

УДК 342.95:323.285:004

ТРОФІМОВ С.А., кандидат юридичних наук, доцент кафедри адміністративно-правових та кримінально-правових дисциплін Кримського юридичного інституту Національного університету “Юридична академія України імені Ярослава Мудрого”

УРЕГУЛЮВАННЯ ПОРЯДКУ НАДАННЯ ХОСТИНГ-ПОСЛУГ ЯК ФАКТОР ЗАБЕЗПЕЧЕННЯ ЕФЕКТИВНОЇ АНТИТЕРОРИСТИЧНОЇ ДІЯЛЬНОСТІ

***Анотація.** До проблеми врегулювання порядку надання хостинг-послуг як фактору забезпечення ефективної антитерористичної діяльності.*

***Ключові слова:** протидія тероризму, терористична діяльність, послуги з надання хостингу, антитерористична діяльність.*

***Аннотация.** К проблеме урегулирования порядка предоставления хостинг-услуг как фактора обеспечения эффективной антитеррористической деятельности.*

***Ключевые слова:** противодействие терроризму, террористическая деятельность, услуги по предоставлению хостинга, антитеррористическая деятельность.*

***Summary.** To the problem of settlement of procedure of grant of hosting-services as a factor of providing of effective counterterrorist activity.*

***Keywords:** counteraction to terrorism, terrorist activity, services of hosting, counterterrorist activity.*

Постановка проблеми. Суспільство впродовж століть мало стійку тенденцію до вдосконалення технологій, якими все частіше користуються значна кількість його представників. Протягом останніх десяти років лідером у поширеності технологій стала мережа Інтернет, без якого неможливо уявити людство на даному етапі еволюції.

Окремими проблемами забезпечення антитерористичної діяльності в інформаційно-правовому аспекті у своїх наукових дослідженнях займалися І.В. Арістова, К.І. Беляков, В.В. Грибакін, В.В. Коноплев, О.В. Лукасевич, Т.А. Мартиросян, А.І. Марушак, В.Я. Настюк, О.В. Петришин, О.О. Погрібний, В.Г. Пилипчук, Г.П. Середа, Є.Д. Скулиш, Д.А. Соломін, Д.В. Сорокін та інші вітчизняні та іноземні науковці, але питанням запровадження адміністративної відповідальності суб'єкта господарювання, який надає хостинг-послуги за інформацію терористичного спрямування, що розміщена на його технічних потужностях, приділялася недостатня увага.

Метою статті є висвітлення небезпеки безконтрольного використання інформаційних технологій, зокрема послуг з надання хостингу, та визначення шляхів унормування цієї сфери діяльності.

Виклад основних положень. З урахуванням розвитку телекомунікаційної сфери та швидко зростаючого інтересу провідників тероризму до мережі Інтернет в якості своєрідної платформи до поширення ідеології тероризму, передачі інформації своїм прибічникам, а також дослідження потенційного деструктивного впливу на електронні системи різних державних органів, установ, підприємств та організацій постає питання про необхідність врегулювання процедури надання хостинг-послуг, під якими розуміються послуги з надання обчислювальних потужностей для фізичного розміщення інформації на сервері, що постійно знаходиться у мережі. Як правило, це мережа Інтернет.

Зазначимо, що виділяють багато різновидів хостинг-послуг, зокрема:

1. Віртуальний сервер. В даному випадку надається місце на диску для розміщення веб-сайтів, середовище виконання веб-сервісів єдине для багатьох користувачів, ресурси розподілені між усіма користувачами на одному сервері, де може розміщуватись від 50 до 1000 користувачів. Невеликі дешеві хостинг-провайдери часто нехтують безпекою і взагалі не розмежовують привілеїв користувачів, що дозволяє одному користувачеві на сервері мати доступ до сайтів сотень інших користувачів.

2. Віртуальний виділений сервер (VPS або VDS). Це послуга, в рамках якої користувачеві надається так званий віртуальний виділений сервер. У плані управління операційною системою здебільшого вона відповідає фізичному виділеному серверу, зокрема передбачає права адміністратора, root-доступ, власні IP-адреси, порти, правила фільтрування і таблиці маршрутизації.

3. Виділений сервер. В цьому випадку надається сервер повністю. Використовується для реалізації нестандартних завдань (сервісів), а також розміщення “важких” веб-проектів, які не можуть співіснувати на одному сервері з іншими проектами і вимагають під себе всі ресурси сервера.

4. Колокація, яка передбачає надання місця в дата-центрі провайдера для обладнання клієнта (зазвичай шляхом монтажу в стійці) і підключення його до мережі Інтернет.

5. E-mail хостинг. Він являє собою сервіс у телекомунікаційній галузі, відповідно до якого постачальник послуги створює електронну поштову скриньку та надає вільний простір на своєму сервері, щоб клієнти могли тримати свої дані на сервері. Клієнти можуть отримати доступ до електронної пошти, адресної книги, управління завданнями та документи з різних місць і за допомогою різних способів передачі інформації.

За умовами надання хостинг часто поділяється на платний і безкоштовний. Зазвичай компанія, що надає безкоштовний хостинг, заробляє шляхом показу реклами на сторінках, розміщених на ньому. Безкоштовний хостинг, як правило, повільніше платного, надає тільки базові послуги і ненадійний. Приватні особи для своїх домашніх сторінок на початковому етапі їх розвитку використовують безкоштовний хостинг. Громадські організації можуть використовувати як платний хостинг, так і безкоштовний. Комерційні організації практично завжди користуються послугами платного хостингу [1].

Слід підкреслити, що на сьогодні надання телекомунікаційних хостинг-послуг здійснюється у спрощеному порядку без необхідності проходження ліцензування або отримання будь-якого спеціального дозволу. Фактично суб'єкт господарювання, який надає названі послуги, не несе будь-якої відповідальності за зміст інформації, що розміщена на його ресурсах. За відповідним договором між оператором (провайдером) хостинг-послуг та клієнтом відповідальність за розміщену інформацію покладається лише на клієнта хостинг-послуг. Оператор (провайдер) не має обов'язку контролювати відповідне наповнювання веб-сайтів, які розміщені на його серверах, що створює можливість для їх використання провідниками терористичної діяльності та їх прибічниками задля досягнення своєї мети.

З урахуванням вищевикладеного можна дійти висновку про необхідність запровадження адміністративної відповідальності суб'єкта господарювання, який надає хостинг-послуги, тобто можливості для розміщення на серверах, що йому належать, інформації терористичного спрямування (приміром, заклики до вчинення терористичних актів, пропаганда ідеології тероризму тощо), яка буде доступна користувачам веб-сайтів у мережі Інтернет. В даному випадку є пропозиція щодо

солідарної відповідальності суб'єкта, який розмістив інформацію терористичного спрямування, і суб'єкта, який надав технічну можливість розміщення інформації. Перший суб'єкт повинен нести відповідальність кримінального характеру, а другий – адміністративного. Також необхідно враховувати те, що у разі, якщо суб'єкт господарювання, який надає хостинг-послуги, знає, що користувач хостинг-послуг буде використовувати його технічні можливості для розміщення інформації терористичного спрямування, та не зважаючи на це дає таку можливість, то в даному випадку постає питання про притягнення винуватих осіб не до адміністративної, а до кримінальної відповідальності.

З огляду на вищевикладене, на нашу думку, слід рекомендувати внести відповідні зміни у вітчизняне законодавство, зокрема у:

1. Закон України “Про телекомунікації” від 18.11.03 р. № 1280-IV [2] щодо встановлення обов'язку щоденного моніторингу суб'єктами підприємницької діяльності, які надають хостинг-послуги, інформації, яка розміщена на їх серверах, з метою виявлення інформації терористичного спрямування й оповіщення відповідних державних органів про встановлені ними випадки. Технічна можливість такого моніторингу існує й не потребує суттєвих витрат фінансового та часового характеру.

2. Кодекс України про адміністративні правопорушення щодо закріплення відповідальності посадової особи або громадянина, який займається підприємницькою діяльністю, що надають хостинг-послуги, за інформацію терористичного спрямування, яка розміщена на його технічних потужностях, у випадку невиконання обов'язку щоденного моніторингу такої інформації або недонесення до відома державних органів про випадки використання його можливостей з терористичною метою.

У зв'язку з цим ми пропонуємо до Закону України “Про телекомунікації” від 18.11.03 р. № 1280-IV [2] внести наступні зміни:

а) статтю 1 доповнити поняттями “послуги з надання хостингу” та “інформації терористичного спрямування”:

“Послуги з надання хостингу – послуги з надання обчислювальних потужностей для фізичного розміщення інформації на сервері, що постійно знаходиться у мережі”;

“Інформація терористичного спрямування – відомості:

- про спеціальні засоби, технічні прийоми і тактику проведення антитерористичних операцій;

- що мають на меті пропаганду або виправдання тероризму;

- що містять висловлювання осіб, які чинять опір чи закликають до опору суб'єктам антитерористичної діяльності;

- що містять висловлювання осіб, які закликають до терористичної діяльності;

- що містять дані про предмети та речовини, які безпосередньо можуть бути використані для вчинення терористичних актів”;

б) доповнити вищевказаний Закон статтею наступного змісту:

“Порядок адміністрування послуг з надання хостингу

1. Суб'єкти, які надають на платній чи безоплатній основі послуги з надання хостингу, зобов'язані здійснювати щоденний моніторинг інформації, яка розміщена на серверах, що знаходяться під їх адмініструванням, з метою виявлення інформації терористичного спрямування.

2. У разі виявлення інформації терористичного спрямування суб'єкти, які надають на платній чи безоплатній основі послуги з надання хостингу, зобов'язані закрити доступ користувачів до такої інформації та невідкладно повідомити про це до територіального управління Служби безпеки України.

3. Особи, винні у недотриманні вимог законодавства щодо адміністрування послуг з надання хостингу, несуть відповідальність згідно із законом”.

Задля створення матеріальних норм, що нададуть можливість притягувати суб'єктів господарювання, які надають хостинг-послуги, за недотримання вищевказаних правил, пропонуємо доповнити главу 15 КпАП України статтею з назвою: “Порушення встановленого порядку адміністрування послуг з надання хостингу”, в якій передбачити адміністративну відповідальність за наступні діяння:

1. Порушення встановлених законом термінів моніторингу інформації, розміщеної в рамках надання послуг з хостингу, – тягнуть за собою накладення штрафу в розмірі від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян.

2. Повторне протягом року вчинення правопорушення, передбаченого частиною першою цієї статті, за яке особу вже було піддано адміністративному стягненню, – тягне за собою накладення штрафу в розмірі від тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян з конфіскацією обладнання, яке використовувалося для поширення інформації терористичного спрямування, або без такої.

3. Порушення встановленого законом порядку дій у випадку виявлення інформації терористичного спрямування – тягнуть за собою накладення штрафу в розмірі від трьох тисяч до п'яти тисяч неоподатковуваних мінімумів доходів громадян з конфіскацією обладнання, яке використовувалося для поширення інформації терористичного спрямування, або без такої.

Пропонуємо наступний аналіз складу даного правопорушення.

- об'єкт адміністративного правопорушення – суспільні відносини щодо дотримання встановленого порядку адміністрування послуг з надання хостингу;
- об'єктивна сторона може виражатися лише у пасивній формі, тобто бездіяльності;
- суб'єктом відповідальності може бути посадова особа або громадянин, який займається підприємницькою діяльністю – оператори (провайдери) хостинг-послуг;
- суб'єктивна сторона передбачає умисну форму вини.

Висновки.

Підсумовуючи викладене, слід вказати, що такі зміни, на нашу думку, створять суттєві додаткові бар'єри на шляху провідників тероризму щодо поширення ідеології тероризму та нададуть ефективний інструментарій з притягнення до відповідальності суб'єктів, що нехтують безпекою всього суспільства заради певних корисних мотивів.

Необхідно зазначити, що більшість вітчизняних та зарубіжних правознавців активно підтримують позицію щодо безпосередньої залежності між ефективністю заходів з протидії тероризму й розмірів фінансування цієї сфери. Як приклад можна навести думку А.Ф. Істоміна, В.А. Горбуліна, В.І. Зарубіна, що прийняття комплексу заходів щодо створення загальнодержавної системи протидії тероризму, яка включає в себе зміцнення державних органів, що беруть участь у попередженні й припиненні його проявів; поліпшення матеріально-технічної оснащеності й озброєння, впровадження додаткових соціальних пільг співробітникам і членам їх родин, посилення гарантій правової захищеності й особистої безпеки учасників антитерористичних операцій, включаючи свідків і потерпілих, особливо на стадії розслідування й судового розгляду, – все це дозволить істотно обмежити тероризм і терористичну діяльність і стабілізувати обстановку в країні [3, с. 14].

Беручи до уваги досвід Російської Федерації, яка щороку витрачає мільярди доларів на фінансування ефективної роботи суб'єктів протидії тероризму й керівників “неблагополучних” в плані розвитку терористичної діяльності регіонів Російської Федерації. Як свідчить практика, більшість цих коштів за допомогою різноманітних

«схем» привласнюються вищевказаними суб'єктами та їх прибічниками. Частина із цих коштів витрачається на фінансування діяльності провідників тероризму задля змушення влади через суспільство витратити ще більше, аргументуючи це необхідністю тотальної протидії цьому негативному явищу [4]. Саме цим пояснюються вчинення актів тероризму в таких місцях і в такий спосіб, які можуть викликати найбільш суттєвий суспільний резонанс, та їх стабільна кількість.

Із врахуванням вищевикладеного можна стверджувати про відсутність прямого зв'язку між ефективністю протидії тероризму та обсягом її фінансування. Безумовно, ефективно протидіяти тероризму неможливо без відповідних ресурсів (людських, технічних, фінансових тощо), але насамперед необхідно зробити акцент на оптимізації структури органів влади, які задіяні у цій протидії, розробити чіткий механізм контролю за діяльністю та витратами як цих органів, так і безпосередніх керівників, а також членів їх родин та родичів. За відповідні порушення слід розробити жорстку систему покарань з обов'язковою конфіскацією майна.

Запропоновані нами зміни у вітчизняне законодавство не потребують значних фінансових ресурсів, але позитивний ефект, що можна отримати від їх впровадження, на нашу думку, буде достатньо суттєвим.

Як висновок слід зазначити про суттєву небезпеку безконтрольного використання ринку послуг в інформаційній сфері для рівня захищеності нашої держави від загрози тероризму. Саме названа сфера викликає підвищений інтерес з боку провідників тероризму з огляду на масовість використання та потенційні складнощі щодо ідентифікації таких осіб. Отже, порядок адміністрування послуг з надання хостингу потребує чіткого регламентування та буде запорукою становлення в Україні ефективної антитерористичної діяльності.

Використана література

1. Значення слова “хостинг”. – Режим доступу : [//www.uk.wikipedia.org/wiki/%D0%A5%D0%BE%D1%81%D1%82%D0%B8%D0%BD%D0%B3](http://www.uk.wikipedia.org/wiki/%D0%A5%D0%BE%D1%81%D1%82%D0%B8%D0%BD%D0%B3)
2. Про телекомунікації : Закон України від 18.11.03 р. № 1280-IV // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.
3. Истомин А.Ф. Пути совершенствования норм Уголовного кодекса РФ как законодательной основы борьбы с терроризмом / А.Ф. Истомин, В.А. Горбулин, В.И. Зарубин // Журнал российского права. – 2001. – № 1. – С. 8 – 14.
4. Терроризм : угроза Вашему дому. – Режим доступа : [//www.apn.ru/opinions/article22734.htm](http://www.apn.ru/opinions/article22734.htm)

~~~~~ \* \* \* ~~~~~