Макаренко Є.А.*

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: РЕГІОНАЛЬНИЙ КОНТЕКСТ

У статті проаналізовано стратегії регіональних міжнародних організацій у сфері інформаційної безпеки, розглянуто спільні і відмінні чинники їх діяльності, визначено перспективи забезпечення інформаційної та кібербезпеки регіональних спільнот з різним рівнем інформаційного розвитку.

Ключові слова: глобалізація, інформаційна безпека, регіональні організації, кібербезпека, європейська інтеграція, посткризовий світ, інтелектуалізація суспільства.

В статье проанализированы стратегии региональных международных организаций в сфере информационной безопасности, общие и отличительные факторы их деятельности, определены перспективы обеспечения информационной и кибербезопасности региональных сообществ с разным уровнем информационного развития.

Ключевые слова: глобализация, информационная безопасность, региональные организации, кибербезопасность, европейская интеграция, посткризисный мир, интеллектуализация общества.

The article is devoted to the analysis of regional and international organizations strategies in the field of information security, common and distinguishing factors of their activities, identified the prospects of information and cyber security of regional communities with different levels of information development.

Keywords: globalization, information security, regional organizations, cyber security, European integration, post-crisis world, intellectualization of society.

Початок XXI століття ознаменувався проявами системної кризи міжнародної безпеки щодо викликів і загроз, які були зумовлені розвитком глобального інформаційного суспільства і які призвели до переосмислення концептуальних і практичних засад міжнародного співробітництва у сфері інформаційної безпеки, з'ясування взаємовпливу глобального розвитку та міжнародної інформаційної безпеки, до диференціації пріоритетів світової, регіональної і національної політики у контексті протидії новим загрозам.. Розробка стратегій міжнародного співробітництва у сфері інформаційної безпеки свідчить про зміну політичних позицій провідних акторів міжнародних відносин, трансформацію пріоритетів забезпечення інформаційної безпеки регіональному рівні [1-2].

Регіональне співробітництво у сфері інформаційної безпеки зумовлює необхідність пошуку спільних рішень у межах регіональних організацій щодо протидії інформаційним та кіберзагрозам, вироблення спільної стратегії інформаційної безпеки для протидії

* доктор політичних наук, професор, провідний науковий співробітник Інституту світової економіки і міжнародних відносин НАН України

кібервійнам, інформаційному тероризму та інформаційній злочинності. Так, Організація Американських Держав сприйняла ініціативу США щодо ідеології глобальної культури кібербезпеки, протидії тероризму, зокрема, інформаційному, ухвалила резолюцію «Розробка міжамериканської стратегії щодо боротьби з загрозами для кібербезпеки», якою визнала, що інформаційні загрози потребують координації діяльності державного і приватного секторів, тобто впровадження основного принципу культури кібербезпеки. Держави-члени ОАД заявили про свій намір виконувати стратегію кібербезпеки, яка має бути спрямована на попередження й знешкодження кібератак, боротьбу з кіберзагрозами і кіберзлочинністю, захист критично важливих інфраструктур і мережевих систем.

Підсумком цієї стратегії було створення Міжамериканської мережі груп реагування на надзвичайні ситуації в комп'ютерній сфері, визначення і ухвалення єдиних стандартів галузі, модернізація нормативно-правової бази щодо боротьби з кіберзлочинністю, зокрема, приєднання до Європейської конвенції про кіберзлочинність як модельного інструменту у боротьбі з кіберзлочинами у межах асоціації. Сучасна стратегія інформаційної безпеки ОАД пов'язана з концепціями інформаційного протиборства президента США Б.Обами та пріоритетами діяльності американського уряду у форматі «інформаційної парадигми». Саме інформаційні переваги держави, на думку експертів з питань міжнародної і національної безпеки адміністрації Б.Обами, спроможні зберегти досягнуту у попередній докризовий період стабільність та забезпечити посткризовий розвиток, зробити більш прогнозованим перебіг соціальних конфліктів, запобігти руйнації суспільства.

Відповідно, співпраця ОАД і США позначена виразним поворотом до мілітаризації інформаційної сфери, яка означає більш тісну координацію політичних і силових структур з «кібербезпеки», а також визначенням військових й невійськових аспектів психологічних та інформаційних операцій. У забезпеченні регіональної безпеки і США, і ОАД готові на далекосяжні ідеологічні компроміси з Росією та Китаєм аж до згоди на закріплення за цими та іншими потужними державними чи наддержавними утвореннями «сфер відповідальності» для підтримання регіональної безпеки й стабільності. Така політика супроводжується активним використанням високих технологій подвійного призначення, які дозволяють конфіденційно створювати й використовувати «інформаційні озброєння» під прикриттям реалізації загальних науково-дослідних програм, коли йдеться не лише про заходи превентивно-оборонного характеру, але й про наступальні «інформаційні озброєння», здатні забезпечувати переваги у кризових ситуаціях та регіональних конфліктах. Принциповою новизною ініціативи інформаційної безпеки у північноамериканському регіоні можна вважати залучення до програм обороноздатності військових структур, хоча до 2008 року питання інформаційної безпеки розглядалися як суто технічні завдання для цивільних фахівців, а упродовж останніх двадцяти років вони були віднесені до компетенції інституцій з стандартів та технологій.

До характерних рис «інформаційних озброєнь» експерти відносять їх універсальність, транскордонність, відносну дешевизну й доступність, що уможливлює використання таких озброєнь не тільки організованими військовими формуваннями, але й злочинними та терористичними організаціями. «Інформаційні озброєння» за своєю природою є асиметричними, їх легко замаскувати під інші види деструктивних інформаційних впливів, а реальне джерело й приналежність цих озброєнь можуть бути конфіденційно прихованими в кіберпросторі. Агресія може здійснюватися латентно з території третіх країн, які не будуть простежувати інформаційні операції, а нарощування воєнно-інформаційного потенціалу можна видати за «наслідки науково-технічного прогресу». Як вважає директор Національної розвідки США Д.Блер, головними суб'єктами атак на американські ін-

формаційні системи є Росія й Китай, на другому місці – структури організованої злочинності, метою яких є виведення інформаційних систем з ладу або істотне уповільнення їх роботи, щоб створити перешкоди для протидії кібератакам, зокрема, правоохоронними органами США. У відповідь на подібні агресивні дії американці запропонували тактику зменшення кількості порталів, які сполучають урядові сервери з Інтернетом, хоча тенденції до скорочення «точок доступу» до федеральної урядової інформаційної мережі в інтересах інформаційної безпеки не є чимось принципово новим, оскільки така політика проводилася протягом останніх років і також має свої негативні прояви, тобто звужує можливості електронного урядування та оперативного реагування на потреби суспільства.

Поширення інформаційних озброєнь як зброї масового ураження, прагнення екстремістських та терористичних груп одержати до неї доступ, інформаційна революція у військовій справі, заснована на високих технологіях, висока уразливість сучасних суспільств до медіа-впливів у своїй сукупності та у поєднанні з викликами глобальної кризи вимагають від держав ОАД, щоб вони повною мірою скористалась можливостями застосування «інформаційних озброєнь» врахували у національних стратегіях інформаційної безпеки. Водночас, враховуючи різновекторність інформаційних загроз, Пентагон пропонує державам ОАД істотно збільшити витрати на «психологічні операції» та «зв'язки з громадськістю» з метою просування регіональних і національних інтересів у міжнародному співтоваристві, тобто йдеться про психологічну обробку світової спільноти з дотриманням вимог конфіденційності «цільових зарубіжних аудиторій». Зокрема, військове командування США встановило для збройних сил новий польовий статут з проведення інформаційних операцій, де вказується на умови їх ефективного поєднання з традиційними видами озброєнь, оскільки дослідження зарубіжних аудиторій для потенційного інформаційно-психологічного впливу вважається необхідною передумовою ефективних стратегічних комунікацій. З цією метою при Бібліотеці Конгресу США створено центральний депозитарій документів щодо громадської думки про США та їх політику у різних країнах світу, в якому зібрано матеріали, отримані як державними, так і недержавними дослідницькими структурами. Інформація з цього депозитарію доступна для фахівців з проблем кібер-, медіа- та психотероризму, зокрема, для дослідників «Контртерористичного комунікативного центру», з метою моніторингу теорії і практики інформаційно-психологічних впливів у сучасному світі Відтак, радники Б.Обами рекомендують об'єднати зусилля держав-членів ОАД для створення ефективної регіональної системи протиборства з інформаційними загрозами і, зокрема, з інформаційним тероризмом.

Подібна тенденція до мілітаризації інформаційної безпеки характерна й для інших розвинених країн світу, зокрема, Федеративна Німеччина створила спеціальний армійський підрозділ для ведення кібервійн у зв'язку з електронними атаками на бюро канцлера А.Меркель і ключових міністерств країни, завданням якого є виявлення й знищення ворожих зарубіжних комп'ютерних мереж, а також попередження кібератак та маніпулювання ними в інформаційному просторі держави. Ідейні підходи нового президента США щодо «інформаційних озброєнь» істотно зближує позиції Америки й Росії, яка з 1998 року постійно ставить в Першому комітеті Генеральної Асамблеї ООН (займається проблемами нерозповсюдження зброї масового ураження) питання щодо «інформаційної зброї» як зброї масового ураження, наражаючись на вето США та їх союзників, які відмовлялися визнавати реальність існування «інформаційних озброєнь» [3-8].

Для європейських регіональних організацій діяльність у сфері спільної політики безпеки, зокрема й інформаційної, спрямована на інтеграцію європейського інформаційного

простору, розвиток інформаційного суспільства, створення європейських правових норм у галузі комунікації, забезпечення свободи слова та обміну інформацією, функціонування засобів масової комунікації на основі новітніх технологій, оскільки в умовах становлення інформаційного суспільства регіональні організації захищають стандарти Європейської Конвенції з прав людини, соціальні пріоритети європейського суспільства, плюралістичні принципи ЗМК, європейський зміст електронної демократії тощо. Так, питання формулювання теоретичного поняття «кіберзлочинності» у тексті Європейської Конвенції з кіберзлочинності стало найбільш дискусійним, оскільки фахівці у галузі кримінального права Ради Європи при розробці багатьох рекомендацій щодо протидії комп'ютерним злочинам обмежилися лише переліком таких посягань, який охоплює: кіберзлочинність у вузькому сенсі («комп'ютерний злочин») – будь-яке протиправне діяння, що здійснюється шляхом електронних операцій, метою якого є подолання захисту комп'ютерних систем та оброблюваних ними даних: несанкціонований доступ, пошкодження комп'ютерних даних або комп'ютерних програм, комп'ютерний саботаж, несанкціоноване перехоплення, комп'ютерне шпигунство, шахрайство, фальсифікація; кіберзлочинність у широкому сенсі («злочин, пов'язаний з використанням комп'ютерів») – будь-яке протиправне діяння, що здійснюється шляхом або у зв'язку з комп'ютерною системою чи мережею, включаючи такі злочини, як незаконне збереження або поширення інформації через комп'ютерну систему або мережу. Основна мета Конвенції - розширення повноважень урядів при розслідуванні звичайних злочинів, при вчиненні яких був задіяний обмін інформацією чи передача сигналу через комп'ютерну мережу. На сьогодні, крім європейських держав, Конвенцію підписали також Канада, Японія та США, які брали активну участь у підготовці її тексту, які багато в чому пов'язують продовження міжнародного співробітництва в галузі міжнародної інформаційної безпеки з виконанням положень Конвенції.

Враховуючи нові підходи провідних держав світу до проблеми інформаційної безпеки, Рада Європи акцентувала свою діяльність на проблемах боротьби з використанням Інтернету в терористичних цілях та захисту Інтернету і основних інфраструктур від кібератак з боку терористичних угруповань. Зокрема, у політичних дискусіях на спільній конференції РЄ та ОАД «Тероризм та кібербезпека» (Іспанія, 2009 р.) було обговорено програми міжнародного співробітництва щодо протидії використанню Інтернет в терористичних цілях, визначено механізми моніторингу ризиків кібератак з боку терористичних організацій, проаналізовано наявні міжнародно-правові документи щодо протидії терористичній діяльності з використанням Інтернет та запропоновано інструментарій розробки нових стандартів для запобігання інформаційному тероризму. У підсумковому документі «Боротьба з тероризмом і свобода слова та інформації» Першої Міністерської конференції Ради Європи у справах ЗМІ і сучасних засобів комунікації (Ісландія, 2009) також було висловлено оцінку сучасних соціальних, культурних і технологічних змін, які впливають на підходи до принципів поширення інформації та обміну нею, оцінку професійної відповідальності сучасних засобів комунікації за дотримання на практиці стандартів регіональної організації у сфері свободи слова та інформації в контексті боротьби з тероризмом, оскільки «Європа і все міжнародне співтовариство переживають небезпечні кризові нестабільні часи, проте забезпечення прав людини, свободи слова і демократії залишаються провідним напрямком діяльності організації, переважаючи будь-які політичні або економічні інтереси будь-яких злочинних чи терористичних угруповань».

Розширення ЄС спричинило нові лінії політичного, економічного та державного розподілу в європейському регіоні, зумовило виокремлення в стратегії євроінтеграції та структурі ЄС мети спільної зовнішньої та безпекової політики, створення і функціону-

вання департаменту зовнішньої політики і безпеки Європейського Союзу. Актуальність формування нової архітектури європейської безпеки зумовила суперечності як у підходах до визначення її мети і завдань, так і до впливу на регіональну політику безпеки, оскільки процеси європейської інтеграції супроводжуються також хвилею розширення НАТО і визначенням нових пріоритетів діяльності оборонної регіональної організації. Концепція спільної політики інформаційної безпеки зумовлює й пошук спільних рішень щодо протидії інформаційним та комунікаційним загрозам, визначає вироблення загальної стратегії європейської інформаційної безпеки, протидії кібервійнам, інформаційному тероризму та боротьби з інформаційною злочинністю.

План дій ЄС у сфері інформаційної безпеки стосується стратегічного аналізу і планування щодо протидії інформаційним загрозам у співробітництві з Радою Безпеки ООН; зміцнення стратегічного партнерства щодо протидії інформаційним загрозам з США, Росією, Японією, Китаєм, Канадою та Індією; вдосконалення регуляторної політики ЄС з інформаційної безпеки, зокрема, розробки і ухвалення конвенцій, директив, рекомендацій та резолюцій про європейську інформаційну безпеку та конфіденційність електронних комунікацій; визначення та оцінки інформаційних загроз для критично важливих сфер життєдіяльності європейського співтовариства; розробки засад європейської та національної політики інформаційної безпеки і зростання ролі ЄС у забезпеченні регіональної інформаційної безпеки. У сфері протидії кіберзлочинності ЄС ініціював проведення огляду існуючого законодавства європейських держав і підтримав розробку та прийняття Європейської Конвенції про кіберзлочинність та визнав її базовим документом, спрямованим на розвиток національного законодавства країн ЄС, прийняття відповідних норм матеріального і процесуального права, а також активізацію європейського права в цій галузі з метою захисту суспільства від кіберзлочинності. Так, у резолюції від 28 січня 2002 року «Про єдиний підхід і конкретні дії у галузі інформаційної безпеки» ЄС закликає держави-члени активізувати проведення освітніх програм з метою підвищення обізнаності про інформаційну безпеку, проводити обмін досвідом в галузі управління безпекою і зміцнювати діалог ЄС з іншими міжнародними організаціями в цій галузі. У резолюції підкреслюється важливість проведення активних наукових досліджень в таких сферах, як підвищення надійності мереж і зміцнення їх безпеки, криптографія, захист приватного життя. Результатом цієї роботи стало заснування Європейського агентства мережевої та інформаційної безпеки (ENISA, 2004), основна мета якого – сприяння розвиткові культури безпеки мереж та інформації в Європейському Союзі. Європейське агентство мережевої та інформаційної безпеки не виконує оперативних функцій; його роль полягає в тому, щоб виступати як центр компетенції для Європейської Комісії ЄС, держав-членів і ділового співтовариства, сприяти загальноєвропейському співробітництву, обмінові передовим досвідом, підвищувати поінформованість і здійснювати консультування з питань дослідницької програми Європейської Комісії в контексті осмислення ризиків і загроз, що з'являються.

Європейський Союз за планом дій з інформаційної безпеки бере участь у Форумі Груп реагування на надзвичайні ситуації в комп'ютерній галузі шляхом функціонування європейської цільової групи сприяння співробітництву між Групами реагування на надзвичайні ситуації в комп'ютерній галузі. Ще один напрямок роботи під егідою ЄС – стимулювання взаємного визнання сертифікатів, що видаються державами Європейського Союзу щодо апаратних і програмних засобів, а також засобів забезпечення інформаційної безпеки і захисту. У межах цієї діяльності було підписано Угоду про взаємне визнання державами, які її підписали, сертифікаційних атестатів, виданих національними сертифі-

каційними центрами, що підтверджують рівень захищеності інформаційних продуктів і технологій. Угоду підписали Велика Британія, Франція, Німеччина, США, Канада, Австралія, Нова Зеландія і Японія (країни, що видають сертифікаційні атестати), а також Австрія, Іспанія, Фінляндія, Греція, Угорщина, Ізраїль, Італія, Норвегія, Нідерланди, Швеція і Туреччина. По суті ці угоди є інструментом просування експорту апаратних і програмних технологій і продуктів у цілу низку держав ЄС, які визнають результати сертифікації без проведення додаткових національних атестацій. Водночас це дає змогу обмеженому колу держав контролювати і фактично визначати реальну інформаційну захищеність продуктів, що постачаються на європейський ринок та використовуються в інших європейських країнах. Відтак, взаємодія держав європейського регіону в процесі освоєння та застосування ІКТ (інформаційно-комунікаційних технологій) стала однією з найдинамічніших та багатообіцяючих сфер міжнародного співробітництва. У зв'язку з цим у доктрині зовнішньої політики ЄС з'являються нові положення, а в дипломатичній діяльності нові завдання, пов'язані з забезпеченням інформаційної безпеки в регіоні. Важливо враховувати й той факт, що вдосконалення інформаційних технологій сприяє не лише зміцненню суспільних зв'язків, а й веде до появи невідомих раніше джерел ризику та небезпеки. тому головною метою європейської політики інформаційної безпеки визначено захист інформації та інформаційних систем або мереж за допомогою відповідних технічних та законодавчих механізмів. Формування нової європейської системи безпеки здійснюється на підставі основних загальноприйнятих принципів, зокрема: чіткого усвідомлення важливості чинників, що впливають на стан національної безпеки, зокрема, політичних, економічних, військових, етнічних, екологічних, інформаційних та інші складових демократичних процесів, і формування взаємовигідних міждержавних відносин; необхідності створення механізмів колективного реагування на нові загрози, що набули трансконтинентального характеру(міжнародний тероризм, поширення зброї масового ураження і обігу наркотиків, організована злочинність тощо); визначення фундаментальних вимог до системи колективної європейської безпеки – неподільності безпеки та її всеохоплюючого і комплексного характеру [9-12].

Інформаційна безпека в діяльності регіональної організації АТЕС, яка є міжурядовим форумом Азіатсько-Тихоокеанського регіону, розглядається передусім в контексті економічного співробітництва з питань лібералізації торгівлі та інвестицій, оскільки АТЕС об'єднує 21 економіку АТР – Австралії, Брунея, В'єтнаму, Гонконгу (Китай), Індонезії, Канади, КНР, Республіки Корея, Малайзії, Мексики, Нової Зеландії, Папуа Нової Гвінеї, Перу, Росії, Сінгапуру, США, Таїланду, Тайваню, Філіппін, Чилі, Японії та стосується проблем захисту критично важливої інфраструктури від терористичних загроз. На саміті АТЕС в Шанхаї (2002 р.) було прийнято окрему Заяву з питань безпеки інформаційних і телекомунікаційних інфраструктур, в якій йшлося про необхідність боротьби зі злочинним використанням ІКТ, та Програму дій, відповідно до якої був розширений спектр діяльності АТЕС з питань зв'язку та інформації, зміцнення інформаційно-комунікаційної і мережевої безпеки. На зустрічі в Мексиці в 2002 році лідери АТЕС заявили, що в контексті зростання масштабів тероризму, в умовах наростаючої глобалізації і становлення цифрового суспільства, критично важливою для безпеки суспільства є система захисту інформаційної інфраструктури, включаючи телекомунікаційні мережі. Особливу увагу лідери АТЕС звернули на проблему кібертероризму, оскільки Інтернет став важливою основою для формування «нової економіки», заснованої на знаннях, розвитку електронної комерції, електронного уряду, соціального забезпечення потреб суспільства країн АТР на основі ІКТ. постійній підставі, розвивати культуру кібербезпеки. Учасники саміту під-

тримали розроблену Робочою групою з питань телекомунікацій та інформації Стратегію кібербезпеки регіону, яка зорієнтована на сприяння кібербезпеці шляхом прийняття всеохоплюючих матеріальних і процесуальних законів, створення системи обміну інформацією, заснування національних контактних пунктів у форматі «24/7» і організацій, аналогічних Групам реагування на надзвичайні ситуації в комп'ютерній галузі, виявлення найкращих стандартів і досвіду, навчання та підвищення обізнаності з інформаційної безпеки. Була проведена відповідна практична робота, внаслідок якої в рамках АТЕС був прийнятий Закон про кіберзлочинність, реалізований Проект Робочої групи АТЕС з питань зв'язку та інформації законодавчої ініціативи та нарощування правозастосовного потенціалу у сфері кібербезпеки. Була також розпочата ініціатива з заснування і координації Груп реагування на надзвичайні ситуації в комп'ютерній галузі у країнах регіону.

На саміті лідерів у Бангкоку (2003 р.) «Світ відмінностей: партнерство заради майбутнього» також було підкреслено важливість лібералізації торгівлі та інвестицій, забезпечення безпеки для побудови економіки знань. У «Декларації Бангкока», зокрема, йдеться про те, що для ефективного економічного розвитку країн АТЕС необхідно просувати всі ініціативи, включаючи ініціативу в сфері цифрової економіки, протидії піратству у сфері оптичних носіїв і розширенню технологічних можливостей для ділових кіл; активізувати зусилля по формуванню інформаційної економіки, підвищувати і покращувати координацію дій для протидії тероризму, сприяти програмам технічної взаємодопомоги і зусиллям з нарощування потенціалу, а також розвивати співпрацю між Спеціальною групою АТЕС й іншими міжнародними, регіональними та функціональними організаціями. Учасники саміту також ухвалили рішення про прискорення досягнення цілей в частині забезпечення ширшого доступу до мережі Інтернет, посилення захисту прав інтелектуальної власності і правозастосування в даній області, а також по здійсненню стратегії «Електронний АТЕС».

На зустрічі міністрів АТЕС з питань розвитку телекомунікації і інформаційної індустрії в Лімі (2005 р.) обговорювалися питання лібералізації ринку телекомунікацій, розширення масштабів використання широкосмугових мереж, розвитку електронного уряду і електронної комерції, активне застосування додатків на базі ІКТ. У підсумковій декларації підкреслювалася важлива роль державної політики в розвитку інформаційної інфраструктури, розширенні спектру інформаційних послуг, що надаються громадянам (електронне управління), створення сприятливого інвестиційного клімату для інвестицій в інформаційний сектор. Учасники зустрічі також обговорювали питання, пов'язані із зростанням масштабів кібертероризму і його наслідків для економічного і інформаційного розвитку регіону. У декларації підкреслено необхідність співпраці на політичному рівні між всіма державами-членами АТЕС з метою вироблення комплексної стратегії протидії інформаційним загрозам і розвитку регіональної системи інформаційної безпеки, а також удосконалення законодавств країн регіону відносно регулювання інформаційного сектора в контексті інформаційної безпеки, відповідно до міжнародних норм і принципів.

Безпекові імперативи регіональної оборонної організації АСЕАН також реалізується через стратегії інформаційної безпеки і боротьби з кібертероризмом. Так, за ініціативою АСЕАН (1994 р.) був утворений Регіональний форум з безпеки, який на сьогоднішній день є єдиним в АТР механізмом багатостороннього регіонального політичного діалогу з усього спектру питань, пов'язаних із підтриманням миру і стабільності. Його завданням є забезпечення шляхом діалогу і консультацій безконфліктного розвитку Південно-Східної Азії і всього Азіатсько-Тихоокеанського регіону через створення надійної системи інформаційної безпеки. Важливим напрямом діяльності Форуму є превентивні заходи

інформаційної безпеки, що зафіксовано в «Концепції і принципах превентивної дипломатії», а також співпраця з метою протистояння інформаційному тероризму [13-15].

Координація позицій держав-членів ШОС з міжнародної інформаційної безпеки стала якісно новим явищем практичної співпраці в рамках Євразійського регіону. У спеціальній заяві Ради Шанхайської Організації Співпраці (2006 р.), керівники Республіки Казахстан, Китайської Народної Республіки, Киргизької Республіки, Російської Федерації, Республіки Таджикистан і Республіки Узбекистан висловили занепокоєність щодо реальної небезпеки використання інформаційно-комунікаційних технологій з неправомірною метою, зокрема, для порушення безпеки людини, суспільства й держави, фундаментальних принципів суверенності, рівноправності і взаємоповаги, невтручання у внутрішні справи суверенних держав, мирного врегулювання конфліктів, незастосування сили, дотримання прав людини. У заяві підкреслювалося, що загрози використання ІКТ в злочинних, терористичних і військово-політичних цілях, несумісних із забезпеченням міжнародної безпеки, можуть реалізовуватися як в цивільній, так і у військовій сфері і призвести до тяжких політичних й соціально-економічних наслідків в окремих країнах, регіонах і в світі в цілому, до дестабілізації суспільного життя держав, можуть мати глобальні наслідки, катастрофічні за своїми характеристиками як «зброя масового ураження».

У документі підкреслено, що транснаціональний характер ІКТ, поява нових викликів і нестабільності диктує необхідність доповнення національних зусиль по забезпеченню інформаційної безпеки спільними діями на двосторонньому, регіональному і міжнародному рівні, оскільки лише координовані заходи держав зможуть дати адекватну відповідь загрозам безпеці в інформаційній сфері. У цьому контексті лідери держав-членів ШОС підтримали діяльність, яка здійснюється в рамках ООН щодо визнання потенційних загроз у сфері інформаційної безпеки і можливих спільних заходів протидії, а також розроблення відповідних міжнародних концепцій, спрямованих на зміцнення безпеки глобальних інформаційних і телекомунікаційних систем, і встановлення міжнародно-правових принципів і норм у сфері інформаційної безпеки.

Глави держав заявили про близькість позицій своїх країн з ключових проблем, пов'язаних з міжнародною інформаційною безпекою, і про наміри об'єднати зусилля в рамках ШОС з метою протидії новим інформаційним викликам і загрозам відповідно до принципів і норм міжнародного права, включаючи Статут ООН і Загальну декларацію прав людини. В зв'язку з цим було прийнято рішення про створення групи експертів держав-членів ШОС з міжнародної інформаційної безпеки за участю представників Секретаріату Організації і Виконкому Регіональної антитерористичної структури для вироблення плану дій і визначення можливих шляхів і засобів розв'язання в рамках ШОС проблеми міжнародної інформаційної безпеки у всіх її аспектах.

Відтак, у відповідь на ухвалене рішення, що містилося у Заяві глав держав-членів ШОС з міжнародної інформаційної безпеки (2006 р.), відбулося засідання Групи експертів держав-членів ШОС з міжнародної інформаційної безпеки, у якому взяли участь експерти всіх держав-членів ШОС. Під час засідання була офіційно утворена Група і узгоджені інституційні основи її роботи, а головою консенсусом був обраний експерт Російської Федерації як держави, що ініціювала розгляд в ШОС проблематики міжнародної інформаційної безпеки. Вироблений Групою План дій держав-членів ШОС щодо міжнародної інформаційної безпеки був схвалений Рішенням Ради міністрів закордонних справ держав-членів організації 9 липня 2007 року і затверджений Рішенням Ради глав держав-членів ШОС, яка відбулася 16 серпня 2007 року. Планом передбачається співпраця держав-членів ШОС в таких питаннях, як вироблення єдиного понятійного апарату щодо

сфери міжнародної інформаційної безпеки; здійснення аналізу загроз у сфері міжнародної інформаційної безпеки і вироблення пропозицій щодо протидії ним; вироблення пропозицій щодо створення практичних механізмів моніторингу загроз у сфері міжнародної інформаційної безпеки і координації дій із забезпечення міжнародної інформаційної безпеки в просторі ШОС; вивчення і адаптація національних законодавств у сфері забезпечення інформаційної безпеки; дослідження питання про міжнародно-правове регулювання і стан міжнародно-правової бази сфери міжнародної інформаційної безпеки; співпраця з питань інформаційної безпеки в рамках міжнародних організацій і форумів; розробка і здійснення заходів довіри між державами-членами ШОС у сфері забезпечення інформаційної безпеки; вивчення можливих шляхів надання взаємної допомоги щодо запобігання деструктивним інформаційним впливам і надзвичайним ситуаціям у сфері інформаційної безпеки, координація оперативного реагування на них і ліквідація їх наслідків. У розвиток ініціативи глав держав-членів ШОС відбувся круглий стіл «ШОС: клімат довіри та інформаційна безпека»(2009 р.), в якому взяли участь керівники структур організації, представники дипломатичного корпусу, експерти з питань інформаційної безпеки регіональної організації. Під час зустрічі обговорювалися особливості функціонування інформаційного простору ШОС, можливості країн регіону у сфері інформаційної безпеки, необхідність протидії використанню інформаційних технологій у злочинних, терористичних і ворожих військово-політичних цілях, оскільки інформаційна складова стала чутливим аспектом в діяльності кожної держави. Відтак зміцненню клімату довіри між країнами ШОС може сприяти саме інформаційна інтеграція й формування повноцінної системи міжнародної інформаційної безпеки. Учасники зустрічі також підтримали ідею щодо встановлення міжнародно-правового режиму у сфері інформаційної безпеки, оскільки використання інформаційних технологій та впливів у реальних збройних конфліктах набуло геополітичного характеру, зокрема, наводилися приклади здійснення спеціальних інформаційних операцій під час бойових дій на Балканах, Північному Кавказі, в Афганістані, Іраку тощо. Експерти відзначали, що локальні військові конфлікти з використанням інформаційних озброєнь безпосередньо безпеці ШОС не загрожують, проте наведені дані центру Східної Азії та Інституту Далекого Сходу говорять про те, що проблема інформаційних воєн в регіоні ШОС реально існує, зокрема, для створення як позитивних, так і негативних іміджів організації [16-19]. Таким чином, можна стверджувати, що в межах діяльності ШОС здійснюються ініціативи щодо ухвалення міжнародної концепції і міжнародної конвенції з інформаційної безпеки на регіональному та глобальному рівнях міжнародного співробітництва.

Регіональне об'єднання Співдружність Незалежних Держав з 1990-х років здійснює роботу щодо забезпечення, підтримки і зміцнення інформаційної безпеки. Так, виконавчими органами СНД було прийнято рішення(1996 р.), відповідно до якого було розроблено і затверджено Концепцію формування інформаційного простору СНД як основу співробітництва держав-учасниць СНД у сфері інформації та інформатизації, спрямовану на підвищення ефективності інформаційної взаємодії між державами-учасницями СНД та на здійснення узгодженої політики з урахуванням відповідних національних і спільних інтересів, включаючи інформаційну безпеку. Одним з першочергових напрямів діяльності країн СНД у цій сфері і одним із головних принципів формування інформаційного простору Співдружності планувалося забезпечення безпеки інформаційних і телекомунікаційних систем. Представники держав-учасниць СНД дійшли висновку про те, що основними загрозами інформаційній безпеці є, зокрема, зростання транснаціональної злочинності у сфері комп'ютерної інформації, можливість використання терористичними

та іншими екстремістськими організаціями й окремими особами мережі та технологій ІКТ для досягнення злочинних цілей, а також державами для вирішення військово-політичних завдань. Об'єктами загроз визнано права і свободи людини, інтереси суспільства, держави і Співдружності в інформаційній сфері. Відповідно, 1 червня 2001 року було підписано Угоду про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації, яка заклала правову базу для здійснення на просторі СНД взаємодії, спрямованої на протидію комп'ютерній злочинності. У ній наводиться перелік дій, які Сторони Угоди визнають відповідно до своїх національних законодавств кримінальними, визначаються форми співробітництва, а також конкретизуються механізми реалізації співробітництва в цих формах

Практичні заходи щодо реалізації співпраці планувалося здійснювати у формі взаємних консультацій, координації співпраці, кооперації в наукових дослідженнях, розробці і виробництві відповідних засобів захисту інформації, а також шляхом виконання державами заходів згідно з прийнятими на себе зобов'язаннями. Зокрема, планувалося забезпечити узгоджену розробку міждержавних договорів, національних нормативних правових актів і нормативно-методичних документів, які регламентують відносини і дії суб'єктів в інформаційній сфері; розробку правових механізмів недопущення в СНД протизаконних інформаційних впливів на свідомість особи і суспільства; активізацію діяльності компетентних правоохоронних органів держав-учасниць СНД з попередження і припинення правопорушень в інформаційній сфері; законодавче стимулювання розвитку інформаційної індустрії в державах-учасницях СНД і передусім виробництво засобів захисту інформації; співпрацю держав-учасниць СНД з підготовки кадрів в галузі забезпечення інформаційної безпеки.

Проте вищезазначені заходи не були реалізовані, і на сучасному етапі держави-учасниці СНД розглядають взаємодію у сфері інформаційної безпеки на основі двосторонніх міждержавних договорів, які стосуються обміну конфіденційною інформацією, законного перехоплення телекомунікацій, діяльності ЗМІ під час збройних конфліктів або здійснення терористичних актів тощо. Зокрема, в рамках діяльності Антитерористичного центру держав-учасниць СНД було представлено Концепцію інформаційної протидії тероризму і іншим насильницьким проявам екстремізму, яка уможливлює вдосконалення національних законодавств щодо боротьби з тероризмом в інформаційній сфері. У зв'язку з цим Антитерористичний центр має намір реалізувати комплекс заходів, спрямованих на створення єдиного правового поля у сфері інформаційної протидії тероризму.

У рамках реалізації Концепції 5 жовтня 2006 року в м. Баку (Азербайджанська Республіка) відбулося XXI засідання Ради керівників органів безпеки і спеціальних служб держав-учасниць Співдружності Незалежних Держав, присвячене обміну досвідом боротьби з кібертероризмом, на якому було визнано доцільною співпрацю в даній сфері здійснювати за такими напрямами, як обмін інформацією про ознаки і факти кібертероризму, про наміри і діяльність терористичних організацій у сфері інформаційно-телекомунікаційних технологій; обмін позитивним досвідом щодо захисту інформаційних систем об'єктів національної критичної інфраструктури; проведення аналізу національних законодавств щодо наявності в них відповідальності за діяння, що мають ознаки кібертероризму [20].

На засіданні також обговорювалися проблеми оперативного обміну інформацією між органами безпеки і спеціальними службами країн Співдружності при розслідуванні і документуванні злочинів у сфері інформаційних технологій, які здійснюються національними і міжнародними хакерськими об'єднаннями і пов'язані, зокрема, з несанкціонованим

доступом до державних інформаційних ресурсів та розповсюдженням в мережі Інтернет конфіденційних баз даних. Члени Ради керівників органів безпеки і спеціальних служб держав-учасниць Співдружності Незалежних Держав визнали необхідним ініціювати внесення змін до національних законодавств, спрямованих на встановлення кримінальної відповідальності за несанкціонований збут або розповсюдження інформації з обмеженим доступом, яка зберігається і обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на інших інформаційних носіях. Також розглядалася можливість створення контактних пунктів при оперативних підрозділах органів безпеки і спеціальних служб з протидії комп'ютерній злочинності з цілодобовим режимом роботи, до функцій яких буде віднесено організацію оперативного виконання звернень в рамках міжнародної взаємодії при розслідуванні комп'ютерних злочинів.

Таким чином, аналіз діяльності регіональних міжнародних організацій у сфері інформаційної безпеки з огляду на стан і загрози інформаційного характеру свідчить, що ефективність боротьби з цими явищами залежить не тільки від заходів, які здійснюються на рівні національних інституцій, правоохоронних органів, інших установ і організацій, на які покладено загальні завдання забезпечення інформаційної безпеки , але й від координації політики і співпраці держав на багатосторонній основі в кожному регіону світу.

Література

1. Mapping The Global Future. Report of the National Intelligence Council's 2020 Project. – http://www.dni.gov/nic/NIC_globaltrend2020.html
2. Столетов О.В. Тренды трансформации властных отношений в мировой политике: smart power? / О.В.Столетов // Полис. 2009. №4. С. 173-178.
3. Adoption of a comprehensive Inter-American strategy to combat threats to cybersecurity: a multidimensional and multidisciplinary approach to creating a culture of cybersecurity (2004) [Electronic resource]. – Access mode: http://www.oas.org/XXXIVGA/english/docs/approved_documents/adoption_strategy_combat_threats_cybersecurity.htm
4. Дэвис Т. Ответ терроризму должен быть международным. Доклад Генерального Секретаря Совета Европы на совместной конференции Совета Европы и Организации американских государств (Испания, 2009 р.) [Электронный ресурс] / Т.Дэвис. – Режим доступа: https://wcd.coe.int/ViewDoc.jsp?Ref=PR320(2009)&Language=lanRussian&Ver= original&Site=DC&BackColorInternet=F5CA75&BackColorIntranet=F5CA75&BackColorLogged=A9BACE.
5. The National Security Strategy of the United States of America [Електронний ресурс]. – Washington, DC: White House, 2010, May. – 52 p. - Режим доступу: www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf
6. Kagan R. The Need for Power [Електронний ресурс] / Kagan R.// The Wall Street Journal. - 2010. - Режим доступу: http://online.wsj.com/article/SB10001424052748703652104574652372456526440.html
7. Barack Obama's speech at the University of Purdue (July 16, 2008) [Електронний ресурс]. - Режим доступу: http://www.cfr.org/publication/ 16807/barack_obamas_speech_at_the_university_of_purdue.html.

8. Нова стратегія безпеки США в баченні Обами [Електронний ресурс] / Режим доступу: http://otherside.com.ua/news/ detail.php?lang=1&id=83241
9. Семенюк О. Нова архітектура європейської безпеки: тенденції, виклики, перспективи [Електронний ресурс] / Олександр Семенюк. - Режим доступу: http://cs.cirs.kiev.ua/uk/news/commentary/102-2010-01-20-15-13-26.html
10. Європейські комунікації: політичні, економічні, правові, безпекові, дипломатичні, суспільні та культурні аспекти: [кол. монографія] / [Макаренко Є.А., Ожеван М.А.. Рижков М.М. та ін.]. – К. : Центр вільної преси, 2007. – 535 с.
11. Internal security strategy for The European Union «Towards a European Security Model» [Електронний ресурс]. - Режим доступу: register.consilium.europa.eu/pdf/en/10/st05/st05842-re02.en10.pdf.
12. Міжнародна інформаційна безпека: сучасні виклики та загрози / [Макаренко Є.А., Гондюл В.П., Рижков М.М. та ін.]. – К.: Центр вільної преси, 2006. – 916 с.
13. APEC Leaders' statement on recent acts of terrorism in apec member economies (Los Cabos, Mexico, 2002) [Electronic resource]. – Access mode: http://www.apec.org/apec/leaders__declarations/ 2002/ statement_on_recent.htm
14. Bangkok Declaration on Partnership for the Future (Bangkok, 2003) [Electronic resource]. – Access mode: http://www.apec.org/apec/leaders__declarations/2003.html.
15. Lima Declaration. The Sixth APEC Ministerial Meeting on the Telecommunications and Information Industry (Lima, 2005) [Electronic resource]. – Access mode: http://www.apec-sec.com.sg/apec/ministerial_statements/sectoral_ministerial/telecomunications/2005.html
16. Заявление глав государств-членов ШОС по международной информационной безопасности (Шанхай, 2006) [Электронный ресурс]. – Режим доступа: http://www.sectsco.org/RU/show.asp?id=107.
17. Заявление глав государств-членов ШОС по международной информационной безопасности (Шанхай, 2006) [Электронный ресурс]. – Режим доступа: http://www.sectsco.org/RU/show.asp?id=107.
18. Бишкекская Декларация. Заседание Совета глав государств-членов ШОС (2007) [Электронный ресурс]. – Режим доступа: http://www.sectsco.org/RU/show.asp?id=111.
19. ШОС: Климат доверия и информационная безопасность. Материалы Круглого стола (2009) [Электронный ресурс]. – Режим доступа: http://www.fapmc.ru/ news/media/2009/05/item7627.html.
20. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 2001) // Содружество. Информационный вестник Совета глав государств и Совета глав правительств СНГ. – 2001. – № 1(37). – С. 138-149