Список бібліографічних посилань

1. Торгівля людьми в Україні. Оцінка заходів, спрямованих на протидію. ЮНІСЕФ, ОБСЄ, АМР США, Британська Рада. Київ. 2004. 247 с.
2. Кушнір О. Міжнародні стандарти протидії торгівлі людьми // Глобальна організація союзницького лідерства. URL: http://goal-int.org/mizhnarodni-standarti-protidii-torgivlilyudmi/ (дата звернення: 30.10.2018).
3. International Agreement for the Suppression of the «White Slave Traffic». 18 May 1904, 35 Stat. 1979, 1 L.N.T.S. 83, entered into force 18 July 1905 // Human Rights Library / University Of Minnesota. URL: http://www1.umn.edu/humanrts/instree/whiteslavetraffic1904.html (дата звернення: 30.10.2018).
4. Конвенція про боротьбу з торгівлею людьми і з експлуатацією проституції третіми особами від 02 грудня 1949 р. // БД «Законодавство України» // ВР України. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=995_162 (дата звернення: 30.10.2018).
5. Протокол про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї, прийнятий резолюцією 55/25 Генеральної Асамблеї ООН від 15 листопада 2000 р. // БД «Законодавство України» // ВР України. URL: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=995_791 (дата звернення: 30.10.2018).ч’

Одержано 30.10.2018

УДК 004.77

Максим Володимирович КОРЖОВ,
курсант 1 курсу групи Ф4-102 факультету № 4 (кіберполіції)
Харківського національного університету внутрішніх справ

СВІТОВИЙ ДОСВІД БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Вступ і постановка проблеми. Розвиток інформаційних та телекомунікаційних технологій призвів до того, що сучасне суспільство у значній мірі залежить від управління різними процесами за допомогою комп’ютерної техніки – електронної обробки, зберігання, доступу і 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 даного процесу, відіграє все більш істотну роль як у житті окремої людини, так і в житті всього суспільства і кожної держави. Становлення інформаційного суспільства має як безсумнівні позитивні, так і певні негативні наслідки. З одного боку, пришвидшилася передача інформації великого обсягу, прискорились її обробка та впровадження. З іншого – серйозне занепокоєння викликає поширення фактів протизаконного збору і використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання

інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків та баз даних, порушення технологій обробки інформації, запуск програм-вірусів, знищення та модифікація даних у інформаційних системах, перехоплення інформації в технічних каналах її витоку, маніпулювання суспільною та індивідуальною свідомістю тощо. Перетворення суспільства в інформаційне змінив статус інформації. На сьогодні вона може бути як засобом забезпечення безпеки, так і загрозою та небезпекою. У зв'язку з цим інформаційна безпека є однією зі складових національної безпеки держави.

Показується, що сформована в світі ситуація з кіберзлочинністю, вимагає постійного удосконалення методів боротьби з кіберзлочинами та побудову моделі, спрямованої на забезпечення кібербезпеки країни. Для покращення співпраці передбачено створення сторонами на національному рівні органу для здійснення контактів цілодобово з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних із комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення. Така допомога включає в себе сприяння або, якщо це дозволяється внутрішньодержавним законодавством і практикою, пряме: a) надання технічних порад; b) збереження даних відповідно до статей 29 («Термінове збереження комп'ютерних даних, які зберігаються») і 30 («Термінове розкриття збережених даних про рух інформації»); c) збирання доказів, надання юридичної інформації і встановлення місцезнаходження підозрюваних. Конвенцією встановлені також обов'язкові вимоги для врахування у законодавстві країн, які приєдналися:

– надання органам дізнання та слідства повноважень щодо видачі обов'язкових до виконання приписів про термінове фіксування та подальше зберігання комп'ютерних даних, необхідних для розкриття злочину;

–збереження провайдерськими установами даних про трафік інформації на термін до 90 днів з можливістю подальшого продовження цього строку;

– встановлення для суб'єктів, які зберігають комп'ютерні дані, зобов'язання не розголошувати факт проведення оперативно-розшукових та процесуальних дій протягом періоду, що визначається законодавством держави.

Питання боротьби з кіберзлочинністю знаходяться й у центрі уваги органів та інституцій Організації Об'єднаних Націй, зокрема Генеральної Асамблеї, Економічної і Соціальної Ради, Комісії з попередження злочинності і кримінального правосуддя, конгресів ООН з попередження злочинності і кримінального правосуддя, рішення яких потребують розробки шляхів і засобів їх вирішення

В багатьох країнах світу практикується створення спеціальних підрозділів поліції у сфері протидії кіберзлочинності, зокрема в Австралії, Бельгії, Білорусі, Великобританії, Данії, Естонії, Індії, Канаді, Малайзії, Нідерландах, Німеччині, Норвегії, Польщі, США, Швейцарії, Швеції та ін. Серед основних функцій цих підрозділів виділяють:

– моніторинг кіберпростору з метою виявлення кіберзлочинів, вірусів або шкідливого програмного забезпечення;

– здійснення оперативно-розшукових та розвідувальних заходів з метою фіксування протиправної діяльності кіберзлочинців;

– розслідування кіберзлочинів, надання методичної та практичної допомоги іншим галузевим службам і правоохоронним органам у межах своєї компетенції;

– накопичення, узагальнення та аналіз інформації про кіберзлочинність;

– профілактику кіберзлочинів за допомогою громадськості та засобів масової інформації;

– навчання працівників поліції.

Деякі зі спеціальних підрозділів поліції у сфері протидії кіберзлочинності (або їх ще називають спеціальними підрозділами щодо протидії злочинам з використанням інформаційних технологій) виконують ще й додаткові функції:

– розкриття кіберзлочинів;

– профілактики та нагляду за телекомунікаційними послугами;

– експертного дослідження доказів на електронних носіях;

– створення відповідної бази даних щодо злочинів у сфері кіберпростору та постійного її оновлення;

– надання послуг банкам щодо захисту персональної інформації клієнтів тощо.

Наприклад, в Індії підрозділи з розслідування кіберзлочинів для їх розкриття можуть залучати професійних хакерів. Слід зазначити, що під час розслідування кіберзлочинів значну увагу приділяють допомозі постраждалому у відновленні пошкодженої або втраченої інформації, вживають всі необхідні заходи для збереження доказів у справі.

У в Таліні, Естонія існує Спільний Центр передового досвіду з кіберзахисту, який був акредитований як Центр передового досвіду НАТО. Він проводить дослідження та навчання у сфері кіберзахисту. У січні 2013 року в Гаазі, Нідерланди, почав роботу Європейський центр по боротьбі з кіберзлочинністю. Збільшується чисельність підрозділів, зайнятих у системі кіберзахисту. У Великобританії створено три регіональних поліцейських кіберпідрозділу. У США оголошено про додатковий набір 1000 співробітників до спеціального департаменту кібербезпеки Управління національної безпеки (Department of Homeland Security), які будуть займатися виключно безпекою високотехнологічних систем у США.

Крім того, провідні держави світу активно беруть участь у навчаннях щодо протидії кібератакам. Військовий досвід США (Cyber Storm) та ЄС (Cyber Europe 2010), а також можливість отримання гранту від компанії Northrop Grumman доводить, що подібні програми навчання мають значний ефект для виявлення проблемних зон захисту інфраструктури, моделювання можливих інцидентів, і вироблення типових схем реагування, поліпшення міжвідомчої взаємодії. Наприклад, у Великобританії створено новий Інститут віртуальних досліджень (Virtual ResearchI nstitute) з метою забезпечення розуміння науки щодо зростаючої кількості загроз кібербезпеки. Як відомо, ще в 2011 році між США і Великобританією було укладено угоду про проведення масштабних тренінгів та програм навчання американських і європейських ІТ-експертів, спрямованих на боротьбу з терористичними ІТ-загрозами. У підписаному документі сказано, що протягом майбутніх декількох років навчання повинні пройти не менше п’яти тисяч осіб, які працюють у сфері держбезпеки.

Висновок. Україна вже сьогодні відчуває вплив кіберзлочинності, і об'єктивно зацікавлена в тому, щоб брати у цих дискусіях активну участь, оскільки міжнародний досвід у боротьбі з загрозами інформаційної безпеки є необхідним для неї як приклад у формуванні відповідної політики і побудові власної системи кібербезпеки, оскільки з керівних документів державної політики України, що визначають діяльність органів влади в інформаційній сфері визначені тільки питання безпеки; закони і основні принципи регулюють лише питання, пов'язані з новітніми інформаційними технологіями.

Одержано 02.11.2018

УДК 343.1+004

Ірина Андріївна МАНЖАЙ,
завідувач навчального відділу
Харківського економіко-правового університету

ОКРЕМІ АСПЕКТИ АМЕРИКАНСЬКОГО ДОСВІДУ ПРОТИДІЇ РОЗПОВСЮДЖЕННЮ ДИТЯЧОЇ ПОРНОГРАФІЇ В МЕРЕЖІ ІНТЕРНЕТ

Поява комп’ютерних технологій докорінно змінила людську поведінку. Передусім це стосується нових напрямків діяльності у кіберсфері. Правопорушники першими почали пристосовувати нові шаблони поведінки у кіберсфері для досягнення злочинної мети. З’явилися цілком нові види злочинів, які вимагають специфічних знань як для їх вчинення, так і для протидії. Разом з тим частину злочинного промислу було адаптовано для умов кіберпростору. Серед останніх і розповсюдження дитячої порнографії через комп’ютерні мережі.