***Гринкевич О .Й.,*[*] *Гринкевич О. О.*[**]

АСПЕКТИ НЕБЕЗПЕК, ЩО ПОРОДЖУЮТЬСЯ З'ЯВЛЕННЯМ ТА ПОШИРЕННЯМ НОВІТНІХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ

У статті доводиться необхідність прискіпливого аналізу процесів освоєння нових і новітніх досягнень ІКТ на предмет викриття можливих негативних соціально-політичних наслідків. Розглядаються механізми та динаміка розвитку негативних проявів. Виявлено основні елементи сучасної технології повалення неугодних режимів з використанням можливостей ІКТ. Накреслені шляхи та напрями подальшого дослідження проблеми.

Ключові слова: нові і новітні інформаційно-комунікаційні технології, негативні аспекти поширення ІКТ, ризики, виклики, загрози, небезпеки, основні елементи сучасної технології повалення неугодних режимів, шляхи та напрями подальших досліджень.

The article proves the necessity of meticulous analyses of implementing newest achievements of ICT as regards their sphere of negative social-political consequences. It takes into account the mechanisms and dynamics of ICT development from the level of native risks through the phase of challenges formation then to their transition into the level of threats and real insecurity realization. The main elements in the technologies of demolition the inconvenient regimes by using ICT capabilities are revealed. The ways and directions of further researches of the question that is formulated in the article are scheduled.

Key words: new and newest informational-communication technologies, negative aspects of spreading ICT, risks, challenges, threats, insecurity, main elements of demolition the inconvenient regimes, ways and directions of further researches.

В статье показана необходимость глубокого анализа процессов освоения новых и новейших достижений ИКТ с точки зрения выявления возможных негативных социально-политических последствий. Рассматриваются механизмы и динамика развития негативных последствий. Выявлены основные элементы современной технологии свержения неугодных режимов с использованием возможностей ИКТ. Очерчены пути и направления дальнейшего исследования проблемы.

Ключевые слова: новые и новейшие информационно-коммуникативные технологии, негативные аспекты расширения использования ИКТ, риски, вызовы, угрозы, опасности, основные элементы современной технологии свержения неугодных режимов, пути и направления дальнейших исследований.

[*] кандидат юридичних наук, доцент кафедри міжнародного права Інституту міжнародних відносин Київського національного університету імені Тараса Шевченка.

[**] магістр політології, аспірант Національного інституту стратегічних досліджень.

Сьогодення характеризується бурхливим характером розвитку інформаційно-комунікаційних технологій (ІКТ). В роботах вітчизняних вчених, присвячених дослідженню наслідків втілення у соціальну практику цих досягнень, В. Гондюла, Г. Почепцова, М. Рижкова, Є. Макаренко, В. Коломійця, М. Ожевана та інших, переважно розглядаються можливості і позитиви з опанування ІКТ. І тільки в останні роки стали з'являтися матеріали, у яких ставляться питання щодо ризиків, викликів, загроз та небезпек масового поширення ІКТ (можна згадати роботи Г. Почепцова, І. Решетняка, А. Григор'єва). Саме тому, з нашої точки зору, актуальним представляється прискіпливий аналіз ситуації під визначеним кутом зору.

У підґрунтя такого аналізу слід покласти загальну характеристику механізмів та динаміки розвитку негативних проявів від звичайних природних ризиків втілення у людське життя будь-яких новітніх досягнень до небезпек, що стали реальністю [1].

Нагадаємо, що ІКТ за суттю складають підґрунтя міжнародних інформаційних відносин, а останні найбільш повно забезпечують процеси втягування суспільства у його інформаційну стадію розвитку.

У зв'язку з вищевикладеним все більш наполегливою стає необхідність знаходження механізмів, певних обмежень та норм оптимізації процесів опановування і поширення нововведень ІКТ. Вказане завдання не є легким, на цьому шляху у людському суспільстві поки не вироблено єдності позицій.

Об'єктивний характер ризиків з'явлення негативних проявів процесів втілення у життя новітніх інформаційних технологій, наявність суб'єктів здатних генерувати прагнення та дії асоціального плану визначають завдання суспільства щодо врахування цих факторів, потребують організації своєчасних зусиль щодо нейтралізації або відвернення подібних проявів.

В інформаційному просторі розгортаються змагання «анонімних» творців кіберзброї. Дехто вважає, що атака на ядерні об'єкти Ірану вірусу Stuxnet ознаменував початок епохи кібернетичних війн. Орієнтовна оцінка втрат від цієї атаки показує, що вони співставні з тими, що могли б бути результатом атаки ізраїльських ВПС. І це на сьогодні не останній приклад кібернебезпеки [2; 3].

Як би там не було, а реальністю є те, що кіберозброєння є (і вже не поодинокі), підрозділи створюються і діють у армійських або подібних їм державних структурах вже ряду провідних країн світу, є вже подібні підрозділи в українській міліції та СБУ [4-8].

Але при всьому тому загальновизнаних обмежень на військові дії у світовому кіберпросторі не існує, нормативно-правових міжнародних актів нема, а вони конче потрібні.

Один з головних напрямків у цій справі це питання удосконалення управління у мережі Інтернет. Правове регулювання мережі Інтернет питання дуже дискусійне, де стікаються дуже протилежні позиції [9]. При всьому тому, навряд чи значна кількість країн світу, особливо після відомих подій «арабської весни», будуть продовжувати миритися з тим, що управління всесвітньою мережею здійснюється інституцією, що тісна пов'язана з урядом США [10].

Розбіжності у підходах до управління інтернетом оформилися у певний розкол у позиціях учасників Всесвітньої конференції з питань міжнародного електрозв'язку, що відбулася у грудні 2012 року в Дубаї.

Зрозуміло, що після ряду т.зв. кольорових революцій, подій «арабської весни 2011 року» та навколо Сирії у 2011-2013 рр. – у значного числа національних урядів зростають бажання регулювати (і серйозно) Інтернет простір.

До речі, регулярний моніторинг подій, що передували «арабській весні» 2011 р. та її продовження дозволяє стверджувати, що певні соціально-політичні небезпеки останніх

часів породжуються в тому разі і нововведеннями ІКТ. *Так, реальністю стали наднові технології повалення неугодних режимів.*

Сьогодні вже виявилися факти, що свідчать про те, що підготовка подій соціально-політичного протистояння суспільств у Північної Африки починалася задовго до початку самих подій і далеко за кордонами зруйнованих держав. Основні елементи такої відпрацьованої технології можна відстежити за матеріалами наступних публікацій [11-22].

Заздалегідь готувалася відповідна інфраструктура ІКТ, яка всіляко використовувалась для координації і управління діями опозиційних угрупувань в країнах Південної Африки [23-28].

Моніторинг попередніх подій дозволяє відслідкувати – звідки і хто підготував тих осіб, що стали тим «ядром», яке підготовлювало, організовувало та координувало дії мас у «твітерних революціях». Оцінюючи таку підготовку Башем Фатхи, засновник молодіжного руху, який взяв активну участь в подіях в Єгипті, говорів: «Ми навчилися, як організовувати і розвивати коаліції. …Це нам звичайно допомогло під час революції» [28].

Про те як і чому навчали багатьох з майбутніх «польових командирів» свідчать матеріали наступних публікацій [29, 30].

В цілому стан справ в людському суспільстві під впливом ІКТ інновацій характеризується суттєвим підвищенням активності громадян (особливо молоді). Наочно видимий зріст числа учасників масових протестних дій, таких як: «арабська весна 2011», «захопи Уолл-Стріт», або «нас 99%», «за чесні вибори» РФ (2011-2012), «помаранчева революція» (2004) та «цифровий майдан» (лютий 2012) в Україні. Події початку 2012 р. в РФ теж переконливо доводять той факт, що соціальні мережі виступають важливим засобом радикалізації молодого населення країни.

Глибока фінансово-економічна криза, що сьогодні руйнує капіталістичний спосіб виробництва, одночасно створює умови для знищення середнього класу, котрий кілька десятиліть був підґрунтям тієї реальної (суттєво обмеженої) демократії, за якої сьогодні нема майбутнього.

Підбиваючи підсумки бачимо, що небезпеки масового засвоєння ІКТ в ряді країн, що розвиваються, стимульовані завчасним використанням певними закордонними силами: підготовчих зусиль технічного і «кадрового» характеру; маніпуляційною активізацією певних масових прошарків; цілеспрямованим управлінням антидержавницькою активністю мас; інформаційно-пропагандистським освітленням подій з позицій підтримки антиурядових сил; навмисним викривленням образу реальності, створенням фантомів віртуальної (неіснуючої, нереальної) картинки перебігу подій); і кінець кінцем силовою компонентою дій деяких країн Заходу з використанням гасла «обов'язків з захисту», що ідеологічно ґрунтуються на концепції так званої гуманітарної інтервенції.

Глибокого дослідження потребують наступні запитання: «*Друга світова інформаційна війна реальність чи пропагандистський фантом*?» [31]. Засоби інформаційної війни в сфері міжнародної інформації? Асиметричність сучасних інформаційних потоків – що базується на цифровій нерівності країн. Підсумкові документи ВКМЕ (грудень 2012) про завдання досягнення рівності у інтернет-просторі [32].

Не отримали поки що наукового осмислення питання використання *можливостей інформаційних технологій угрупуваннями криміналу, об'єднаннями педофілів та різноманітних збоченців і інших асоціальних сил, терористами тощо.* Ще на початку 2012 року експерти у доповіді «Глобальні ризики – 2012» попереджали учасників Всесвітнього економічного форуму, що одним з головних ризиків року буде ризик кібернебезпеки [33]. Наскільки нам відомо, на сьогодні відсутні дані, які б заперечували подібне попередження у наші дні.

Кіберзроя у руках терористів та кримінальних осіб це вже не фантастика, а сувора реальність часу. Дослідникам вже час відповісти і на запитання: чи потрібні міжнародні механізми та інститути захисту нормальних міжнародних інформаційних обмінів, якими вони повинні бути?

На часі і пошук відповідей стосовно того, як поєднати (безпечно для суспільства): оперативність і певну анонімність спілкування в мережі; надзвичайні організаційні можливості комп'ютерних мереж різного рівня; таємність фінансових операцій, банківських рахунків з загальною соціальною, державною та індивідуальною безпекою.

Давно вже слід розібратися, чому і як при тих можливостях забезпечення прозорості будь-яких дій осіб та їх об'єднань продовжуються: незаконні поставки потоків зброї та техніки подвійного призначення; існує феномен сучасного піратства.

Особливої уваги потребує визначення динаміки переростання ризиків у виклики, а останніх в загрози і реалізація останніх у реальних небезпеках використання можливостей віртуального міжнародного інформаційного простору у спілкуванні організаціями кримінальних співтовариств, рекрутування ними кадрів і т.п., а також для задоволення викривлених потреб збоченців та кримінальників.

Інтернет та соціальні мережі: видима стихійність розширення, зростання атомізації членів суспільства, особливо молоді, заміна реального людського спілкування – віртуальним; суттєве падіння «ціни» людського життя, привичка реалізації «десятків життів» у різноманітного роду «стрілялках» та «стратегіях» електронних ігор; суттєва втрата відчуття реальності людського буття та розуміння святості життя людської особи, суттєве погіршення фізичної складової здоров'я молоді у зв'язку з відсутністю нормального відпочинку (заміна його «навігацією» за допомогою електронних маніпуляторів за комп'ютером) – далеко не всі небезпеки, що породжуються колом ІКТ, що все поширюється.

Нормалізація віртуального простору спілкування, нівелювання та зняття низки *небезпек для все нових поколінь юнаків, які підключаються* до спілкування без набуття досвіду реальних людських стосунків – такі завдання провайдерського співтовариства, громадянського суспільства та державних установ. Зменшення ризиків, відвернення викликів та загроз, ліквідація наслідків проявів небезпек, що стали реальністю всілякого поширення нововведень ІКТ стали нагальними питаннями забезпечення виживання людського співтовариства [34].

Список використаних джерел

1. Гринкевич О. Й. На шляху до системи категорій безпекознавства / О. Й. Гринкевич // Безпекотворення в Україні та Росії: Питання теорії і практики та правові аспекти. Рейдерство : збірка наукових праць. – К. : Вид-во Європ. ун-ту, 2008. – С. 195-213.
2. Мельников Дмитрий. Охота на «Красный октябрь»: в кибероружии нашли русско-китайский след / Дмитрий Мельников [Електронний ресурс]. – Режим доступу: http://www.vesti.ru/videos?vid=479114.
3. Касперский Евгений. «Сила в правде» – мой ответ на статью Ноа Шахтмана в журнале «Wired» / Евгений Касперский [Електронний ресурс]. – Режим доступу: http://eugene.kaspersky.ru/2012/07/26/kaspersky-response-wired-noah-shachtman/.
4. Орлова Е. Кибератаки на заказ / Елизавета Орлова // Красная звезда. – 2013. – 12 февр. [Електронний ресурс]. – Режим доступу: http://www.redstar.ru/index.php/2011-07-25-15-57-07/item/7455-kiberataki-na-zakaz.
5. ФРГ признала наличие военизированного киберподразделения [Електронний ресурс]. – Режим доступу: http://www.warandpeace.ru/ru/news/vprint/70171/.

6. Група швидкого реагування НАТО для боротьби проти кібернападівю. – [Електронний ресурс]. – Режим доступу: http://www.nato.int/cps/uk/SID-5A71FD38-ECA1B579/natolive/news_85161.htm?blnSublanguage=true&selectedLocale=&submit=select.
7. Рогозин Дмитрий. В России будет создана своя DARPA и Киберкомандование. [Електронний ресурс]. – Режим доступу: http://itstrateg.net/news/dmitrij-rogozin-v-rossii-budet-sozdana-svoya-darpa-i-kiberkomandovanie.
8. Рада согласилась создать в структуре СБУ информационную контрразведку. [Електронний ресурс]. – Режим доступу: http://lb.ua/news/2011/12/09/127553_rada_soglasilas_sozdat_v_strukture.html.
9. Курбалийя Й. Управление Интернетом / Й. Курбалийя. [Електронний ресурс]. – Режим доступу: http://www.twirpx.com/file/210654/.
10. Вайден Алекс. Судьба интернета решится в Дубае («Русская Германия», Германия) / Алекс Вайден. [Електронний ресурс]. – Режим доступу: http://inosmi.ru/world/20121209/203139277.html.
11. Седов Дмитрий. Башар Асад: «демонизация объекта» / Дмитрий Седов. [Електронний ресурс]. – Режим доступу: http://www.fondsk.ru/pview/2011/11/23/bashar-asad-demonizacia-obekta.html.
12. Engdahl F. William. Creative Destruction: Libya in Washington's Greater Middle East Project Part II / F. William Engdahl. – 2011. – 03 листопада [Електронний ресурс]. – Режим доступу: http://www.globalresearch.ca/index.php?context=va&aid.
13. Седов Дмитрий. Ложный след сирийского «великомученика» / Дмитрий Седов. – [Електронний ресурс]. – Режим доступу: http://www.fondsk.ru/pview/2011/08/02/lozhnyj-sled-sirijskogo-velikomuchenika.html/. – На 09.02.2011 р.
14. Ливия глазами очевидца. – 2011, 23 лютого / [Електронний ресурс]. – Режим доступу: http://www,nstarikov.livejournal.com/219280.html.
15. На конференции в Париже собрались страны, поддержавшие власть повстанцев в Ливии. – 2011. – 01 сентября. [Електронний ресурс]. – Режим доступу: http://www.ntv.ru/novosti/238048/.
16. Спецназ Британии и Катара уже в Сирии. [Електронний ресурс]. – Режим доступу: http://www.imperiya.by/news.html?id=85186.
17. Спецназ США, Франции и Британии высадился в Ливии [Електронний ресурс]. – Режим доступу: http://www.newsland.com/news/detail/id/646603/.
18. Провокационные игры западных СМИ вокруг российско-китайского вето по Сирии. [Електронний ресурс]. – Режим доступу: http://www.fondsk.ru/news/2012/02/05/provokacionnye-igry-zapadnyh-smi-vokrug-veto-po-sirii-12640.html.
19. Американские сенаторы поддерживают удары НАТО = В Триполи толпа напала на посольства Великобритании и Италии / Голос Америки [Електронний ресурс]. – Режим доступу: http://www.voanews.com/russian/news/world-news/Libya-1st-Update-2011-05-01-121054659.html.
20. МО стран НАТО назвали большим успехом операцию в Ливии. – 2011. 05 жовтня. [Електронний ресурс]. – Режим доступу: http://www.warandpeace.ru/ru/news/vprint/62451/.
21. Барак Обама: Башар Асад потерял легитимность [Електронний ресурс]. – Режим доступу: http://new.mignews.com/news/politic/world/130711_42052_48304.html.
22. Кэмерон: Асад утратил легитимность, Сирии нужны санкции. – 2012. – 13 січня. [Електронний ресурс]. – Режим доступу: http://rss.novostimira.com/n_2031565.html.
23. Революция не на бумаге уроки страны рукотворных гор [Електронний ресурс]. – Режим доступу: http://79.174.78.50/forum/index.php?topic=125184.0.

24. На саміті ООН в Тунісі представили комп'ютер для бідних за $100. [Електронний ресурс]. – Режим доступу: http://www.securitylab.ru/news/242122.php?R1=RSS&R2=all-news.
25. Благовещенськая Юлія. Ноутбук від OLPC отримає кожен лівійський школяр / Юлія Благовещенськая. [Електронний ресурс]. – Режим доступу: http://www.ferra.ru/ru/notebooks/news/2006/10/16/noutbuk-ot-olpc-poluchit-kajdyy-liviyskiy-shkolnik/.
26. Откуда в странах «интернет-революций» компьютеры? [Електронний ресурс]. – Режим доступу: http hard.compulenta.ru/337824/?r1=yandex&r2=news&country=Russia.
27. Школьникам сектора Газа раздадут 200 тысяч ноутбуков. [Електронний ресурс]. – Режим доступу: http://lenta.ru/news/2010/04/29/olpc.
28. Nixon Ron. U.S. Groups Helped Nurture Arab Uprisings / Ron Nixon; New York Times. – 2011. – 14 April. [Електронний ресурс]. – Режим доступу: http://www.nytimes.com/2011/04/15/world/15aid.html?_r=2.
29. Announcement on Alliance of Youth Movements Summit, December 3-5. Summit brings youth groups, tech experts together to promote freedom. 20 November 2008. [Електронний ресурс]. – Режим доступу: http://www.america.gov/st/texttrans-english/2008/November/20081120122321eaifas0.3440363.html.
30. Цветные революции. 2011. – 28 квітня. [Електронний ресурс]. – Режим доступу: http://gifakt.ru/archives/sots/cvetnye-revolyucii.
31. Панарин Игорь. Вторая мировая информационная – война против России / Игорь Панарин. [Електронний ресурс]. – Режим доступу: http://www.km.ru/spetsproekty/2012/01/10/vzaimootnosheniya-vlasti-i-smi-v-mire/vtoraya-mirovaya-informatsionnaya-voina.
32. Всемирная конференция по международной электросвязи (ВКМЭ – 12). Заключительные акты (Дубай, 2012 г.). [Електронний ресурс]. – Режим доступу: http://www.itu.int/ru/wcit-12/Pages/default.aspx.
33. Одним из вероятных рисков года является кибербезопасность – эксперты. [Електронний ресурс]. – Режим доступу: http://itstrateg.net/news/odnim-iz-veroyatnykh-riskov-goda-yavlyaetsya-kiberbezopasnovst-eksperty/.
34. Гринкевич Г. О. Зміни у житті світової спільноти, що породжуються новітніми інформаційно-комунікаційними технологіями (ІКТ) / Г. О. Гринкевич, О. Й. Гринкевич. // Проблеми міжнародних відносин : збірник наукових праць. – К. : КиМУ, 2012. – 387-400 с.