УДК 351.865

Ганна Володимирівна ФОРОС,
кандидат юридичних наук, доцент,
професор кафедри кібербезпеки та інформаційного забезпечення
Одеського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0001-6377-3287;
Віктор Сергійович ЖОГОВ,
ад'юнкт кафедри кібербезпеки та інформаційного забезпечення
Одеського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0001-6069-839X

ШЛЯХИ ВДОСКОНАЛЕННЯ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА У ГАЛУЗІ КІБЕРБЕЗПЕКИ

Причини розширення напрямків міжнародного співробітництва у галузі кібернетичної безпеки лежать на поверхні. Настає епоха, в якій кібербезпека стане глобальним завданням. Такі країни світу, як США, Німеччина, Великобританія, Ізраїль, Іран, КНДР, КНР, Нідерланди та Південна Корея вже провели тренування з підготовки до кібервоєн, а за інформацією з інших джерел таких країн вже більше 120. Настав час, коли не тільки хакери, а й деякі держави використовують кібертехнології для втручання в справи інших країн. І це не просто напади - це спроби знайти вразливі місця.

Без розширення міжнародного співробітництва в сфері кібербезпеки навряд чи можна робити прогнози про готовність будь-якої з країн до такого розвороту подій. Стрімкий розвиток робототехніки і впровадження чіпів в людські тіла, безпілотний транспорт і розумні будинки, електронне управління інфраструктурою міст і виробничими об'єктами, блокчейн-технології, електронна економіка - з кожним роком наше життя все глибше занурюється в інформаційну сферу, надаючи хакерам все більше можливостей.

Основним міжнародним документом, який регулює дану сферу є Конвенція про кіберзлочинність від 23 листопада 2001 р., підготовлена в контексті Ради Європи. Цим документом також визначено, що попередження та протидія кіберзлочинності є обов'язком усіх держав і вони повинні взаємодіяти між собою у цій сфері. Про важливість налагодження міжнародного співробітництва говорить й те, що серед основних своїх цілей в Конвенції зазначається активізація та розширення механізмів міжнародної співпраці у галузі кібербезпеки, впровадження механізмів правової допомоги у кримінальних провадженнях, що пов'язані з кіберзлочинністю; формування міжнародної системи органів для боротьби з кібератаками; надання допомоги державам світу у подоланні цих явищ та ін.

Здійснене нами дослідження нормативної і теоретичної бази, а також матеріалів практики міжнародної взаємодії у галузі кібербезпеки свідчить, що до обставин, які ускладнюють зусилля Ради Європи, Інтерполу та інших організацій по боротьбі з

кіберзлочинністю та укріплення поліцейської взаємодії, варто відносити як об'єктивні, так і суб'єктивні чинники. Зокрема, до об'єктивних причин необхідно віднести: прагнення держав, які намагаються включитися до системи міжнародного співробітництва задовольнити, в першу чергу, власні інтереси за рахунок цих міжнародних структур; ідеологічні розходження багатьох країн, що проявляється насамперед у відмінностях політичних режимів, існуючих у різних країнах; значні відмінності у кадровому, матеріально-технічному та іншому забезпеченні національних поліцейських систем; протистояння домінуючих світових політичних систем, що загострилося після 2014 року.

Суб'єктивні чинники стосуються: зіткнення принципів національного суверенітету та принципів екстрадиції злочинців; побоювання витоку оперативної інформації, що пов'язане з загрозою успіху проведення відповідних операцій; відсутність зацікавленості деяких країн у співробітництві, що проявляється у зайнятті позиції очікування щодо співробітництва.

Подолання вказаних та деяких інших негативних чинників, можливо як за рахунок удосконалення концептуальних засад такої взаємодії, так і шляхом започаткування конкретних практичних заходів, а саме:

– взаємообмін розвідувальними даними про можливі кіберзагрози. В Інтернеті є велика кількість інформації, яка може бути структурована, а деяка – ні. Це має вирішальне значення для визначення майбутніх кібератак та намірів проводити потенційні напади. Необхідно створити умови щодо обміну інструментами та джерелами, які містять розвідувальні звіти, що відповідають потребам основних інформаційних вимог сьогодення;

– центр кібероповіщення, що включає в себе найсучасніші можливості для моніторингу та аналізу подій на організаційних, галузевих та національних рівнях. На нашу думку, створення центрів, які б були оснащенні алгоритмами, що ідентифікують атаки шляхом моніторингу кінцевих точок, серверів, елементів мережі та повідомлених подій, та їх співпраця дозволили б накопичувати моніторингову інформацію та вихідні дані зібрані міжнародним співтовариством за допомогою штучного інтелекту для виявлення та відбиття складних кібератак;

– організація підготовки та навчання співробітників для центру кібероповіщення;

– створення міжнародної лабораторії кібердосліджень, до якої були б залучені провідні фахівці світу для розслідування та дослідження минулих кібератак, проведення відповідного аналізу та визначення відповідних контрзаходів в майбутньому;

– організація роботи аналітичних служб кібербезпеки для моніторингу країн та організацій, які не мають задовільної кіберінфраструктури.

Міжнародну кібербезпеку необхідно будувати на загальних для усіх держав-учасників принципах з метою її оптимізації. Проведений нами аналіз документів та деяких наукових публікацій дозволяє до специфічних принципів міжнародно-правової взаємодії віднести такі: добросовісне виконання зобов'язань у міжнародному праві; невтручання у внутрішні справи інших держав; повага прав людини та неухильне дотримання міжнародних стандартів щодо них; невідворотність покарання; захист прав своїх громадян за кордоном; укріплення довіри між органами, які беруть участь у взаємодії; рівноправність сторін.

Підсумовуючи вищевикладене, з метою вдосконалення міжнародного співробітництва України з іншими державами у галузі кібербезпеки, вважаємо за необхідне: 1) створити єдине правове поле для забезпечення кібербезпеки; 2) постійно здійснювати аналіз перспектив розвитку міжнародного і національного законодавства у сфері кібербезпеки; 3) удосконалити системи обміну інформацією між спеціалізованими органами європейських країн; 4) розробити Концепцію взаємодії держав-учасників ЄС, кандидатів до ЄС та третіх країн щодо вдосконалення кібербезпеки; 5) збільшити кількість представництв Національної поліції, СБУ, Генеральної прокуратури в державах, які є стратегічним партнерами України; 6) визначитися з порядком обміну оперативною інформацією, втому числі й такою, що має обмежений доступ; 7) визначитися з можливістю спрощення порядку перетинання кордонів держав-учасниць міжнародних угод співробітниками компетентних органів у службових справах; 8) збільшити кількість працівників правоохоронних органів України, які б відвідали інші держави для обміну досвідом у галузі кібербезпеки, навчання або стажування; 9) удосконалити навчальні програми та плани підготовки працівників правоохоронних органів з метою навчання фахівців формам, методам та прийомам міжнародної взаємодії у галузі кібербезпеки.

Список бібліографічних посилань

1. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : указ Президента України від 15.03.2016 № 96/2016 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 02.11.2018).

2. Конвенція про кіберзлочинність : від 23.11.2001 ратифікована із застереженнями і заявами Законом від 07.09.2005 № 2824-IV // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 02.11.2018).

3. Bar-Chaim O., Edry C. International Collaboration // Cyber Security Review URL: http://www.cybersecurity-review.com/industry-perspective/international-collaboration/ (дата звернення: 02.11.2018).

4. Tara LaCapra L. Wall Street banks learn how to survive in staged cyber attack // Reuters. October 21, 2013. URL: https://www.reuters.com/article/net-us-usa-banks-cyberattack-drill/wall-street-banks-learn-how-to-survive-in-staged-cyber-attack-idUSBRE99K06O20131021 (дата звернення: 02.11.2018).

Одержано 05.11.2018