

10. Концепція (основи державної політики) національної безпеки України, схвалена Постановою Верховної Ради України від 16 січня 1997 року. Режим доступу: <http://zakon5.rada.gov.ua/laws/show/964-15>

11. Конвенції про кіберзлочинність, ратифікована ЗУ № 2824-IV (2824-15) від 07.09.2005, чинна з 01.07.2006. Режим доступу: http://zakon3.rada.gov.ua/laws/show/994_575

12. Воєнна доктрина України затверджена Указом Президента України від 15 червня 2004 року № 648 (в редакції Указу Президента України від 8 червня 2012 року № 390/2012). Розділ 2 п. 7; розділ 3 п. 19; розділу 3 п. 17. Режим доступу: <http://zakon2.rada.gov.ua/laws/show/390/2012/paran12#n12>

13. Інформаційна та кібербезпека: соціотехнічний аспект: підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа; за заг. ред. д-ра техн. наук, професора В. Б. Толубка. – К.: ДУТ, 2015. – 288 с. Режим доступу: http://www.dut.edu.ua/uploads/p_303_79299367.pdf

14. Постанова Верховної Ради України «Про прийняття за основу проекту Закону України про основні засади забезпечення кібербезпеки України» № 1524-VIII від 20 вересня 2016 року. <http://zakon5.rada.gov.ua/laws/show/1524-19>

15. Інформаційний Інтернет ресурс: сайт Верховної Ради України Режим доступу: <http://rada.gov.ua/news/Novyny/106345.html>

16. Доктрина інформаційної безпеки України, затверджена Указом Президента України від 8 липня 2009 року № 514/2009 [Електронний ресурс]. – Режим доступу: <http://zakon0.rada.gov.ua/laws/show/514/2009>

17. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): моногр. / В. М. Бутузов. – К.: КИТ, 2010. – 408 с. Режим доступу Національної бібліотеки ім. Вернадського: <http://www.nbuv.gov.ua/node/300>

18. Боротьба з комп'ютерною злочинністю в контексті забезпечення національної безпеки України: нормативно-правовий та організаційний аспекти М. М. Чеховська та І. М. Ничитайло. Режим доступу: file:///C:/Documents%20and%20Settings/Lanos/%D0%9C%D0%BE%D0%B8%20%D0%B4%D0%BE%D0%BA%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D1%8B/Downloads/iblsd_2014_1_14.pdf

19. Розслідування комп'ютерних злочинів: моногр. / В. О. Голубев. – Запоріжжя: Гуманітарний університет «ІДМУ», 2003. – 296 с. Режим доступу: <http://www.naiu.kiev.ua/biblio/bibliografichni-pokazhchiki/protidiya-kiberzlochinnosti.pdf>

Томилко М.М.

студент,

Національна академія Служби безпеки України

ВИКОРИСТАННЯ СОЦІАЛЬНИХ МЕРЕЖ ДЛЯ ОРГАНІЗАЦІЇ МАСОВИХ ЗАВОРУШЕНЬ

На сьогодні, соціальні мережі є одними з найбільш відвідуваних ресурсів в глобальній мережі інтернет. Згідно даних компанії comScore їх використовують близько 80% всіх користувачів Інтернету. З їх допомогою аудиторія отримує новини від традиційних до альтернативних, коментує їх, тлумачить та займається поширенням з них інформації, стаючи співучасником своєрідного інформаційного процесу. Інтенсивний розвиток науки й техніки, вже набув такого рівня, при якому нові комунікаційні технології багатократно збільшили

можливості деструктивного інформаційного впливу на великі групи людей. Виникла загроза соціальної небезпеки, із застосуванням технологій штучної зміни поведінкових реакцій людини і впливу на свободу її волевиявлення, для досягнення політичних, економічних та інших переваг.

«Арабська весна» є прикладом, що соціальні мережі можуть бути потужною силою для соціальних змін, спроможні вплинути на напрямок розвитку політичних рухів і навіть допомагають повалити режими влади та замінити їх на свої, більш вигідні. Перша – мережева революція відбулася на Філіпінах 17 січня 2001 р., коли після блокування парламентом процедури імпічменту президента Д. Естради, громадяни країни послали один одному понад 7 млн. електронних повідомлень із закликами вийти на вулиці та брати участь Сучасний захист інформації № 1, 2016 55 в акціях протесту. Через три роки наступна – мережева революція відбулася в Іспанії (2004 р.). У подальшому революції мали місце в Молдові (2009 р.), Ірані (2009 р., 2010 р.), Таїланді (2010 р.), згодом в Тунісі, Єгипті та Україні. Разом із засобами масової інформації вони швидко та якісно оволоділи аудиторією, до початку перевороту. У той час, коли традиційні медіа – телебачення, радіо та преса не були готові виконувати інформаційні та по'єднуючі запити суспільства, цю роль на себе взяли Facebook і Twitter, а в деяких країнах до них приєднався «Вконтакте». Як стверджує старший радника з питань інновацій в офісі Державного секретаря США Гілларі Клінтон, Алек Росс: – Мережа не просто змінила міжнародну політику. Я впевнений, що без інтернету не були б успішними недавні революції в Арабському світі. На мою думку, Україна також стала не виключенням цього [1].

6 серпня 2011 року у Великобританії розпочались масові заворушення. Формальною причиною їх початку вважають вбивство 4 серпня співробітниками поліції 29-річного темношкірого Марка Даггана, який при спробі обшуку чинив активний опір. Після цього в лондонському районі Тоттенхем розпочались масові акції протесту з вимогою розслідування загибелі М. Даггана, однак вже в ніч з 6 на 7 серпня ці протести перетворились на масові мародерства які супроводжувались биттям вітрин та пограбуваннями магазинів і будівель. В наступні дні схожі акції охопили сусідні райони та інші міста. Станом на 12 серпня 2011 року основні заворушення були придушені, а суди почали виносити вироки тим особам, які приймали в заворушеннях найбільш активну участь. Британська поліція із самого початку заворушень розпочала моніторинг соціальних мереж та виявлення акаунтів тих, хто закликає до погромів чи агресивних дій. Однак звернувшись до адміністрацій соціальних мереж з вимогою заблокувати такі акаунти вони не завжди отримували підтримку [2].

Адміністрація Twitter однозначно заявила, що буде дотримуватись політики «свободи самовираження та обговорень». Крім того, Twitter буде і надалі дотримуватись принципу повідомляти своїх користувачів про ситуації, коли сервіс вимушений передавати будь-яку персональну інформацію владі, для того, щоб у людей була можливість видалити небажану інформацію.

Адміністрація Facebook була більш стриманою, заявивши, що вони самі активно видаляють повідомлення екстремістського змісту і готові до перемовин із урядом.

Використовуються ІТ-технології як для пошуку мародерів, так і в якості доказової бази в судах. Активно використовуються так звані «дігі-вени» [5] («digi-van» – машини, які обладнано великим телеекраном, на якому демонструються фото мародерів, знятих ССТV – розгалуженої системи відеокамер, призначеної для візуального контролю чи автоматичного аналізу зображень).

Британські парламентарі вимагають від представників основних соціальних мереж блокувати доступ користувачів під час масових заворушень. Менеджери основних соціальних мереж Facebook, Twitter та BlackBerry та представники поліції сьогодні зустрінуться з міністром внутрішніх справ Великобританії Терезою Мей. На засіданні будуть підняті питання щодо ролі соціальних мереж під час масових акцій громадської непокори, а також їх відповідальність за зміст повідомлень, які публікуються на сайтах. Серед іншого буде обговорюватись можливість заборони доступу підозрюваних бунтівників до соціальних мереж. Мей пропонує провести конструктивну дискусію щодо того, як соціальні мережі можуть допомогти уряду під час заворушень замість обговорення закриття сайтів взагалі. Депутати від Консервативної партії Тім Голдвін та Луїза Менш запропонували закрити сайти на час надзвичайного стану. У свою чергу Twitter та Facebook оприлюдняють заходи, які вже вживаються, для видалення повідомлень, які потенційно підбурюють до насильства. Нагадаємо, суд англійського міста Честер засудив до чотирьох років в'язниці двох молодих людей за заклики до насильства в соціальній мережі Facebook під час недавніх вуличних безладів в Британії.

Список використаних джерел:

1. Почепцов Г. Г. Інформаційна війна як інтелектуальна війна [Електронний ресурс] / Г. Почепцов. – Режим доступу: <http://osvita.mediasapiens.ua/material/13303>
2. Дубов Д. В. Мобільний зв'язок та соціальні мережі під час «BlackBerry-бунту» у Великобританії. [Електронний ресурс] Дубов Д. В. – Режим доступу: <http://www.niss.gov.ua/articles/553/>

Харицька О.М.

студент,

*Навчально-науковий інститут інформаційної безпеки
Національної академії Служби безпеки України*

МЕТОДИ ВЕРИФІКАЦІЇ ЗОБРАЖЕНЬ В МЕРЕЖІ ІНТЕРНЕТ

Сьогодні цифрове середовище сповнене чуток та недостовірних фактів, що змушує користувачів активно відсортовувати правдиву і справжню інформацію від брехні.