РОЛЬ APCERT В ЗАБЕЗПЕЧЕННІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРОВІДНИХ КРАЇН АЗІЇ

Тиртова Тетяна Павлівна,
студентка 2-го курсу магістратури
факультету міжнародних економічних відносин та туристичного бізнесу,
Харківський національний університет імені В. Н. Каразіна
tanyatirtova1661@gmail.com

На сучасному етапі невід'ємною частиною соціально-економічних змін не тільки країни, а й світу в цілому є динамічний розвиток інформаційно-комунікаційних технологій і, як наслідок, формування нового типу суспільства – інформаційного. Незважаючи на те, що інформаційне суспільство є визначальним фактором життя сучасної людини, слід звернути увагу й на негативний аспект повсюдного поширення інформатизації та комп'ютеризації. Загрози, які несе за собою такий тип суспільства, найчастіше проявляються в кіберпросторі. Тому міжнародні актори змушені переглянути звичну для них категорію «безпеки» відповідно до сучасних реалій. Тепер під «безпекою» слід розуміти не тільки безпеку на суші, у воді та у повітрі, а й безпеку в інформаційному (кібер-) просторі.

На сьогодні, провідним регіоном в забезпеченні інформаційної безпеки в світі вважають Євро-Атлантичний регіон. Однак Азія останні десятиліття проявляє значне економічне зростання, політичні трансформації та соціальні зміни, що говорить про формування ще одного центру сили на арені сучасних міжнародних відносин. Тому не дивно, що значення рівня забезпечення інформаційної безпеки як інструменту вираження своєї політичної та соціальної позиції в Азіатських країнах надзвичайно велике.

Азіатський регіон активно бере участь в діалозі з питань забезпечення інформаційної безпеки. Так, більшість урядів держав Азіатського регіону ставлять пріоритетним завданням своєї політичної діяльності проблему інформаційної безпеки та протидії кіберзлочинам. У багатьох країнах регіону відбулися докорінні зміни в рамках політики по відношенню до інформаційного

(кібер-) простору. Так, наприклад, Японія, Індія та Сінгапур повністю оновили або запустили нову політику щодо забезпечення кібербезпеки; Камбоджа почала розробку нового законодавства, що обмежує кіберзлочинність [6, с. 21]. Однак, в регіоні є країни, в яких інформаційній безпеці поки не приділяється належної уваги: М'янма, Філіппіні, Таїланд. Однією з причин цього є недостатній економічний розвиток кожної з країн. [1, с. 18].

Крім внутрішньодержавних змін у сфері інформаційної безпеки не можна залишити поза увагою той факт, що Азіатський регіон також характеризується створенням окремої установи – Asia-Pacific Computer Emergency Response Team (APCERT) – спеціальної групи реагування на надзвичайні ситуації в інформаційному комп'ютерному просторі в Азіатсько-Тихоокеанському регіоні (далі по тексту – АТР), визначення ролі якої у забезпеченні інформаційної безпеки провідних країн Азії і становить мету даної роботи.

Слід зазначити, що APCERT є частиною глобальної системи CERT (Computer Emergency Response Team – Комп'ютерна група реагування на надзвичайні ситуації), осередки якої розташовані по всьому світу. Так, CERT – це загальна назва для групи дослідників, інженерів-програмістів, аналітиків безпеки і фахівців з цифрової розвідки, які працюють разом над дослідженням вразливостей безпеки в програмних продуктах, вносять вклад в довгострокові зміни в мережевих системах, а також навчають інші команди. На сьогодні, CERT широко визнана авторитетною, що заслуговує на довіру, організацією, яка регулярно співпрацює з урядами, промисловістю та науковими колами для розробки передових методів та технологій для протидії масштабним і складним кіберзагрозам [3]. В АТР представлені як центри CERT більшості країн окремо, так і APCERT.

APCERT була заснована в лютому 2003 року з метою заохочення і підтримки діяльності CERT в регіоні. Вона підтримує мережу експертів з кібербезпеки в АТР для підвищення обізнаності регіону про зловмисну кіберактивність та його здатності виявляти та запобігати таким діям за допомогою розширення регіонального та міжнародного співробітництва в

області кібербезпеки; спільної розробки заходів з боротьби з кіберінцидентів; сприяння обміну інформацією, технологіями, дослідженнями та розробками з кібербезпеки серед своїх членів; надання правової допомоги, а також надання допомоги іншим CERT у регіоні в проведенні ефективного і дієвого комп'ютерного реагування на надзвичайні ситуації [4, с. 6–7].

Діяльність APCERT спрямована на створення «чистого, безпечного і надійного» кіберпростору, на налагодження ефективної комунікації з питань кібербезпеки та кіберзагроз у регіоні.

Організаційна структура APCERT використовує систему «контактних точок» (point-of-contact, POC), за якою кожна країна-член організації делегує свого представника, який є POC в разі кризової ситуації. Робиться це для того, щоб прискорити комунікації та скоротити час реакції на інцидент [2].

Для розбудови глобального співробітництва APCERT координує діяльність з іншими регіональними та глобальними організаціями, такими як:

• Азіатсько-Тихоокеанський мережевий інформаційний центр (APNIC) – APCERT та APNIC підписали Меморандум про взаєморозуміння у 2015 році;

• Форум груп реагування на інциденти та безпеку (FIRST) – Койчіро Коміяма з JPCERT / CC (команда з питань реагування на комп'ютерні надзвичайні події Японії) займав посаду члена Ради директорів FIRST з червня 2014 по червень 2018 року;

• DotAsia (Гонконгська неприбуткова організація, мета якої сприяти розвитку та впровадженню Інтернету в Азії) – APCERT виступає членом Консультативної ради DotAsia для надання допомоги у розробці політики та відповідних громадських проектах. HKCERT (Гонконгська група з питань реагування на комп'ютерні надзвичайні події) представляє APCERT під час відвідування засідань Консультативної ради;

• STOP. THINK. CONNECT program (STC) – APCERT співпрацює із STC в рамках Меморандуму про взаєморозуміння з червня 2012 року з метою сприяння обізнаності щодо кібербезпеки та більш безпечного мережевого середовища [4, с. 16].

Співпраця з такими організаціями як STC, APNIC та FIRST, дозволяє APCERT більш точно та своєчасно впроваджувати необхідні міри з забезпечення інформаційної безпеки всередині регіону, що робить Інтернет більш безпечним для його громадян.

На даний момент в APCERT входить 30 команд / 21 економіка – Австралія, Бангладеш, Бруней, Бутан, В'єтнам, Гонконг, Індія, Індонезія, Китай, Корея, Лаос, Макао, Малайзія, Монголія, М'янма, Нова Зеландія, Сінгапур, Таїланд, Тайвань, Шрі-Ланка, Японія. Всі вони є чинними членами APCERT. Однак регламентом даної організації передбачена ще одна форма членства – через надання підтримки організації. До них відносяться організації, які можуть надати технічну підтримку APCERT та функціонування осередків CSIRT / CERT. На сьогодні 4 великі корпорації підтримують організацію – Корпорація Bkav, компанії Dell SecureWorks, Microsoft Corporation, Panasonic PSIRT [5].

В цілому, APCERT є важливою складовою в діяльності щодо забезпечення інформаційної безпеки регіону, причому не тільки забезпечення конфіденційності, цілісності та доступності інформації, але й захисту систем, мереж і програмних додатків від цифрових атак в кіберсередовищі. Що робить APCERT так само важливою складовою забезпечення кібербезпеки регіону. Координуючи діяльність локальних CERT, APCERT можна вважати мало чи не єдиним інститутом на міждержавному рівні, який би займався питаннями забезпечення інформаційної безпеки в регіоні. APCERT працює над створенням безпечного, чистого та надійного кіберпростіру в АТР. Такого простору, яке було б не тільки комфортним для жителів регіону і жодним чином не обмежувало їх можливість користуватися Інтернетом, але так само і таким, яке б нічим не відрізнялося за рівнем надійності і безпеки від Євро-Атлантичного кіберпростору.

Список використаних джерел:

1. Гроссман Е. О. Проблема информационной безопасности и кибертерроризма в странах Азии. Санкт-Петербург: СПбГУ, 2016. 79 с.

2. Хатауэй М. Индекс киберготовности 2.0. *Digital.Report*. 01.04.2016. URL: https://digital.report/indeks-kibergotovnosti-2-0-chast-1/ (дата обращения: 27.09.2019).

3. Pethia R. About the SEI. *Carnegie Mellon University*. URL: https://www.sei.cmu.edu/about/leadership/display.cfm?customel_datapageid_2623=3545 (Last Accessed: 27.09.2019).

4. APCERT Annual Report 2018. Shanghai: APCERT, 2018. 260 p.

5. Member Teams. *APCERT*. URL: https://www.apcert.org/about/structure/members.html (Last Accessed: 27.09.2019).

6. Cyber Maturity in Asia-Pacific Region 2014. Sidney: Australian Strategic Policy Institute, 2014. 76 p.

Науковий керівник: ***Доценко Олена Михайлівна***, доцент кафедри міжнародних відносин, міжнародної інформації та безпеки Харківського національного університету імені В. Н. Каразіна, канд. юрид. наук.