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

довгий час знаходяться в сфері уваги, як державних органів, так і міжнародної спільноти.

Беручи до уваги, що розвиток технологій йде швидше, ніж приймаються нормативно-правові акти, якими вони регулюються, а обсяги незаконно отриманих кіберзлочинцями коштів ростуть, необхідно на постійній основі знаходити шляхи вирішення нових завдань, пов'язаних з такими сферами, як захист даних, транскордонний доступ правоохоронних органів до даних і обмін інформацією між державними і приватними структурами.

Міжнародне співтовариство, враховуючи негативні наслідки цього явища, знаходиться в постійному пошуку заходів, які дозволяють мінімізувати загрози впливу кіберзлочинності на суспільство. Останніми роками спостерігається значна активність в ухваленні міжнародних і регіональних документів, спрямованих на протидія кіберзлочинності, які включають як обов'язкові, так і необов'язкові до виконання вимоги.

Так, в дослідженні, проведеному Управлінням Організації Об'єднаних Націй з наркотиків і злочинності на тему «Всебічне дослідження проблеми кіберзлочинності та заходів у відповідь з боку країн-учасниць, міжнародної спільноти та приватного сектора», виділено 5 груп документів, в які входять акти, розроблені в контексті або під егідою: I) Ради Європи або Європейського Союзу; II) Співдружності незалежних держав і Шанхайської організації співробітництва; III) Міжурядових африканських організацій; IV) Ліги арабських держав; V) Організації Об'єднаних Націй (далі – ООН).

Всі ці документи значною мірою доповнюють один одного, в тому числі в частині, яка стосується концепцій і підходів, описаних в Конвенції Ради Європи про кіберзлочинність, прийнятої 23 листопада 2001 року в Будапешті, Угорщина (далі – Будапештська конвенція). В даний час Будапештська конвенція є фундаментом для розробки законодавства по боротьбі з кіберзлочинами як для кожної країни окремо, так і для загальносвітового законодавства.

Будапештська Конвенція вимагає від держав: криміналізувати атаки на комп'ютерні дані і системи (тобто незаконний доступ, нелегальне перехоплення, втручання в дані, втручання в систему, зловживання пристроями), а також правопорушення з використанням комп'ютерів (підробка та шахрайство), правопорушення, пов'язані з утриманням (дитяча порнографія) та правопорушення в сфері авторських і суміжних прав; удосконалювати законодавство для того, щоб компетентні органи змогли ефективно проводити розслідування кіберзлочинів і зберігати електронні докази, включаючи термінове збереження комп'ютерних даних, термінове збереження і часткове розкриття даних про рух інформації, обшук і арешт комп'ютерних даних, збір даних про рух інформації в режимі реального часу, перехоплення даних про зміст інформації; розширювати міжнародне співробітництво з іншими країнами учасницями Конвенції через

загальні (видача, взаємна допомога, добровільне надання інформації тощо) і спеціальні заходи (термінове збереження і розкриття збережених даних про рух інформації, взаємна допомога щодо доступу до комп'ютерних даними, транскордонний доступ до комп'ютерних даних, створення цілодобових мереж тощо).

Комітет Конвенції проти кіберзлочинності (T-CY) був створений для того, щоб допомогти країнам-учасницям обмінюватися інформацією і розглядати необхідність внесення доповнень або протоколів до Конвенції.

Крім того, в 2006 році Рада Європи ініціювала Міжнародний проект по боротьбі з кіберзлочинністю, який спрямований на: сприяння країнам в питаннях вдосконалення законодавства; навчання співробітників правоохоронних органів, органів прокуратури та суддівського корпусу; зміцнення співпраці між державним і приватним сектором; вироблення заходів для захисту персональних даних, а також захисту дітей від сексуальної експлуатації та насильства.

Власна стратегія щодо вирішення проблем протидії кіберзлочинності розроблена також Європейським поліцейським відомством (Європол). В даний час Європол надає членам ЄС слідчу та аналітичну підтримку через свою систему за допомогою онлайн розслідувань і базу даних злочинів.

З січня 2013 року за сприянням Європолу почав діяльність новий Європейський центр боротьби з кіберзлочинністю (далі – ЄЦБК). Серед пріоритетів ЄЦБК – розслідування шахрайства через онлайн-сервіси, в тому числі в системі електронного банкінгу та інших видах фінансової діяльності, протидія сексуальній експлуатації дітей через Інтернет, а також розслідування інших злочинів, які зазіхають на безпеку важливої інфраструктури та інформаційних систем ЄС.

За перший рік свого існування Європейський центр боротьби з кіберзлочинністю провів дев'ятнадцять великих операцій проти шахрайства в Інтернеті, злому фінансових сайтів і поширення дитячої порнографії. В даний час ЄЦБК підтримує дев'ять проведених в рамках ЄС великих поліцейських операцій проти сексуальної експлуатації дітей в Інтернеті. Розслідуються факти поширення дитячої порнографії і її використання в цілях шантажу. ЄЦБК надає оперативну та аналітичну підтримку в 16 розслідуваннях шахрайства в платіжних мережах.

У 2013 році було розкрито три міжнародних організації шахраїв з кредитними картами. В результаті однієї з них заарештовані 29 підозрюваних, які вкрали 9 мільйонів євро у 30 тисяч власників карток. В ході ліквідації іншої мережі заарештовані 59 осіб, розкриті два підпільні цехи зчитувальних пристроїв і програмного забезпечення, вилучені фальшиві карти і готівку. Члени групи пограбували 36 тисяч власників банківських карт в 16 європейських країнах.

Третя операція була спрямована проти азіатської злочинної мережі, яка перехоплювала дані кредитних карт при купівлі авіаквитків. Дані 15 тисяч карт знайдені в вилучених у злочинців комп'ютерах. ЄЦБК координував операцію в 38 аеропортах 16 європейських країн. Заарештовано 117 осіб, виявлено їх зв'язок з іншими злочинами: наркотрафіком, торгівлею людьми, підробкою документів.

Значну роль в подоланні проблем міжнародного співпраці в сфері боротьби з кіберзлочинністю грає ООН, яка приділяє достатню увагу питанням поширення злочинів, пов'язаних з використанням інформаційних і комп'ютерних систем, і боротьби з таким злочинами.

ООН неодноразово підкреслювала транснаціональний характер кіберзлочинів і необхідність координації в світовому масштабі заходів щодо запобігання таких злочинів і їх розслідування.

У травні 2011 року Управлінням ООН з наркотиків і злочинності і Міжнародним союзом електрозв'язку було підписано угоду про боротьбу з кіберзлочинністю, спрямоване на розробку правових рамок і юридичних механізмів протидії загрозам.

З метою обмеження загроз і незахищеності в інформаційному просторі Міжнародним союзом електрозв'язку, як спеціалізованою установою ООН, розроблені: Глобальна програма кібербезпеки; Вказівки щодо захисту дітей в онлайн-середовищі; Вказівки для батьків, опікунів і вчителів щодо захисту дитини в онлайновому середовищі; Вказівки для галузі щодо захисту дитини в онлайновій середовищі; Вказівки для директивних органів щодо захисту дитини в онлайновій середовищі; Елементи для створення глобальної культури кібербезпеки.

Експертами Управління ООН з наркотиків і злочинності також відзначається, що форми міжнародного співробітництва включають видачу злочинців, надання взаємної правової допомоги, взаємне визнання іноземних судових рішень і неофіційне співробітництво між правоохоронними органами різних країн.

Крім того, нестійкий характер електронних доказів в рамках міжнародного співпраці в кримінальних питаннях в сфері кіберзлочинності вимагає своєчасного надання відповідей і наявності можливостей звертатися з проханням про проведення спеціалізованих слідчих дій, таких як збереження комп'ютерних даних.

У вересні 2014 року в Сінгапурі відбулася презентація будівлі Міжнародного центру Інтерполу з інновацій. Завдання Центру – консолідація зусиль правоохоронних органів різних країн у боротьбі з кіберзлочинністю. Функціонувати Міжнародний центр почав в 2015 року. Робота в новому Центрі сконцентрована на чотирьох основних напрямках: оперативна підтримка і сприяння розслідуванням, інновації, дослідження і комп'ютерна безпека, підготовка поліцейських кадрів, міжнародне партнерство і розвиток.

Глави країн БРІКС підписали в серпні 2018 року в ході саміту, що відбувся в Йоганнесбурзі, підсумкову декларацію про співпрацю в різних сферах. У числі іншого, в документі фігурує пункт про створення об'єднаної кіберполіції. Передбачається, що об'єднана кіберполіція буде працювати за принципом Інтерполу і мати наднаціональний характер, проте діяльність нового правоохоронного органу буде обмежуватися країнами-учасницями.

Таким чином, незважаючи на відсутність на сьогодні загальноприйнятого визначення кіберзлочину спостерігається досить широке і вичерпне розуміння його суті і способів його здійснення, а також загроз і ризиків, що дає можливість розробляти і впроваджувати заходи протидії цьому виду злочину.

Відсутність фізичного контакту з жертвою або представниками фінансової установи, а також анонімність, швидкість здійснення і невисока вартість злочину стали ключовими передумовами підвищення зацікавленості злочинців киберпростором.

Одержано 06.11.2018

УДК 65.012.8+004

Олександра Миколаївна СТАУРСЬКА,
аспірант кафедри криміналістики
факультету прокуратури та слідства
Національного університету «Одеська юридична академія»

ПРОБЛЕМИ БОРОТЬБИ ІЗ КІБЕРЗЛОЧИННІСТЮ У КОНТЕКСТІ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА

Боротьба з кіберзлочинністю неможлива без глибокого розуміння і правових проблем регулювання інформаційних мереж. Саме аналіз взаємозв`язку між технічними характеристиками мережі і зумовленими цими характеристиками правовими і соціальними труднощами, з якими стикаються законодавці та правоохоронні органи, є першим кроком до можливого вироблення механізмів адекватного реагування на розвиток і зростання кіберзлочинності.

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