РУЛЬОВ ІЛЛЯ МИХАЙЛОВИЧ

Національний університет «Одеська юридична академія»,
аспірант кафедри міжнародного та європейського права

ПРЕВЕНТИВНІ МЕХАНІЗМИ ПРОТИДІЇ КІБЕРТЕРОРИЗМУ, ДОСВІД КНР

Важливим у досліджені механізму протидії кібертероризму є досвід інших країн, саме тому ми розглянемо Китайський досвід у забезпечені безпеки свого інформаційного простору. Китайська модель механізму протидії кібертероризму носить декілька авторитарну модель з імперативними методами контролю за діяльністю громадян в мережі інтернет.

По перше треба зазначити концептуальну різницю між західним підходом до мережі інтернет та Китайським, у той час як Западні системи розглядають мережу інтернет розважальну платформу Китай розглядає інтернет у першу чергу як інструмент, а саме платформу обміну важливою інформацією та розвивальним контентом, тому з самого початку вистроював механізми взаємодії цивільних осіб та мережі інтернет на принципах відкритості та офіційності.

По-друге значним превентивним заходом протидії кібертероризму є те що кожна фізична особа в Китайському сегменті немає анонімності що є важливим фактором впливаючим на кількість кіберзлочинів в мережі інтернет, це забезпечується спеціальним алгоритмом доступу громадян до мережі інтернет, а саме доступ до інтернету громадянин може здобути тільки підключившись до провайдеру за своїм реальним ім'ям а також може реєструватися на інтернет платформах також тільки за реальним ім'ям пройшовши перевірку с боку платформи.

Важливим механізмом протидії кібертероризму у КНР є фільтрування інформації в мережі інтернет через так званий Великий Китайський Фаервол. Блокування небезпечного контенту здійснюється декількома засобами а саме: Блокування зовнішніх ресурсів таких як соціальні мережі, медіа, новини які згідно з нормативними актами КНР є небезпечними. Також є нейромережі як здійснюють моніторинг ресурсів по ключовим словам та блокують контент який підпадає під блокувальні алгоритмі нейромережі, закріпляє такий превентивний механізм саме ручне блокування контенту в мережі працівниками Бюро громадського контролю.

З ціллю забезпечити інформаційну політику у КНР прийнята «Національна стратегія безпеки у кіберпросторі» яка визначається як запорука забезпечення політичної стабільності в країні. В цьому документі зазначено що необхідно захищати політичне, культурне та соціальне життя держави. Важливим є те що стратегія направлена не тільки на забезпечення кібербезпеки країни а й ще на захист інформаційного простору держави, тобто пріоритетним є не тільки безпека при праці з мережею інтернет а в цілому з інформаційним простором [1].

Інформаційна політика КНР забезпечується великим колом нормативних актів: У 2000 р. Всекитайськими зборами народних представників здійснили спробу визначити класифікацію правопорушень в інформаційній сфері та було опубліковано «Постанову ВЗНП із захисту інтернет-простору», де відокремили ті галузі, в яких можуть бути порушення а саме: економічна, освітня, сфера підтримки суспільної стабільності та захисту громадян, тобто держава спробувала створити класифікацію інформаційних загроз і розробити механізми щодо протидії кібертероризму.

У 2003 р. була опублікована «Постанова державної інформатизованої керівної групи з роботи в області зміцнення інформаційної безпеки». Текст документа закріплює за відповідальними особами необхідність робити діяльність щодо створення механізмів захисту інформаційної інфраструктури, моніторинг мережі інтернет на наявність можливих загроз для КНР, розроблення заходів для залучення кваліфікованих спеціалістів у галузі інформаційної безпеки, захисту комп'ютерних систем, що містить у собі секретну інформацію.

У 2006 р. була прийнята «Державна стратегія розвитку інформатизації на період з 2006 по 2020 р.» У цьому документі визначається пріоритетні напрямки у галузі інформаційної безпеки. Зокрема, передбачається на первинному етапі створити відповідні структури для регулювання діяльності в інформаційній сфері, тим самим роблячи кроки щодо зміцнення системи забезпечення технологічної та інформаційної безпеки. Передбачається встановлення напрямів розвитку інформатизації, визначаються базові вектори державної політики у цій галузі. Також стратегія дотримується установки поєднання військової та цивільної продукції, передбачається створення власного програмного забезпечення. Іноземні компанії та програмне забезпечення повинні проходити обов'язкову сертифікацію у державних служб для функціонування на території Китаю.

Всекитайськими зборами народних представників 7 листопада 2016 р. було ухвалено Закон КНР про кібербезпеку. Він став прецедентом у китайському законодавстві: відповідно до нього офіційний Пекін має право на законодавчому рівні контролювати події, що відбуваються в китайському сегменті Інтернету. Тепер публікований контент повинен буде зберігатися на території Китаю не менше шести місяців. Це стосується соціальних мереж, відео- та письмового блогінгу. У законі дуже велика увага приділяється системі ідентифікації користувачів: для реєстрації та проведення будь-яких операцій у мережі Інтернет буде необхідно вказати реальні дані користувачів. Якщо раніше подібна практика мала місце на окремих технологічних підприємствах, то тепер вона поширилася на всю територію країни.

Китай, як передбачає його недавня політика, вживає заходів. войовничий підхід до обох аспектів, що підкреслює державно-орієнтований та всеосяжний контроль над онлайн-інформацією, з одного боку, та націоналістичну промислову політику у технологічному секторі, з іншого [2].

Таким чином ми можемо прийти до висновку що КНР зосереджує діяльність щодо захисту інформаційного простору як систему запобіжних та превентивних заходів спрямованих на контроль внутрішніх інформаційних систем та перешкоджання здійснення кіберправопорушень цивільними особами та корпораціями. Китайська система протидії кіберзагрозам є цікавою з точки зору запозичення законодавства у інформаційній сфері але треба відрізняти законні механізми протидії злочинності та авторитарні та імперативні методи які можуть зачіпати свободу слова.

Як зазначає Hauke Johannes Gierow закордонні компанії в Китаї повинні дотримуватися все більш суворих правил в IT-секторі, перешкоджаючи їх здатності захищати конфіденційну інформацію та перешкоджають міжнародному співробітництву [3].

При подальшій розробці нашого законодавства треба врахувати досвіт КНР, а саме їх механізми протидії кібертероризму але треба зауважити що ці механізми повинні не перешкоджати свободі слова та не створювати перешкоди у діяльності іноземних кампаній.

Список використаних джерел:

1. Heinl C. H. New Trends in Chinese Foreign Policy: The Evolving Role of Cyber // Asian Security. 2017. Vol. 13. Iss. 2. P. 132–147. DOI: 10.1080/14799855.2017.1286160
2. Samson Y. Becoming a Cyber Power: China's cybersecurity upgrade and its consequences // China Perspectives 2015 // Hong Kong Baptist University DOI:10.4000/chinaperspectives.6731
3. Hauke J. G. Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses Cyber sovereignty, intensified internet censorship, shadow IT economy // China Monitor 2015.

Ключові слова: кібербезпека, інформаційна безпека, кіберзлочинність.
Key words: cybersecurity, information security, cybercrime.