4. Разведка на основе открытых источников. URL: http://www.in4sec.com.ua/razvedka-na-osnove-otkry-ty-h-istochnikov-open-source-intelligence-osint/ (дата звернення: 29.10.2018).

Одержано 31.10.2018

УДК 341.4

Тетяна Леонідівна СИРОЇД,
доктор юридичних наук, професор,
завідувач кафедри міжнародного і європейського права
Харківського національного університету імені В. Н. Каразіна

ІНСТИТУЦІЙНИЙ МЕХАНІЗМ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ЄВРОПЕЙСЬКОГО СОЮЗУ

Задля вирішення завдань, пов'язаних з транснаціональною злочинністю складовою якої є кіберзлочинність, Європейський Союз (далі – ЄС) заснував низку спеціалізованих установ (агентств, центрів), кожна з яких є унікальним і виконує індивідуальну функцію та робить внесок у спільну справу, забезпечуючи безпеку фізичних осіб, держав-членів, органів та інституцій ЄС і їх посадових осіб. Серед таких структур чільне місце посідає Європейське поліцейське агентство (далі – Європол), яке з 2009 р. функціонує на підставі Рішення Ради ЄС (2009/371/JHA) [1].

Відповідно до ст 88 Договору про Функціонування Європейського Союзу, завданням Європолу є підтримка та зміцнення діяльності поліцейських органів та інших правоохоронних служб держав-членів, їхньої взаємної співпраці щодо запобігання та боротьби проти тяжких злочинів, що впливають на дві або більше держав-членів, тероризму та тих форм злочинів, що впливають на спільні інтереси, охоплені політикою Союзу [2], а також … торгівлею людьми, нелегальною міграцією і відмиванням брудних грошей, корупцією, комп'ютерною злочинністю, незаконною торгівлею зброєю, боєприпасами і вибуховими речовинами, незаконною торгівлею культурними цінностями, расизмом і ксенофобією, навмисним вбивством, тяжкими тілесними ушкодженнями, екологічною злочинністю, виготовлення контрафактної і піратської продукції тощо [3].

Європол здійснює такі функції: a) зібрання, збереження, обробка, аналіз інформації і даних, а також обмін інформацією і даними; b) безвідкладне повідомлення компетентним органам держав-членів через спеціальний відділ про факти, які їх зачіпають, і сповіщення про зв'язок, який констатовано між злочинами; c) сприяння розслідуванням у державах-членах, особливо, шляхом передачі національним відділам усієї необхідної інформації з цього приводу; d) звернення до компетентних органів відповідних держав-членів із запитами про порушення, проведення і координацію розслідувань і висунення пропозицій щодо створення сумісних слідчих бригад щодо

визначених справ; e) надання державам-членам інформації та допомоги в аналізі при проведенні масштабних заходів («зустрічі у верхах», міжнародні спортивні змагання тощо); f) підготовка оцінок загрози, стратегічних аналізів і загальних доповідей, які належать до його мети, оцінок загрози, що породжена організованою злочинністю; g) розробка, спільне використання і просування спеціальних знань про методи запобігання злочинності, слідчі процедури і технічні та криміналістичні методи, а також надання рекомендацій державам-членам; h) надання допомоги державам-членам у транскордонному обміні інформацією щодо операцій і досліджень, а також спільних слідчих груп, в тому числі шляхом надання оперативної, технічної та фінансової підтримки; i) забезпечує спеціалізовану підготовку та надає допомогу державам-членам в організації навчання, в тому числі шляхом надання фінансової підтримки у межах своїх завдань і відповідно до існуючих людських і бюджетних ресурсів у співпраці з Агентством Європейського союзу з підготовки кадрів для правоохоронних органів (CEPOL); j) співпрацює з органами ЄС, встановленими відповідно до розділу V Договору про функціонування ЄС і з Європейським бюро по боротьбі з шахрайством (OLAF), зокрема, шляхом обміну інформацією та надання аналітичної підтримки у сферах, що належать до їх компетенції; k) у межах визначеної мети (цілей) надає інформацію та підтримку структурам та місіям ЄС з урегулювання кризових ситуацій, створених відповідно до положень Договору про Європейський Союз; l) розвиває експертні центри Союзу, що спеціалізуються на боротьбі з певними формами злочинності, які підпадають під дію цілей Європол, зокрема, Європейський центр по боротьбі з кіберзлочинністю; m) підтримує дії держав-членів щодо запобігання та боротьби з формами злочинності, перерахованими в Додатку I Регламенту № 2016/794, вчинення яких полегшується або здійснюється з використанням Інтернету, в тому числі у співпраці з державами-членами, надаючи інформацію про інтернет-провайдерів веб-контенту в мережі Інтернет, за допомогою або за сприяння яких полегшується вчинення або вчиняються такі форми злочинності, для того щоб вони добровільно розглянули питання про сумісність інтернет-контенту з їх власними умовами [4].

Європейське бюро боротьби із шахрайством (OLAF) (далі – Бюро) створено на підставі Рішення 1999/352/ЕС, ECSC, Euratom від 28 квітня 1999 р. [5] (у подальшому в означений документ було внесено зміни на підставі Резолюції Комісії 2013/478/ЄС від 27 вересня 2013 р., Рішення Комісії (ЄС)2015/512 від 25 березня 2015 р., Рішення Комісії 2015/2418 від 18 грудня 2018 р.). Відповідно до означеного Рішення Бюро відповідає за проведення внутрішніх адміністративних розслідувань, призначених: (a) боротися з шахрайством, корупцією та іншою незаконною діяльністю, що шкодить фінансовим інтересам Союзу, (b) розслідувати серйозні факти, пов'язані з виконанням професійної діяльності, що можуть становити порушення обов'язків з

боку посадових осіб і службовців Співтовариств, які ймовірно можуть призвести до дисциплінарних і, у відповідних випадках, кримінальних проваджень або аналогічного порушення зобов'язань членами установ і органів, керівниками органів або працівниками інституцій і органів, які не підпадають під дію Положення про посадових осіб Європейських співтовариств і Умов працевлаштування інших службовців Співтовариств.

У 2013 році відбулося офіційне відкриття Європейського центру по боротьбі з кіберзлочинністю (далі – ЄСЗ). Новий підрозділ Європолу покликаний відігравати провідну роль у боротьбі з кіберзлочинністю на території Європейського Союзу. ЕС3 займається створенням оперативних і аналітичних потужностей, необхідних для забезпечення швидкого реагування на кіберзлочини, а також організацією взаємодії офіційних відомств ЄС і країн-членів з міжнародними партнерами. Мандат Центру визначає такі сфери відповідальності: боротьба зі злочинами, які вчиняються організованими злочинними групами та тягнуть за собою отримання незаконних доходів в особливо великих розмірах (шахрайство з кредитними картками або банківськими операціями); боротьба зі злочинами, що завдають серйозної шкоди жертві, зокрема з розбещенням малолітніх; боротьба з діями, спрямованими на спричинення шкоди або виведення з ладу інфраструктури та інформаційних систем ЄС.

Також Центр відповідальний за збір та обробку даних, надання інформаційної, технічної та криміналістичної підтримки відповідним підрозділам правоохоронних органів країн-членів ЄС, координацію спільних розслідувань, навчання і підготовку фахівців (у співпраці з CEPOL). Центр сприяє проведенню необхідних досліджень і створенню програмного забезпечення, опікується оцінкою і аналізом існуючих і потенційних загроз, складанням прогнозів і випуском завчасних попереджень. До сфери діяльності Центру також входить допомога суддям і прокурорам [6].

Кожен рік ЕС3 публікує оцінку загрози організованої злочинності в Інтернеті (далі – IOCTA) – її флагманський стратегічний звіт про ключові результати та виникаючі загрози та події в кіберзлочинності. IOCTA демонструє наскільки широкою і різноманітною є кіберзлочинність і як ЕС3 є ключовою частиною Європолу та відповідних заходів ЄС. ЕС3 використовує тристоронній підхід до боротьби з кіберзлочинністю: криміналістика, стратегія та операції.

Ці заходи також підтримуються групою кіберрозвідки (CIT), аналітики якої збирають та обробляють інформацію, пов'язану з кіберзлочинністю, з державних, приватних та відкритих джерел і визначають загрози та моделі, що виникають.

Спільно з ЕС3 працює Спільна цільова група по боротьбі з кіберзлочинністю (далі – J-CAT) (створена у 2014 р.), що надає допомогу у боротьбі з кіберзлочинністю всередині та за межами ЄС.

Вона розташована в Європейському центрі по боротьбі з кіберзлочинністю. Її мета полягає в тому, щоб стимулювати та координувати дії, засновані на інтелекті, з ключовими загрозами та цілями кіберзлочинності, полегшуючи спільну ідентифікацію, встановлення пріоритетів, підготовку та початок транскордонних розслідувань та операцій з боку своїх партнерів.

До компетенції J-CAT належать: високотехнологічні злочини (зокрема, (шкідливе програмне забезпечення, бет-мережі, вторгнення; сприяння скоєнню злочинів (куленепробивний хостинг, контр-антивірусні послуги, лізинг та оренда інфраструктури, відмивання грошей, включаючи віртуальні валюти); онлайн-шахрайство (онлайн-платіжні системи, кардінг, соціальна інженерія).

J-CAT складається з постійної оперативної групи офіцерів зв'язку з кібернетиками з кількох держав-членів ЄС та партнерів по співробітництву, не входячи в ЄС, які базуються в штаб-квартирі Європолу і доповнюються персоналом ЕС3 [7].

Вищеозначене свідчить, що в межах ЄС створено розгалужену інституційну систему складовою якої є органи як з широкою компетенцією у сфері протидії транснаціональній злочинності, включаючи корупцію (Європол, Європейське бюро боротьби із шахрайством), так і органи з вузько спеціалізованим напрямом у цій сфері (Європейський центр по боротьбі з кіберзлочинністю, Спільна цільова група по боротьбі з кіберзлочинністю). Виконуючи покладені на них завдання, установи забезпечують безпеку фізичних осіб, держав-членів ЄС, органів та інституцій ЄС і їх посадових осіб, що сприяє належному функціонуванню інтеграційного утворення у цілому.

Список бібліографічних посилань

1. Council Decision of 6 April 2009 establishing the European Police Office (Europol) (2009/371/JHA). URL: https://www.europol.europa.eu/publications-documents/council-decision-of-6-april-2009-establishing-european-police-office-europol.

2. Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union 2012/C 326/01. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012M/TXT.

3. Приложение. Список других тяжких форм преступности, подведомственных Европолу в соответствии с параграфом 1 статьи 4. URL: http://zakon.rada.gov.ua/laws/show/994_a78/paran623#n623.

4. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA // Official Journal of the European Union. 2016, L 135/53. P. 1–62.

5. 1999/352/EC, ECSC, Euratom: Commission Decision of 28 April 1999 establishing the European Anti-fraud Office (OLAF) (notified under document number SEC(1999) 802) Official Journal L 136, 31/05/1999 P. 0020 – 0022. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31999D0352.

6. European Cybercrime Centre. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.
7. Joint Cybercrime Action Taskforce. URL: https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce.

Одержано 02.11.2018

УДК 004.056.53

Валерій Васильович СОЛОДОВНИК,
магістр факультету № 6
Харківського національного університету внутрішніх справ

ДЕЯКІ МІЖНАРОДНІ АСПЕКТИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Останнім часом кіберзлочинність набуває світового масштабу, новітні технології перетворюють реальних злочинців в анонімних, а можливість швидкого збагачення привертає все більше людей до цієї злочинної діяльності.

За різними оцінками Інтернетом користується до 40% населення планети (тобто близько 2,5 млрд. чоловік) і при цьому, кількість інтернет-користувачів постійно зростає. Прогнозується, що ще близько 1,5 млрд. осіб отримають доступ до Інтернету в найближчі чотири роки. Популярність мережі Інтернет цілком закономірна, оскільки користувач має можливість: цілодобового доступу до значного обсягом інформації; швидкого обміну інформацією з іншими користувачами; проведення банківських, торгових, біржових операцій з будь-якого місця в зручний час і багато іншого.

Банківська система є однією зі сфер, де найбільш широко і активно використовуються сучасні можливості інформаційних технологій і мережі Інтернет. А враховуючи, що зазначені технології використовуються для грошових переказів, зазначена сфера привертає все більша увага злочинців. За оцінками деяких експертів щорічні збитки від діяльності кіберзлочинців в світовому масштабі перевищують 100 млрд. дол. США.

Підготовка та здійснення кіберзлочинів може здійснено не відходячи від «робочого місця», тобто такі злочини є доступними, оскільки комп'ютерна техніка постійно дешевшає, злочину можна здійснювати з будь-якої точки планети, в будь-якому населеному пункті, а об'єкти злочинних посягань можуть перебувати за тисячі кілометрів від злочинця. Крім того, досить складно виявити, зафіксувати і вилучити криміналістично значиму інформацію при виконанні слідчих дій для використання її в якості речового доказу.

Вищевказані особливості даного виду злочинів поряд з їх значною прибутковістю стали, безумовно, істотними перевагами в порівнянні з іншими злочинами. Питання пошуку шляхів запобігання та протидії злочинів з використанням інформаційно-комунікаційних систем вже