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.

Такий спосіб є більш вигідним для злочинців, оскільки спрощує комунікацію та дозволяє використовувати різні, не надто складні, методи перешкоджання встановленню місця знаходження та особистих даних правопорушника.

Одними з перших гостроту проблеми розповсюдження дитячої порнографії через мережу Інтернет усвідомили правоохоронні органи в США. Окрім нормативно-правових заходів для подолання цього негативного явища було вжито низку організаційних заходів. Передусім було вирішено питання налагодження взаємодії та координації діяльності різних правоохоронних органів для підвищення ефективності протидії розповсюдженню дитячій порнографії.

Одним з механізмів, завдяки якому вдалося реалізувати частину описаних завдань стала робота груп протидії Інтернет злочинам проти дітей (Internet Crimes against Children – ICAC). У рамках спеціальної програми, запровадженої у 1998 році, вказані групи забезпечують взаємодію правоохоронних органів місцевого та федерального рівнів, рівня штату, а також прокуратури.

На теперішній час налічується 61 ICAC-група. Географія присутності цих груп забезпечує охоплення усієї території США. Їх основна діяльність зосереджена на протидії кіберзлочинам проти дітей, таким як розповсюдження дитячої порнографії, торгівля дітьми, розбещення неповнолітніх тощо. Правоохоронці в описаних групах регулярно проходять тренінги з питань цифрової криміналістики та розслідування описаних категорій злочинів за підтримки різних федеральних агентств. Серед таких агентств провідні ролі у протидії кіберзлочинам проти дітей відіграють ФБР, Імміграційна та митна поліція, Поштова служба.

Одним із ресурсів забезпечення описаних груп є ICACCOPS. Він дозволяє переглядати IP-адреси, з яких здійснювалося або здійснюється розповсюдження дитячої порнографії, візуалізувати їх місце розташування на мапі, здійснювати комунікацію з правоохоронцями з різних країн, проводити аналітичні дослідження та проходити тренінги. Для роботи з ресурсом ICACCOPS слід зареєструватися за адресою www.icaccops.com/users/login.aspx. Для реєстрації потрібно використовувати службову електронну поштову скриньку

Крім наведеного, для організації міжнародної взаємодії за досліджуваним напрямом використовуються можливості Віртуальних глобальних сил (Virtual Global Task Force – VGT), які за своєю сутністю є дещо подібними до європейського кіберцентру Європолу (Europol's European Cybercrime Centre – EC3).

VGT було утворено у 2003 році для координації транснаціональних розслідувань. Його діяльність охоплює правоохоронні органи Австралії, Канади, Колумбії, Нідерландів, Нової Зеландії, Філіппін, Південної Кореї, Швейцарії, ОАЕ, Великобританії та США.

Враховуючи наведене представляється доцільним використання окремих аспектів американського досвіду у вітчизняній правоохоронній практиці протидії кіберзлочинам стосовно дітей.

Одержано 26.10.2018

УДК 004.056:341.4

Володимир Георгійович ПЯДИШЕВ,
кандидат технічних наук, доцент
доцент кафедри кібербезпеки та інформаційного забезпечення
Одеського державного університету внутрішніх справ

ЗАХОДИ ЄВРОСОЮЗУ ЩОДО БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

У 2010 році ЄС встановив чотирирічний цикл політики, щоб забезпечити більший ступінь наступності у боротьбі з серйозною міжнародною та організованою злочинністю. Ця політика передбачає ефективну співпрацю правоохоронних органів, інших агентства і установ ЄС, відповідних третіх сторін. З цією метою ЄС також закликає до рішучих дій, спрямованих на боротьбу з найбільш нагальними кримінальними погрозами, з якими стикається ЄС. На своєму засіданні 18 травня 2017 року: Рада ЄС визначила пріоритети щодо боротьби з організованою і серйозною міжнародною злочинністю на період з 2018 по 2021 рік. серед них перше місце посіла кіберзлочинність, При цьому вона випередила незаконний обіг наркотиків, сприяння нелегальній імміграції, торгівлю людьми, шахрайство з акцизами і податком на додану вартість, незаконний обіг вогнепальної зброї, екологічну злочинність, кримінальну діяльність з фінансами та відмиванням коштів і шахрайство з документами [1].

У зв'язку з цим, Євросоюз приступив до всебічного розвитку заходів щодо боротьби з кіберзлочинністю.

Законодавчі заходи. Для боротьби з кіберпреступростью [2], ЄС запровадив необхідне законодавство і організував підтримку співпраці в рамках стратегії ЄС з кібербезпеки 2013 року [3].

З урахуванням зростання частоти і суворості кіберзлочинів [4], 3 жовтня 2017 року Європарламент прийняв резолюцію про боротьбу з кіберзлочинністю [5].

Члени Європарламенту, серед іншого, «засуджують будь-яке втручання до системи, здійснюване або що направляється іноземною нацією або її агентами, з метою порушення демократичного процесу іншої держави». Крім того, Європарламент підкреслює, що «підвищення обізнаності про ризики, пов'язані з кіберзлочинністю, збільшилася, але запобіжні заходи, вжиті окремими користувачами, державними установами та підприємствами, залишаються абсолютно недостатніми, в першу чергу через нестачу знань і ресурсів».