пропускної здатності міжнародних автомобільних пунктів пропуску був розроблений авторський умовний знак у вигляді стрілок різного кольору, заштрихованості та форм.

Окрім далекоглядних планів розвитку інтеграції України в європейську транспортну мережу, а, як наслідок, і економіку, логістичні карти покликані виконувати нагальні потреби вітчизняних перевізників.

Джерела та література

1. Бочаров М. К. Основы теории проектирования систем картографических знаков / М. К.Бочаров. – М. : Недра, 1966. – 186 с.
2. Востокова А. В. Оформление карт. Компьютерный дизайн : учеб. / А. А. Востокова, С. М. Кошель, Л. А. Ушакова / под ред. А. В. Востоковой. – М. : Аспект Пресс, 2002. – 288 с.
3. Гаман Н. О. Картографічне забезпечення транспортних вантажних логістичних потоків в Україні / Н. О. Гаман // Часопис картографії : зб. наук. пр. – К. : КНУ ім. Т. Шевченка, 2012. – Вип. 4. – 208 с.
4. Коваленко В. М. Вантажні автомобільні перевезення : підручник / В. М. Коваленко, В. К. Щуріхін, Н. Б. Машика. – К. : Літера ЛТД, 2006. – 304 с.
5. Про результати перевірки ефективності функціонування пунктів пропуску (прикордонних переходів) через державний кордон з Республікою Польща / Підготовлено департаментом із питань безпеки держави та правоохоронної діяльності й затверджено постановою Колегії Рахункової палати від 07.12.2004 № 27-4/. – К. : Рахункова палата України, 2005. – Вип. 3.
6. Сайт телеканалу ТВІ. Карта ганьби Укравтодору [Електронний ресурс]. – Режим доступу : http://tvi.ua/new/2013/02/15/karta_hanby_ukravtodoru.

УДК 327:[343.2/.7:004.4]

А. А. Лісайчук – студентка 5 курсу факультету міжнародних відносин Східноєвропейського національного університету імені Лесі Українки

Проблеми боротьби з кіберзлочинністю на міжнародному рівні

Роботу виконано на кафедрі країнознавства і міжнародних відносин СНУ ім. Лесі Українки
Науковий керівник: ***Н. І. Романюк*** *– кандидат географічних наук, доцент кафедри країнознавства і міжнародних відносин СНУ ім. Лесі Українки*

Розглядаються особливості кіберзлочинності як суспільно-небезпечного явища та її вплив на міжнародну безпеку. Характеризуються механізми боротьби з кіберзлочинністю на міжнародному рівні, окреслюються проблеми, які постають перед світовою спільнотою внаслідок її поширення. Визначаються перспективи зміцнення глобальної інформаційної безпеки.

Ключові слова: кіберзлочинність, Інтернет, інформаційні технології, інформаційна безпека, співробітництво.

Lisaychuk A. A. Problems of Struggling With Cybercrime at the International Level. The article reviews the features of cybercrime as socially dangerous phenomenon and its impact on international security. It characterizes mechanisms of struggling with cybercrimes at the international level, outlines the challenges faced by the international community because of their widening. The article also defines the prospects of strengthening the global information security.
Key words: cybercrime, Internet, information technology, information security, cooperation.

Розвиток інформаційних і телекомунікаційних технологій призвів до того, що сучасне суспільство значною мірою залежить від управління різними процесами за допомогою комп'ютерної техніки – електронної обробки, зберігання, доступу та передачі інформації. Використання інформаційних технологій розширює свою дію на всі нові сфери людської діяльності: від контролю за повітряним і наземним транспортом до вирішення проблем національної безпеки. Інформація як один з основних елементів цього процесу відіграє все більш істотну роль як у житті окремої людини, так і в житті всього суспільства та кожної держави. У зв'язку з цим інформаційна безпека є одним із складників національної безпеки держави.

Однак розвиток науково-технічного прогресу, пов'язаний із впровадженням сучасних інформаційних технологій, призвів до появи нових видів злочинів, зокрема, до незаконного втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж, викрадення, привласнення, вимагання комп'ютерної інформації, які узагальнені у небезпечному антисоціальному явищі, що отримало назву «кіберзлочинність» [5].

Поняття «кіберзлочинність» вперше з'явилося в американській, а потім і в іншій іноземній літературі на початку 1960-х рр. і визначалося як порушення чужих прав та інтересів стосовно автоматизованих систем обробки даних. Кіберзлочинність (англ. *cybercrime*) – це поняття, яке охоплює комп'ютерну злочинність (де комп'ютер – предмет злочину, а інформаційна безпека – об'єкт злочину) та інші зазіхання, де комп'ютер є знаряддям або способом злочину проти власності, авторських прав, громадської безпеки, моралі тощо [4].

Найбільш поширена класифікація кіберзлочинів нині ґрунтується на Конвенції Ради Європи про кіберзлочинність, що була відкрита для підписання у листопаді 2001 р. У цьому документі кіберзлочини поділяються на п'ять груп:

1) злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему);

2) злочини, пов'язані з використанням комп'ютера як засобу скоєння злочинів, а саме – для маніпуляцій з інформацією (комп'ютерне шахрайство та комп'ютерні підроблення);

3) злочини, пов'язані з контентом (змістом даних);

4) злочини, пов'язані з порушенням авторського права і суміжних прав;

5) акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж [3].

Основною проблемою боротьби зі злочинністю в мережі Інтернет є транснаціональність самої мережі й відсутність механізмів контролю, необхідних для правозастосування. Мережа Інтернет створювалася технологічно як структура без ієрархії й без якогось «ядра», зруйнувавши які можна було б паралізувати її роботу й навряд чи хтось міг уявити масштаби розвитку проекту, спочатку не призначеного для широкої аудиторії. Основною метою створення цієї мережі була стійкість до атак ззовні, й навряд чи хтось міг передбачити подальший масштаб її розвитку, її економічну та соціальну роль у майбутньому. Саме відсутність розроблених механізмів контролю мережі зсередини укупі з її доступністю й легкістю використання стало однією з глобальних проблем інформаційного співтовариства: децентралізована структура мережі та відсутність національних кордонів у

кіберпросторі зумовили можливості для росту злочинності та на роки відклали розроблення механізмів правового та соціального контролю в сфері використання інформаційних мереж для вчинення злочинів [6].

Із моменту, коли держава включається в інформаційний обмін за допомогою мережі Інтернет, безпосередньо вона та її громадяни стають уразливими для зазіхань із будь-якої точки земної кулі. Механізми контролю, запобігання та розслідування посягань у кіберпросторі дуже обмежені як соціально, так і технологічно. Як показує приклад атак на ядерне виробництво Ірану, навіть відключення особливо важливих для держави об'єктів від глобальних інформаційних мереж не захищає їх від можливих атак: вірус Stuxnet поширювався через портативні накопичувальні пристрої, що підключаються до комп'ютера через порт USB [1]. Єдиний спосіб повністю убезпечити особливо важливі об'єкти для функціонування суспільства – це повністю відключити мережу Інтернет не тільки від об'єктів захисту, а й у державі загалом. Зрозуміло, це неможливо, оскільки інформаційні технології відіграють найважливішу роль у функціонуванні суспільства.

Зі збільшенням кількості користувачів мережі Інтернет зростають такі фактори ризику: збільшується залежність суспільства від інформаційних технологій, що, у свою чергу, обумовлює його вразливість до різного роду інформаційних зазіхань; збільшується можливість використання мережі для вчинення злочинів, а також росте потенційна можливість стати жертвою використання інформаційних технологій у злочинних цілях. При цьому вчинення злочину не вимагає великих зусиль і затрат – достатньо мати комп'ютер, програмне забезпечення та підключення до інформаційної мережі. Не потрібно навіть глибоких технічних знань: існують спеціальні форуми, на яких можна придбати програмне забезпечення для вчинення злочинів, викрадені номери кредитних карт та ідентифікаційні дані користувачів, а також скористатися послугами з допомоги у здійсненні електронних розкрадань й атак на комп'ютерні системи [6].

Комп'ютерні дані можуть бути передані з однієї точки світу в іншу за кілька секунд. Більш того, практично будь-яка передача даних у мережі зазвичай включає декілька країн, оскільки інформація розбивається на частини та йде найзручнішими й доступними каналами. Контролювати передачу даних, з урахуванням їх обсягу та кількості користувачів, майже неможливо. Злочинець, потерпілий та сервер із необхідною інформацією можуть знаходитися в різних країнах і на різних континентах, що вимагає співпраці правоохоронних органів декількох країн при розслідуванні злочину.

Автоматизація збільшує ризик здійснення множинних злочинів без особливих фінансових витрат. Більш того, вона даєзмогу злочинцям акумулювати більший фінансовий прибуток шляхом розкрадання невеликих сум у тисячі користувачів, що створює проблеми виявлення злочинів (наприклад, власник банківського рахунку може просто не помітити зникнення фінансових коштів) і порушення кримінальних справ [2].

Анонімність мережі Інтернет, вразливість бездротового доступу та використання проксі–серверів істотно ускладнюють виявлення злочинців: для вчинення злочину може використовуватися «ланцюжок» серверів, злочини можуть бути вчинені шляхом виходу в Інтернет через точки загального доступу, такі, як Інтернет-кафе, технології дають змогу також отримати доступ до чужої бездротової мережі Wi–Fi. Таким чином, існує достатньо способів ускладнити розслідування злочинів.

Розслідування злочинів в інформаційних мережах зазвичай вимагає швидкого аналізу та збереження комп'ютерних даних, які дуже вразливі за своєю природою й можуть бути швидко знищені. У цій ситуації традиційні механізми правової взаємодопомоги й принцип суверенітету вимагають безліч формальних узгоджень, роблячи розслідування транснаціональних кіберзлочинів проблематичним. Також

постає питання про дотримання фундаментального принципу «nullum crimen, nulla poena sine lege» (немає злочину без вказівки на закон), коли необхідна подвійна криміналізація діяння: як у країні, з території якої діяв правопорушник, так і в державі, де знаходиться потерпілий. Різниця в криміналізації діянь, відмінності у визначенні тяжкості вчиненого діяння, особливо у сфері релігійних злочинів і злочинів проти громадського порядку значно ускладнюють процес співробітництва правоохоронних органів, іноді роблячи його неможливим [2].

Інформаційна безпека вже розглядається державами як одне з пріоритетних завдань у сфері національної безпеки та міжнародної політики. При цьому концепція інформаційної безпеки включає як захист користувачів мереж, так і захист держави загалом. Однак, оскільки жодна держава не може захистити себе, здійснюючи заходи лише на національному рівні, для комплексної протидії кіберзлочинності необхідні:

– гармонізація кримінального законодавства про кіберзлочини на міжнародному рівні;

– розробка на міжнародному рівні та імплементація в національне законодавство процесуальних стандартів, що дають змогу ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати й представляти електронні докази з урахуванням транскордонності цієї проблеми;

– налагоджене співробітництво правоохоронних органів при розслідуванні кіберзлочинів на оперативному рівні;

– механізм вирішення юрисдикційних питань у кіберпросторі.

На сучасному етапі важливу роль у боротьбі з кіберзлочинністю відіграють спеціалізовані міжнародні угоди (наприклад, Конвенція Ради Європи про кіберзлочинність, рішення Ради Європейського Союзу, спільний проект Європейського Союзу й Міжнародного союзу електрозв'язку для держав Тихоокеанського регіону (проект ICB4PAC), проект ООН із розробки законодавства у сфері кіберзлочинності для країн Африки (проект ESCWA), однак вони не є за своєю суттю універсальними міжнародними інструментами, незважаючи на те, що деякі з них вийшли за своїм впливом далеко за межі регіону, в якому вони були прийняті.

Таким чином, кіберзлочинність є порівняно новим видом суспільно небезпечних діянь, проте на відміну від традиційних крадіжок і шахрайства, вона постійно удосконалюється та йде в ногу з технологіями, що, у свою чергу, ускладнює виявлення та протидію зазначеним протиправним діям. Ефективний контроль за кіберзлочинністю вимагає більш інтенсивного міжнародного співробітництва, ніж існуючі заходи по боротьбі з будь-якими іншими формами транснаціональної злочинності.

Джерела та література

1. Біблійна Естер і кіберверсія війни з Іраном // InoPressa. – 2010. – 10 жовтня [Електронний ресурс]. – Режим доступу : http://txt.newsru.ua/press/01oct2010/ cyber.html

2. Киберпреступность набирает обороты с развитием безналичных платежей // Экономическая аналитика. – 2013. – 17 мая [Электронный ресурс] – Режим доступа : http://ea.vuk.com.ua/2013/05/17/киберпреступность–набирает–обороты

3. Номоконов В. А. Киберпреступность: прогнозы и проблемы борьбы / В. А. Номоконов, Т. Л. Тропина // Библиотека криминалиста. – 2013. – № 5. – С. 148–160.

4. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби / Н. В. Савчук // Теоретичні та прикладні питання економіки : зб. наук. пр. – К. : Вид.-поліграф. центр «Київ. ун-т», 2009. – Вип. 19. – С. 338–342.

5. Шакирова З. Х. Киберпреступность как масштабная проблема / З. Х. Шакирова // Современные научные исследования и инновации. – 2013. – № 8 [Электронный ресурс]. – Режим доступа : http://web.snauka.ru/issues/2013/08/25764

6. Ben–Itzhak Y. Organized Cybercrime / Y. Ben–Itzhak // ISSA Journal. – 2008. – October [Electronic source]. – Access mode : https://dev.issa.org/Library/Journals/ 2008/October/Ben–Itzhak–Organized%20Cybercrime.pdf.

УДК 001.92:32:355.4

Ю. В. Сидор – студентка 4 курсу факультету міжнародних відносин Східноєвропейського національного університету імені Лесі Українки

Інформаційні війни як виклик міжнародній безпеці

Роботу виконано на кафедрі країнознавства і міжнародних відносин СНУ ім. Лесі Українки
*Науковий керівник: **Н. І. Романюк** – кандидат географічних наук, доцент кафедри країнознавства і міжнародних відносин СНУ ім. Лесі Українки*

У статті розкрито поняття «інформаційна війна», її основні форми прояву. Проаналізовано вплив інформаційних війн на міжнародну безпеку. Наведено приклади інформаційних війн у світі. Визначено засоби захисту міжнародних відносин від інформаційних війн.

Ключові слова: інформаційна війна, міжнародна безпека, глобалізація, міжнародні відносини, інформаційне суспільство.

Sydor Y. V. Information Wars as a Challenge to International Security. The article deals with the concept of «information warfare», its main forms of expression. Impact of information warfare on international security is analysed. Examples of information wars in the world are considered. Means of international security protection against information war are defined.

Key words: information warfare, international security, globalization, international relations, information society.

Актуальність теми зумовлена тим, що протягом всього існування світ зазнав різноманітних змін, які мали як позитивні, так і негативні наслідки. Міжнародні відносини вступили в еру нової постбіполярної системи. Вона є результатом світового прогресу та активних глобалізаційних процесів. Суспільство увійшло в сучасну інформаційну епоху й, разом із тим, отримало нові загрози для власної безпеки як індивідуальної, так і міжнародної. XXI ст., без вагань, можна назвати «століттям інформаційного прориву», адже в цей час інформація набула неабиякого статусу на всій планеті Земля.

Позитивними сторонами використання інформації є науково-технічний прогрес, розвиток інноваційних технологій, широка база інформаційних ресурсів та задоволення інформаційних потреб суспільства. На жаль, інформацію почали використовувати як засіб маніпулювання громадською думкою та спосіб деморалізації суспільства. Цей негативний процес і призвів до нового явища у міжнародних відносинах, яке отримало назву «інформаційні війни».