УДК 341.1:354.42

Гіда Олександр Федорович –
головний науковий співробітник Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при Раді національної безпеки і оборони України, кандидат юридичних наук, доцент, Заслужений працівник освіти України

Міжнародні ініціативи у сфері інформаційної безпеки (порівняльний аналіз)

У статті розглянуто міжнародні ініціативи в сфері інформаційної безпеки та зроблено порівняльний аналіз їх основних положень. Також виділено проблемні питання, для практичної реалізації яких необхідно досягти взаєморозуміння між державами з метою безпечного спільного використання міжнародного інформаційного простору.

Ключові слова: інформаційна безпека, міжнародна ініціатива, національна безпека, несанкціоноване втручання, кібератаки, кіберзлочинність, кібертероризм, кіберпростір.

Постановка проблеми. На сучасному етапі глобальної інформатизації суспільства все більшої ваги набуває проблема забезпечення надійного захисту комп'ютерних мереж від спроб деструктивного чи злочинного втручання. Суттєво це питання загострюється у зв'язку зі стрімким упровадженням автоматизованих систем у галузях, надійне функціонування яких прямо впливає на рівень національної безпеки України.

Високий ступінь ураженості інформаційної інфраструктури змушує постійно вести пошук надійних способів і засобів забезпечення їх захищеності. У той же час, безсумнівно і те, що невпинний розвиток високих технологій, створення нових видів комп'ютерної та іншої електронної техніки робить цей процес безперервним і, на жаль, не завжди ефективним.

У цьому зв'язку, поряд із розробкою і удосконаленням технічних систем захисту національного інформаційного середовища та окремих його компонентів, особливе місце в забезпеченні інформаційної безпеки держави має займати робота над формуванням і впровадженням відповідної законодавчо-нормативної бази.

Важливо зважати і на те, що сучасний світ надто неоднорідний у можливостях забезпечення національних систем сучасними інформаційно-комунікаційними технологіями обробки, передачі, накопичення та збереження інформації і їх захисту від зовнішніх загроз. Це ще один вагомий аргумент на користь формування єдиної міжнародної системи інформаційної безпеки, яка б дозволила в однаковій мірі гарантувати захист національного інформаційного простору кожній державі.

Аналіз останніх досліджень і публікацій. Проблема інформаційної безпеки є предметом дослідження багатьох вітчизняних та зарубіжних вчених. Причому ці дослідження носять багатовекторний характер і здійснюються в різних напрямах. Зокрема, це створення нових та модернізація існуючих технічних засобів передачі, накопичення, збереження та захисту інформації, розробка нових інформаційних технологій та програмного продукту, формування ефективної нормативно-правової бази для регламентації дій в інформаційному просторі й напрацювання дієвих механізмів протидії деструктивним проявам.

Різні аспекти протидії кіберзагрозам висвітлювались у роботах І. В. Авдошина, О. М. Бабіча, В. М. Бутузова, В. Д. Гавловського, А. К. Гриня, О. Д. Довганя, О І. Матяша, О. М. Сьомкіна, С. М. Сьомкіна, В. Г. Хлая, В. П. Шеломенцева, О. М. Юрченка та інших.

Як правило, переважна більшість праць охоплює конкретні питання теоретичної чи прикладної складової інформаційної безпеки, формування понятійного апарату або протидії злочинним проявам у кібернетичній сфері. Однак, ще недостатньо уваги приділяється аналізу міжнародних ініціатив у цій галузі, порівнянню їх змісту та пріоритетів, оптимізації на цій основі системи захисту національного інформаційного простору.

Тому **метою даної роботи** є проведення порівняльного аналізу міжнародних ініціатив у сфері інформаційної безпеки для пошуку найбільш оптимальних напрямів формування комплексної системи протидії викликам в інформаційному середовищі України, яка б відповідала сучасним вимогам.

Виклад основного матеріалу. Сучасне життя неможливо уявити без широкого використання інформації. Вона дедалі активніше стає головним ресурсом науково-технічного та соціально-економічного розвитку, впливає на політичне життя країн і морально-психологічний стан суспільств. Проте можливості, закладені у використанні новітніх інформаційно-комунікаційних технологій, використовуються не лише задля творення і прогресу. Достатньо часто вони стають серйозним джерелом загроз життєво важливим інтересам людини, суспільства і держави.

Зазначені проблеми змушують вести активний пошук шляхів урегулювання питань інформаційної безпеки на глобальному рівні. Сьогодні жодна країна, яким би сучасним технічним чи технологічним арсеналом

вона не володіла, не може відчувати себе повністю захищеною в кіберпросторі. Адже з упровадженням усе більш досконалих способів захисту інформаційних мереж, не менше активними і витонченими стають розробники програм злому захисних систем.

Іншими словами, модернізація технічного захисту інформаційно-комунікаційної інфраструктури, тотальний контроль за комп'ютерними мережами чи забезпечення кібербезпеки в інший спосіб, не можуть повністю гарантувати надійність інформаційного простору.

Однією з важливих умов розв'язання даного питання є належне нормативно-правове регулювання проблем інформаційної безпеки як на національному, так і міжнародному рівнях. Перші спроби напрацювання міжнародних механізмів протидії злочинності в кіберпросторі були здійснені Радою Європи у 2001 році.

В прийнятій Конвенції про кіберзлочинність (далі – Конвенція) висловлено стурбованість, "що комп'ютерні мережі та електронна інформація може також використовуватись для здійснення кримінальних правопорушень і підкреслено "необхідність швидкодіючої та ефективної системи міжнародного співробітництва, яка б належним чином врахувала специфічні вимоги боротьби з кіберзлочинністю" [1].

Водночас, цей, безумовно, потрібний та актуальний документ не повною мірою враховує всю різноманітність порушень і загроз, пов'язаних з використанням інформаційного простору. Адже Конвенція обмежується лише питаннями протидії кіберзлочинам (при цьому навіть не даючи визначення цього поняття). Зокрема, нею рекомендується встановити кримінальну відповідальність за правопорушення, пов'язані з незаконним доступом, нелегальним перехопленням і втручанням у комп'ютерні дані чи систему. В число кіберзлочинів увійшли зловживання пристроями, підробка та шахрайство, пов'язані з комп'ютерами, дитяча порнографія, порушення авторських прав та деякі інші. Не можна обійти увагою і те, що Конвенція містить низку спірних питань, що пояснює відмову частини країн ратифікувати даний міжнародний документ. Одним із них є положення ст. 32, де для держав передбачено право здійснювати транскордонний доступ до публічно відкритих комп'ютерних даних, не отримуючи згоди країни, де ці дані знаходяться [1].

Це значно звужує можливості застосування Конвенції у міжнародній юридичній та регулятивній практиці й спонукає вести пошук єдиних підходів до формування безпечного інформаційного середовища.

Останнім часом світовому співтовариству запропоновано низку ініціатив, які мають дати поштовх для формування єдиної міжнародної політики в сфері кібербезпеки. Це, зокрема, оприлюднена в травні 2011 року зовнішньополітична ініціатива США "Міжнародна стратегія стосовно дій в кіберпросторі" (далі – Стратегія). В цьому документі дається бачення

Сполучених Штатів щодо майбутнього кіберпростору та форм співробітництва з іншими країнами для досягнення "процвітання, безпеки і відкритості у світовій мережі [2].

Як видно з документу, стратегічний підхід США до проблем безпеки в кіберпросторі передбачає підтримку інновацій, які просувають вперед економіку та підвищують якість життя, перш за все, в цій країні, а також "непохитну прихильність" основним свободам самовираження, об'єднань, особистого життя і вільного потоку інформації. При цьому США пропонуються і головні орієнтири щодо "бажаного кіберсередовища". Зокрема, в ньому має забезпечуватись підтримка основних свобод; повага до власності; цінність особистого життя; захист від злочинів; право на самооборону; глобальна сумісність; мережева стабільність; надійність доступу; участь в управлінні безлічі сторін; належна увага кібербезпеці [2].

Особливо слід наголосити на позиції Сполучених Штатів стосовно ворожих дій в кіберсередовищі. Це – право використовувати будь-які засоби: дипломатичні, політичні, воєнні та економічні, які є адекватними і не протирічать міжнародному законодавству для захисту країни, союзників, партнерів та інтересів США [2].

Запрошуючи держави, громадянське суспільство та приватний сектор приєднатись для реалізації в рамках Стратегії до ідеї "процвітання, безпеки і відкритості", уряд США має намір спонукати відповідні урядові структури інших країн визначитись щодо їх ролі у міжнародній кіберпросторовій політиці та координації подальших дій.

Співробітництво з міжнародними партнерами та приватним сектором Сполучені Штати передбачають здійснювати за такими напрямами:

– у галузі економіки: просування міжнародних стандартів й інноваційних відкритих ринків. США висловлюють готовність підтримувати вільне ринкове оточення, захищати інтелектуальну власність і комерційну таємницю від крадіжок, забезпечувати верховенство сумісних і безпечних стандартів;

– у галузі захисту національних кібермереж: стимулювання дотримання норм поведінки в кіберпросторі як в двосторонньому порядку, так і шляхом формування багатосторонніх організацій та багатонаціонального партнерства. Поряд з цим Сполучені Штати вживатимуть заходи по зменшенню кількості вторгнень у власні мережі, забезпеченню швидкого реагування на них та розширенню можливостей оперативного відновлення інформаційної інфраструктури після атак;

– у галузі правозастосування: розширення співробітництва і верховенство закону. В цьому зв'язку проводиться ідея щодо підтримки і поширення прийнятої Радою Європи Конвенції про кіберзлочинність, із внесенням до неї певних доповнень і поправок. При цьому не береться до

уваги не тільки регіональний характер Конвенції, а й те, що деякі викладені в ній положення вже сьогодні не влаштовують частину країн;

– у галузі збройних сил: підготовка до проблем безпеки XXI століття. Наголошується, що США беруть на себе обов'язок захищати своїх громадян, союзників та інтереси у будь-якій точці, де вони опиняться в небезпеці. Для цього планується удосконалити існуючі та створювати нові воєнні союзи для протидії можливим кіберзагрозам;

– у галузі управління мережею Інтернет: просування ефективних і всеосяжних структур, де будуть віддані пріоритети відкритості інновацій у мережі Інтернет, збереженню стабільності та безпеки глобальної мережі;

– у галузі міжнародного розвитку: питання глобального просування переваг мережевих технологій, підвищення надійності мережі загального користування і побудови співтовариства відповідальних учасників у кіберпросторі. США мають намір підвищувати здатність країн до боротьби з кіберзлочинністю, у тому числі шляхом підготовки правоохоронців, судових фахівців, юристів і законодавців, налагоджувати стосунки з вищими посадовими особами для забезпечення їх постійних й тривалих контактів з експертами з уряду Сполучених Штатів;

– у галузі свободи мережі Інтернет: підтримка основних свобод та приватного життя в кіберпросторі. Мова фактично йде про підтримку діячів громадянського суспільства та міжнародних неурядових організацій в створенні надійних, захищених і безпечних платформ для свободи самовираження та об'єднання й захисту їх інтересів від незаконного цифрового втручання.

Зазначені напрями відіграють вирішальну роль у збереженні "знайомого США кіберпростору" і слугують платформою для спільного формування його майбутнього.

Таким чином, зміст Стратегії свідчить, що США розроблена модель використання та захисту кіберпростору, яка здебільшого спрямована на реалізацію стратегічних інтересів цієї країни та її національних пріоритетів.

Виникає багато запитань і стосовно задекларованої в Стратегії підтримки лідерів громадянського суспільства та міжнародних неурядових організацій. Особливо, коли взяти до уваги, що частина з них цілеспрямовано займається проведенням деструктивних кампаній на територіях інших країн з використанням їх інформаційного простору для поширення недостовірних або викривлених фактів, які суттєво впливають на моральний стан суспільства.

Альтернативою американським ініціативам може слугувати презентована Російською Федерацією у вересні 2011 року "Конвенція про забезпечення міжнародної інформаційної безпеки (концепція)" (далі – Конвенція РФ).

Головна її відмінність полягає в розгляді проблем, пов'язаних з міжнародною інформаційною безпекою, у більш широкому аспекті та

через призму забезпечення міжнародного миру і безпеки, які повинні підтримуватись у будь-який спосіб [3].

Необхідно зазначити, що в Конвенції РФ запропоновано принципи, дотримання яких має спонукати, щоб діяльність держав у інформаційному просторі:

– сприяла загальному соціальному та економічному розвитку;

– була сумісною із завданнями підтримання міжнародного миру і безпеки;

– відповідала загальноприйнятим принципам і нормам міжнародного права, включаючи принципи мирного урегулювання суперечок і конфліктів, незастосування сили, невтручання у внутрішні справи, повагу прав і основних свобод людини;

– створювала можливості для реалізації права кожного шукати, отримувати і розповсюджувати інформацію та ідеї, як це зафіксовано в документах ООН, але в той же час визначала законодавчі обмеження такого права в разі необхідності захисту національної і суспільної безпеки кожної держави та запобігання несанкціонованого втручання в інформаційні ресурси;

– гарантувала свободу технологічного обміну та свободу обміну інформацією з урахуванням поваги до суверенітету держав і їх існуючих політичних, історичних й культурних особливостей [3].

Варто звернути увагу, що в Конвенції РФ значно розширений перелік основних загроз в інформаційному просторі. Крім перелічених у Стратегії дій, які призводять до руйнації систем і мереж чи порушення їх стабільності; атак на мережі; кіберзлочинності та нелегальної діяльності в мережах; терористичної діяльності та її фінансування через мережу Інтернет, у Конвенції РФ загрозою, перш за все, вважається порушення суверенітету інформаційного простору держави.

Зокрема, до цього відноситься неправомірне використання інформаційних ресурсів іншої держави без її відома та дії в інформаційному просторі з метою підриву політичної, економічної і соціальної систем іншої держави та психологічна обробка населення з метою дестабілізації суспільства.

До переліку також включені спроби використання інформаційної інфраструктури для розповсюдження відомостей, які розпалюють міжнаціональну, міжрасову і міжконфесійну ворожнечу. Звертається увага на такі деструктивні прояви, як дезінформація і приховування інформації з метою викривлення психологічного і духовного середовища суспільства, ерозія традиційних культурних, моральних, етичних і естетичних цінностей, інформаційна експансія, набуття контролю над національними інформаційними ресурсами іншої держави тощо [3].

Конвенція РФ також містить спеціальну главу, де йдеться про основні заходи запобігання воєнним конфліктам у відповідь на пору-

шення в інформаційному просторі. Для цього держави повинні завчасно виявляти потенціальні конфлікти в інформаційному просторі, а також докладати зусилля для їх запобігання з метою подальшого мирного урегулювання кризових ситуацій і суперечок [3].

Така позиція є логічною і послідовною, оскільки вирішення питань, пов'язаних з реагуванням на загрози в інформаційному просторі, залишається надзвичайно складним. По-перше, не завжди з достатньою мірою точності можна ідентифікувати джерело ворожих дій. По-друге, існує постійна небезпека застосування абсолютно нових технологій для несанкціонованого втручання в інформаційний простір, що може призвести до неочікуваних наслідків їх деструктивного впливу. По-третє, необхідно враховувати, що інформаційно-комунікаційні можливості держав надзвичайно різняться як за рівнем оснащеності, так і здатністю забезпечувати безпеку своїх мереж та можливість відновлення існуючої інфраструктури після несанкціонованого впливу. По-четверте, необхідно враховувати значні відмінності у законодавчо-нормативній базі різних країн щодо протидії порушенням в інформаційно-комунікаційній сфері, а також відсутність чіткої міжнародної регламентації дій у світовому інформаційному просторі для його безпечного функціонування.

У цьому зв'язку доцільно згадати ще один документ, який стосується зазначених проблем. Це – внесені у вересні 2011 року для розгляду на сесії Генеральної асамблеї ООН Китайською Народною Республікою, Російською Федерацією, Таджикистаном та Узбекистаном "Правила поведінки у сфері забезпечення міжнародної інформаційної безпеки" (далі – Правила).

Їх головною метою є визначення прав і обов'язків держав у інформаційному просторі, стимулювання конструктивної і відповідальної поведінки та співробітництва держав з метою протистояння загальним викликам і загрозам у цій сфері, спонукання до використання інформаційно-комунікаційних технологій виключно для повномасштабного соціального і економічного розвитку та добробуту народів, забезпечення миру і безпеки.

Порівняно з переліченими раніше міжнародними ініціативами щодо безпеки інформаційного простору, Правила по суті повторюють основні положення Конвенції РФ, хоч за своїм обсягом є значно меншими.

В них варто виділити декілька найбільш принципових питань, які можуть суттєво вплинути на формування майбутнього міжнародного інформаційного простору. Зокрема, це:

– повага суверенітету, територіальної цілісності та політичної незалежності усіх держав, різноманіття їх історії, культури і соціального ладу, повага до прав та основних свобод людини;

– заборона на використання інформаційно-комунікаційних технологій для здійснення актів агресії, які спричиняють загрозу миру і безпеці, а також на розповсюдження інформаційної зброї та її технологій;

– співробітництво проти злочинної, екстремістської і терористичної діяльності з використанням інформаційних технологій, стримування розповсюдження інформації, що підриває політичну, економічну і соціальну стабільність держав, їх культурний і духовний уклад;

– запобігання використання іншими державами своїх ресурсів для підриву права іншої держави на незалежний контроль над сферою інформаційно-комунікаційних технологій чи для створення загрози політичній, економічній і соціальній безпеці;

– сприяння створенню багатосторонніх, прозорих і демократичних міжнародних механізмів управління мережею Інтернет на основі рівності, справедливості, стабільності та безпеки;

– стимулювання до вироблення міжнародних норм у сфері інформаційної безпеки для мирного урегулювання міжнародних суперечок та підвищення якості співробітництва, утримання від застосування воєнної сили чи загрози силою [4].

Таким чином, зазначеними Правилами пропонується ввести певні обмеження у використанні інформаційного простору і соціальних мереж для здійснення інформаційних атак, пов'язаних з дискредитацією чинної влади, політичного устрою та підриву соціальних і культурних цінностей.

Висновки. Підсумовуючи викладене, варто підкреслити, що питання інформаційної безпеки продовжують залишатись актуальними і вимагають нарощування зусиль для протидії загрозам національним інтересам у цій сфері. Особливої ваги сьогодні набуває проблема нормативно-правового урегулювання принципів і норм поведінки держав у міжнародному кіберпросторі. Адже наведені вище зовнішньополітичні ініціативи, на жаль, не можуть бути в повній мірі прийнятними для світового співтовариства.

І цьому є декілька причин. По-перше, суттєві відмінності між державами в розвитку інформаційно-комунікаційних інфраструктур і можливостях їх захисту. По-друге, різноманіття історичного розвитку, культурних і моральних цінностей, політичного і соціального ладу країн. По-третє, невідповідність національних законодавств і практики реагування на виклики в інформаційному просторі.

Тому, спираючись на запропоновані країнами-ініціаторами шляхи формування безпечного інформаційного середовища, необхідно, перш за все, визначитись, наскільки повно вони відповідають національним інтересам України:

– наскільки, або в якій мірі може бути прийнятне поширення "вільних потоків інформації"?

– якою буде модель підтримання і захисту суверенітету національного інформаційного простору?

– чи реально з економічної точки зору стимулювати розробку вітчизняного інформаційно-телекомунікаційного обладнання та програмного забезпечення тощо?

Для відповіді на ці запитання необхідно акумулювати міжнародні ініціативи, які мають спільні риси і не викликають сумніву в доцільності й корисності їх впровадження. З іншого боку, необхідно почати розробку альтернативних шляхів вирішення проблем, які світовим співтовариством не сприймаються однозначно і гальмують процес формування міжнародного консенсусу з проблем кібербезпеки. У свою чергу, це сприятиме, щоб Україна стала активним учасником міжнародного нормотворчого процесу для протидії викликам в інформаційній сфері.

Список використаних джерел

1. Про кіберзлочинність : Конвенція Ради Європи від 23 листоп. 2001 р // Офіц. вісник України. – 2007. – № 65. – С. 107. – Ст. 2535. – Код акту 40846/2007. – 10 верес.

2. Международная стратегия по действиям в киберпространстве – [Электронный ресурс]. – Режим доступа :
http://кибервоин.рф/strategiya/mezhdunarodnaya-strategiya-ssha-v-kiberprostranstve. html.

3. Конвенция об обеспечении международной информационной безопасности (концепция) / [Электронный ресурс]. – Режим доступа :
http://www. scrf. gov. ru/documents/6/112. html.

4. Правила поведения в области обеспечения международной информационной безопасности / [Электронный ресурс]. – Режим доступа :
http://rus. rusemb. org. uk/data/doc/internationalcoderus. pdf.

В статье рассмотрены международные инициативы в сфере информационной безопасности и дан сравнительный анализ их основных положений. Также выделены проблемные вопросы, для практической реализации которых необходимо достичь взаимопонимания между государствами для безопасного совместного использования международного информационного пространства.

The article deals with the examination of the international initiatives in the information security sphere and the comparative analysis of their main provisions is given. The problems, for practical realization of which it is necessary to attain the mutual understanding between the states for the safe sharing of international information space, are also set off.

Стаття надійшла до редакції журналу 18 жовтня 2012 року.