столиць та інших великих міст до менших міст та поселень, які добре знайомі атакуючому. Найважливіші міста будуть залишати свою привабливість як цілі транснаціональних терористичних груп, але вони більше не є основними. Ця динаміка, ймовірно, зберігатиметься в 2018 р., оскільки ІД буде намагатися помститися за втрату свого територіального «халіфату».

Список використаних джерел:

1. Gupta D. K. Waves of International Terrorism: An Explanation of the Process by which Ideas Flood the World. In Terrorism, Identity and Legitimacy. Ed. E. Rosenfeld // New York: Routledge, 2011. – P. 30-44.
2. Walls E.B.A. Waves of modern terrorism: examining the past and predicting the future // Washington: Georgetown University, 2017. – 114 pp.
3. Honig O. A Fifth Wave of Terrorism? The Emergence of Terrorist Semi-States // Terrorism and Political Violence, June 2017. URL: https://www.tandfonline.com/doi/abs/10.1080/09546553.2017.1330201?journalCode=ftpv20.
4. Lia B. Globalisation and the Future of Terrorism: Patterns and Predictions // New York: Routledge, 2005. – 272 pp.
5. Wood J., VanSlyke S. Terrirism and new ideologies. // RiskMap 2018. URL: https://www.controlrisks.com/-/media/3c6cfbc84397463bbe955f1c844cf78e.ashx.

Саган О.В.
аспірантка,
Національний інститут стратегічних досліджень

«ХАЛІФАТ В КІБЕРПРОСТОРІ» АБО НОВИЙ ТИП ТЕРОРИЗМУ

Поняття «кіберпростір» увійшло до наукового лексикону та повсякденне життя інформаційної людини порівняно нещодавно. Характер його функціонування засвідчив дві головні особливості інформаційного середовища, а саме: зростаючу повсякденну залежність сучасної людини від інформаційних технологій та силу впливу інформаційних технологій на стиль і якість її життя.

Відповідно до міжнародного стандарту [1], кіберпростір – це середовище яке створене за допомогою технічних пристроїв, технологій, мереж та підключених до них користувачів, яке не існує у будь-якій фізичній формі. Існують й інше визначення. Нормативна база США [2] розглядає його як сферу, що характеризується можливістю використання електронних та електромагнітних засобів для запам’ятовування, модифікування та обміну даними через мережеві системи та пов’язану з ними фізичну інфраструктуру. В офіційних документах Євросоюзу [3] кіберпростір розглядається як віртуальний простір, в якому циркулюють електронні дані світових персональних комп’ютерів.

Кіберпростір постійно розширюється, охоплюючи все більше сфер людської діяльності та надає людству досі небачені можливості. Водночас з появою віртуального простору пов’язане виникнення й такого небезпечного

явища як кібертероризм, або «мережевий тероризм». У діяльності злочинних та терористичних угрупувань переваги кіберпростору матеріалізувалися у нову тактику боротьби проти владних структур й укладів життя, які вони вважали неприпустимими. Передусім цьому посприяли можливість вільного доступу, невисока вартість зв'язку, відсутність цензури та інших форм державного контролю, швидкість передачі інформації, величезна аудиторія і технічні можливості, та що найважливіше анонімність.

Звернула увагу на такий арсенал боротьби і така терористична організація як Ісламська держава, яка згодом розгорнула у мережі активну діяльність, кинувши виклик не лише так званим «західним цінностям», а й існуючому світоустрою взагалі.

Військова поразка терористичної мережі Ісламської держави в Іраку та Сирії змусила джихадистів зосередити зусилля на діяльності у світовій мережі. Насамперед йдеться про вербування нових бойовиків для здійснення терористичних актів на Заході та пропаганду «цінностей Ісламської держави» серед молоді. Результатом цієї діяльності стали десятки терористичних актів та акції спрямовані проти інтересів країн Заходу в мережі. Країнами, які більш всього зазнали різноманітних форм терористичних акцій стали Німеччина, Франція, Голландія, Англія та Швеція. Це надало підстави аналітикам спецслужб засвідчити, що починаючи з 2015 року джихадисти змінили тактику дій на користь нарощування «мережевого тероризму». Голова комітету Сенату США з питань нацбезпеки Рон Джонсон назвав таку тактику «новим халіфатом в кіберпросторі» [4].

Вимоги національної безпеки змусили спеціалістів багатьох країн світу звернути увагу на нову особливість тактичних схем терористів і зайнятися пошуком шляхів подолання цієї загрози. З цією метою було враховано низку способів використання мережі Інтернет терористами, а саме:

розміщення сайтів з інформацією про історію організації, звітом про її найгучніші справи, біографіями лідерів, засновників та «героїв», даними про політичні та ідеологічні цілі руху, а також жорсткою критикою ворогів;

узгодження в мережі часу та місця майбутніх терактів, з використанням таких сервісів як електронні мапи місцевості та знімки з супутника; розміщення інструкцій з виготовлення вибухових пристроїв, зброї, підготовки терактів тощо;

проникнення або атаки на комп'ютерні мережі різних установ та об'єктів інфраструктури;

проведення психологічних атак, спрямованих на нагнітання страху та відчуття громадянами власної незахищеності; залякування потенційних ворогів та залучення прибічників, передусім серед молоді.

поповнення фондів організації шляхом збору грошових коштів на підтримку злочинних операцій та утримання бойовиків;

Виходячи з вищезазначеного можна зробити висновок, що наразі найбільш ефективним способом протистояння явищу, яке отримало назву «халіфат в кіберпросторі» є скоординована політика державних інститутів та побудована на цій основі ефективна система інформування суспільства. Всі групи населення країни мають отримати доступ до повної й одночасно

диференційованої інформації з метою усвідомлення таких речей як: що таке тероризм, як він проявляється в Інтернеті та соціальних мережах, які сайти пропагують терористичний контент і яка мета їхньої діяльності, правові наслідки у разі участі в терористичних угрупованнях та інше [5]. У даному випадку знання стає своєрідним оберегом, який робить людину здатною протистояти шкідливому впливу, адже знаючу людину не так просто збити з правильного шляху.

Список використаних джерел:

1. ISO/IEC 27032, Information technology – Security techniques – Guidelines for cybersecurity. – 2012. – 50 p.
2. National Military Strategy for Cyberspace Operations. URL: http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf.
3. Glossary and Acronyms (Archived) / European Commission. URL: http://ec.europa.eu/information_society/tl/help/glossary/index_en.htm#c.
4. В американском сенате назвали новую угрозу от ИГ – «киберхалифат». URL: https://ukrbiz.net/news/56904-v-amerikanskom-senate-nazvali-novuyu-ugrozu-ot-ig-kiberhalifat.html.
5. Використання інтернету терористичними організаціями в сучасному світі. URL: http://social-science.com.ua/article/1390.

Шумейко З.Г.
студентка,
Науковий керівник: **Бусленко В.В.**
кандидат політичних наук, доцент,
Східноєвропейський національний університет
імені Лесі Українки

ЧИННИКИ ЛЕГІТИМАЦІЇ ПОЛІТИЧНОЇ ВЛАДИ В УКРАЇНІ

Питання легітимності перебувало у сфері дослідження таких вчених, як М. Макіавелі, А. Сміта, А. де Токвіля, М. Вебера. Серед сучасних західних учених розробкою даного питання займались С. Хантінгтон [6], Л. Даймонд, Ф. Шмітер, П. Розанвалон [3].

Метою статті є аналіз чинників легітимації політичної влади.

В умовах переходу України до демократії ключовою проблемою стала легітимація політичної влади. Термін легітимація визначається дослідниками як процес визнання влади, добровільна згода на панування представницької влади над громадянами [1; 3; 6].

Чинники легітимації політичної влади безпосередньо пов’язані із ефективністю діяльності владних інститутів та політичної системи в цілому. У державах із демократичною формою правління рівень легітимації залежить від того, наскільки правитель відповідає очікуванням ключових груп виборців [6, с. 368]. В умовах, коли дії влади погоджені із очікуваннями громадян,