичної) є контактами власника, розпорядника чи адміністратора відповідного інформаційного ресурсу (якщо це там не зазначено прямо, як часто буває на веб-сайтах).

Ч. 1 ст. 213-5 КПК України – корупціогенні вади законодавчої техніки

Пропонується встановити: слідчий суддя, суд відмовляє у задоволенні клопотання про тимчасове блокування (обмеження) доступу до визначеного інформаційного ресурсу, *«якщо сторона кримінального провадження, яка звернулась з клопотанням, слідчий, прокурор не доведе необхідність цього заходу»*. Проте, ч. 2 ст. 213-1 КПК України визначає, що лише прокурор, слідчий за погодженням прокурора можуть клопотати про застосування відповідного заходу забезпечення кримінального провадження. Таким чином, на іншу сторону кримінального провадження такий обов’язок покладено бути не може.

Ч. 5 ст. 213-5 КПК України – широта дискреційних повноважень

У запропонованому положенні передбачено, що постановлення слідчим суддею, судом ухвали про відмову у застосуванні тимчасового обмеження (блокування) доступу до інформаційного ресурсу не перешкоджає повторному зверненню з новим клопотанням про надання такого доступу. Таке формулювання також є корупціогенним за своїм змістом, оскільки дозволятиме прокурорам, слідчим вимагати неправомірну вигоду при ухваленні ними на власний розсуд рішення щодо повторного направлення клопотання до слідчого судді, суду щодо застосування відповідних заходів.

Ст. 6 Закону «Про тимчасові особливості здійснення заходів державного нагляду (контролю) у сфері господарської діяльності» – корупціогенні вади законодавчої техніки

Пропонується, щоб дія зазначеного Закону не поширювалась на відносини, що виникають під час проведення заходів нагляду (контролю), зокрема, національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації. Водночас, Прикінцевими положеннями Закону «Про Державний бюджет України на 2018 рік» це положення було змінене і чинна редакція Закону передбачає, що дія Закону «Про тимчасові особливості здійснення заходів державного нагляду (контролю) у сфері господарської діяльності» не поширюється на відносини, що виникають під час проведення заходів нагляду (контролю) органами, перелік яких встановлюється Кабінетом Міністрів України. Таким чином, виникає вада законодавчої техніки, яку необхідно усунути.

Неправдиві цілі прийняття законопроекту

Як зазначалось вище, цей законопроект був розроблений з метою створення і впровадження ефективної системи кібербезпеки шляхом створення дієвих механізмів, спрямованих на оперативне виявлення, реагування, попередження, запобігання, нейтралізацію кіберзагроз, кібератак та кіберзлочинів, ліквідацію їх наслідків та відновлення сталості і надійності функціонування комунікаційних, технологічних систем.

Водночас, сумнівною є можливість досягнути зазначених цілей завдяки механізмам, які визначені у цьому законопроекті.

Окремі його положення досить складно виконати з технічної точки зору. Для прикладу можна взяти DDoS-атаку, яку цілком можна розглядати як кібератаку. Вона полягає у надсиланні масованої кількості запитів до веб-сайту чи іншого ресурсу, які він не може обробити, через що виходить із ладу. Один зі способів здійснення такої атаки – ботнет: попередньо зловмисники заражають певну велику кількість (йдеться про сотні тисяч чи навіть мільйони) комп'ютерів

чи інших пристроїв (власники яких про це не підозрюють) програмами, які у необхідний момент починають здійснювати запити до необхідного ресурсу та виводять його з ладу.

За такої DDoS-атаки запропоновані законопроектом заходи не будуть ефективними.

Чисельні положення законопроекту можуть бути використані з метою вимагання неправомірної вигоди слідчими і прокурорами, які отримують надширокі дискреційні повноваження щодо здійснення тимчасового блокування доступу до окремих інформаційних ресурсів.

Положення щодо обов'язкового встановлення технічних засобів операторами телекомунікацій містить високі корупційні ризики щонайменше на етапі визначення вимог до цього обладнання, створює додаткові можливості до монополізації ринку надання послуг телекомунікацій і накладає додаткові значні витрати на користувачів телекомунікаційних послуг.

Прийняття цього законопроекту у такій редакції видається недоцільним, оскільки його положення має ознаки надлишкового регулювання та надмірних адміністративних бар'єрів для діяльності у сфері телекомунікацій. При цьому вища ефективність забезпечення кібербезпеки все одно залишається під серйозним сумнівом.

Виявлені корупціогенні фактори

	Корупціогенний фактор	*Кількість норм*
1)	**неправильне визначення функцій, повноважень (обов'язків) і відповідальності певних суб'єктів (органів державної влади, органів місцевого самоврядування, їхніх посадових і службових осіб, інших осіб, на яких поширюється дія Закону «Про запобігання корупції»):**	**8**
	- визначення компетенції за формулою «має право»;	-
	- широта дискреційних повноважень;	4
	- надмірна свобода підзаконної нормотворчості;	4
	- відсутність відповідальності за правопорушення;	-
2)	**колізії і вади законодавчої техніки:**	**7**
	- колізії;	1
	- корупціогенні вади законодавчої техніки;	6
3)	**прогалини в регулюванні:**	**1**
	- прогалини в нормах матеріального права;	1
	- відсутність або недостатність контролю і прозорості;	-
	- відсутність або недостатність адміністративних і судових процедур;	-
	- відсутність або недостатність конкурсних (аукціонних) процедур;	-
4)	**дискримінація: протекціонізм щодо певних осіб, просування групових чи особистих інтересів і вигід або, навпаки, неправильне визначення умов реалізації права, належного особі – одержувачу публічних послуг (необґрунтовані, надмірні обтяження при його реалізації), чи умов виконання нею обов'язку;**	**1**
5)	**неправдиві цілі прийняття законопроекту.**	**1**
	Всього:	**18**

Виконавець: Антон Марчук, експерт Центру політико-правових реформ.
Перевірив: Микола Хавронюк, директор з наукового розвитку Центру політико-правових реформ, доктор юридичних наук, професор.
Методологія проведення експертизи: http://pravo.org.ua/ua/news/5226-metodologiya-provedennya-gromadskoyi-antikoruptsiynoyi-ekspertizi
З іншими висновками громадської антикорупційної експертизи можна ознайомитись тут.