УДК 343.9:354.42/.44

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 посилення інформаційної безпеки та протидії організованій злочинності

В статті розглянуто окремі аспекти кібербезпеки та міжнародних ініціатив стосовно майбутнього кіберпростору. Наведено види злочинів, які вчиняються організованими кримінальними угрупуваннями з використанням комп'ютерних мереж, а також форми використання інформаційних потоків для здійснення деструктивного впливу.

Ключові слова: кіберпростір, кібербезпека, організовані злочинні угрупування, міжнародні ініціативи, майбутнє кіберпростору.

Постановка проблеми. Подальше просування України на шляху європейської інтеграції тісно пов'язане з необхідністю подальшого розвитку інформаційного середовища країни, тобто кіберпростору. Для успішного вирішення цих завдань принципового значення набуває широке впровадження в усі сфери життя новітніх телекомунікаційних та інформаційних технологій. Адже сьогодні без комп'ютеризації не можна уявити практично жодної галузі діяльності людини: від проектування споруд чи механізмів, до забезпечення безперебійного функціонування державних інституцій і галузей, які складають сферу національної безпеки країни.

Але поряд з безсумнівними перевагами, пов'язаними з інтеграцією у світовий інформаційний простір, існує немало чинників, які складають реальну загрозу державним інтересам. Зокрема, стрімке розширення світового кіберпростору, завдяки бурхливому розвитку всесвітньої мережі Інтернет, і глобалізація у цій сфері означає, що значна частина

об'єктів інфраструктури будь-якої країни може стати предметом посягань зловмисників.

Це, безумовно, стосується і України. Проте процес її формування як ефективної європейської держави передбачає подолання наявних політичних, економічних і соціальних проблем. Частина з них пов'язана з наявністю організованої злочинності, яка останнім часом зазнала суттєвих змін. Дедалі частіше кримінальні угрупування використовують найновіші досягнення науково-технічного прогресу для дестабілізації криміногенної обстановки і посилення свого впливу на економічні та соціальні процеси. Таким чином, надзвичайно високі темпи інформатизації сучасного суспільства, які охоплюють практично всі сфери виробничої діяльності, фінансів, науки та управління, а також життєві інтереси окремих громадян, створили умови для виникнення нових об'єктів протиправних посягань з боку організованих злочинних угрупувань.

І якщо сьогодні, в основному, зберігається і підтримується певний стратегічний баланс між країнами у сфері озброєнь та армій, то залишається практично неконтрольованим процес розширення можливостей для вчинення, деструктивних дій через кіберпростір. Причому, число суб'єктів, здатних негативно впливати на внутрішнє життя країни та її міжнародний імідж, невпинно зростає. Поряд з організованими злочинними угрупуваннями, надзвичайно велику загрозу національним інтересам складають екстремістські та терористичні організації, зловмисники-індивідуали та спеціальні служби окремих держав.

Саме ці обставини виносять проблему посилення кібернетичної безпеки України в число першочергових. І ігнорування цієї загрози чи зволікання у пошуку й подальшій реалізації ефективних способів протидії різного роду викликам у сфері кібербезпеки може призвести до руйнівних наслідків у життєдіяльності людини, суспільства, держави. Все це потребує формування послідовної державної політики та прийняття на вищому рівні національної програми, спрямованої на забезпечення дієвої протидії кібернетичним загрозам.

Аналіз останніх досліджень і публікацій. Дослідження тематики, пов'язаної з проблемами кібербезпеки, здійснює багато вітчизняних та зарубіжних учених і практиків. Зокрема, це В. М. Бутузов, В. Д. Гавловський, Д. В. Дубов, М. В. Карчевський, В. Г. Поліщук, О. О. Поляруш, В. П. Шеломенцев, О. М. Юрченко та інші. В їх дослідженнях відмічається, що існуючий стан кібербезпеки в Україні ще не відповідає її національним інтересам. Тому назріла гостра необхідність розробки та вжиття комплексу заходів, спрямованих на посилення регулятивних і попереджувальних функцій держави для формування безпечного інформаційного середовища і розширення міжнародного співробітництва у цій сфері діяльності.

Метою статті є спроба проаналізувати використання організованими кримінальними угрупуваннями сучасного інформаційного простору в учиненні окремих видів злочинів і визначення шляхів протидії кримінальним та іншим протиправним проявам у цій сфері. Також передбачається розглянути міжнародні ініціативи щодо регулювання майбутнього кіберпростору.

Виклад основного матеріалу. Постійний розвиток інформатизації суспільства створює надзвичайно широкі можливості для використання кіберпростору. А оскільки сам він не має обмежень і державних кордонів, то це робить його привабливим для використання, зокрема, різного роду злочинними організаціями.

В останні роки спостерігається різка активізація діяльності різного роду організованих кримінальних угрупувань, а також екстремістських і терористичних організацій, які втручаються в інформаційний простір для реалізації своїх, далеких від благородних, намірів. Це і вчинення злочинів у різних сферах господарювання та управління, і хакерські атаки на урядові сайти і портали та банківські бази даних, і спроби дестабілізувати діяльність об'єктів критичної інфраструктури та суспільно-політичну обстановку в певному регіоні чи державі в цілому тощо. Все більшого поширення набуває кібершпигунство [1]. У багатьох випадках кібератаки чітко вмотивовані. Одні з них переслідують суто економічні чи фінансові інтереси, або спрямовані на завдання людям фізичної шкоди, інші – мають яскраво виражене політичне забарвлення і спрямовані на посилення деструктивних настроїв у суспільстві [2]. Немало випадків, коли кіберпростір використовується з хуліганських спонукань.

Варто підкреслити, що інфраструктура, яка забезпечує формування і використання інформаційного простору, залишається надзвичайно уразливою до зовнішнього втручання та має низьку захищеність від несанкціонованого впливу. Паралельно зі створенням технологій і програм, покликаних захистити мережу від зловмисників, активно ведуться новітні інноваційні розробки для нападу і проникнення в інформаційні системи, які користуються широким попитом у різного роду деструктивних сил. І такому розвитку подій, здебільшого, не вдається ефективно протистояти.

Комп'ютерні технології все частіше порівнюють зі зброєю масового ураження XXI-го століття. Іншими словами, кіберсвіт створює багато можливостей для зловмисних дій. А значить необхідно передбачати, що в майбутньому інциденти, пов'язані з використанням кіберпростру, будуть поширюватись.

Сьогодні питання щодо регулювання діяльності суб'єктів в інформаційному середовищі знаходяться на порядку денному практично кожної держави [3]. У першу чергу, це пов'язане зі збільшенням кількості протиправних проявів у цій сфері.

Практика свідчить, що сфери інтересів організованих злочинних співтовариств надзвичайно різнопланові. Це і реалізація схем, спрямованих на "відмивання брудних грошей", і махінації в кредитно-банківській сфері, і розповсюдження дезінформації, і спроби вивести із ладу автоматизовані системи в галузях, на які розповсюджуються їх інтереси. Можливості мережі Інтернет дозволили останнім часом суттєво "удосконалити" способи організованої торгівлі наркотиками. Крім цього, через інформаційну мережу криміналітет отримав широкі можливості для використання досвіду кваліфікованих фахівців, які добре знайомі з наявними прогалинами в національних і міжнародному законодавствах, розуміються на реалізації різного роду фінансових схем. Здебільшого подібна "співпраця" здійснюється в умовах конспіративності, що практично зводить нанівець можливість викриття таких оборудок.

Зазвичай, кіберзлочини дедалі частіше вчиняються з територій держав, де практично відсутні закони, спрямовані на боротьбу з кіберзлочинністю, чи надзвичайно мала вірогідність їх застосування. Це забезпечує значно ширші й безпечніші можливості кримінальним співтовариствам для реалізації злочинних намірів і створює їм умови для уникнення проблем, пов'язаних з діяльністю правоохоронних органів. У результаті створюються ідеальні умови для отримання максимальних прибутків при мінімальному ризику.

За допомогою мережі Інтернет постійно "модернізуються" способи вчинення різного роду шахрайств. А використання організованою злочинністю таких традиційних форм "впливу", як застосування сили і залякування, створило підґрунтя для виникнення нового виду злочинної діяльності – кібервимагання. Здебільшого воно поєднується із загрозою знищення інформації, відомостей та комунікаційних систем [1]. При цьому активно використовується одна з унікальних особливостей мережі Інтернет – її анонімність, що створює ідеальні умови для вчинення подібних протиправних дій.

Як свідчить практика, організована злочинність практично миттєво пристосовується до будь-яких змін у суспільному житті. Тобто, є всі підстави вважати, що в майбутньому кримінальні тенденції в мережі Інтернет будуть розширюватись і удосконалюватись. Отже, подальший розвиток і посилення криміналізації інформаційного середовища та його використання для вчинення інших деструктивних дій, які загрожують національним інтересам країни, можуть мати надзвичайно тяжкі наслідки. Тому вкрай важливо навчитись оперативно виявляти способи вчинення злочинів у кіберпросторі сьогодні та прогнозувати найбільш криміногенні напрями його розвитку в перспективі. Необхідна негайна та адекватна реакція влади на ці виклики. Причому вона має бути комплексною, всебічною і носити міжнародний характер.

Варто звернути увагу і на те, що діяльність правоохоронних структур по розслідуванню злочинів, пов'язаних з використанням кіберпростору, особливо, які вчинені на території декількох держав, має низьку ефективність. Головна причина в тому, що існують суттєві розбіжності в національних законодавствах, які регулюють правові відносини у цій сфері, а також відсутність єдиних підходів до шляхів вирішення цієї проблеми у світовому співтоваристві.

Тому необхідні постійна співпраця та взаєморозуміння між країнами у протидії новим викликам сучасності, одним з яких є кіберзлочиннність. Причому, така взаємодія має здійснюватись як на найвищому державному рівні, так і шляхом об'єднання зусиль відповідних державних інституцій з представниками неурядових організацій, що працюють у сфері інформаційно-комунікаційних технологій.

Сьогодні більшістю держав світу прийняті відповідні законодавчі акти та створені спеціальні підрозділи в правоохоронних і військових відомствах, покликані протидіяти кіберзагрозам [4]. Проте, відсутність на міжнародному рівні єдиних підходів у сфері кібербезпеки змушує активно вести пошук способів захисту інформаційного простору, які б задовольняли інтереси кожної країни. Така спроба була зроблена у 2001 році Радою Європи, яка прийняла Конвенцію про кіберзлочинність [5]. Проте це не повною мірою вирішує дану проблему. До того ж далеко не всі країни, що входять до Ради Європи, ратифікували даний документ.

Тому останнім часом низкою держав, перш за все, такими, що претендують на домінування в геополітичному просторі (зокрема, США, КНР та Російська Федерація) запропоновано низку ініціатив щодо впорядкування питань кібербезпеки на глобальному рівні. Ними вносяться відповідні пропозиції, проводяться дискусії та експертні консультації з питань захисту інформаційних мереж. Перш за все, мова йде про захист інформації, яка є власністю держави, має високий рівень таємності чи конфіденційності й неправомірне використання якої може нанести шкоду національним інтересам країни.

Так, зовнішньополітична ініціатива США щодо майбутнього кіберпростору, яка викладена в Міжнародній стратегії для кіберпростору, передбачає його **відкритість і сумісність,** що сприятиме розширенню доступу до інформаційного простору значно більшій кількості користувачів [6]. При цьому мають забезпечуватись **безпека і надійність** збереження даних, що, в свою чергу, передбачає встановлення міжнародних технічних стандартів і узгоджених міжнародних норм щодо поведінки держав у цій сфері. Також США проголосили необхідність вироблення єдиних правил поведінки у кіберпросторі з метою забезпечення **стабільності через норми.**

Крім зазначених засад, у Стратегії визначено орієнтовні пріоритети щодо поведінки держав стосовно мережі Інтернет і деяких проблемних питань її діяльності. Зокрема, вони (держави) повинні:

– дотримуватись основних свобод (свободи слова, зібрань тощо, що стає дедалі актуальніше для всесвітньої мережі);

– поважати право власності (зокрема, авторські права, патенти, торгову таємницю, право на інтелектуальну власність тощо);

– не допускати втручання у приватне життя (тобто, захищати користувачів мережі Інтернет від зазіхань на їх особисті інтереси);

– забезпечувати захист від злочинів (мова йде про розробку і прийняття країнами законодавчих актів та юридичну практику, які б не давали можливості зловмисникам діяти і переховуватись на їх територіях);

– мати право на самозахист (це означає, що відповідно до Статуту ООН держави можуть застосовувати санкції, включаючи військові засоби, у відповідь на агресивні дії у кіберпросторі);

– сприяти глобальній сумісності (тобто, вживати необхідних заходів для забезпечення доступу та зручності використання мережі Інтернет з метою залучення до неї якомога більшої кількості користувачів);

– підтримувати мережеву стабільність (іншими словами, забезпечувати свободу розповсюдження інформації на своїй території та не втручатись у роботу структур, пов'язаних з міжнародною діяльністю системи);

– вживати заходів щодо забезпечення надійного доступу (це означає, що не можуть створюватись штучні перешкоди для доступу громадян до всесвітньої мережі);

– формувати багатостороннє управління (тобто, управління мережею Інтернет не має обмежуватись лише на рівні урядових структур, але й здійснюватись іншими власниками Інтернет-ресурсу);

– приділяти особливу увагу кібербезпеці (мається на увазі усвідомлення своєї відповідальності за надійність і безпечність роботи національної мережі).

Наскільки успішним буде втілення запропонованої Стратегії у життя – покаже час. Однак, низка викладених у ній позицій є досить неоднозначними і може розцінюватись частиною держав як спроба розширити вплив США на їх внутрішні національні процеси.

Альтернативне бачення принципів функціонування кіберпростору висловлює й Російська Федерація. Вона, зокрема, вважає, що поняття кібербезпеки повинне включати спроби використання сучасних інформаційних технологій для деструктивного впливу на соціальні, політичні, економічні та військові процеси в країні та їх наслідки.

В розробленій Росією Концепції забезпечення міжнародної інформаційної безпеки підкреслюється суверенне право держави формувати власну політику щодо мережі Інтернет і використання кіберпрос-

тору [7]. У зв'язку з цим розширений перелік загроз у сфері міжнародної інформаційної безпеки, зокрема мова йде про неприпустимість:

– використання інформаційних ресурсів іншої держави без попереднього узгодження з державою, в інформаційному просторі якої знаходяться ці ресурси;

– діяльності, спрямованої через інформаційний простір на підрив політичної, економічної та соціальної систем певної держави, здійснення психологічного тиску на населення з метою дестабілізації суспільства;

– дезінформації, приховування інформації та інших спроб маніпулювання інформаційними потоками та інформаційним простором інших держав з метою руйнівного впливу на психологічну і духовну сфери суспільства, традиційні культурні, етичні й естетичні цінності народу;

– протидії доступу до новітніх інформаційних технологій та штучне створення технологічної залежності будь-якої держави у сфері інформатизації;

– встановлення контролю над національними інформаційними ресурсами іншої держави.

Таким чином, у даному документі суттєво розширений перелік загроз в інформаційному просторі, що принципово відрізняє його від Конвенції про кіберзлочинність, прийнятої Радою Європи, та Міжнародної стратегії для кіберпростору, запропонованої США.

Ще один недавній документ, спрямований на регулювання діяльності держав у кіберпросторі, запропонований спільно КНР, Російською Федерацією, Узбекистаном і Таджикистаном. Це – проект Правил поведінки у сфері забезпечення міжнародної інформаційної безпеки [8].

Зокрема, тут йдеться про необхідність виявлення поваги до основних прав і свобод людини, а також до історії, культури та соціального розвитку всіх країн при використанні інформаційного простору.

Також тут проголошується необхідність співпраці у боротьбі з терористичною та злочинною діяльністю, які здійснюються з використанням інформаційних технологій і підривають політичну, економічну і соціальну стабільність держав та їх культурний і духовний стан.

Крім цього, Правила мають на меті сприяти формуванню багатосторонніх і демократичних міжнародних механізмів управління мережею Інтернет, що повинно гарантувати його безпечне і стабільне функціонування.

Таким чином, зміст кожного з наведених документів щодо регулювання міжнародних відносин у кіберпросторі містить низку положень, котрі носять дискусійних характер і не сприймаються однозначно міжнародним співтовариством.

У той же час, збитки, які завдаються кіберзлочинністю, змушують шукати компроміси для формування стабільних і прозорих міжнародних відносин у спільному використанні інформаційного простору.

Тому першочерговим завданням на сучасному етапі варто вважати правове обмеження злочинної і деструктивної діяльності в кіберпросторі та розвиток міжнародної співпраці у цьому напрямі. Адже лише заходами технічного характеру кібератаки зупинити неможливо. Для вирішення цієї проблеми необхідні інтенсивна політична і правова співпраця кожної країни та міжнародних організацій, оскільки лише це може створити надійний бар'єр для недопущення та припинення різного роду порушень у кіберпросторі.

В контексті забезпечення кібербезпеки України, перш за все, мова йде про необхідність формування та уточнення національної стратегії у цій сфері. Для цього необхідно задіяти всі внутрішні можливості країни, починаючи з розробки і прийняття ефективних законів і закінчуючи створенням привабливих умов для співпраці в галузі інформаційної безпеки державних і громадських організацій та бізнес-структур. Також важливо врахувати наявний світовий досвід організації цієї роботи.

Висновки. Таким чином, необхідно зазначити, що кіберпростір відіграє в сучасних умовах значну роль у забезпеченні нормального функціонування держави та суспільства. Тому необхідність протидії кіберзагрозам, що можуть нанести шкоду національній безпеці України, потребує створення власної дієвої системи інформаційної безпеки.

Нагальним є вирішення проблеми формування цілеспрямованої державної політики у сфері кібербезпеки. Зокрема, активна робота повинна вестись у межах створення національної правової бази, що має регулювати відносини в сфері забезпечення кібербезпеки.

Однією з важливих умов вирішення цієї проблеми є створення умов для постійного, ефективного і зацікавленого співробітництва між органами державної влади та установами і організаціями, що працюють у секторі інформаційних технологій.

Більш широко повинен використовуватись міжнародний досвід протидії злочинній діяльності в кіберпросторі. Необхідно напрацювати нові підходи і правила щодо пошуку, збору та вилучення електронних доказів учинення злочинів, розробити державну програму підготовки фахівців з різних напрямів забезпечення інформаційної безпеки.

Насамкінець, Україна має активно брати участь у формуванні компромісних міжнародних рішень з проблем майбутнього кіберпростору.

Список використаних джерел

1. Ющук Е. Интернет-разведка: руководство к действию / Евгений Ющук. – Москва : Вершина, 2007. – 256 с.

2. Поляруш А. А. Информационная война против Украины: причины и социально-политические технологии / Поляруш А. А., Юрченко А. М. – К. : Изд-во "Кий", 2011. – 200 с.

3. Міжнародні політичні та правові ініціативи щодо майбутнього кіберпростору : круглий стіл, організований Нац. ін-том стратегічних досліджень спільно з Наук.-досл. центром правової інформатики НАПрН України 29 трав. 2012 р. / [Електронний ресурс] . – Режим доступу : http://www. niss. gov. ua/artikles/835/.

4. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В. М. Бутузов – К. : КИТ, 2010. – 408 с.

5. Про кіберзлочинність : Конвенція Ради Європи // Офіц. вісник України. – 2007. – № 65. – С. 107. – Ст. 2535. – Код акту 40846/2007. – 10 верес.

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

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

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

В статье рассмотрены отдельные аспекты кибербезопасности и международных инициатив относительно будущего киберпространства. Приведены виды преступлений, совершаемых организованными криминальными сообществами с использованием компьютерных сетей, а также использования информационных потоков для совершения деструктивного влияния.

The article deals with some aspects of cybersecurity and international initiatives concerning the future of cyberspace. The types of crimes, committing by the organized criminal associations with the use of the computer networks, and also use of the informative streams for the stream of the destructive influence are given.

Стаття надійшла до редакції журналу 14 червня 2012 року.