інформації є пріоритетом з метою забезпечення належної роботи оперативних підрозділів.

Спеціальні відповідні фактори злочинності беруться до уваги правоохоронними органами з метою попередження злочину. Ідентифікація та опис факторів, пов'язаних зі злочинністю, дозволяє краще зрозуміти поточні і майбутні можливості чи перешкоди для ОЗУ. Використання факторів, пов'язаних зі злочинністю, не націлено на забезпечення повноцінного сценарію або іншого типу майбутнього аналізу, але забезпечують розуміння поточних умов і основних змін, які можуть відбутися в навколишньому середовищі. Ідентифікація та опис факторів, пов'язаних зі злочинністю, дозволяє краще зрозуміти поточні і майбутні можливості чи перешкоди для ОЗУ і сфер злочинної діяльності. Крім того, це дозволить зробити рекомендовані пріоритети більш точними і краще їх сформулювати. Дані про майбутні зміни відповідних факторів у сфері злочинності, отримані шляхом аналізу різних джерел даних, можуть допомогти визначити нові загрози сфер злочинної діяльності.

1. Кримінальний кодекс України [Текст] : Закон України від 05.04.2001 р. № 2341-III // ВВР. – 2001. – № 25-26. – Ст. 131.

2. Про оперативно-розшукову діяльність [Текст] : Закон України від 18.02.1992 р. № 2135-XII // ВВР. – 1992. – № 22. – Ст. 303.

3. Klerks P., Kop N. Societal Trends and Crime-relevant factors : An Overview for the Dutch National Threat Assessment on Organized Crime : 2008-20012 [Текст] / P. Klerks, N. Kop // Police Academy of the Netherlands. – Apeldoorn, 2008 . – P. 77.

4. Шостко О.Ю. Протидія організованій злочинності в європейських країнах : монографія / О.Ю. Шостко. – Х. : Право, 2009. – 400 с.

Шраго А.О.
ад'юнкт кафедри
оперативно-розшукової діяльності
та спеціальної техніки
факультету підготовки фахівців
для підрозділів кримінальної поліції
Дніпропетровського державного
університету внутрішніх справ

МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ ЕКСПЛУАТАЦІЇ ДІТЕЙ У МЕРЕЖІ ІНТЕРНЕТ ТА ЙОГО ВИКОРИСТАННЯ У ДІЯЛЬНОСТІ ОПЕРАТИВНИХ ТА СЛІДЧИХ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Характерною рисою сучасної кіберзлочинності є високий рівень віктимізації. Це сприяє відчуттю злочинцями безкарності й спричиненню істотної шкоди фізичним і юридичним особам. І у реальному, і у віртуальному середо-

вищі, де переважає цифрова інформація, вчиняються злочини та кіберзлочини. Складовою загальновживаного поняття «кіберзлочинність» є, зокрема, розповсюдження дитячої порнографії.

Методологічним підґрунтям нашого дослідження є праці провідних вітчизняних і зарубіжних вчених у галузі ОРД, кримінального права та процесу, криміналістики (Ю. Аленін, В. Бахін, Р. Бєлкін, І. Возгрін,), а також тих, хто безпосередньо студіював проблеми web-порнографії (А. Волобуєв, Д. Паляничко, С. Хільченко, А. Старушкевич, І. Сугаков, О. Хабаров, М. Коллінз, С. Кондраніна, С. Денисов, Р. Джинджолія) та інші.

Водночас, потребують поглибленого та системного дослідження питання наявних відмінностей у законодавстві різних країн щодо протидії цьому явищу, а також спроби пошуку дієвих юридичних механізмів, здатних врегулювати Інтернет-відносини та запобігти виникненню деструктивних аморальних явищ у формі порнографії в мережі Інтернет. У зв'язку з цим здійснимо спробу дослідити теоретичні, практичні та технічні проблеми правового регулювання проблемних питань кіберзлочинності в аспекті дитячої web-порнографії та запропонувати комплекс заходів, що дозволив би ефективно протидіяти зазначеній проблемі.

Як свідчить аналіз досвіду роботи поліції зарубіжних країн, організаційно боротьба зі злочинами у сфері високих технологій забезпечується двома основними способами: 1) покладення додаткових функцій на вже існуючі підрозділи, або 2) створення спеціалізованих галузевих служб.

Виокремлення підрозділів боротьби зі злочинами у сфері високих технологій у спеціалізовані галузеві служби запроваджено у Австралії, Бельгії, Білорусі, Великобританії, Данії, Естонії, Індії, Китаї, Нідерландах, Німеччині, Норвегії, США, Швейцарії, Швеції та ін. Заслуговує на увагу досвід Канадської асоціації провайдерів, якою розроблено Кодекс поведінки в Інтернеті в якості заходу, що дозволяє створити систему саморегулювання і не допустити передачу сумнівних матеріалів. Проте, використання системи Інтернет для розповсюдження порнографії призводить до появи нових способів боротьби зі злочинцями.

Однією з актуальних проблем протидії цим злочинам є належна та ефективна діяльність щодо виявлення у мережі Інтернет розповсюджувачів порносайтів. Так, аналіз практики протидії кіберзлочинам дозволив виокремити узагальнені способи виявлення кінцевого користувача та розповсюджувача, а також визначити наявні проблеми. Зокрема, провайдером на кожного користувача може заводитися рахунок та реєстраційний запис (account), схожий на банківський. Рахунок містить ім'я і таємний пароль користувача, а назва рахунку вважається ідентифікатором користувача (user ID) або реєстраційним ім'ям. Отже, інформація спочатку спрямовується до провайдера, а від нього – до індивідуальних користувачів. Це дозволяє відшукати конкретний комп'ютер, на який надходила інформація з порносайту.

Але розповсюдженість вірусів, що уразивши ПК, з'єднуються із порно-

сайтами і ставлять їх як стартові сторінки веб-браузера, створюють ситуацію, коли веб-браузер зберігає «заборонені» зображення на жорсткому диску. Вони зводять нанівець захисні функції, перетворюючи власника комп'ютера на об'єкт інтересу правоохоронних органів. І саме ця обставина ставить під сумнів сам механізм відстеження злочинців у подібний спосіб [1].

На наш погляд, у цьому контексті доцільним може бути дозвіл провайдерам на ініціювання зняття/вимкнення/блокування сайту, що містить відповідні факти його неправомірності, із подальшим зверненням а прийняття остаточного рішення покласти на судові органи. Таку думку підтримали опитані нами працівники підрозділів протидії кіберзлочинності (65% опитаних) та слідчих (68% опитаних), що спеціалізуються на розслідуванні кіберзлочинів.

Друга проблема, що потребує розв'язання, пов'язана з практикою анонімних передплатників (зазначають 53% оперативників та 46% слідчих), що полягає у тому, що будь-який користувач може присвоїти собі відповідне ім'я і вказати інформаційний маршрут з однієї країни до іншої із поверненням до своєї країни. Як наслідок, практично неможливим є визначення місця, звідки був направлений перший сигнал. Водночас, активно розробляються дешеві та зручні у використанні кодовані комп'ютерні програми, які найчастіше використовують розповсюджувачі web-порнографії. Декодування ж файлів виявляється дуже складною справою для правоохоронців, а необхідної кількості висококваліфікованих фахівців, здатних активно протидіяти цим злочинам, на сьогодні недостатньо [1].

Вважаємо, у цьому аспекті може виявитися ефективним досвід окремих країн щодо прийняття законів про заборону власникам порносайтів створювати сайти, співзвучні з доменами популярних Інтернет-ресурсів, оскільки, припустившись помилки в наборі ір-адреси, користувач потрапляв на зовсім інший ресурс. Наприклад, замість сайту «телепузики» (Teletubbies.com) з'являвся на екрані порносайт Teltubbies.com.

Ефективним напрямком протидії розповсюдженню порнографічних матеріалів вважаємо посилення міжнародної координації зусиль правоохоронців різних країн, зокрема укладання двосторонніх та багатосторонніх договорів та інших угод про співпрацю. В умовах сьогодення гострою проблемою міжнародного співробітництва є розбіжності законодавства різних країн та практики його застосування. Особливо це стосується країн, де існують відмінності у системах покарання за подібні злочини. Також наявні проблеми щодо формулювання обвинувачення, видів покарань та строків розслідування. Наприклад, у одній країні використання дитини як суб'єкта порнографії може бути одним з елементів класифікації злочину, в той час як в іншій для визнання особи винною може бути достатнім візуальне зображення дитини [2].

Оскільки проблема експлуатації дітей в мережі Інтернет набуває міжнародного характеру, потребує міжнародного визначення поняття порнографії з урахуванням тих уявлень, що є пристойним чи непристойним у культурах різних народів. При цьому слід враховувати, що існування мережі Інтернет ніве-

лює традиційне визначення дитячої порнографії. За своїм змістом ст. 34 Конвенції про права дитини має тлумачитись як така, що забороняє і «псевдодитячу порнографію», у тому числі «морфінг» дитячих та дорослих тіл з метою створення порнографічного зображення дитини. Саме таких змін зазнало законодавство Великобританії, Північної Ірландії та Канади, що сприяло боротьбі з дитячою порнографією [3]. На нашу думку, доцільним було б запозичення подібних практик і в Україні, що підтримали 89% опитаних нами оперуповноважених та 92% слідчих.

У США дитяча порнографія вважається злочином. П. 2252 гл. 110 Федерального кримінального кодексу США забороняє перевезення, відправку чи отримання дитячої порнографії каналами зв'язку, у т.ч. поштові та комп'ютерні засоби. У Данії, у 1998 р. Національний комісаріат поліції відкрив у Інтернет власну веб-сторінку, що дало можливість поліції отримувати від громадян інформацію про дитячу порнографію. Законодавство Японії карає позбавленням волі на строк до трьох років осіб, які розповсюджують через Інтернет порнографічні зображення дітей. Канада прийняла закон, згідно з яким пошук дитячої порнографії в Інтернеті – кримінально каране діяння, навіть якщо обвинувачений нічого не знайшов. Порушнику загрожує позбавлення волі до п'яти років [3].

Закони різних країн передбачають відповідальність за виготовлення, поширення і перегляд дитячої порнографії. У США за поширення дитячої порнографії мережею Інтернет відповідальність несе провайдер, у Канаді й низці країн ЄС вистежують і карають споживачів – і за пошук відповідних сайтів, і за збереження подібного матеріалу у своєму ПК (ув'язнення від півроку до п'яти). Загалом, покарання за виготовлення і поширення дитячого порно в різних країнах Заходу та Сходу – від 10 років позбавлення волі до довічного ув'язнення чи навіть страти [3].

Аналіз наявної фахової літератури, досліджень міжнародних програм та асоціацій, опитування працівників оперативних та слідчих підрозділів дозволяє визначити основні напрямки діяльності підрозділів Національної поліції у боротьбі із забороненим контентом, що впроваджуються на міжнародному, державному та індивідуальному рівнях: 1) створення та координація роботи «гарячих ліній» та можливість надсилання анонімних повідомлень щодо незаконного контенту в Інтернет-мережі; 2) боротьба з незаконним контентом та спамом; 3) своєчасність інформування користувачів Інтернет-мережі через засоби масової інформації та офіційний сайт Національної поліції про загрози та небезпеки віртуального простору [3].

Ми вважаємо, що для ефективної протидії кіберзлочинності необхідний інтегрований підхід, який можна забезпечити лише колективними зусиллями міжнародної спільноти через тісну взаємодію державних інститутів. Допоки не знайдено комплексного вирішення окреслених та інших, пов'язаних із цим проблем, як тимчасовий вихід, можливо скористатися окремими ефективними механізмами фільтрації веб-контенту, що довели свою дієвість у низці зарубіжних

країн [4].

Отже, проведене нами системне і комплексне узагальнення наявних проблем щодо розповсюдження порнографії мережею Інтернет, а також аналіз міжнародного досвіду протидії порнографії, врахування думок практиків, особистий досвід виявлення та розслідування злочинів, дозволили запропонувати можливі ефективні напрямки такої протидії:

1) створення нормативної бази, яка б забезпечила нормальну діяльність користувачів Інтернет і звела нанівець можливі правопорушення;

2) посилення санкцій щодо правопорушників;

3) прийняття кодексу поведінки провайдерів в Інтернет та надання їм певних повноважень щодо ініціювання питання про блокування сайту;

4) створення відповідних умов для підготовки кваліфікованих фахівців-правоохоронців з досвідом роботи у ІТ-сфері;

5) заборонити на законодавчому рівні створювати порносайти зі співзвучними доменними назвами Інтернет-ресурсів загального користування;

6) координація зусиль правоохоронців у протидії розповсюдженню порнографічних матеріалів та укладання двосторонніх і багатосторонніх договорів, міжвідомчих угод про співпрацю;

8) юридичне визначення поняття порнографії та ратифікація змін до ст. 34 Конвенції про права дитини;

9) визнання мережі Інтернет засобом масової інформації.

---

1. Шраго А. Проблема web-порнографії та шляхи її подолання [Електронний ресурс] / А. Шраго. – Режим доступу: http://www.crime-research.ru/articles/2995/

2. Лисенко І. Використання світової системи Інтернет як засіб експлуатації дітей // Право України. – 2003. – № 2. – С. 148-153.

3. Плахотнюк Н. Міжнародно-правові аспекти боротьби з дитячою порнографією в Інтернеті // Право України. – 2001. – № 10. – С. 104-109.

4. Санакоєв Д.Б. Засоби протидії неправомірному контенту підрозділами кіберполіції України: міжнародний досвід / Д.Б. Санакоєв // Оперативно-розшукова діяльність Національної поліції: проблеми теорії та практики: Матеріали Всеукраїнської науково- практичної конференції, 18 листопада 2016 року. – Дніпро: ДДУВС, 2016. – С.141-144.