

5. Кіберзлочинність та відмивання коштів [Електронний ресурс] / Департамент фінансових розслідувань. Державна служба фінансового моніторингу. – 2013. – Режим доступу: http://www.sdfm.gov.ua/content/file/Site_docs/2013/20131230/tipolog2013.pdf

КІБЕРТЕРОРИЗМ ЯК ПРОБЛЕМА ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

Бойко О.В.

*курсант 3-го курсу факультету № 3
Одеського державного університету внутрішніх справ*

Ісмайлов К.Ю.

*кандидат юридичних наук, майор поліції
завідувач кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ*

Сьогодні використання інформаційного поля може бути настільки ж небезпечним і навіть смертельним для людської спільноти, як і застосування зброї масового ураження. Проблема загроз в галузі інформаційно-комунікаційних технологій – вже вийшла на міжнародний рівень і становить собою одну з найсерйозніших у сучасному світі [1].

Зараз виникають принципово нові потужні засоби, здатні призвести до небувалих руйнівних наслідків, порушити роботу виробничої та економічної сфери, соціальної інфраструктури та держуправління, загрожувати життю мільйонів людей. Одним із найяскравіших методів створення жаху і хаосу у інформаційно-телекомунікаційній сфері є кібертероризм, або комп'ютерний тероризм.

На даний час найбільш популярним і часто застосовуваним ресурсом у світі являється Інтернет, який будучи прямим благом для суспільства, несе в собі й потенційну руйнуючу силу. Це може проявлятися в різноманітних формах, як використання його для пропаганди екстремізму, расизму, ксенофобії, так і для суто кримінальних цілей – наприклад, для злову банківських електронних мереж, державних сайтів та баз даних [2]. У наш час за допомогою всесвітньої мережі Інтернет про себе відкрито заявляють міжнародні терористичні структури та організації, з протиправною діяльністю яких не можуть впоратися передові держави Європейського Союзу та США. Для досягнення своїх цілей і задоволення власних інтересів активні учасники терористичної діяльності намагаються мати у своєму арсеналі найновітнішу і найпотужнішу зброю – ядерну, хімічну, бактеріологічну, та, звісно, інформаційні засоби (Інтернет мережу), які за своєю суттю мають руйнуючу силу та можуть бути порівнянні зі зброєю масового ураження.

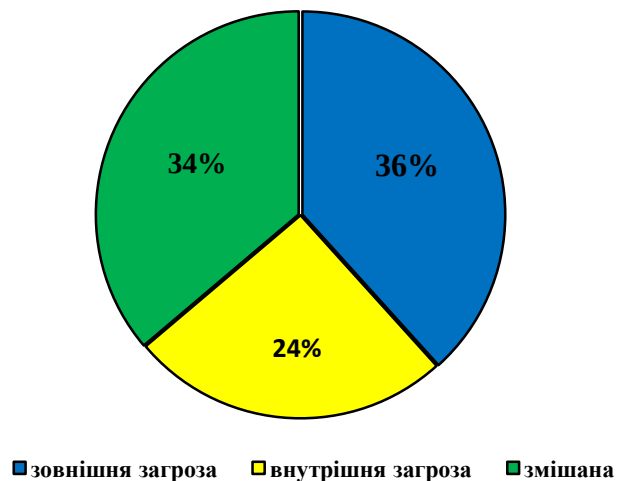
Кібертероризм – це суспільно-небезпечне явище, котре характеризується різноманітними ознаками та являється серйозною загрозою людству, причому ступінь цієї загрози в силу своєї новизни, не до кінця ще усвідомлена і вивчена [3]. Практика, яка склалася у світової спільноти в даній сфері показує про безсумнівну уразливість будь-якої держави, а саме тому, що кібертероризм не має чітко визначених кордонів, і для кібертерористів не стане складністю загрожувати інформаційним системам, які розташовані в будь-якій точці земної кулі. Діяльність кібертерористів дуже важко виявити та нейтралізувати, це пов'язано з тим, що вони практично не лишають «слідів» від вчиненого протиправного діяння.

Дані огляду в сфері інформаційної безпеки свідчать про те, що кіберзлочини стають більш витонченими, що ускладнює їх виявлення та запобігання. Це може привести до ще більших збитків і втрат у майбутньому.

Кібертероризму притаманні різні форми, але інформаційну атаку слід, вважати, як основну. Так, інформаційна атака виражається на комп'ютерну інформацію, обчислювальні системи, апаратуру передачі даних, інші складові інформаційної інфраструктури, які здійснюються групами чи окремими особами. Дана атака дає змогу проникати в будь-яку систему, перехоплювати управління чи стримувати кошти мережевого інформаційного обміну тощо.

Яскравими прийомами кібертероризму виступають такі як: знищення мереж електроживлення, використання хімічних засобів для руйнування елементної бази; крадіжка інформаційних, програмних та технічних ресурсів, шляхом подолання систем захисту, впровадження вірусів та програмних закладок [4]. За статичними показниками визначено, що 36% респондентів в Україні вважають, що кіберзлочинність це зовнішня загроза, 24% – внутрішня загроза. 34% – вважають, що загроза може виходити як ззовні, так і зсередини організації.

Кібертероризм – зовнішня або внутрішня загроза?

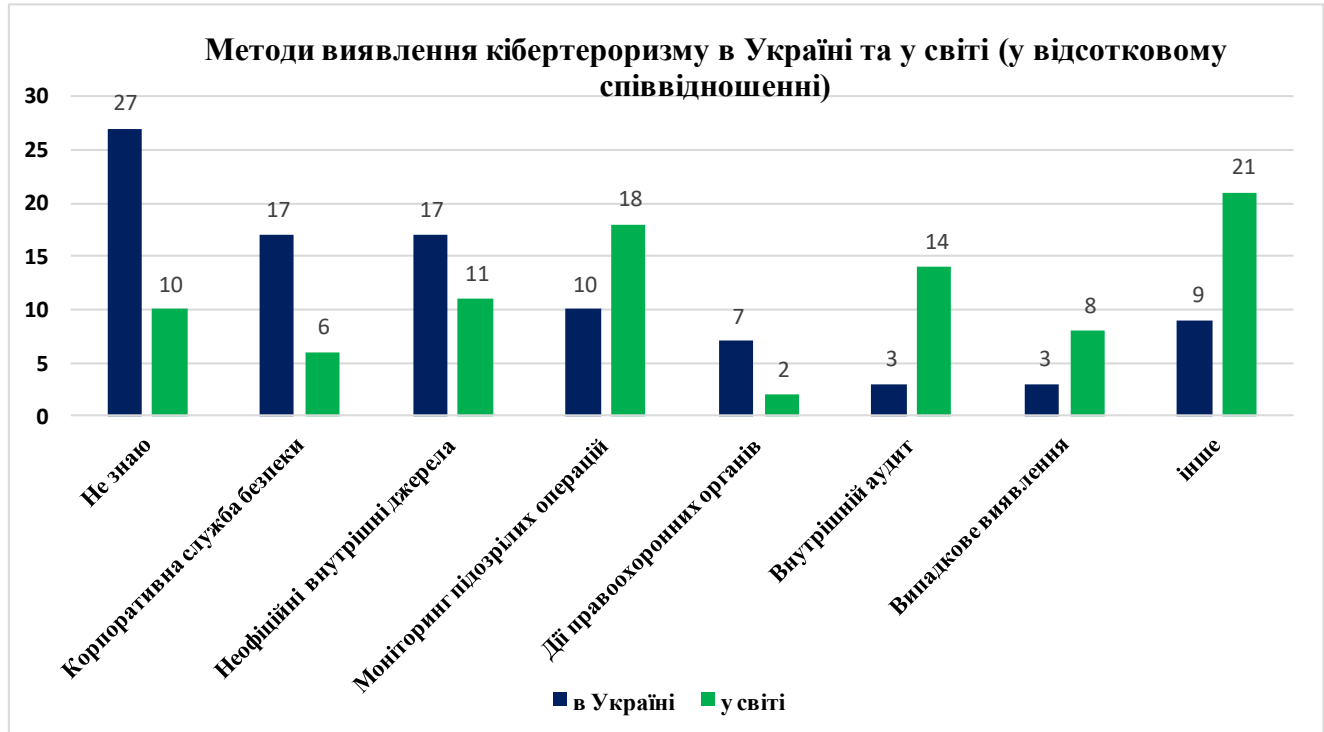


Поява кібертероризма пов'язана з незахищеністю інформаційного простору країни від негативного зовнішнього і внутрішнього впливу. Тобто, це умисне зловживання можливостями цифрових інформаційних систем з метою підтримки проведення злочинних терористичних дій. Кібертерористи мають тільки одне на меті – це досягти якнайшвидше потрібної цілі та набити побільше галасу у суспільстві.

З метою підвищення ефективності у боротьбі з тероризмом доцільно було б прийняти до уваги такі заходи, як: по-перше, організація ефективної співпраці з іноземними державами, їх правоохоронними органами і спеціальними службами, до компетенції яких відноситься боротьба з кібертероризмом. По-друге, розширення транскордонного співробітництва у сфері правової допомоги в протидії комп'ютерній злочинності і кібертероризму. По-третє, удосконалення міжнародної організаційно-правової взаємодії з питань протидії комп'ютерній злочинності й комп'ютерному тероризму, та удосконалення системи підготовки кадрів у сфері інформаційної безпеки [5].

Ці практичні методи стануть ефективними у запобіганні даного небезпечного явища, застосування яких надасть певні гарантії у сфері інформаційної безпеки.

У сучасному суспільстві існує низка методів виявлення кібертероризму, а за допомогою статистичних показників є можливість порівняти в Україні та у світі тенденцію застосування тих чи інших методів.



Таким чином, кібертероризм є комплексною акцією, що виражається в навмисній, політично вмотивованій атаці на інформацію, оброблювану комп'ютером і комп'ютерними системами, що створює небезпеку для життя чи здоров'я людей або настання інших тяжких наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації військового конфлікту. Тому органи та служби компетентні у попередженні і протидії даному суспільно-небезпечному явищу повинні швидко, оперативно та професійно за допомогою комп'ютерів, телекомунікаційних та комп'ютерних мереж застосовувати правомірні засоби по запобіганню і профілактиці кібертероризму та будь-яких кіберзлочинів.

Література

1. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи [Електронний ресурс] / С. Гнатюк // Безпека інформації. - 2013. - Т. 19, № 2. - С. 118-129. - Режим доступу: http://nbuv.gov.ua/UJRN/bezin_2013_19_2_8
2. Кібертероризм у складі сучасних проблем національної безпеки [Електронний ресурс] / О. В. Бойченко, О. О. Ончурова // Форум права. - 2010. - № 2. - С. 57-62. - Режим доступу: http://nbuv.gov.ua/UJRN/FP_index
3. Кіберзлочинність та кібертероризм як загроза інформаційній безпеці: міжнародно-правовий аспект [Електронний ресурс] / О. Г. Широкова-Мурараш, Ю. Р. Акчурін // Інформація і право. - 2011. - № 1. - С. 76-81. - Режим доступу: http://nbuv.gov.ua/UJRN/Infpr_2011_1_16

4. Кібертероризм у контексті сучасних маргінальних процесів [Електронний ресурс] / О. В. Матвеева // Актуальні проблеми міжнародних відносин. - 2011. - Вип.103(1). - С. 184-190. – Режим доступу: [http://nbuv.gov.ua/UJRN/apmv_2011_103\(1\)__27](http://nbuv.gov.ua/UJRN/apmv_2011_103(1)__27)

5. Комп'ютерний тероризм: сучасний стан, прогнози розвитку та шляхи протидії [Електронний ресурс] / С. Б. Гавриш // Боротьба з організованою злочинністю і корупцією (теорія і практика). - 2009. - Вип. 20. - С. 3-14. - Режим доступу: http://nbuv.gov.ua/UJRN/boz_2009_20_1

НОВІ ТЕНДЕНЦІЇ У ФОРМУВАННІ ДЖЕРЕЛ ІНФОРМАЦІЙНОГО ПРАВА В УКРАЇНІ ЗА РОКИ НЕЗАЛЕЖНОСТІ

Обертинський В.А.

слухач 2-го ННІЗДН факультету №2

Одеського державного університету внутрішніх справ

Ісмайлов К.Ю.

кандидат юридичних наук, майор поліції

завідувач кафедри кібербезпеки та інформаційного забезпечення

Одеського державного університету внутрішніх справ

Зміни у правовій системі України не минули і систему джерел інформаційного права і законодавства, яка переживає трансформацію у зв'язку з реформаційними процесами в законодавчій сфері (зокрема яка стосується інформаційного соціального обороту), з відновленням правового звичаю як джерела права, включенням до неї практики Європейського суду з прав людини, що свідчить про існування тенденції до наступного розширення системи джерел вітчизняного права. Зазначені зміни є проявом реалізації в Україні принципу верховенства права, який не лише закріплений у ст. 8 Конституції України, але й поступово займає очільне місце у правосвідомості, насамперед правників-практиків.

Актуальність даного питання набуває і завдяки невинному зросту ролі судових процесів, починаючи з 2004-2005 років. Так судові процеси, що проводяться вищими спеціалізованими судами України, Верховним судом України, Вищим Адміністративним Судом України та, безумовно, Конституційним Судом України суттєво змінили сучасне ставлення науковців і практиків юриспруденції до впливовості судових рішень на соціальні інформаційні відносини та форми інформаційного права взагалі в національній правовій системі.

Особливої уваги зазначена проблема набула з моменту створення Конституційного Суду України. Відповідно до ч. 2 ст. 147 Конституції України КСУ розв'язує питання про відповідність законів та інших правових актів Конституції України і дає офіційне тлумачення Конституції і законів України. Але аналіз рішень КСУ показує, що вони не тільки роз'яснюють чинне законодавство, але і встановлюють нові приписи нормативного характеру. До того ж рішення Конституційного Суду мають загальний характер і є обов'язковими для виконання.

Таким чином, Конституційний Суд отримав право не лише тлумачити закон, але й