## Реферат

***не тему:***

Міжнародне право інформаційної безпеки

Співробітництво держав у сфері інформації базується на загальновизнаних міжнародно-правових принципах, таких, як суверенна рівність держав, зобов’язання держав утримуватися в міжнародних відносинах від застосування сили або загрози силою, невтручання у внутрішні справи держав, зобов’язання співробітничати за Статутом ООН, рівність і самовизначення народів, заборона пропаганди війни, расової та національної ворожнечі.

Наразі склалися, діють і розвиваються спеціальні норми і принципи, які безпосередньо регулюють питання міжнародного обміну інформацією. В міжнародно-правових документах можна виділити такі спеціальні принципи, на яких організується співробітництво в інформаційній сфері:

* 1. питання закордонного поширення інформації повинні регулюватися міжнародними документами;
  2. ЗМІ можуть правомірно використовуватися для міжнародного поширення демократичних ідей;
  3. держави повинні попереджати використання ЗМІ для транскордонного поширення ідей, заборонених міжнародним співтовариством;
  4. держави несуть міжнародну політичну відповідальність за відповідність міжнародної діяльності національних ЗМІ загальновизнаним нормам міжнародного права

Процес формування цих принципів почався ще у довоєнний період (наприкінці ХІХ ст. на початку ХХ ст.). 23.11.1936р. у Женеві було прийнято Конвенцію про використання радіомовлення в інтересах миру. Конвенція забороняє державам вести на своїй території, радіомовлення, яке підбурює населення однієї країни до насильницьких дій проти внутрішнього порядку або безпеки іншої країни. Вона зобов’язує держави вживати заходів до припинення такого мовлення на своїй території, стежити за тим, щоб радіостанції не закликали до війни або інших дій, що її спричиняють

Практично в той же час була розроблена південно - американська угода про радіомовлення (підписана 1935р. в Буенос-Айресі і переглянута у 1937р. в Ріо-де-Жанейро), яка закріпила чинний принцип між латиноамериканськими державами заборони передачі недостовірної інформації та програм, метою яких є порушення дружніх відносин між країнами, образливих для національних почуттів, а також протиправних для підтримання миру і стабільності, суверенітету та цілісності держав.

В післявоєнний період (1945р.) питання обміну інформацією розглядалися на ГА ООН. Серед документів ГА ООН – Резолюція 110 „заходи проти пропаганди і розпалювання агресивних (насильницьких) воєн, в якій ООН засудила „будь-яку форму пропаганди, метою якої є створення або посилення загрози миру, порушення миру або акт агресії”. Одночасно Асамблея прийняла резолюцію 127 „Недостовірна або перекручена інформація”, в якій також містяться формулювання регламентуючого характеру щодо дій держав на міжнародній інформаційній арені і засуджується поширення інформації, яка підриває співробітництво і взаєморозуміння між народами.

Права людини на отримання або поширення інформації та ідеї усно, письмово та іншими способами було зафіксовано у Міжнародному пакті про громадянські та політичні права 1966р. Там передбачені і обмеження на використання цього права, зумовлені необхідністю охорони прав інших осіб, захисту національної безпеки, суспільного порядку, здоров’я або моральності населення (ст.19)

Ідея про розвиток міжнародного інформаційного права втілилась у низку інших документів ООН, серед яких:

1. Декларація про поширення серед молоді ідеалів миру, взаємної поваги та взаєморозуміння між народами 1965р. Декларація підкреслює важливу роль ЗМІ у справі „поширення серед молоді ідеалів миру, гуманізму, свободи і міжнародної солідарності, а також всіх інших ідеалів, що сприяють зближенню народів”, ознайомлення молоді з роллю ООН як інструмента збереження і підтримання миру, а також сприяння міжнародному взаєморозумінню і співробітництву;
2. Декларація про неприпустимість втручання у внутрішні справи держав, про захист їх незалежності і суверенітету 1965р., яка проголошує, що „всі держави повинні утримуватися від того, щоб організовувати, допомагати, створювати, фінансувати, заохочувати або сприяти збройній, підривній або терористичній діяльності, спрямованій на зміну устрою іншої держави”, і що „практика втручання в будь-якій формі не тільки є порушення духу і букви статуту ООН, але призводить до ситуації, що загрожує міжнародному миру і безпеці”;
3. Декларація про принципи міжнародного права, що стосуються дружніх відносин і співробітництва між державами відповідно до Статуту ООН 1970р., в якій йдеться про таке: „Агресивна війна є злочином проти миру, який витікає з принципу відповідальності міжнародного права. Відповідно до принципів і цілей ООН держави повинні утримуватися від пропаганди агресивних воєн;
4. Декларація ООН про виховання народів в дусі миру 1978 р., яка закликає всі держави „припиняти пропаганду ненависті і упередженого ставлення до інших народів як такого, що суперечить принципам мирного співіснування і дружнього співробітництва. Вона закликає держави забезпечувати відповідність діяльності національних ЗМІ щодо поширення серед молоді ідеалів миру;
5. Декларація про неприпустимість інтервенції або втручання у внутрішні справи держав 1981р., яка закликає держави „утримуватися від будь-яких наклепницьких кампаній, образливої або ворожої пропаганди, а також проголошує „право і зобов’язання держав боротися в рамках своїх конституційних повноважень проти фальсифікованої або перекрученої інформації, яка може розглядатися як втручання у внутрішні справи інших держав або як такі, які завдають шкоди зміцненню миру, співробітництву і дружніх відносин між державами і націями.

Процес формування міжнародно-правових принципів відбувається на різних рінях – Міжнародних конференціях, корпоративних нарадах, в рамках міжнародних організацій\*\*\*\*\*\*\*\*\*\*\*\*.....

**довідник** Традиційна міжнародна безпека (тобто колективна) є визначеною системою міжнародних відносин держав з метою підтримання міжнародного миру і безпеки, що регламентується принципами і нормами статуту ООН. Ця колективна безпека охоплює: 1) основні принципи міжнародного права; 2) процедури мирного вирішення спорів; 3) колективні дії для попередження загрози миру; 4) повноваження ГА ООН та Ради Безпеки ООН з розгляду питань роззброєння та обмеження озброєнь. Практика ООН внаслідок трансформацій сучасного світу та досягнень нових технологій здійснюється шляхом розробки нових угод та рекомендацій з різних конкретних питань міжнародних відносин, зокрема питань міжнародної безпеки. Норми цих угод та рекомендацій складають вторинний відносно Статуту ООН конкретний шар міжнародного правопорядку, який базується на цілях і принципах Статуту ООН і є регулярною основою міжнародних відносин в галузі міжнародної безпеки. Стан договірних норм у системі колективної безпеки має різноманітний характер. Існують міжнародні договори, які мають імперативний характер, деякі принципи, прийняті у вигляді резолюцій, потребують кодифікації, щоб їх сучасний зміст набув зобов’язальної юридичної сили, окрім того виникають нові принципи міжнародного права, які не зафіксовані в Статуті ООН, і які потребують розробки і юридичного закріплення.

З проблем міжнародної інформаційної безпеки існують лише резолюції ГА ООН, які передбачають прийняття міжнародних договорів відповідного змісту. В інформаційній сфері необхідна кодифікація спеціальних принципів і норм, що склалися на основі Статуту ООН і досягнення нових угод, щоб впорядкувати і стабілізувати відносини держав, прогнозувати їх подальший розвиток, а також інших відносин, пов’язаних з проблемою інформаційної безпеки, зокрема політичних, соціальних, економічних, гуманітарних, екологічних тощо. У зв’язку зі значенням міжнародних договорів, які входять до системи міжнародної безпеки, особливий інтерес виникає з таких питань, як тривалість чинності договорів, можливість виходу з них, їх універсальність і забезпечення виконання.

Головним форумом для конкретної практики права міжнародної інформаційної безпеки є ООН – універсальна міжнародна організація з безпеки і співробітництва держав, яка відповідно до статуту є центром для узгоджених дій всіх націй у досягненні своїх цілей. Практично діяльність ООН охоплює всі сфери міжнародної безпеки: військову, політичну, економічну, гуманітарну, екологічну, інформаційну тощо. В резолюції 42/93 від 7.12.1987р. ГА ООН відзначила, що з часу прийняття статуту ООН у світі відбулися значні трансформації, зумовлені процесами політичної, економічної та технологічної глобалізації, зросла взаємозалежність держав та їх зацікавленість у підтриманні сталого миру і безпеки, що зумовлює необхідність спільних зусиль всіх акторів міжнародних відносин у сфері безпеки, мирного врегулювання конфліктів та кризових ситуацій, захисту прав людини і основних свобод. ГА ООН у Резолюції 44/21 від 15.11.1989р. закликала всі держави примножувати їх практичні зусилля в усіх напрямах забезпечення міжнародної безпеки, підтвердила дієвість і значення статуту ООН, необхідність дотримання основних його принципів, висловилась за співробітництво в рамках Організації та її основних структур (спеціалізованих установ) з метою знайти багатогранні підходи до зміцнення принципів і систем міжнародної безпеки на основі нормативних документів ООН. Міжнародна правова практика свідчить, що міжнародні угоди проходять тривалий шлях через ухвалення резолюцій і декларацій, але саме угоди є основою правового регулювання міжнародних відносин у сфері безпеки, зокрема міжнародної інформаційної безпеки.

**Крутських А. Кримаренко Г. (м.ж.) + документи ООН** Нормотворча діяльність ООН має першочергове значення для вирішення проблеми міжнародної інформаційної безпеки. Вперше ця проблема розглядалася на 53 сесії ГА ООН на підставі доповідей Генерального Секретаря ООН (К. Анана) та Першого комітету (доповідач М. Захрейн (Єгипет), 18.11.1998р.) „Роль науки і техніки в контексті міжнародної безпеки і роззброєння”, коли було проголосовано (за – 77, переважно держави Південної Америки, Африки, Тихоокеанського регіону та Близького Сходу, тобто, країни, що розвиваються; проти – 43, переважно держави Північної Америки, Європи, Балтії, Австралії та Нової Зеландії, утримались – 16, переважно держави СНД, Японія, деякі країни Південної Америки та ПАР) проект резолюції А/С.1/53/L.15 „Роль науки і техніки в контексті міжнародної безпеки і роззброєння”. В ній зазначалися положення про подвійну природу досягнень науки і техніки (як у цивільній, так і у воєнній сферах), про застосування новітніх досягнень у модернізації сучасних озброєнь, зокрема зброї масового ураження, про здатність досягнень науки і техніки здійснювати негативний вплив на міжнародну безпеку. В резолюції підкреслюється, що новітні технології (пристрої, послуги „ноу-хау” подвійного призначення) мають важливе значення для економічного і соціального розвитку держав і водночас висловлюється занепокоєність щодо розповсюдження спеціальних та особливих режимів і механізмів регулювання експорту продукті і технологій подвійного призначення, здатних негативно вплинути на економічний та соціальний розвиток країн так званого „третього світу”.

Визнаючи необхідність регулювання передачі новітніх технологій подвійного призначення (у Заключному документі 12 Конференції глав держав та урядів країн Руху Неприєднання (Дурбан, Південна Африка, 29.08. - 03.9.1998рр.) було визначено проблему жорстких обмежень на експорт у країни, що розвиваються, новітніх матеріалів, обладнання та технологій для використання у мирних цілях. У проекті резолюції вказується на застосування узгоджених, на багатосторонній основі, загальноприйнятих, недискримінаційних керівних принципів, які мають врахувати законні оборонні потреби всіх держав і потреби з підтримання міжнародного миру і безпеки, сприяти використанню досягнень науки і техніки на основі передачі технічних знань та обміну ними в мирних цілях.

В Резолюції було запропоновано державам-членам вжити додаткових заходів із застосування досягнень науки і техніки з метою роззброєння та надання технологій відповідного характеру. Резолюція закликала держави-члени до багатосторонніх переговорів, щоб розробити керівні принципи щодо регулювання міжнародної передачі новітніх технологій подвійного призначення та високих технологій військового застосування. На основі проекту резолюції було прийнято постанову ГА ООН 53/70 „Досягнення у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки” (А/RES/53/70, від 4.12.1998р.) в якій підкреслюється необхідність розробки міжнародно-правової бази у сфері міжнародної інформаційної безпеки, вироблення документів на рівні конвенції та закріплення міжнародних принципів в національних законодавствах.

З ініціативи Росії (у 1996 році Федеральне агентство урядового зв’язку та інформації при Президентові РФ опублікувала аналітичну довідку „Інформаційні озброєння як загроза національної безпеці Росії”, у 1997-1998рр. Державна Дума РФ, потім Міжпарламентська Асамблея СНД звернулась до ООН, НБСЄ та РЄ з пропозицією прийняти міжнародну конвенцію про заборону інформаційних воєн та обмеження обігу інформаційної зброї) на 54 сесії ГА ООН було ухвалено оновлену резолюцію 54/49 від 1.12.1999р. „Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки”, якою концепцію міжнародної інформаційної безпеки було визнано глобальною проблемою сучасності. Об’єктивними умовами її прийняття були принципово нові потенціальні загрози для міжнародного миру, зумовлені науковотехнологічним прогресом та глобальною взаємозалежністю всіх сфер життєдіяльності міжнародного співтовариства. В контексті Резолюції запропоновано державам-членам висловитися щодо загальних проблем інформаційної безпеки, розглянути конкретну технологію інформаційних загроз, в тому числі несанкціоноване втручання та неправомірне використання інформаційних і телекомунікаційних систем та інформаційних ресурсів, розробити міжнародні принципи, спрямовані на зміцнення безпеки глобальних інформаційних та комунікаційних систем та боротьбу з інформаційним тероризмом і криміналом.

ГА ООН продовжила роботу над резолюцією „Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки” протягом 55 сесії, обговоривши доповіді Генерального Секретаря та представника Першого комітету Р. Габріеля, в яких містився аналіз позицій держав-членів у відповідь на вербальну ноту Генерального секретаря ГА ООН щодо міжнародної інформаційної безпеки. Так, позиція Польщі щодо загальної оцінки проблем інформаційної безпеки та визначення основних понять полягає у констатації впливу ІКТ на світовий розвиток, які стимулюють економіку, полегшують вільні потоки інформації, сприяють зміцненню демократії та свободі слова, формуванню громадського суспільства.

Польща вважає за необхідне заохочувати та забезпечувати подальший розвиток ІКТ та цивільне їх використання. Разом з тим Польща визнає наявність потенційних загроз несанкціонованого втручання або неправомірного використання ІКТ-систем, цілісності критично важливих інфоінфраструктур та інформаційних ресурсів урядових, неурядових, комерційних установ та приватних банків даних. Інформаційна безпека охоплює широкий спекр проблем, зокрема проблем доступу, конфіденційності, наявності і збереження інформації у процесі обробки. Недостатній захист інформаційних ресурсів та ІКТ-систем, що мають життєво-важливе значення для національної безпеки держав, розглядається і як загроза міжнародної безпеки. Ці загрози неможливо класифікувати виключно як цивільні або військові, ІКТ можуть бути використані окремими особами, терористичними організаціями та злочинними угрупуваннями, тому міжнародне співтовариство має сконцентруватися на захисті інформаційних ресурсів та інформаційних систем. Польща виступає за ефективне і багатостороннє міжнародне співробітництво, розробку нових законодавчих актів та за жорстке виконання чинного внутрішнього законодавства.

На міжнародному рівні було запропоновано підтвердити керівну роль ООН щодо розробки міжнародних принципів інформаційної безпеки, сприяти координації діяльності міжрегіональних та регіональних структур з попередження злочинного використання ІКТ. На національному рівні визначено за доцільне прийняти відповідні закони, зокрема про захист секретної інформації, приватної інформації в процесі автоматизованої обробки даних, встановити кримінальну відповідальність за руйнування, модифікацію та викрадення комп’ютерних даних, або передачі інформації щодо питань національної безпеки, безпеки ІКТ-систем та функціонування органів державної влади, укласти двосторонні міжнародні угоди (Польща веде переговори з ФРН, Угорщиною, Словаччиною, Україною, Францією, Естонією) про захист інформації щодо медичних даних, інтелектуальної власності, наукових досліджень від будь-якого несанкціонованого втручання, включаючи незаконні банківські та фінансові операції.

Іорданія, Катар також підтвердили необхідність розробки міжнародно-правових принципів щодо інформаційної безпеки, включивши до переліку загроз: „шпіонаж” (попередження несанкціонованого доступу до змісту ІКТ-систем); „саботаж” (попередження часткового або повного знищення ІКТ-систем); „підробку” (попередження підробки інформації в глобальному кіберпросторі). Від імені урядів цих держав було запропоновано ухвалити концепцію міжнародної інформаційної безпеки і сприяти підтриманню системи сталого миру.

Найбільш розгорнута відповідь на вербальну ноту від Генерального секретаря ООН та пропозиції надійшли від Російської Федерації, що представила на розгляд Асамблеї типологію термінів (інформаційний простір, інформаційні ресурси, інформаційні війни, інформаційна зброя, інформаційна безпека, загрози інформаційної безпеки, міжнародна інформаційна безпека, неправомірне використання ІКТ-систем та ресурсів, несанкціоноване втручання в ІКТ-системи та ресурси, критично важливі структури, міжнародний інформаційний тероризм, міжнародна інформаційна злочинність) та принципи взаємодії держав у сфері міжнародної інформаційної безпеки. Серед них:

**Принцип 1.**

1. Діяльність кожної держави та інших суб’єктів міжнародного права в міжнародному інформаційному просторі повинна сприяти загальному соціальному та економічного розвитку і здійснюватися таким чином, щоб відповідати завданням підтримання сталого миру і безпеки, суверенних прав інших держав, інтересам безпеки, принципам мирного врегулювання спорів та конфліктів, незастосування сили, невтручання у внутрішні справи, поваги до прав і свобод людини.
2. Така діяльність повинна відповідати праву кожного шукати, отримувати та поширювати інформацію та ідеї, як це зафіксовано у документах ООН, з врахуванням того, що таке право може бути обмежене законом з метою захисту інтересів національної безпеки кожної держави.
3. При цьому кожна держава та інші суб’єкти міжнародного права повинні мати рівні права на захист своїх інформаційних ресурсів та критично важливих структур від неправомірного використання; несанкціонованого інформаційного втручання і можуть сподіватися на підтримку світового співтовариства в реалізації цих прав.

**Принцип 2.**

Держави повинні прагнути до обмеження загроз у сфері міжнародної інформаційної безпеки і з цією метою утримуватися від:

1. розробки, створення і використання засобів впливу і завдання шкоди інформаційним ресурсам і системам іншої держави ;
2. спрямуваного інформаційного впливу на критично важливі структури іншої держави;
3. інформаційного впливу з метою руйнування політичної, економічної та соціальної системи інших держав і задля дестабілізації суспільства;
4. несанкціонованого втручання в інформаційно-телекомунікаційні системи та інформаційні ресурси, їх неправомірне використання;
5. дій, що сприяють домінуванню і контролю в інформаційному просторі;
6. протидії доступу до новітніх ІКТ, створення умов технологічної залежності у сфері інформатизації як загрозу іншим державам;
7. заохочення дій міжнародних терористичних, екстремістських і злочинних угрупувань, що загрожують інформаційним ресурсам та критично важливим структурам інших держав;
8. розробки та ухвалення планів, доктрин, які передбачають ведення інформаційних воєн, здатних спровокувати гонку озброєнь, а також викликати напруженість у відносинах між державами і самих інформаційних воєн;
9. використання ІКТ проти основних прав і свобод людини, які реалізуються в інформаційній сфері;
10. транскордонного поширення інформації, яка суперечить принципам і нормам міжнародного права, а також внутрішньому законодавству конкретних країн;
11. маніпулюванню інформаційними потоками, дезінформації та засекречування інформації з метою викривлення психологічного і духовного середовища суспільства, ерозії традиційних культурних, моральних та етичних і естетичних цінностей;
12. інформаційної експансії, монополії в національних інформаційних системах інших держав, включаючи умови їх функціонування в міжнародному інформаційному просторі.

**Принцип 3.**

ООН та її спеціалізовані установи сприятимуть міжнародному співробітництву, метою якого є обмеження загроз у сфері міжнародної інформаційної безпеки і формування відповідної міжнародно-правової бази для:

1. визначення ознак та класифікації інформаційних воєн;
2. визначення ознак і класифікації інформаційних озброєнь і засобів відповідного призначення;
3. обмеження обігу інформаційних озброєнь;
4. заборону розробки, поширення і використання інформаційної зброї;
5. попередження загрози виникнення інформаційної війни;
6. визнання безпеки застосування інформаційної зброї щодо критично важливих структур як зброї масового ураження;
7. створення умов для рівноправного і безпечного міжнародного інформаційного обміну на основі загальновизнаних норм і принципів міжнародного права;
8. попередження використання інформаційних технологій і засобів впливу на суспільну свідомість з метою дестабілізації суспільства і держави;
9. розробки процедури взаємного інформування та попередження транскордонного несанкціонованого інформаційного впливу;
10. створення системи міжнародного моніторингу для відстеження загроз в інформаційній сфері;
11. створення міжнародної системи сертифікації технологій і засобів інформатизації і телекомунікацій (в тому числі програмно-технічних) щодо гарантій їх інформаційної безпеки;
12. створення механізму контролю виконання умов режиму міжнародної інформаційної безпеки;
13. створення механізму врегулювання конфліктних ситуацій у сфері інформаційної безпеки;
14. розвитку систем міжнародної взаємодії правоохоронних органів з попередження і припинення правопорушень в інформаційному просторі;
15. гармонізації на добровільній основі національних законодавств для забезпечення міжнародної інформаційної безпеки.

**Принцип 4.**

Держави та інші суб’єкти міжнародного права повинні нести міжнародну відповідальність за діяльність в інформаційному просторі, яка здійснюється ними, під їхньою юрисдикцією або в рамках міжнародних організацій, членами якої вони є і за відповідність такої діяльності принципам, які містяться у цьому документі.

**Принцип 5**.

Будь-які спори між державами та іншими суб’єктами міжнародного права, які виникають при застосуванні цих принципів, регулюються за допомогою встановлених процедур мирного врегулювання спорів.

55 сесія ГА ООН прийняла Резолюцію 55/28 (А/RES/55/28) від 20.11.2000р. „Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки”, в якій, посилаючись на попередні резолюції про роль науки і техніки в контексті міжнародної безпеки та відзначаючи відповіді держав щодо оцінки проблем інформаційної безпеки, закликає всі держави-члени ООН сприяти на багатосторонній основі подальшому розгляду концепцій глобальної інформаційної безпеки та загроз у сфері ІКТ для завершення дискусії і ухвалення міжнародної конвенції з інформаційної безпеки.

56 сесія ГА ООН розглянула доповіді Генерального Секретаря та представника Першого комітету С. Екундайо Рове (Сьєра-Леоне) щодо визнання інформаційної безпеки глобальною проблемою, обговорила відповіді держав щодо загальної оцінки, визначення основних критеріїв і змісту відповідних міжнародних концепцій і прийняла резолюцію 56/19/А/PES/56/19) від 29.11.2001р. „Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки”, в якій відзначено, що поширення і використання інформаційних технологій і засобів торкається інтересів всього міжнародного співтовариства. Ці технології і засоби потенційно можуть бути використані з метою нестабільності міжнародної безпеки як у воєнній, так і у цивільній сферах, тому необхідно проведення міжнародної зустрічі експертів для конкретизації сутності проблеми міжнародної інформаційної безпеки та її правового забезпечення.

Серед відповідей держав (Болівія, Мексика, Філіппіни та Швеція) особливу увагу привертає позиція держав Європейського союзу, в якій підкреслюється, що країни ЄС підтримали ухвалену консенсусом резолюцію 55/28 ГА ООН „Досягнення у сфері інформації і телекомунікацій в контексті міжнародної безпеки”. Щодо загальної оцінки проблеми інформаційної безпеки то ЄС вважає, що ІКТ сприяють вільному потоку інформації, демократизації суспільства та економічному прогресу. ЄС визнає, що існують потенційні загрози неправомірного та несанкціонованого використання ІКТ у різних сферах життєдіяльності держав, що створює небезпеку для міжнародної безпеки. Щодо змісту міжнародних концепцій про безпеку глобальних ІКТ-систем ЄС підкреслює, що, незважаючи на ефективність міжнародного співробітництва у сфері інформаційної безпеки, в першу чергу кожна держава має право і несе відповідальність за захист власних інформаційних ресурсів та інформаційних систем. Існуючі ризики мають транскордонний характер, і будь-які превентивні заходи спрямовані на обмеження потенційних втрат від злочинного чи терористичного нападу, зокрема і для міжнародної безпеки, повинні здійснюватися з урахуванням захисту ІКТ-ресурсів та систем.

ЄС вважає, що саме ООН має стати основним форумом з обговорення проблем міжнародної інформаційної безпеки.

У відповідях урядів Мексики, Гватемали та Болівії представлені різні підходи до проблеми глобальної інформаційної безпеки. Зокрема, Болівія не передбачає виробництва інформаційних озброєнь або оснащення ними своїх збройних сил у найближчому майбутньому. Разом з тим Мексика та Філіппіни внесли пропозиції і щодо оцінки проблеми інформаційної безпеки, визначення основних понять в цій сфері, конкретизувавши як загрози, зокрема міжнародний інформаційний тероризм, кіберзлочинність, так і заходи протидії цим загрозам. Так, Мексика підкреслила, що підтримує положення резолюції 51/210 від 17.12.1996р. щодо міжнародного тероризму (п. 3(с)ч.1.) та можливості використання ІКТ-систем і ресурсів для злочинних протиправних дій і сприятиме попередженню такого роду злочинності на основі узгоджених міжнародних підходів на різних рівнях.

Філіппіни визнали інформаційні озброєння такою ж загрозою, як і зброя масового ураження, підкреслили, що всі досягнення у сфері науки і техніки можуть бути використані з протиправною метою, тому ця проблема є глобальною і для розвинутих в технічному відношення країн, і для країн, що розвиваються. Серед понять (несанкціоноване втручання, проникнення, санкціоноване втручання, несанкціоноване використання інформації, протиправне використання ІКТ, інформаційні ресурси, інформаційна зброя, інформаційна війна, інформаційний тероризм, електронно-кіберзлочинні злочини, кібернетичні злочинці, технологічно передові держави) новим є поняття „інформаційна колонізація”, яка визначається як дії однієї держави або держав проти інших з метою встановлення монополії та контролю в інформаційній сфері, попередження доступу до новітніх технологій або встановлення технологічної залежності в інформаційній сфері, акти інформаційної експансії і встановлення монополії над національними ІКТ, інфраструктурами іншої держави з метою створення умов залежності і контролю.

19.12.2001р. ГА ООН проголосувала також резолюцію 56/121 під загальною назвою „Боротьба зі злочинним використанням інформаційних технологій” в якій запропоновано різні заходи боротьби з тероризмом у зв’язку з використанням терористичними та злочинними угрупованнями високих технологій. Серед заходів: удосконалення національних законодавств у сфері боротьби з кіберзлочинністю; співробітництво правоохоронних органів у разі транскордонного злочинного використання ІКТ; обмін інформацією щодо проблем боротьби із злочинним використанням ІКТ; правовий захист конфіденційності, цілісності і доступності даних; захист комп’ютерних систем від несанкціонованого втручання; покарання за неправомірне зловживання ІКТ; режим взаємодопомоги у розслідуванні злочинів з ІКТ; інформування громадськості щодо попередження злочинів; вдосконалення ІКТ з превентивною складовою; необхідність захисту основних прав і свобод приватного життя.

57 сесія ГА ООН на підставі Доповіді Генерального Секретаря та представника Першого комітету М. Самсара (Туреччина), посилаючись на попередні резолюції з питань ролі науки і техніки в контексті міжнародної безпеки, підкреслюючи значний прогрес у розробці та впровадженні високих технологій, відзначаючи, що бачить у цьому процесі широкі позитивні можливості взаємодії держав задля підвищення інтелектуального потенціалу людства і обміну інформації у глобальному співтоваристві, підтвердила важливість проблеми міжнародної інформаційної безпеки і ухвалила Резолюцію 57/53 (А/RES/57/53) від 22.11.2002р. про необхідність обговорення існуючих та потенційних загроз у сфері інформаційної безпеки, можливі заходи з їх попередження, а також дослідження міжнародних концепцій на рівні урядових експертів з цієї проблеми. У додатку (відповідь Уряду Гватемали) запропоновано заходи на національному рівні, пов’язані з правовим забезпеченням інформаційної безпеки (при передачі інформації сучасними ІКТ-мережами, порушені зв’язку, модифікації і заміни інформації), для чого у Кримінальний кодекс внесено зміни до ст. 295, 274, 274 „К”, 274 „Д”, 274 „Е”, 274 „F”, 274 „G” Кримінального кодексу країни за такі порушення, як „порушення зв’язку”, „порушення авторських і суміжних прав”, „збирання забороненої (конфіденційної) інформації”, „маніпулювання інформацією”, „злочинні програми”, тощо. Разом з тим гарантовано свободу слова та обміну інформацією, невтручання у приватні бази даних, заборони цензури відповідно до ст. 13 Американської конвенції про права людини.

У розвиток резолюцій про „Досягнення ІКТ у контексті міжнародної безпеки” ГА ООН ухвалила резолюцію 57/239 від 31.01.2003р. „Створення глобальної культури кібербезпеки”, до преамбули якої увійшли посилання на резолюції ГА ООН з міжнародної інформаційної безпеки і боротьби із злочинним використанням ІКТ, що підкреслює багатогранність проблеми інформаційної безпеки і наявність тісного зв’язку між її різними аспектами. У резолюції, зокрема, йдеться про те, що кібербезпека залежить не тільки від дій державних чи правоохоронних органів, а й превентивних заходів і підтримки всього світового співтовариства. У додатку до резолюції міститься перелік „складових”, на основі яких має забезпечуватися безпека мереж – від етики і демократії до відповідальності, реагування, оцінки ризиків та управління безпекою – і які сприятимуть державам-членам ООН у розробці міжнародно-правової бази інформаційного суспільства.

58 (18.12.2003) та 59 (2004) сесії ГА ООН закликали держави-члени сприяти і в подальшому розробці міжнародних документів у сфері міжнародної безпеки з метою включення цих норм до національних законодавств і регулювання міжнародних відносин в інформаційній сфері.

В обговоренні було підкреслено, що наукові та технологічні розробки потребують міжнародного контролю за їх поширенням, оскільки можуть бути застосовані як в мирних, так і військових цілях, водночас підтримуючи вільний розвиток науки та вільний обмін науковою інформацією. Проблемним є забезпечення вільного доступу до новітніх технологій в інформаційній сфері в умовах необхідності інформаційної безпеки та запобігання тероризму.

Міжнародне співтовариство зацікавлене в поширенні та використанні ІКТ та технологічних інновацій, бо це впливає на інтереси всього міжнародного співтовариства і вимагає максимальної ефективності дій всієї світової спільноти.

ІКТ, зазначається у резолюціях, створюють принципово нові моделі діяльності в науці, глобальному управлінні, проектуванні, медицині, валютно-банківських операціях, стають вирішальним чинником трудових ресурсів та трудового потенціалу, стрімкого зростання творчої праці. Саме ІКТ-технології забезпечують соціальні економічні, правові, культурні і технологічні умови зберігання та активізації нових ідей та їх широкого використання.\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*60 сесія

Регіональні інститути і форуми також відіграють значну роль у зміцненні програми колективної безпеки. На регіональному рівні можуть конкретизуватися та розвиватися принципи і норми міжнародного права у сфері інформаційного співробітництва, зокрема на базі таких організацій, як Рада Європи, Європейський Союз, ОБСЄ, НАТО. В документах цих організацій викладені основні принципи міжнародного права - суверенна рівність держав, незастосування сили або загрози силою, непорушність кордонів, територіальна цілісність, невтручання у внутрішні справи держав, захист основних прав і свобод, співробітництво держав в галузі науки і техніки, гуманітарній та інших сферах. Це свідчить про те, що на регіональному рівні можливий розвиток важливих принципів міжнародного права і розробка заходів, які можуть стати складовою міжнародної інформаційної безпеки.

Документи регіонального характеру з інформаційної безпеки представлені рекомендаціями Ради Європи, директивами та резолюціями ЄС, конвенціями європейського рівня, рішеннями і актами НАТО та ОБСЄ.\*\*\*

# Список використаних джерел

1. резолюція про досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки R53/70 (4.01.99)

а) Доповідь 1 Комітету - „Роль науки і техніки в контексті міжнародної безпеки і роззброєння” Д а /53/579 (16.11.1998)

б) Доповідь Генсека ООН а/53/202 - ?

2. резолюція „Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки” R 54149 (23.12.1999)

а) Доповідь 1 Комітету а/54/558

б) Доповідь Генсека а/54/213 (9.11.1999)

в) \*\*\*\*\*\*\*\*\*\*\*\*\* справ та руху \*\*\*\* 23.09.1999?

3. Резолюція „Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки” R 55/28 (20.12.2000)

а) доповідь 1 Комітету а/55/554, а/55/68 (8.11.2000)

б) доповідь Генсека а/55/69, а/55/140

4. Досягнення у сфері інформатизації і телекомунікацій 56/69, 2001 14.11.2001. доповідь 1 Комітету (а/56/533)

а) Резолюція ГАООН „Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки” А/56/19 (7.01.2002)

б) Доповідь Генсека „Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки” А/56/164 (3.08.2001)

в) Доповідь Генсека „Права людини і тероризм” А/56/150 (17.08.2001)

5) Резолюція „Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки” по доповіді 1 комітету А/57/505 (30.12.2002)

а) Доповідь 1 Комітету „Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки” А/57/505 (7.12.2002)

б) Доповідь Генсека ООН „Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки” А/57/166 (2.08.2002)

6) Резолюція а/RES/57/239 “Створення глобальної культури кібернетики” 31.01.2003

а)Доповідь 2 Комітету а/57/529/add.3

7) Резолюція ГАООН „Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки” А/58/32 (18.12.2003)

а) Доповідь 1 Комітету А/58/457

8) 2004

9) 2005

Право ІБ РЄ

1. Конвенція Ради Європи з кіберзлочинності (23.11.2003)
2. Додатковий Протокол до Конвенції РЄ з кіберзлочинності з питань криміналізації актів расизму або ксенофобії, що здійснюється через комп’ютерні мережі (28.01.2003)
3. Рекомендація №R (95)13 РЄ з проблем кримінального процедурного права, пов’язаного з інформаційними технологіями
4. Конвенція про захист осіб щодо автоматизованої обробки даних персонального характеру (28.01.1981\*)
5. R №(81) 1 (23.01.1981) про загальні правила для автоматизованих банків медичних даних\*
6. R №(83) 10 (23.09.1993) про персональні дані, що використовуються для наукових досліджень і систем
7. R №(81) 1 (23.01.1986) соціальне забезпечення

Право ІБ ЄС

1. Директива (1991) 91/250 про правову охорону програм для ЕОМ
2. Про захист фізичних осіб при обробці персональних даних і вільне переміщення таких даних /994/017
3. Про правовий захист баз даних (1996) 96/9
4. Резолюція про оперативні записи правоохоронних органів щодо суспільних телекомунікаційних мереж та послуг 2001
5. Резолюція РЄ ЄС від 28.01.2002 щодо спільного підходу та спеціальної діяльності у сфері безпеки електронної мережі та інформаційної безпеки С/43/02 (2002)

Регіональні документи

1. Рекомендація R №(95) 13 RМ РЄ з проблем кримінального процедурного права, пов’язаного з ІКТ.
2. Конвенція РЄ з кіберзлочинності (23.11.2001)
3. Додатковий протокол до Конвенції РЄ з кіберзлочинності з питань криміналізації актів расизму або ксенофобії, що здійснюється через комп’ютерні мережі
4. Резолюція РЄ ЄС (30.09.2002) №2002/836/ЄС про програму 2002-2006 досліджень з проблем кіберзлочинності
5. Резолюція Ради ЄС (28.01.2002) щодо спільних підходів та спільної діяльності у сфері безпеки електронної мережі та інформаційної безпеки (2002/С43/02)