ВИКОРИСТАННЯ КІБЕРПРОСТОРУ І СОЦІАЛЬНИХ МЕРЕЖ З МЕТОЮ ПРОТИДІЇ ТЕРОРИСТИЧНИМ ЗАГРОЗАМ

Романюк А. В., студ. (гр. БЕ-71, ФБТ КПІ ім. Ігоря Сікорського)

Анотація. У роботі розглядається питання про те, як нові технології можуть полегшити боротьбу з тероризмом завдяки використанню кіберпростору та соціальних мереж, які стали місцем, де терористичні групи вербують і поширюють пропаганду й тероризм. Розглянуто впровадження та адаптація технологій для створення потенціалу виявлення, запобігання, припинення та ліквідації терористів.

Ключові слова: кіберпростір, соціальні мережі, тероризм, суспільство.

Abstract. This work discusses how new technologies can facilitate the fight against terrorism through the use of cyberspace and social media, which have become a venue for terrorists groups for recruiting and proliferating propaganda and terrorism. Incorporation and adaptation of technology to build capabilities of detection, prevention, pre-emption and elimination of terrorists.

Keywords: cyberspace, social media, terrorism, society.

Вступ. Суспільство постійно прагне розробляти більш ефективні та дієві способи комунікації з використанням технологій. Однак, поряд з гонкою за технологіями, зростає і зловживання, особливо передовими концепціями кіберпростору. Комунікаційні технології дозволяють терористичним групам здійснювати напади віддалено, часто за допомогою зашифрованих повідомлень.

Очевидно, що соціальні мережі не послаблять свого впливу в повсякденному житті кожної людини. Розроблювати стратегії боротьби з тероризмом, що засновані виключно на людських навичках і інстинктах, практично неможливо, тому інвестиції в технології для боротьби з виникаючими загрозами тероризму є необхідністю. Це означає, що стратегії боротьби з тероризмом повинні використовувати одну і ту ж технологію - цифрова проблема потребує цифрового вирішення [1].

Правоохоронні органи повинні розуміти, як терористи використовують конкретні платформи, щоб ефективно призначати контрзаходи.

Аналіз стану питання. Терористичні групи все частіше використовують соціальні мережі для досягнення своїх цілей, через те що це дешево та полегшує доступ до великої аудиторії. Багато статей присвячені електронним стратегіям і використанню інтернету для вербування, проте існує дуже мало досліджень, що розглядають ефективність застосування соціальних медіа в боротьбі з терористичним контентом.

Мета роботи: визначення положення тероризму в кіберпросторі, використання соціальних мереж та інтернету для виявлення і усунення терористичних агітацій та облікових записів.

Методики, матеріали і результати досліджень. Приватні суб'єкти вже давно беруть участь в зусиллях по боротьбі з тероризмом: банки, оператори

найважливіших об'єктів інфраструктури і авіакомпанії є важливими елементами громадських зусиль щодо захисту від тероризму. Однак використання інтернету терористами призвело до того, що на передній план у боротьбі з тероризмом вийшов абсолютно новий клас приватних суб'єктів. Компанії соціальних мереж, як в індивідуальному порядку, так і в координації одна з одною, розробили надійні операції із запобігання зловживанню терористами своїми платформами. Як і всі антитерористичні програми, ці зусилля недосконалі, але вони відіграють важливу роль в реагуванні суспільства на терористичне насильство.

Одним з найбільш фундаментальних рішень, з якими стикаються технологічні компанії, є визначення терориста. Існує кілька варіантів, кожен зі своїми плюсами і мінусами. Першим є використання міжнародних списків призначень, таких як списки, які веде Організація Об'єднаних Націй або Європейський союз. Компанії, які хочуть звернутися до більш широкого кола терористів, використовуючи свої платформи, можуть замість цього прийняти рішення покладатися на списки, що складаються різними урядами по всьому світу. Такий підхід дозволяє уникнути проблеми з найменшими розбіжностями в базі, а також дозволить вести злагоджену роботу з правовими органами в усьому світі [2].

Останній варіант полягає в тому, що компанії можуть самі визначати терористичні організації. Проте він вимагає від компаній проведення великої аналітичної роботи, вироблення чіткого плану визначення тероризму та утвердження ролі уряду до даних дій.

Технологічні компанії повинні не просто «заборонити тероризм» на своїй платформі, але й розробити надійну інформаційну політику. Наприклад, компанії повинні визначити, чи слід встановлювати обмеження на рівні контенту, облікового запису або користувача, а також які види взаємодії з терористичним контентом або групами є прийнятними, а які - ні.

Обмеження на рівні контенту забороняють підтримку тероризму в окремих матеріалах в інтернеті. «Контент» відрізняється в залежності від платформи: в Twitter це буде твіт; на Facebook - пост, коментар або аналогічна інформація, створена користувачами; і на YouTube - завантажене відео [3].

Навіть на рівні контенту компанії повинні визначити, який матеріал порушує їх правила. Один з механізмів полягає в тому, щоб просто заборонити офіційну пропаганду, створену або явно призначену для просування повідомлення терориста чи терористичної групи.

Деякі компанії можуть прийти до висновку, що просто заборонити поширення терористичного контенту на їх сайті є неефективним. Вони вважають, що краще видалити облікові записи після певної кількості порушень, пов'язаних з контентом, який несе певні повідомлення, що демонструють підтримку тероризму або терористичним організаціям. Перевага такого підходу полягає в простоті. Технологічні компанії, можуть оцінювати акаунти, використовуючи більш широкий набір показників для визначення того, чи є видалення виправданим. Це може включати в себе IP-адреса облікового запису, її взаємодія з іншими небезпечними обліковими записами, а також технічні

ознаки, зібрані за допомогою техніки боротьби зі спамом, які вказують на те, що обліковий запис було створено недобросовісно або відображати раніше видалений обліковий запис [4]. Важливо відзначити, що інструменти, які базуються на метаданих, можуть працювати навіть тоді, коли контент зашифрований, що робить їх потенційно дуже цінними для зашифрованих платформ.

Технологія оптичного розпізнавання дозволяє платформам сканувати логотипи, зброю та інші потенційно небезпечні індикатори в зображенні або відео - навіть якщо загальне зображення або відео не збігається з відомим цифровим відбитком пальця. Ця технологія складніша, ніж моніторинг контенту, і тому важче впроваджується в невеликих компаніях. Подібно контентному збігу, оптичне розпізнавання також генерує показники достовірності, які оцінюють імовірність того, що щось, виявлене алгоритмом, насправді викликає підозру. Однак ця технологія може сканувати тільки той контент, який був завантажений на платформу, вимагає спеціального навчання персоналу і не буде працювати з зашифрованим контентом [5].

Перетворення кіберпростору в стратегічну комунікацію в структурі національної безпеки, сприятиме швидкому реагуванню правоохоронних органів на потенційну небезпеку, і застосуванню наступних заходів та дій.

Висновки. Соціальні мережі надали терористичним організаціям цифрову платформу, що дало можливість здійснення кібератак, просто за допомогою розповсюдження повідомлень. Масштаби цієї проблеми величезні, тому інформаційні технології боротьби з тероризмом стають необхідністю, яку не можна обійти увагою. Нові технології розширюють діапазон доступних можливостей для держави, щоб забезпечувати національну безпеку. Переваги соціальних мереж включають в себе доступність корисних для використання баз, які можуть допомогти в оперативному плануванні, аналізі розвідувальних даних, а також в забезпеченні організаційної стійкості за рахунок фінансових ресурсів. Сайти соціальних мереж повинні фільтрувати та обробляти контент з терористичних груп або облікових записів, особливо з урахуванням того, що компанії надають доступ в інтернет країнам третього світу. Ідея полягає в тому, щоб дати людям можливість визначити загрозу і вжити відповідних заходів до того, як терористи зможуть завдати шкоди.

Технологічні компанії повинні адаптувати аналіз даних і рекомендації для тих, хто приймає рішення в області антитерористичної політики, тобто повинна здійснюватися злагоджена робота правоохоронних органів з онлайн-платформами.

Науковий керівник: Ільчук О. С., канд. техн. наук, ст. вик. (каф. ОППЦБ КПІ ім. Ігоря Сікорського)

Література

1. Eijkman Q. Counter-Terrorism, Technology and Transparency: Reconsidering state accountability? ICCT International Centre for Counter-Terrorism - The Hague. 2012. URL : https://icct.nl/publication/counter-terrorism-technology-and-transparency-reconsidering-state-accountability/.

2. Bertram L. Terrorism, the Internet and the Social Media Advantage. Journal for deradicalization. 2016. №7. С. 225–230.

3. D. Bieda, L. Halawi. Cyberspace: a venue for terrorism. Issues in Information Systems. 2015. №16. С. 33–42.

4. Kumar N. Use of Modern Technology to Counter Terrorism. ResearchGate. 2019.
URL:https://www.researchgate.net/publication/333609468_Use_of_Modern_Technology_to_Counter_Terrorism.

5. Fishman B. Crossroads: Counter-terrorism and the Internet. Yale University Press. 2016. URL : https://tnsr.org/2019/02/crossroads-counter-terrorism-and-the-internet/.