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

мережі і відсутність національних кордонів у кіберпросторі зумовили можливості для зростання злочинності та на роки відклали розробку механізмів соціального та правового контролю у сфері використання інформаційних мереж для вчинення злочинів.

В останні роки інформаційні мережі розвиваються занадто швидко, щоб існуючі механізми контролю встигали реагувати на нові проблеми. Хмарна обробка даних, автоматизація атак, вразливість персональної інформації в соціальних мережах: поширення так званої «інформаційної зброї», прикладом якого є вірус Stuxnet, розроблений, на думку фахівців, для атак на ядерну промисловість Ірану, але при цьому заподіяв чималої шкоди інфраструктурі багатьох інших країн - на всі ці проблеми правове регулювання поки не може знайти адекватної відповіді.

З того моменту, держава включається в інформаційний обмін за допомогою мережі Інтернет, вона сама та її громадяни стають вразливими для посягань з точки земної кулі. Механізми контролю, запобігання та розслідування посягань у кіберпросторі дуже обмежені як соціально, так і технологічно. Наприклад, 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. 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 всій державі в цілому. Зрозуміло, це неможливо, оскільки інформаційні технології відіграють найважливішу роль у функціонуванні суспільства.

Кількість користувачів. Із збільшенням числа користувачів 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 в злочинних цілях. При цьому вчинення злочину не вимагає великих зусиль і витрат – 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, вкрадені номери кредитних карт і ідентифікаційні дані користувачів, а також скористатися послугами з допомоги в здійсненні електронних розкрадань і атак на комп`ютерні системи як в цілому, так і на окремих стадіях вчинення злочинів.

Автоматизація та швидкість використання. Комп`ютерні дані можуть бути передані з однієї точки світу в іншу за кілька секунд. Більше того, практично будь-яка передача даних у мережі зазвичай включає декілька країн, оскільки, коли інформація розбивається на частини і йде по найбільш зручним та доступним каналам. Контролювати передачу даних, з урахуванням їх обсягу та кількості

користувачів, дуже важко, якщо не неможливо. Злочинець, потерпілий, сервер з необхідною інформацією можуть перебувати в різних країнах і на різних континентах, що вимагає співпраці правоохоронних органів декількох країн при розслідуванні злочину.

Анонімність мережі Інтернет, вразливість бездротового доступу і 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 дозволяють також «зламати» доступ в чужу бездротову мережу Wi-Fi. Таким чином, існує достатньо способів ускладнити розслідування злочинів.

Проблема територіальної юрисдикції в кіберпросторі та правового співробітництва. Розслідування злочинів в інформаційних мережах зазвичай вимагає швидкого аналізу та збереження комп`ютерних даних, які дуже вразливі за своєю природою і можуть бути швидко знищені. У цій ситуації традиційні механізми правової взаємодопомоги і принцип суверенітету, одним з проявів якого є те, що тільки правоохоронні органи держави можуть проводити слідчі дії на його території, вимагають безліч формальних погоджень, роблячи розслідування транснаціональних кіберзлочинів проблематичним. Окрім співробітництва правоохоронних органів, яке вимагає тимчасових витрат і дотримання безлічі формальностей, встає також питання про дотримання фундаментального принципу nullum crimen, nulla poena sine lege, коли необхідна подвійна криміналізація діяння: як у країні, з території якої діяв правопорушник, так і в державі, де знаходиться потерпілий. Різниця у криміналізації діянь, відмінності у визначенні тяжкості вчиненого діяння, особливо в сфері релігійних злочинів і злочинів проти громадського порядку, в області нелегального контенту, в екстремістських злочинів значно ускладнюють процес співробітництва правоохоронних органів, іноді роблячи його неможливим.

Таким чином, ефективний контроль негативних явищ у кібепросторі, таких як злочинність, вимагає набагато більш інтенсивного міжнародного співробітництва, ніж існуючі заходи по боротьбі з будь-якими іншими формами транснаціональної злочинності. Саме тому окрім гармонізації кримінально-правових норм потрібна гармонізація процесуальних інструментів і вироблення нових механізмів міжнародного співробітництва. Важливу роль у боротьбі з кіберзлочинністю тому грають міжнародні угоди у відповідній області, такі, як Конвенція Ради Європи про кіберзлочинність, рішення Ради Європейського Союзу, Модельний Закон Співдружності Націй про комп`ютерні злочини 2002 р., Модельний Закон країн Карибського Басейну про кіберзлочинність (проект HIPCAR), спільний проект Європейського союзу і Міжнародного Союзу Електрозв`язку для держав Тихоокеанського регіону (проект ICB4PAC), проект ООН з розробки законодавства в галузі кіберзлочинності для країн Африки (проект ESCWA) та ін.

Всі зазначені інструменти не є за своєю суттю універсальними міжнародними інструментами, незважаючи на те, що такі угоди, як Конвенція Ради Європи, вийшли за своїм впливом далеко за рамки регіону, в якому вони були прийняті. Однак світова спільнота поки не володіє ні міжнародним органом, який спеціально займається інтернет-злочинністю, ні загальносвітовим правовим інструментом, що визначає масштаби відповідальності за відповідні злочини, і, що більш важливо – принципи співробітництва при розслідуванні протиправних діянь.

Однак, оскільки жодна держава не може захистити себе, вживаючи заходів тільки 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 дозволяють ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати і представляти електронні докази з урахуванням транскордонного проблеми;

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

– механізм вирішення юрисдикційних питань у кіберпросторі.

Висновок: Таким чином міжнародне співробітництво є ключовим моментом у ліквідації правового вакууму, існуючого між розвитком інформаційних технологій та реагуванням на них законодавства. Процес вироблення заходів на міжнародному рівні, як показує досвід, сам по собі є комплексною проблемою. Однак це єдиний шлях забезпечити безпеку користувачів і держави від електронних посягань, а також ефективно розслідувати і переслідувати кіберзлочини.

Список бібліографічних посилань

1. Біблійна Естер і кіберверсія війни з Іраном. 10 жовтня 2010 р. URL: http://txt.newsru.ua/press/01oct2010/cyber.html (дата звернення: 26.10.2018).

2. Киберпреступность набирает обороты с развитием безналичных платежей. *Экономическая аналитика.* 2013. 17 мая. URL: http://ea.vuk.com.ua/2013/05/17/киберпреступность–набирает–обороты (дата звернення: 26.10.2018).

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 // Теоретичні та прикладні питання економіки: зб. наук. праць. К. : Видавничо–поліграфічний центр «Київський університет», 2009. Вип. 19. С. 338–342.

5. Шакирова З. Х. Киберпреступность как масштабная проблема // *Современные научные исследования и инновации.* 2013. № 8. URL: http://web.snauka.ru/issues/2013/08/25764 (дата звернення: 26.10.2018).

6. Ben–Itzhak Y. Organized Cybercrime / Y. Ben–Itzhak // ISSA Journal. October 2008. URL: https://dev.issa.org/Library/Journals/2008/October/Ben–Itzhak–Organized%20Cybercrime.pdf (дата звернення: 26.10.2018).

Одержано 26.10.2018