УДК 340.342.951

І. М. Сопілко,
доктор юридичних наук, професор

ТРОЛІ, БОТИ ТА БОТ-МЕРЕЖІ ЯК ЗАГРОЗИ РОЗВИТКУ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА

У статті досліджуються питання подолання нових інформаційних викликів та загроз, таких як тролі, боти та бот-мережі на фоні основних загроз та інформаційних викликів.

Окремо акцентується увага на потребах вдосконалення системи інформаційної безпеки держави на законодавчому рівні.

Ключові слова: *інформація, тролі, боти, бот-мережі, інформаційне суспільство, інформаційні правовідносини, кібербезпека.*

И. Н. Сопилко

Тролли, боты и бот-сети как угрозы развития информационного общества

В статье исследуются вопросы преодоления новых информационных вызовов и угроз, таких как тролли, боты и бот-сети на фоне основных угроз и информационных вызовов.

Отдельно акцентируется внимание на потребностях совершенствования системы информационной безопасности государства на законодательном уровне.

Ключевые слова: *информация, тролли, боты, бот-сети, информационное общество, информационные правоотношения, кибербезопасность.*

I. Sopilko

Trolls, bots and botnets as a threat to the development of the information society

The article examines the issues of overcoming new information challenges and threats, such as trolls, bots and botnets on the background of the main threats and data calls.

Separately, the attention is focused on the needs of improving the information security of the state at the legislative level.

Key words: *information, trolls, bots, botnets, the information society, legal information, cyber security.*

Постановка проблеми та її актуальність. Онлайн-середовище активно входить у життя пересічного громадянина шляхом використання соціальних мереж, онлайн-платформ, електронних, що свідчить про те, що ми живемо в період четвертої індустріальної революції. Термін «четверта індустріальна революція» виник завдяки відомому швейцарському економісту Клаусу Мартіну Швабу після його публікації в журналі Foreign Affairs (її ще називають сучасним «Капіталістичним маніфестом»). Четверту індустріальну революцію він пропонує називати цифровою, бо її особливою характеристикою є стирання відмінностей між фізичною, цифровою та біологічною сферами [9].

Так, на думку учасників 7-го Українського Форуму з управління Інтернетом, українські користувачі віртуального середовища є носіями прав і основоположних свобод людини, гарантованих міжнародним правом і Конституцією України. Українська держава, в особі її посадовців і органів влади, як це випливає з положень Конвенції Ради Європи про захист прав людини та основоположних свобод, має не лише їх не порушувати, але й створити необхідні умови для реалізації шляхом ухвалення необхідних законів, організаційного та фінансового забезпечення. Виклики, що постають на цьому шляху, вимагають об'єднання зусиль держави, громадянського суспільства та бізнесу.

Загалом, важливою тенденцією світового розвитку є зростання ролі гуманітарної безпеки, оскільки вона є складовою національної та міжнародної безпеки й охоплює інтелектуальну, освітньо-виховну, психічну, фізичну, моральну, репродуктивну, духовну, генетичну, майнову, міграційну та культурно-етнічну безпеки [2, с. 124]. Окрему групу викликів становлять пов'язані із засобами масової інформації і тими загрозами, що існують в зазначеній сфері. Це тролі, боти і, відповідно, бот-мережі. При моделюванні шляхів політики подолання таких загроз необхідно зберігати баланс відкритості й безпеки інформаційних мереж.

Крім того, слід відзначити, що Україна вступає в нову еру інформаційного суспільства – в еру інформаційних воєн. Реалізація національних інтересів щодо забезпечення національної безпеки – один із найважливіших напрямів цієї трансформації. Так, в тексті «Доктрини інформаційної безпеки України», яку було прийнято 28 квітня 2014 року, сказано, що за умов швидкого формування і розвитку інформаційного суспільства в Україні та глобального інформаційного простору, широкого використання інформаційно-комунікаційних технологій у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки [3].

Актуальність вказаної проблематики є дуже висока як в українському, так і в європейському суспільствах та наукових середовищах, так як фахівці шукають відповіді на питання про безпеку інформаційного простору, доступність об'єктивної інформації, захист пересічного громадянина від інформаційних атак, інше. Зростання інтересу до тематики безпеки пов'язано із існуючими інформаційними загрозами, які особливо активізувались по мірі становлення інформаційного суспільства та в умовах тотальної політизації інформаційного простору з метою маніпулювання думкою виборців чи інших соціальних груп.

Метою даної статті є аналіз нових інформаційних загроз, таких як: тролі, боти та бот-мережі та шляхів їх подолання або мінімізації.

Інформаційне суспільство забезпечує залучення великої кількості людей до інформаційних ресурсів, сприяє покращенню обміну інформацією між різними суб'єктами інформаційних правовідносин, пришвидшує розвиток інформаційних відносин. Загалом, формування інформаційного суспільства – це тривала діяльність відповідних суб'єктів, як в аспекті проведення організаційних заходів, подолання загроз, так і в питанні формування інформаційно-правового законодавства в зазначеній сфері.

Аналіз досліджень і публікацій. Слід віддати належне провідним дослідникам і засновникам теорії інформаційного суспільства, серед яких особливо можна відзначити П. Дракера, М. Кастельса, Й. Масуду, Е. Тоффлера, Ф. Уебстера, Г. Шилера, М. В. Гуцалюка, Е. Гіденса, Р. А. Калюжного, І. А. Кисарець, В. А. Ліпкана, О. В. Логінова, Є. А. Макаренко, К. Мея, Ю. Є. Максименко, А. І. Марущака, П. Є. Матвієнко, Д. Белла, О. В. Чуприну, В. С. Цимбалюка, М. Я. Швеця, Т. А. Шевцова, О. В. Шепети та інших, проте, незважаючи на те, що теорія інформаційного суспільства є певним чином достатньо розробленою і репрезентованою різноманітними концепціями, питання протидії нових загроз, таких як боти і бот-мережі, в повній мірі не знайшли вирішення в теорії і практиці інформаційного суспільства.

Моделей інформаційного суспільства існує чимало, відповідно кожен автор намагається описати подану ним модель, формуючи відповідну концепцію: постіндустріальне суспільство: Р. Дарендорф; глобальне село: Х. М. Мак-Люен; практопія, суспільство третьої хвилі: О. Тоффлер; концепція нульового росту: Дж. Форрестор, Д. Медоуз; технотронна ера: З. Бжезінський; комп'ютопія: Й. Масуда тощо.

Виклад основного матеріалу. Фундаментального значення у кібернетичному суспільстві набуває переосмислення традиційних підходів щодо розвитку інформаційного суспільства: цілеспрямованого формування нової системи створення високоякісного і технологічного інформаційно-освітнього середовища за участю держави. Не випадково, що у цьому контексті, інтенсивний розвиток сфери знань на основі інформаційних і телекомунікаційних технологій стає найважливішим національним пріоритетом розвинених країн світу [7, с. 20].

В Україні як ніколи активізувалась проблема тролів і ботів та існування відповідних бот-мереж, які несуть загрозу інформаційному середовищу. Подібна проблема є актуальною і для ЄС на фоні загроз радикальних сил та в умовах існуючого воєнного конфлікту на Сході України. Як відомо, інформаційні війни − це дії, розпочаті для досягнення інформаційної переваги шляхом завдання шкоди інформації та процесам, що базуються на інформації та інформаційних системах ворога при одночасному захисті власної інформації та процесів, що базуються на інформації та інформаційних системах. Найбільш поширеним видом таких дій є тролінг, який застосовується в інформаційних мережах, соціальних середовищах та платформах.

Тро́лінг (від англ. trolling) – розміщення в Інтернеті (на форумах, у групах новин Usenet, у вікі-проектах та ін.) провокаційних повідомлень з метою викликати флейм, конфлікти між учасниками, образи, війну редагувань, марнослів'я тощо. Тролінг є грубим порушенням мережевого етикету (нетикету). В інтернет-термінології, «троль» – це людина, яка розміщує брутальні або провокаційні повідомлення в Інтернеті, наприклад, у дискусійних форумах, перешкоджає обговоренню або ображає його учасників. Слово «тролінг» може характеризувати одне конкретне повідомлення, або розміщення таких повідомлень загалом. Поняття «тролінг» також використовується, щоб описати діяльність тролів взагалі [10].

Бот-мережі, або використовується термін ботне́ти (англ. botnet від robot і network) - це комп'ютерна мережа, що складається з деякої кількості хостів, із запущеними ботами - автономним програмним забезпеченням. Найчастіше бот у складі ботнета є програмою, яка приховано встановлюється на комп'ютері жертви і дозволяє зловмисникові виконувати певні дії з використанням ресурсів інфікованого комп'ютера. Зазвичай використовуються для протиправної діяльності – розсилки спаму, перебору паролів на віддаленій системі, атак на відмову в обслуговуванні, отримання персональної інформації про користувачів, крадіжка номерів кредитних карт та паролів доступу [11].

Основним проявом діяльності ботів є DDoS атаки і «боти» в мережі. Вони генерують той паразитний трафік, що заважає роботі інформаційних систем, особливо в умовах неліцензійного програмного забезпечення.

Іншим проявом бот активності є тролінг політичних опонентів у політиці, що дає можливість застосовувати противнику нечесні правила гри. Так, у період виборчих компаній боти і тролі як учасники інформаційного простору забирають до 60 процентів трафіку, що сприяє необ'єктивному сприйнятті інформацією та зловживаннями інформаційними правами. А відсутність можливості офіційно реагувати на такі порушення (так як регулювання мережі Інтернет є досить обмежене) сприяє такій їх діяльності. В результаті таких дій ботів і тролів створюється відповідний інформаційний шум і формулюються нові інформаційні виклики, які є вигідними для окремих груп людей і політичних сил. Відповідно, сприяють формуванню таких викликів і позиції окремих журналістів, в контексті трактування тим чи іншим чином суспільних подій, що створюють певну недовіру до журналістів як учасників інформаційних відносин.

Нівелювання журналістської діяльності призвело до того, що маніпулювання громадською думкою значно полегшилось, що спрощує «роботу» тролів і ботів.

Іншим проявом діяльності ботів і тролів є створення іміджу комерційної діяльності онлайн-магазинів, інших комерційних програм щодо якості товарів, активності на ринку, щодо бренду, інше, що вводить в оману споживача в онлайн-середовищі.

Основні методи інформаційної війни – блокування або перекручування інформаційних потоків і процесів прийняття рішень супротивником, стверджують Д. В. Ланде В. П. Горбулін, О. Г. Додонов, , а також продовжують, що війни в інформаційному середовищі в сучасній науці та військових доктринах, на відміну від журналістської практики, зазвичай прийнято називати інформаційними операціями, наголошуючи, що вони є лише елементами «реальних» багатоаспектних протистоянь. Інформаційні операції є компонентами та супроводом більш за-

гальних процесів. Ареною інформаційних операцій є інформаційний простір [8, с. 7].

Інформаційний простір є ключовим для розвитку країни, бо дозволяє виконати багато завдань. У сучасних умовах ми стаємо свідками, як український інформаційний простір формується в основному під сильним впливом зовнішніх та внутрішніх чинників. Це і триваючі військові дії на Сході, економічна криза, девальвація національної валюти, вплив міжнародних організацій на вирішення конфлікту в Україні, тощо.

Основна задача інформаційних операцій полягає в маніпулюванні масовою свідомістю з такими цілями, як, наприклад: − внесення в суспільну свідомість і свідомість окремих людей визначених ідей і поглядів; − дезорієнтація людей та їхня дезінформація; − ослаблення визначених переконань людей, основ суспільства; − залякування мас [8, с. 8].

Проблемою для пошуку шляхів їх подолання є факт, що інформаційні операції дуже різні та найчастіше вельми складні за своєю природою, тому важко піддаються моделюванню й аналізу, що, серед іншого, пов'язане із двома групами факторів: − суб'єктивними, пов'язаними зі свідомою, цілеспрямованою діяльністю людей, які беруть участь в інформаційних операціях; − об'єктивними, пов'язаними з тим, що в соціальній системі, яка складається з великої кількості елементів, діють «системні ефекти», статистичні закономірності [8, с. 9].

Інформаційний прогрес перетворився на інструмент поневолення людини інформаційними технологіями. Насправді в інформаційному суспільстві відбувається поглинання особистості інформаційними технологіями, в якому люди заради матеріальних благ, отриманих від участі у різних мережевих системах, втрачають духовну свободу та взагалі особистість. Більше того, за такого прискореного інформаційного прогресу, людина може перетворитися на придаток до інформаційних технологій та інформаційних ресурсів. Саме тут можемо згадати футуристичні фільми, в яких малювали встановлення контролю машин над людиною. Іронія цієї ситуації полягає у тому, що згодом людина може втратити ціль існування і перетвориться на заручника розвитку інформаційних технологій і необхідності постійного збільшення інформаційних ресурсів. Прогресивне збільшення споживання інформації призводить до втрати свободи людини, втрати мети існування і підпорядкування своїх цілей цілям збереження і примноження інформаційних ресурсів. За цих умов інформаційного поневолення людини складність подальшого відшукування власного шляху і мети існування, тобто онтологічні проблеми, фактично виходять на перший план.

З метою попередження зловживання інформацією та для захисту інформаційних прав сучасний стан забезпечення національної та інформаційної безпеки України потребує розробки науково обґрунтованої державної політики та стратегії в цій галузі, визначення системи національних цінностей, життєво важливих інтересів особистості, суспільства та держави, визначення зовнішніх і внутрішніх загроз цим інтересам, пошуку ефективних заходів для забезпечення безпеки в усіх її сферах, захисту від інформаційних загроз та реалізації права на отримання достовірної інформації.

В Україні в 2014 році, коли російські інформаційні канали подавали відповідно недостовірну інформацію, виникла необхідність відповідної реакції з боку держави. Тому, судом було прийнято рішення про виключення таких каналів на території України. Подібні загрози можуть виникнути і в ЄС, а досвід реагування в цій сфері буде корисним. Паралельно, усе вищевикладене свідчить про потребу прийняття нормативно-правових актів, у яких був би передбачений механізм захисту інформаційних прав громадян від протиправних дій третіх осіб щодо інформації та обмеження її впливу на особу.

Висновки. Ми приєднуємось до багатосторонньої Декларації-звернення щодо захисту прав і свобод людини онлайн, схваленої на 7-му Українському Форумі з управління Інтернетом 14 жовтня 2016 року, та вважаємо за необхідне підтвердити невідворотність демократичного вибору Українського народу і відданість свободі, повазі до прав людини і прагнення розвивати інтернет-політику, яка сприяє вільному потоку інформації і стимулює інновації, творчість і економічне зростання, – шляхом приєднання до

міждержавної «Коаліції за свободу онлайн» (Freedom Online Coalition).

Більшість проблем щодо порушення та захисту сайтів державних органів України, на думку фахівців, спричинені нелегальним програмним забезпеченням. Неліцензійне ПЗ встановлене на половині комп'ютерів держслужбовців. Крім того, нерідко поштова переписка проводиться з іноземних поштових сервісів, таких, наприклад, як mail.ru. Саме тому, Україна уклала угоду з компанією Microsoft, в рамках якої представники держорганів зможуть оцінити всі недоліки своєї системи у спеціальному центрі прозорості і убезпечити себе від хакерських атак. Так, на думку В. Зверєва, якщо у всіх буде ліцензійне забезпечення, якщо ми будемо нести відповідальність за свій пристрій, у нас ці загрози зменшаться у кілька разів як для держави, так і для кіберпростору України» [12].

Іншим шляхом боротьби з ботами і тролями в мережі Інтернет є шлях їх блокування, а це не завжди правомірно та фізично і організаційно складно, що значно впливає на механізми боротьби з ними та й не завжди законно. Так, право обмежувати право доступу до інформації, належить суду. Крім того практика свідчить, що основна боротьба з ботами – це не блокування, не закриття відповідних мереж чи інше, а якісна, експертна, конкурентна інформація як альтернатива ботам і тролям, яка має бути повною, точною, достовірною та збалансованою.

Крім того, усе вищевикладене свідчить про те, що з метою подолання подібних негативних явищ потрібно, як відзначено в резолюції 7-го Українського Форуму з управління Інтернетом, впроваджувати програми з підвищення медіаграмотності населення, професійних стандартів онлайнової журналістики, продовження реформ щодо прозорості власності, недопущення концентрації на медійному ринку і незалежності редакційної політики ЗМІ від впливу політично-фінансових олігархічних кіл.

Література

1. *Гнатюк С. Л.* Проблеми становлення інформаційного суспільства в Україні / С. Л. Гнатюк // Стратегічні пріоритети. – 2007. – № 1 (2). – С. 95-101.

2. *Новицкий Г. В.* Проблемы обеспечения национальной безопасности в условиях глобализации / Г. В. Новицкий // Геополитика – безопасность – терроризм: сб. ст.; под. ред. Е. А. Вертлиба, Л. М. Бонданца. – Бишкек: Изд-во Бийиктик, 2006. – С. 123-128.

3. Д*октрина* інформаційної безпеки України від 28 квітня 2014 року [Електронний ресурс]. – Режим доступу: http://comin.kmu.gov.ua/control/uk/ publish/ article?art_id=113319&cat_id=61025

4. *Про схвалення* Концепції розвитку електронного урядування в Україні: Розпорядження Кабінету Міністрів України від 13 грудня 2010 р. № 2250-р. [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2250-2010-%D1%80.

5. *Лайон Д.* Інформаційне суспільство: проблеми та ілюзії. Інформація, ідеологія та утопія / Д. Лайон // Сучасна зарубіжна соціальна філософія. – К., 1996. – С. 362-380.

6. *Дракер П.* Посткапиталистическое общество / П. Дракер // Новая постиндустриальная волна на Западе: Антология. – М.: Academia, 1990. – С. 78-90.

7. *Шкарупа В.* Інформатика як основа формування інформаційного суспільства та як об'єкт правознавства / В. Шкарупа, Т. Субіна // Правова інформатика. – 2004. – № 4. – С. 19-26.

8. *Горбулін В. П.* Інформаційні операції та безпека суспільства: загрози, протидія, моделювання: монографія / В. П. Горбулін, О. Г. Додонов, Д. В. Ланде. – К.: Інтертехнологія, 2009. – 164 с.

9. *Пенцак Є.* Четверта індустріальна революція і освіта / Є. Пенцак [Електронний ресурс]. – Режим доступу: http://innovations.com.ua/ua/articles/ op-manage/ 19593/chetverta-industrialna-revolyuciya-i-osvita.

10. *Тролінг* [Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/wiki/%D0%A2%D1%80%D0%BE%D0%BB%D1%96%D0%BD%D0%B3.

11. *Бот-мережі* [Електронний ресурс]. – Режим доступу: https://uk. wikipedia.org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82.

12. *Стельмах І.* Кіберзахист органів влади. Найбільші загрози – DDoS атаки і боти /

І. Стельмах [Електронний ресурс]. – Режим доступу: http://ru. telekritika. ua/ daidzhest/2014-12-28/102080.

References

1. *Gnatjuk S. L.* Problemy stanovlennja informacijnogo suspil'stva v Ukrai'ni / S. L. Gnatjuk // Strategichni priorytety. – 2007. – № 1 (2). – S. 95-101.

2. *Novyckyj G. V.* Problemy obespechenyja nacyonal'noj bezopasnosty v uslovyjah globalyzacyy / G. V. Novyckyj // Geopolitika – bezopasnost' – terrorizm: sb. st.; pod. red. E. A. Vertlyba, L. M. Bondanca. – Byshkek: Izd-vo Byjyktyk, 2006. – S. 123-128.

3. *Doktryna* informacijnoi' bezpeky Ukrai'ny vid 28 kvitnja 2014 roku [Elektronnyj resurs]. – Rezhym dostupu: http://comin.kmu.gov.ua/control/uk/ publish/ article?art_id=113319&cat_id=61025

4. *Pro shvalennja* Koncepcii' rozvytku elektronnogo urjaduvannja v Ukrai'ni: Rozporjadzhennja Kabinetu Ministriv Ukrai'ny vid 13 grudnja 2010 r. № 2250-r. [Elektronnyj resurs]. – Rezhym dostupu: http://zakon2.rada.gov.ua/laws/show/ 2250-2010-%D1%80.

5. *Lajon D.* Informacijne suspil'stvo: problemy ta iljuzii'. Informacija, ideologija ta utopija / D. Lajon // Suchasna zarubizhna social'na filosofija. – K., 1996. – S. 362-380.

6. *Draker P.* Postkapytalystycheskoe obshhestvo / P. Draker // Novaja postyndustryal'naja volna na Zapade: Antologyja. – M.: Academia, 1990. – S. 78-90.

7. *Shkarupa V.* Informatyka jak osnova formuvannja informacijnogo suspil'stva ta jak ob'jekt pravoznavstva / V. Shkarupa, T. Subina // Pravova informatyka. – 2004. – № 4. – S. 19-26.

8. *Gorbulin V. P.* Informacijni operacii' ta bezpeka suspil'stva: zagrozy, protydija, modeljuvannja: monografija / V. P. Gorbulin, O. G. Dodonov, D. V. Lande. – K.: Intertehnologija, 2009. – 164 s.

9. *Pencak Je.* Chetverta industrial'na revoljucija i osvita / Je. Pencak [Elektronnyj resurs]. – Rezhym dostupu: http://innovations.com.ua/ua/ articles/ op-manage/ 19593/chetverta-industrialna-revolyuciya-i-osvita.

10. *Troling* [Elektronnyj resurs]. – Rezhym dostupu: https://uk.wikipedia. org/wiki/%D0%A2%D1%80%D0%BE%D0%

11. *Bot-merezhi* [Elektronnyj resurs]. – Rezhym dostupu: https://uk. wikipedia. org/wiki/%D0%91%D0%BE%D1%82%D0%BD%D0%B5%D1%82.

12. *Stel'mah I.* Kiberzahyst organiv vlady. Najbil'shi zagrozy – DDoS ataky i boty / I. Stel'mah [Elektronnyj resurs]. – Rezhym dostupu: http://ru. telekritika. ua/ daidzhest/2014-12-28/102080.