МВС України
Харківський національний університет
внутрішніх справ

Координатор проектів ОБСЄ в Україні

АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Збірник матеріалів
Всеукраїнської науково-практичної конференції

(15 листопада 2017 року, м. Харків)

Харків
Харківський національний університет внутрішніх справ
2017

Актуальні питання протидії кіберзлочинності та торгівлі людьми. Харків, 2017

УДК [351.74:343.85](062.552)
ББК 67.611.31я43
А43

Друкується згідно з рішенням оргкомітету за дорученнями Харківського національного університету внутрішніх справ від 11.09.2017 № 138, від 20.09.2017 № 144

А43 Актуальні питання протидії кіберзлочинності та торгівлі людьми (15 листоп. 2017 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ; Координатор проектів ОБСЄ в Україні. – Харків : ХНУВС, 2017. – 212 с.

У матеріалах конференції окреслено найбільш актуальні проблеми протидії кіберзлочинності та торгівлі людьми на сучасному етапі; проаналізовано питання правового та організаційного забезпечення протидії кіберзлочинності та торгівлі людьми; кримінально-правові, процесуальні та криміналістичні аспекти протидії цьому негативному явищу; розглянуто відповідний міжнародний досвід, а також кадрове забезпечення правоохоронних органів. Досліджено використання інформаційних технологій і технічних засобів у протидії кіберзлочинності та торгівлі людьми.

УДК [351.74:343.85](062.552)
ББК 67.611.31я43

Публікації наведено в авторській редакції. Оргкомітет не завжди поділяє погляди авторів публікацій. За достовірність наукового матеріалу, професійного формулювання, фактичних даних, цитат, власних імен, географічних назв, а також за розголошення фактів, що не підлягають відкритому друку, тощо відповідають автори публікацій та їх наукові керівники.
Електронна копія збірника безоплатно розміщується у відкритому доступі на сайті Харківського національного університету внутрішніх справ (http://www.univd.edu.ua)у розділі «Видавнича діяльність. Матеріали науково-практичних конференцій, семінарів тощо»), а також у репозитарії ХНУВС (http://dspace.univd.edu.ua/xmlui/)

ЗМІСТ

Розділ 4.

КАДРОВЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Розділ 5.

МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

РОЗДІЛ 1
ОКРЕМІ ПИТАННЯ ПРАВОВОГО ТА ОРГАНІЗАЦІЙНОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 343.1 : 65.012.8

Валерій Васильович СОКУРЕНКО,
ректор Харківського національного університету внутрішніх справ, доктор юридичних наук

АКТУАЛЬНІ ПИТАННЯ ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Протидія кіберзлочинності та торгівлі людьми є сьогодні одним з першочергових завдань, яке стоїть перед правоохоронними органами не тільки України, але й світу. Практика засвідчує, що обидва названі напрями злочинної діяльності перебувають в активній фазі розвитку, а інколи навіть перетинаються, сприяючи утворенню взаємовигідних конгломератів злочинних угруповань. Останнє пояснюється почастілим застосуванням інформаційних технологій для вчинення злочинів торгівлі людьми, і, навпаки, – опануванням кіберправопорушниками нових прибуткових видів злочинного бізнесу, пов'язаного з «живим товаром».

Вибірковий аналіз статистичних даних за останні п'ять років показує різнонаправлені тенденції щодо кількості виявлених кіберзлочинів та злочинів торгівлі людьми в Україні (рис. 1, 2). Це серед іншого пояснюється тим, що якщо торгівлю людьми можливо певним чином приборкати на національному рівні, то кібератаки не мають кордонів. Їх можна очікувати у будь-який час з буд-якої точки світу, у якій є доступ до мережі Інтернет.

Наслідком прогресу у протидії торгівлі людьми, показаного правоохоронними органами України останніми роками, стало переведення нашої країни з третьої до другої групи спостереження згідно зі звітом Державного департаменту США 2017 року.

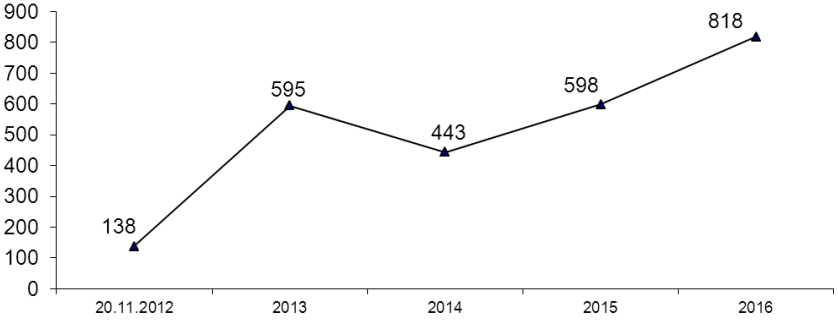

Рис. 1. Відомості про зареєстровані злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку за період 2012-2016 рр.

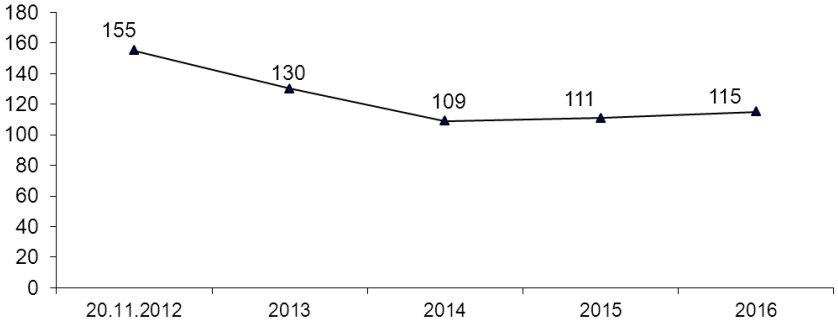

Рис. 2. Відомості про зареєстровані злочини торгівлі людьми за період 2012-2016 рр.

Серед головних проблем, з якими сьогодні стикаються правоохоронні органи під час розслідування кіберзлочинів та злочинів у сфері торгівлі людьми, пов'язаних з використанням комп'ютерних технологій, можна назвати наступні:

- неоднозначна судова практика щодо визнання наявності предмету злочину під час розповсюдження порнографії у формі онлайн-порностудій. Вказана проблема серед іншого обу-

мовлена нечітким розумінням того, що ж у даному випадку буде носієм протиправного контенту та чи утворюється він взагалі у сенсі, визначеному диспозицією ст. 301 Кримінального кодексу України;

- повсюдне використання провайдерами телекомунікацій технології CGN (Carrier-Grade NAT), яка передбачає надання клієнтам провайдера тимчасових внутрішніх IP-адрес, що вже потім використовуються для виходу в мережу Інтернет через єдину зовнішню IP-адресу. Для правоохоронних органів це ускладнює процес ідентифікації правопорушників за відомими зовнішніми IP-адресами, оскільки провайдер не може надати чіткої відповіді, хто ж користувався IP-адресою у визначений правоохоронцями проміжок часу;

- невизначена форма закріплення електронних доказів протоколом огляду. Досі ведуться дебати, який же протокол для цього використовувати: огляду речей чи огляду документів? Більше того існує практика фіксації електронних доказів з використанням протоколу зняття інформації з електронних інформаційних систем, яке не потребує подолання системи логічного захисту, а відтак проводиться без рішення слідчого судді;

- суперечлива практика документування злочинів торгівлі людьми, пов'язаних з використанням інформаційних технологій, за допомогою інституту оперативної (контрольованої) закупки замість спеціального слідчого експерименту;

- переважне нерозуміння працівниками поліції та прокуратури механізму міжнародної взаємодії в частині одержання даних від зарубіжних операторів та провайдерів телекомунікацій і хостерів;

- недостатня увага з боку органів поліції до проблеми дитячого онлайн-ґрумінгу – навмисних дій, спрямованих на встановлення дружніх відносин та емоційного зв'язку з дитиною і зниження рівня чинників стримання дитини з метою сексуального насильства над нею;

- під час розслідувань не в повній мірі застосовується арсенал аналітичної обробки даних, у тому числі інструменти так званої «кримінальної розвідки»;

- недостатнє розуміння працівниками правоохоронних органів механізму роботи сучасних комп'ютерних технологій, що може призвести до «розвалу» кримінального провадження.

Перелік означених проблемних питань не є вичерпним, для їх вирішення правоохоронним органам потрібно скоорди-

новано виходити з пропозиціями щодо внесення змін до чинного законодавства, створювати умови для підвищення ефективності взаємодії правоохоронних органів на національному та міжнародному рівнях, своєчасно опановувати нові інформаційні технології.

Одержано 17.10.2017

Актуальні питання протидії кіберзлочинності та торгівлі людьми. Харків, 2017

УДК 343.43

Олександр Маркович БАНДУРКА,
доктор юридичних наук, професор, академік Національної академії правових наук України, заслужений юрист України, радник ректора Харківського національного університету внутрішніх справ

ЩОДО РОЗУМІННЯ ПРАЦІВНИКАМИ ПРАВООХОРОННИХ ОРГАНІВ МЕХАНІЗМУ РОБОТИ СУЧАСНИХ КОМП'ЮТЕРНИХ ТЕХНОЛОГІЙ

Реформування правоохоронної системи України в сучасних умовах передбачає пошук нових інноваційних рішень, які б за короткий час давали найбільш позитивний ефект з точки зору поточної роботи і розвитку правоохоронної системи в цілому. Одним з напрямів, що потребує покращення, є якісна складова особового складу Національно поліції України.

І тут потрібно розуміти, що з точки зору інтелектуального наповнення, найбільшу складність становить протидія білокомірцевій економічній злочинності та кіберзлочинності. На останньому випадку хотілося б зупинитися більш докладно.

Використання правопорушниками комп'ютерних технологій носить прогресуючий характер. Воно обумовлено відносною легкістю приховування слідів за їх допомогою, значним «прибутком» за невеликий час, створенням у правопорушника психологічної установки на низьку ймовірність покарання за такі злочини в силу об'єктивних та суб'єктивних причин тощо.

Виклики з боку такого прогресуючого злочинного елементу передбачають своєчасне і належне опанування працівниками Національної поліції України знань та вмінь у сфері застосування комп'ютерної техніки. Такі знання мають містити відомості як про методи дій правопорушників, так і технікопроцедурні аспекти документування такої злочинної діяльності. Небажання правоохоронців вникати в цю проблематику може призвести до негативних наслідків під час попередження та розслідування відповідних правопорушень.

У якості прикладів тут можна навести:

1) застосування правопорушниками термінального доступу до операційних систем, розташованих у хмарному сховищі. Як наслідок – просте вилучення засобів комп'ютерної техніки під час обшуку або огляду місця події не дає позитивних результатів. Особливо ця проблема є актуальною при документуванні конверт-центрів, ІТ-фірм, що спеціалізуються на протиправній діяльності;

2) завантаження системи з носіїв, які приховуються в периферійних пристроях (мишах, принтерах, сканерах). Невилучення в ході обшуку таких пристроїв призводить до втрати доказової інформації. А таких випадків стає все більше, у тому числі у сфері нелегального грального бізнесу;

3) використання правопорушниками маловідомих правоохоронцям операційних систем, інформацію з яких вкрай складно вилучити без сторонньої допомоги. А враховуючи подекуди кількарічні черги на проведення комп'ютерно-технічних експертиз, таку допомогу можна не одержати взагалі. У цьому контексті особливу увагу слід звернути на підготовку кваліфікованих експертів, брак яких відчувається сьогодні, як у вітчизняних, так і закордонних органах правопорядку;

4) дії правоохоронних органів, зокрема експертів, щодо зняття образів з SSD-вінчестерів із наступним долученням до них відповідних ґеш-згорток можуть призвести до визнання висновків експертизи недійсними за результатами проведення додаткової експертизи. Це відбувається тому, що процедура TRIM для SSD-вінчестерів регулярно очищує дані в осередках жорсткого диску. Тобто, при наступному знятті геш-згортки новоствореного образу, вона не буде збігатися з попередньою.

Описані приклади є лише невеличкою частиною проблем, з якими стикаються у практичній діяльності правоохоронці. Саме тому потрібно на належному рівні вести підготовку фахівців для органів Національної поліції, створювати технічні умови та методичну основу для набуття ними зань і навичок в означеній сфері.

Крім наведених аспектів потрібно також звернути увагу на те, що нормативно-правова база України потребує змін у частині захисту національного інформаційного простору від протиправного контенту. Тому доцільно у чинному законодавстві передбачити порядок та підстави його блокування та видалення. Здійснення цього можливо у розрізі заходів забезпечення кримінального провадження, передбачених чинним Кримінальним процесуальним кодексом України.

Також потребує удосконалення механізм міжнародної взаємодії, адже більшість кіберзлочинів мають транснаціональний характер, а відтак виникає багато проблем юрисдикційного характеру.

Одержано 01.11.2017

УДК 343.43

Актуальні питання протидії кіберзлочинності та торгівлі людьми. Харків, 2017

Віктор Миколайович БЕСЧАСТНИЙ,
доктор наук з державного управління, професор, ректор Донецького юридичного інституту МВС України

ВЧИНЕННЯ ЗЛОЧИНУ В УМОВАХ ЗБРОЙНОГО КОНФЛІКТУ ЯК КВАЛІФІКУЮЧА ОЗНАКА ТОРГІВЛІ ЛЮДЬМИ

Торгівля людьми є одним з найнебезпечніших злочинів проти особи, на протидію якому спрямовані зусилля не тільки окремих держав, а і світової спільноти. Зокрема, визначення торгівлі людьми дано в Протоколі про попередження та припинення торгівлі людьми, особливо жінками і дітьми, та покарання за неї, що доповнює Конвенцію Організації Об'єднаних Націй проти транснаціональної організованої злочинності, прийнятого резолюцією 55/25 Генеральної Асамблеї від 15 листопада 2000 року. На національному рівні прийнято Закон України «Про протидію торгівлі людьми» від 20.09.2011 № 3739-VI, а кримінальна відповідальність за торгівлю людьми передбачена у статті 149 КК України.

У науковій літературі питанням кримінальної відповідальності за торгівлю людьми в цілому та аналізу кваліфікуючих ознак цього злочину зокрема присвятили свої роботи Ю. В. Александров, О. М. Бандурка, Ю. В. Баулін, Т. В. Варфоломеєва, Т. І. Возна, Н. О. Гуторова, І. М. Даньшин, В. О. Іващенко, В. А. Козак, М. Й. Коржанський, В. М. Куц, Я. Г. Лизогуб, А. А. Музика, О. В. Наден, А. М. Орлеан, В. М. Підгородинський, О. В. Пустова, П. П. Сердюк, М. І. Хавронюк, С. Д. Шапченко та ін. Проте в умовах збройного конфлікту такий злочин має свою специфіку, що обумовлює необхідність подальших досліджень цього питання.

На думку представників ООН торгівля людьми, їх незаконна експлуатація у зоні збройного конфлікту, перш за все, відбувається через підвищену вразливість людей, що рятуються від нього, в результаті повсюдних людських, матеріальних і економічних втрат, загального руйнування правопорядку, зосередження великої кількості осіб, що перебувають у вразливому становищі, в неофіційних оселях і таборах, та нових або більш активних дій озброєних і терористичних груп [1]. Такий стан речей, безумовно, є характерним і для територій Донбасу. Це пояснюється тим, що люди, які живуть поблизу лінії розмежування та на територіях непідконтрольних Україні, позбавлені можливості задоволення основних потреб повсякденного життя та намагаючись їх задовольнити (отримати продукти

харчування, роботу, освіту, соціальні виплати, іншу допомогу), автоматично попадають в так звану «групу ризику», тобто групу осіб, які мають уразливий стан пов'язаний із різними об'єктивними і суб'єктивними обставинами, відносно яких значно легше вчинити акти торгівлі людьми, чим і користуються злочинці.

До того ж, збільшенню вчинення фактів торгівлі людьми в зоні збройних конфліктів сприяє й активна зовнішня імміграція до сусідніх країн, в яких вимушені переселенці формують масив осіб, схильних до ризику стати жертвою торгівлі людьми. Останнє призводить до поширення практик торгівлі в державах, що межують з конфліктуючими територіями. Так, в останні роки у всіх країнах, де відбуваються збройні конфлікти – Югославії, Іраці, Афганістані, Лівії, Сирії, спостерігається збільшення злочинів пов'язаних із торгівлею людьми.

Слід відзначити, що під час збройних конфліктів змінюються види та способи торгівлі людьми, форми експлуатації, злочинці адаптують методи своєї діяльності, з'являються нові групи осіб, які стають жертвами торгівлі людьми.

На відміну від класичних сфер експлуатації людей: для жінок це переважно робота хатньої робітниці, ведення домашнього господарства, проституція, порнографія, сфера розваг (танцівниці), сільське господарство; для чоловіків - робота на будівництві, сільське господарство; для дітей – жебракування, порнографія, секс-послуги, робота наркокур'єром тощо, в умовах збройних конфліктів найбільш розповсюдженими формами торгівлі людьми з метою подальшої експлуатації стають:

- вербування, переміщення, передача, переховування або одержання осіб чоловічої статі з метою поповнення лав особового складу збройних сил сторін, що беруть участь в конфлікті;
- використання примусової праці і рабства для задоволення потреб озброєних груп;
- сексуальна експлуатація (військова проституція, насильницька вагітність);
- втягнення у злочинну діяльність;
- вилучення органів.

Крім того, під час збройного конфлікту факти торгівлі людьми найчастіше супроводжуються вчиненням інших тяжких протиправних дій, як то сексуальне та гендерне насилля, катування тощо, або з погроза застосування таких дій.

Збройний конфлікт на Донбасі став каталізатором збільшення фактів торгівлі людьми, що обумовлюється, на нашу думку, багатьма факторами, серед яких:

- складна криміногенна обстановка в зоні конфлікту;
- послаблення державних інститутів;
- дисфункція правоохоронних органів в зоні проведення АТО;
- складність правового статусу непідконтрольних Україні;
- зміна гендерного балансу на окремих територіях;
- вразливість людей, що проживають поблизу лінії розмежування та на територіях непідконтрольних Україні.

Наявність таких факторів, вимагає від держави вжиття невідкладних заходів щодо їх виявлення і усунення з метою попередження та припинення фактів торгівлі людьми, нарощування національних технічних можливостей в плані боротьби з цією категорією злочинів.

За словами заступника міністра іноземних справ Сергія Кісліци: «Україна рішуче підтримує міжнародні зусилля, спрямовані на протидію та запобіганню повного спектру порушень прав людини і зловживань в умовах збройних конфліктів та в постконфліктних ситуаціях. Україна рішуче виступає за викорінення торгівлі людьми, і боротьба проти цього жахливого явища серед пріоритетів діяльності українського уряду в галузі прав людини» [2]. Одним з таких заходів може стати визнання вчинення такого злочину в умовах збройного конфлікту кваліфікуючою ознакою.

У науковій літературі кваліфікуюча ознака складу злочину визначається як передбачена у диспозиції частини статті Особливої частини КК України ознака, що разом з ознаками основного складу характеризує кваліфікований (особливо кваліфікований) склад злочину, підвищує ступінь суспільної небезпеки злочину та особи, що його вчинила, впливає на кваліфікацію, посилює покарання та виконує функцію диференціації кримінальної відповідальності [3, с. 316]. На наш погляд вчинення злочину в умовах збройного конфлікту цілком відповідає зазначеним ознакам. Тим більше, що досвід застосування схожих ознак як обтяжуючих покарання у законодавця вже є – у пункті 11 частини 1 статті 67 КК України однією з таких обставин визнається вчинення злочину з використанням умов воєнного або надзвичайного стану, інших надзвичайних подій.

Список використаних джерел:

1. Письмо Постоянного представителя Соединенного Королевства Великобритании и Северной Ирландии при Организации Объединенных Наций от 7 марта 2017 года на имя Генерального секретаря: «Концептуальная записка для открытых прений Совета Безопасности на уровне министров по теме «Торговля людьми в условиях конфликта: принудительный труд, рабство и другая аналогичная практика», которые состояться 14 марта 2017 года» // Совет безопасности Организации объединенных наций URL: http://undocs.org/ru/S/2017/198 (дата звернення: 24.10.2017).
2. В МИД рассказали о многочисленных случаях торговли людьми и рабства на оккупированных территориях Донбасса // Інформаційне агентство «УНІАН». URL: https://www.unian.net/society/1825467-v-mid-rasskazali-o-mnogochislennyih-sluchayah-torgovli-lyudmi-i-rabstva-na-okkupirovannyih-territoriyah-donbassa.html (дата звернення: 24.10.2017).
3. Наконечна І. М. Поняття кваліфікуючих (особливо кваліфікуючих) ознак складу злочину. *Часопис Київського університету права*. 2013. № 4. С. 313-317.

Одержано 25.10.2017

УДК 351.74 (477)

Ольга Ігорівна БЕЗПАЛОВА,
доктор юридичних наук, професор, завідувач кафедри адміністративної діяльності поліції факультету № 3 Харківського національного університету внутрішніх справ

ВЗАЄМОДІЯ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ З ІНШИМИ ПРАВООХОРОННИМИ ОРГАНАМИ У СФЕРІ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ ЯК ОДИН ІЗ НАПРЯМКІВ ЗАБЕЗПЕЧЕННЯ СКЛАДОВИХ СЕКТОРУ БЕЗПЕКИ І ОБОРОНИ

Реальні прояви кібератак мало прогнозовані, а їх результатом є, як правило, значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування інформаційно-телекомунікаційних систем, які безпосередньо впливають на стан національної безпеки і оборони. У зв'язку з цим, існуючі загрози вимагають впровадження комплексних заходів, спрямованих на забезпечення кібербезпеки. Варто наголосити на тому, що питання забезпечення кібербезпеки є надзвичайно актуальними для України. В той же час, у нашій державі заходи з протидії викликам і загрозам у зазначеній

сфері знаходяться на початковому етапі та ще не мають комплексного характеру.

У рішенні Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України» звертається увага, що серед основних напрямків досягнення необхідних оперативних та інших спроможностей складових сектору безпеки і оборони виокремлюється удосконалення державного управління та керівництва сектором безпеки і оборони, у тому числі систем забезпечення інформаційної і кібербезпеки, систем захисту інформації та безпеки інформаційних ресурсів, посилення боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері. У зв'язку із зазначеним необхідно розглянути питання взаємодії Національної поліції, як одного із суб'єктів сектору безпеки і оборони, з іншими правоохоронними органами у сфері боротьби з кіберзлочинністю.

У результаті аналізу нормативно-правових актів, які регламентують діяльність Національної поліції та враховуючи особливості правопорушень у сфері інформаційно-комунікаційних технологій, що передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; економіки, яка включає в себе фінансові та торгові транзакції, що здійснюються за допомогою мереж електрозв'язку чи комп'ютерних мереж, а також протидію забороненим видам господарської діяльності у цій сфері; надання телекомунікаційних послуг, а також шахрайствам і легалізації (відмиванню) доходів, одержаних від зазначених вище діянь, то важливе значення має взаємодія на наступних рівнях: 1) внутрішньовідомчому; 2) внутрішньодержавному (з органами і підрозділами Служби безпеки України, органами місцевого самоврядування, підприємствами, установами і організаціями різних форм власності у сфері боротьби з кіберзлочинністю); 3) міжнародному (з правоохоронними органами інших країн).

Враховуючи виокремленні вище рівні взаємодії Національної поліції з іншими правоохоронним органами, варто вказати на їх форми реалізації на внутрішньовідомчому та внутрішньодержавному рівні. До зазначених форм варто віднести такі: 1) організація вивчення матеріалів, що утворюються під час здійснення поліцейськими оперативно-розшукової діяль-

ності, у їх числі справ оперативного обліку, матеріалів виконання письмових доручень слідчого, ухвал суду; 2) створення та застосування автоматизованих інформаційних систем (формування й поповнення інформаційних масивів даних) відповідно до потреб оперативно-службової діяльності; 3) організація виконання доручень слідчого щодо проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій у кримінальних провадженнях, які відносяться до компетенції поліції; 4) організація проведення комплексних і цільових оперативно-профілактичних заходів, у тому числі за участю правоохоронних органів інших країн; 5) внесення в установленому порядку пропозицій щодо вдосконалення законодавчої бази у сфері боротьби з кіберзлочинністю, а також участь у розробленні та опрацюванні проектів законодавчих та інших нормативно-правових актів у цій сфері; 6) забезпечення своєчасного розгляду звернень та запитів громадян, підприємств, установ, організацій з питань, віднесених до компетенції поліції, контролю за належним дотриманням порядку їх прийняття, реєстрації, обліку і розгляду; 7) участь в організації та проведенні навчальних та науково-практичних заходів з питань, що відносяться до сфери боротьби з кіберзлочинністю (тренінгів, конференцій, семінарів) тощо.

Говорячи про міжнародний рівень взаємодії, варто зазначити, що ефективна боротьба проти кіберзлочинності вимагає тісного, швидкого та ефективного, функціонального міжнародного співробітництва всіх державних структур, а що найперше – правоохоронних органів, у розслідуванні такого роду правопорушень. Перші серйозні кроки в налагодженні міжнародного співробітництва у протидії кіберзлочинності Україна зробила на початку XXI століття, коли 23 листопада 2001 р. в Будапешті Україна разом із 30-ма іншими державами підписала Європейську конвенцію «Про кіберзлочинність». Наступним важливим кроком України щодо налагодження міждержавної співпраці розглядуваній сфері є ратифікація 7 вересня 2005 р. зазначеної Конвенції, що передбачає надання повноважень, достатніх для ефективної боротьби зі злочинами у сфері інформаційно-телекомунікаційних технологій як на внутрішньодержавному, так і міжнародному рівнях, укладення домовленостей щодо дієвого міжнародного співробітництва. Національна поліція уповноважена здійснювати співробітництво з правоохоронними органами іноземних держав в рамках функціонування цілодобової контактної мережі для надання

невідкладної допомоги при провадженні щодо кримінальних правопорушень, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, які підозрюються або обвинувачуються у їх вчиненні, а також збирання доказів в електронній формі.

Взаємодію Національної поліції з іншими правоохоронними органами щодо протидії правопорушенням у сфері кіберзлочинності умовно слід поділити на внутрішню (в рамках органів та підрозділів поліції) та зовнішню. В залежності від напрямків діяльності Національної поліції слід виокремити такі види взаємодії: 1) взаємодія щодо протидії правопорушенням у сфері телекомунікацій; 2) взаємодія щодо протидії правопорушенням у сфері електронної комерції; 3) взаємодія щодо протидії правопорушенням у сфері шахрайства та легалізації (відмиванню) доходів, одержаних злочинним шляхом тощо.

Одержано 25.10.2017

УДК 343.1 : 65.012.8 + 004

Олег Валерійович БОГІНСЬКИЙ,
аспірант Харківського національного університету внутрішніх справ

МЕТОДИ МЕРЕЖНОГО АНАЛІЗУ ТА КАРТОГРАФУВАННЯ В СИСТЕМІ КРИМІНАЛЬНОЇ РОЗВІДКИ

Для стримування злочинності можуть застосовуватися різні моделі. Найбільшої популярності сьогодні набули такі з них: нульової толерантності; проблемно-орієнтована; небезпечних зон; на основі розвідувальних даних; прогностична. Кримінальна розвідка є елементом описаних проактивних стратегій стримування злочинності.

Центральним елементом кримінальної розвідки як процесу є аналіз, без проведення якого сама ця діяльність втрачає сенс, а накопичення даних буде у більшості випадків марним витрачанням часу. Під час аналізу можуть бути застосовані різні методи та використовуватися конкретні моделі роботи з даними.

Практика показує, що переважна кількість аналітичних висновків містить елементи мережного аналізу. Цей метод є особливо актуальним в умовах дослідження великих злочинних груп та організацій, адже зі збільшенням мережі, яка підлягає аналізу, зростає ймовірність виявити у ній слабкі місця

та простежити відповідні зв'язки. Пошук асоціативних зв'язків в рамках мережного аналізу є достатньо нетривіальним завданням. Для цього можуть застосовуватися різні математичні алгоритми.

Як показує практика значну частину функцій кримінального аналізу можна формалізувати, а відтак і запрограмувати. Це серед іншого досягається використанням моделей (шаблонів), які враховують як просторові так і часові параметри вчинення тих або інших правопорушень. Однією з популярних методологій, застосовуваних для проведення кримінальної розвідки та яка містить велику кількість елементів мережного аналізу, є Anacapa.

Ще одним ефективним методом, застосовуваним під час здійснення кримінальної розвідки, є картографування злочинних проявів. Однією з цілей, яку досягають з використанням цього методу, є побудова так званих географічних профілів. Вказані профілі дозволяють окреслити просторові рамки, в яких правопорушник може мешкати або вести якусь діяльність. Використання описаних профілів в купі з психологічними дозволяють більш цілісно підійти до розслідування кримінальних правопорушень.

В основі побудови географічних профілів знаходиться теорія, згідно з якою як жертви, так і правопорушники мають певні стійкі маршрути руху, у рамках яких вони власне і здійснюють свою повсякденну діяльність.

Ефективне картографічне профілювання в сучасних умовах практично неможливо здійснювати без застосування спеціалізованого програмного забезпечення. У якості прикладу останнього можна назвати продукти Rigel компанії ECRI (ecricanada.com), CrimeStat (www.nij.gov/topics/technology/maps/pages/crimestat.aspx), вітчизняний комплекс RICAS (police.kh.ua). Паралельно зі створенням географічних профілів, як правило, відбувається побудова так званих «теплових мап», які покликані візуалізувати на карті найбільш криміногенні осередки. Ці ділянки позначаються більш насиченим кольором, як правило, червоним.

Одержано 14.10.2017

УДК 341.4:004

Андрій Васильович ВОЙЦІХОВСЬКИЙ,
кандидат юридичних наук, доцент, професор кафедри конституційного і міжнародного права факультету №4 Харківського національного університету внутрішніх справ

КІБЕРЗАГРОЗИ ЯК ВИКЛИК СВІТОВІЙ БЕЗПЕЦІ

Розвиток науково-технічного прогресу і широке використання сучасних інформаційних технологій в суспільстві висуває перед міжнародним співтовариством нові питання щодо вирішення проблем інформаційної безпеки. Якщо раніше головним об'єктом захисту були територія, кордони, державний устрій, людські і матеріальні ресурси суверенної держави, а основну роль у створенні безпеки відгравали правоохоронні органи, то зараз ці поняття вже є застарілими. В сучасних умовах розвитку суспільства державні кордони розмиваються, матеріальні ресурси більше не є першочерговою ціллю, а правоохоронні органи досі неспроможні адекватно відповідати на новітні виклики. Саме в таких умовах виникає таке явище як кібертероризм і інформаційна війна, що є найбільш успішними і потужними засобами дестабілізації, залякування населення, а також інструментами політичного тиску [1].

На жаль, ступінь кіберзагрози не до кінця ще усвідомлена і оцінена в суспільстві. Але навіть той незначний досвід, який вже існує в цій сфері, а тим більше досвід розвинених країн світу (США, Франція, Великобританія, Німеччина, Іспанія, Нідерланди, Італія та ін.) зі всією очевидністю свідчить про уразливість будь-якої країни.

Жодна країна не може на 100% захиститися від кібератак, які постійно удосконалюються. Так, 27 червня 2017 року найбільшої хакерської атаки, яка поширює вірус Petya.A, що блокує роботу комп'ютерних систем, зазнали українські державні установи (Кабінет Міністрів України, Національна поліція України та ін.), аеропорт «Бориспіль», Чорнобильська атомна електростанція, українські банки, енергетичні компанії, державні інтернет-ресурси і локальні мережі, українські медіа і ряд інших великих підприємств. Ця кібератака також призвела до зараження комп'ютерів по всьому світу (США, Великобританія, Німеччина, Польща, Індія, Литва та ін.), і завдала збитків приблизно на 8 млрд. доларів США. На даний час спеціалісти Департаменту кіберполіції Національної поліції України, Служ-

би безпеки України та інших профільних служб спільно з провідними фахівцями українських ІТ-компаній і зарубіжних організацій, працюють над подоланням наслідків ураження українських комп'ютерних мереж шкідливим програмним забезпеченням.

Нині держави повинні пристосовуватись до сучасних умов, які диктує їм науково-технічний прогрес. Однак, існують держави, які саме ці кіберзагрози створюють і ефективно використовують для реалізації власних цілей. Серед таких держав особливо вирізняється Росія, яка використовує кібератаки, як частину гібридної агресії не лише проти України, але й інших країн. Одним із аргументів, які свідчать про таку незаконну активність є нещодавнє створення в Росії так званих «військ інформаційних операцій», які б декларативно мали б захищати державу від кібер-втручання, але реальна суть цього підрозділу – інформаційний напад [1].

Важливо зауважити, що питання забезпечення кібербезпеки належать до сфери національної безпеки. Гарантування міжнародної інформаційної безпеки та її складової – кібербезпеки залишаються одним із стратегічних завдань багатьох країн світу, оскільки більшість політичних і військових конфліктів відбуваються або віддзеркалюються саме у віртуальному просторі. Україна відповідно до укладених нею міжнародних договорів здійснює співробітництво у сфері кібербезпеки з іноземними державами, їх збройними силами, правоохоронними органами і спеціальними службами, а також із міжнародними організаціями.

Український вектор зовнішньої політики має бути спрямований на активізацію міжнародного співробітництва у сфері забезпечення кібербезпеки, продовження взаємодії з питань кібербезпеки за участі органів державної влади України і відповідних органів НАТО шляхом співпраці на двосторонній основі, упровадження інформаційно-комунікаційних та технологічних стандартів НАТО в Україні, розвиток технічних можливостей спільних груп реагування на кіберінциденти.

У сучасних реаліях перед політичним керівництвом нашої держави постає важливе та відповідальне завдання: запозичуючи передовий зарубіжний досвід, разом зі світовим співтовариством спільними зусиллями активізувати реалізацію дієвих заходів щодо протидії кіберзлочинності, кібертероризму і будь-яким іншим кібератакам, що передбачає насамперед побудову ефективної моделі Національної системи кібербезпеки,

її інтеграцію до ЄС та НАТО, дієвого захисту національних та комерційних інформаційно-комунікаційних ресурсів та їх критичної інфраструктури, затвердження офіційної акредитації з боку НАТО Національного центру кіберзахисту та протидії кіберзагрозам з метою розвитку конструктивної співпраці з Альянсом у цій галузі, блокування будь-яких посягань на національну інформаційну сферу, створення оптимальної моделі надійного захисту вітчизняного кіберпростору, формування засад для розробки методів принципів здійснення «електронної оборони» [2, с. 55].

Список використаних джерел:

1. Івахів Б. Кібертероризм як засіб ведення зовнішньої політики РФ // Free Voice Information Analysis Center: сайт. URL: http://iac.org.ua/kiberterorizm-yak-zasib-vedennya-zovnishnoyi-politiki-rf/ (дата звернення: 20.10.2017).
2. Лук`янчук Р. В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник національної академії державного управління при Президентові України*. 2014. № 4. С. 50-56.

Одержано 25.10.2017

УДК 004.056.53

Юрій Валерійович ГНУСОВ,
кандидат технічних наук, доцент, завідувач кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Сергій Володимирович КАЛЯКІН,
завідувач навчальної лабораторії кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

СУЧАСНІ ТЕНДЕНЦІЇ ПОШИРЕННЯ КІБЕРЗАГРОЗ

Інтернет-речі (IoT)

Актуальність проблеми незахищених IoT-мереж невпинно зростає протягом останніх кількох років. Тенденція стосується безлічі пристроїв, задіяних в споживчих і промислових цілях, що підключаються до мережі без дотримання належних заходів безпеки.

В останні роки хакери почали використовувати більшу кількість вразливостей пристроїв для створення масштабних ботнетів з тисяч і мільйонів заражених пристроїв: маршрутизаторів, Smart-TV тощо. Різноманітні Інтернет-речі вже давно перетворилися в улюблену ціль атак хакерів. Їм достатньо

придбати будь-якої пристрій і самостійно вивчити, як він захищений. Якщо його зламати, то система захисту не може бути оновлена оперативно. Використовуючи один пристрій, хакеру дуже легко потрапити всередину мережі, яка може містити цікаву для них інформацію: банківські реквізити, медичні записи, корпоративні дані.

Більшу частину пристроїв для Інтернет-речей виробляють співробітники стартапів, які використовують апаратне і програмне забезпечення зі сторони, придбане у постачальника і недостатньо захищене від зломів. На створення більшості IoT-девайсів було витрачено мінімум грошей, тому не дивно, що їх легко зламати.

З ростом кількості пристроїв і датчиків, підключених до мережі, зростає і кількість кіберзагроз. Наприклад, розумний холодильник став частиною бот-мережі і почав розсилати спам; розумна кавоварка виявилася причиною атаки на індустріальні мережі з подальшим зараженням комп'ютерів для моніторингу технологічного процесу вірусом-здирником.

При проектуванні нових технологій слід брати за основу безпеку. Однак, часом розробники, навмисно або ненавмисно, залишають недокументований канал, який не просто збирає інформацію про застосування пристрою, але і дозволяє проникати в особистий простір кінцевого користувача.

Немає сумнівів в тому, що мережі пристроїв Інтернет-речей (IoT), заражених шкідливими програмами, стануть однією з найпоширеніших у майбутньому проблем забезпечення кібербезпеки.

Кіберзагрози для розумних міст

Термін «розумне місто» зазвичай застосовується по відношенню до міст, які активно використовують Internet-технології безліччю різноманітних способів, щоб більш ефективно функціонувати і відповідати потребам своїх жителів.

Серед мотивів зловмисників, які спонукають їх атакувати розумні міста: бажання перевірити свої хакерські здібності, крадіжка грошей і особистих даних користувачів, а також корпоративної інформації.

Серед цілей хакерів при атаках на критичну інфраструктуру розумних міст: навмисна організація ДТП, організація перебоїв в подачі електроенергії; крадіжка особистої інформації користувачів, крадіжка електроенергії; перехоплення управління пристроями і системами; порушення транспортної системи та інші.

Атака на розумні міста проходить в чотири етапи: статистичний аналіз (аналіз механізмів і систем, чиї уразливості можуть бути використані), сканування (виявлення цілей і точок входу), збір інформації (отримання даних для доступу шляхом фішингу тощо здійснення самої кібератаки.

Вразливим місцем розумних міст є в тому числі некоректне використання розумних технологій на його території.

Перехоплення рахунку (Account takeover)

У разі вчинення крадіжки персональних даних (identity theft), метою шахраїв зазвичай є особисті дані, такі як імена, поштові адреси і адреси електронної пошти, а також дані кредитних карт або інформація про акаунт (рахунку). Це дозволяє шахраям, наприклад, здійснювати замовлення товарів в Інтернеті під чужим ім'ям і оплачувати їх, використовуючи чужу кредитну картку або списання коштів з чужого рахунку. З тією ж метою може використовуватися фішинг (phishing), котрий включає в себе використання фіктивних веб-сайтів, електронної пошти або текстових повідомлень для доступу до персональних даних.

Восени 2017 року організація US-CERT - один з підрозділів Міністерства внутрішньої безпеки США, яке реагує на інциденти, пов'язані з комп'ютерною безпекою, повідомила про потенційну загрозу Wi-Fi мережам. За словами експертів, протокол шифрування WPA2 (Wi-Fi Protected Access II), який забезпечує захищену передачу даних між бездротовою точкою доступу і пристроями, був зламаний. Знайдена вразливість дозволяє хакерам, які перебувають в зоні дії домашньої або офісної мережі, отримати пароль від Wi-Fi, прослуховувати інтернет-трафік і перехоплювати будь-яку інформацію, що передається по незашифрованих каналах зв'язку.

DDoS-атаки

Основне знаряддя хакерів - це ботнет, мережа з пристроїв, заражених шкідливим ПЗ, яке змушує їх виконувати певні дії без відома користувача. Якщо говорити саме про ботнети, що генерують DDoS, то, наприклад, один з найвідоміших ботнетів Mirai налічує 400-500 тисяч заражених IoT-пристроїв, які атакували DNS-сервіс компанії Dyn, паралізував роботу цілого ряду компаній, включаючи Twitter, the Guardian, Netflix, Reddit, CNN та багато інших.

Слід розуміти, що в разі DDoS-атак важлива не кількість ботів, а обсяг і патерни трафіку, які вони генерують. І якщо ботнети, що поширюють трояни і спам - це в основному пер-

сональні комп'ютери, рідше - сервери, то DDoS-ботом може стати абсолютно будь-який пристрій, що має IP-адресу і інтерфейс для підключення до Інтернету.

При цьому, ботнети з IoT-пристроїв кидають справжній виклик фахівцям з кібербезпеки, тому що генерують трафік по TCP- протоколу, який практично не відрізняється від легітимного.

У 2017 році все виразніше стає помітна тенденція вимагання грошей під загрозою DDoS-атак. Такий підхід отримав назву Ransom DDoS або RDoS. Зловмисники посилають компанії жертві повідомлення з вимогою викупу, який може становити від 5 до 200 біткоінів. У разі несплати вони обіцяють організувати DDoS-атаку на критично важливий онлайн-ресурс жертви.

Атаки типу знищення сервісу (DeOS)

Отримання прибутку є основним спонукальним мотивом зловмисників. Тим не менш, деякі з них зосереджені на блокуванні або навіть знищенні атакованих систем і процесів.

Зловмисники шукають шляхи усунення мережі «безпеки», яку організації використовують для відновлення систем і даних після поразки шкідливим або здирницьким ПО, а також інших інцидентів. Як показали результати атаки шифрувальника Nyetya (Petya) влітку 2017 року і Bad Rabbit у жовтні 2017 року, дані атаки не були здирницьким ПО, а справжньою DeOS-атакою, яка просто знищувала дані заражених систем по всьому світу. Кількість подібних атак в майбутньому буде зростати.

Одержано 25.10.2017

УДК 327.84 : 004

Денис Олександрович ГРИЩЕНКО,
провідний фахівець факультету № 4 Харківського національного університету внутрішніх справ

КІБЕРПЕРЕСЛІДУВАННЯ ЯК ІНФОРМАЦІЙНИЙ ЗЛОЧИН

В даний час поняття кіберпереслідування або кібербуллінгу стали актуальними темами для обговорення не тільки серед населення, а й в державних органах, в тому числі й правоохоронних, особливо в зв'язку зі збільшенням випадків суїциду серед неповнолітніх.

В умовах тотальної інформатизації збільшилась кількість випадків інтернет-агресії, яка застосовується здебільшого що-

до неповнолітніх. Зазначений вид агресії є популярним серед підлітків через можливість негативного анонімного впливу на іншу особу, що призводить до насильницької поведінки.

Кібербулінг - це навмисний, неодноразово-повторюваний вплив на підлітка, засобами інформаційних технологій, що включають в себе розсилку повідомлень образливого і загрозливого характеру, поширення в мережі неправдивої інформації, а саме фото і відео за участю потерпілого.

Потрапивши до мережі Інтернет, така інформація стає загальнодоступною, в зв'язку з чим образи, приниження, неприємні фотографії, відео здатні поширюватись нескінченно.

Статистика свідчить про наявність феномена кібербулінгу у багатьох країнах, наприклад в США, Великобританії та Австралії, де місцеві міністерства освіти змушені все більше уваги приділяти цій проблеми. За статистикою, в англомовних країнах з проявами кібербулінгу стикаються більше третини підлітків 12-15 років.

Після декількох голосних випадків самогубства через комп'ютерну агресію парламенти окремих штатів прийняли закони, за якими Інтернет агресорам загрожує покарання: від штрафу до декількох років позбавлення волі.

Закордонні криміналісти пропонують передбачити кримінальну відповідальність за кіберпереслідування, які призводять до тяжких наслідків.

У Німеччині кібербуллінг не має власних ознак об'єктивної сторони злочину, але тим не менше, окремі його елементи підпадають під кримінальну відповідальність. Кібербуллінг в Німеччині зараховується до злочинів, які тягнуть за собою тримання під вартою - для повнолітніх до 10 років. Підлітки, як правило, піддаються меншому покаранню - до 5 років арешту або до примусових виправних робіт.

Існує Закон про «Захист прав молодого покоління», в якому передбачено параграфи, що регламентують використання мережі Інтернет.

Ґрунтуючись на вищесказаному і нормах Кримінального Кодексу України про злочини проти особистості, можна виділити наступні найбільш небезпечні форми переслідування: доведення до самогубства з використанням погроз і шантажу; катування, тобто систематичне заподіяння психічних страждань шляхом переслідування; погроза вбивством або заподіянням тяжкої шкоди здоров'ю; наклеп; спонукання до дій сексуального характеру.

Таким чином, необхідно передбачити кваліфікований склад для вищезазначених злочинів з використанням інформаційних технологій і інформаційно-телекомунікаційних систем.

Одержано 30.10.2017

УДК 343.431 : 004

Сергей Николаевич ГУСАРОВ,
доктор юридических наук, профессор, профессор кафедры административного права и процесса факультета № 3 Харьковского национального университета внутренних дел

Вячеслав Валерьевич МАРКОВ,
кандидат юридических наук, старший научный сотрудник, декан факультета № 4 Харьковского национального университета внутренних дел

ИСПОЛЬЗОВАНИЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В ДЕЯТЕЛЬНОСТИ ТЕРРОРИСТИЧЕСКИХ ОРГАНИЗАЦИЙ НА ПРИМЕРЕ ТАК НАЗЫВАЕМОГО «ИСЛАМСКОГО ГОСУДАРСТВА»

Глобализационные процессы в мировом сообществе приводят к тому, что с каждым годом увеличивается роль информации и информационных технологий практически во всех сферах жизнедеятельности человека, в том числе и в управленческой сфере.

В течение последних лет мировое сообщество (журналисты, эксперты и политики самого высокого уровня) активно обсуждало проблемы и причины распространения международного терроризма на Ближнем Востоке.

Вряд ли, в современном мире можно найти обывателя, который не слышал бы о такой организации, как «Исламское государство Ирака и Леванта» (ИГИЛ), оно же «Исламское государство» (ИГ). Скорость, с которой развивалась данная организация, масштабность ее действий, не поддается сравнению ни с одной другой, существующей террористической организацией. Используемые ею новые информационные технологии и механизмы идеологической и информационной работы, позволяют сделать вывод, что мы имеем дело с принципиально новым явлением терроризма, который сумел перейти на качественно иной уровень своего развития [1].

Необходимо заметить, что Исламское государство единственная в мире террористическая организация, которая имеет характеристики, присущие государству: обозначены грани-

цы «государства», существует основной закон, который гласит, что мусульмане обязаны соблюдать все законы шариата, а неверные — кяфиры — являются воплощением дьявола и должны быть либо убиты, либо взяты в рабство (женщины). Стоит отметить, что на территориях подконтрольных Исламскому государству существует легальный рынок рабов (женщины и подростки) [2].

Военные успехи на Ближнем Востоке, большие финансовые возможности и грамотные действия в киберпространстве позволили Исламскому государству за считанные годы стать одной из самых опасных террористических организаций в мире.

Представители данной террористической организации сумели отказаться от многих религиозных канонов, предписывающих ряд ограничений и активно использовать достижения научно-технического прогресса в собственных целях. Для современной террористической деятельности присуще использование развитой информационно-телекоммуникационной инфраструктуры, что в свою очередь демонстрирует высокий уровень владения передовыми технологиями, включая, использование передовых методик социальной инженерии применяемой в социальных сетях для вербовки новых членов организации [3].

Все вышеуказанное позволяет Исламскому государству не только вести активную пропагандистскую деятельность по всему миру, но и легитимизировать в мусульманском мире идеи «халифата».

Изучив данную проблему, можно прийти к выводу, что информационные технологии, на вооружении Исламского государства, существенно качественно трансформируют привычное для всех понятие терроризма, но и интегрируют террористическую деятельность в киберпространство.

Таким образом, современный терроризм активно включился в информационные войны наравне с ведущими государствами и результат этого противостояния пока что является вопросом дискуссионным.

Список використаних джерел:

1. Анализ пропагандистских технологий ИГИЛ в Интернете // Российское общество политологов URL: http://politmos.ru/2995-analiz-propagandistskih-tehnologiy-igil-v-internete.html (дата обращения: 07.10.2017).
2. ИГИЛ обзавелось 45 тысячами аккаунтов в Twitter для вербовки и пропаганды // Региональная антитеррористическая

структура Шанхайской организации сотрудничества URL: http://ecrats.org/ru/situation/status/4880 (дата обращения: 09.10.2017).
3. Васильченко В. Джихад в Twitter: Как террористы осваивают приёмы социального маркетинга URL: http://apparat.cc/network/isis-social-war/ (дата обращения: 09.10.2017).

Одержано 30.10.2017

УДК 347.440.44

Олексій Леонідович ЗАЙЦЕВ,
кандидат юридичних наук, доцент, завідувач кафедри цивільно-правових дисциплін факультету № 4 Харківського національного університету внутрішніх справ

ВРАЗЛИВІСТЬ ДЕРЖАВНИХ ЗАКУПІВЕЛЬ КІБЕРЗЛОЧИНАМ

Постановка проблеми у загальному вигляді полягає в дуалізмі правової природи відносин (цивільних, господарських, організаційних, адміністративних, кримінальних), що виникають у зв'язку зі здійсненням державних закупівель, та конкуренції серед нормативних актів, які ці відносини регулюють. За загальним правилом, державні закупівлі застосовуються до всіх замовників та закупівель товарів, робіт та послуг, які повністю або частково здійснюються за рахунок державних коштів, за умови, що вартість предмета закупівлі товару (товарів), послуги (послуг) дорівнює або перевищує 100 тис. грн (у будівництві − 300 тис. грн), а робіт − 1 млн грн. Резонансне затримання співробітниками НАБУ за підозрою у розтраті понад 149 млн грн державних коштів заступника Міністра оборони України та директора Департаменту державних закупівель та постачання матеріальних ресурсів Міноборони знову привертає увагу до державних закупівель.

Зв'язок із важливими практичними завданнями полягає в тому, що працівники ОВС у сфері охорони економічної безпеки держави при виконанні покладених на них обов'язків є представниками органу виконавчої влади, діють від імені держави і перебувають під її захистом. Але належне оформлення їх повноважень в державних закупівлях є запорукою дотримання цивільних прав в Україні, що прямо передбачено Проектом Закону України "Про основи запобігання та боротьби з економічними правопорушеннями".

Оскільки автор продовжує науковий пошук у даній галузі основна мета тез (завдання) – це визначення основних суперe-

чностей у законодавстві, що регулює державні закупівлі, та може привести до скоєння злочину у сфері закупівель товарів, робіт і послуг за державні кошти.

Закупівля здійснюється відповідно до річного плану. Річний план, додаток до річного плану та зміни до них безоплатно оприлюднюються на веб-порталі Уповноваженого органу з питань закупівель протягом п'яти днів з дня їх затвердження. Центральний орган виконавчої влади, що реалізує державну політику у сфері казначейського обслуговування бюджетних коштів до здійснення оплати за договором про закупівлю перевіряє наявність договору про закупівлю, річного плану закупівель та звіту про результати проведення процедури закупівлі, які підтверджують проведення процедури закупівлі, за результатами якої укладено договір про закупівлю. Недосконалість процедури закупівель на цьому етапі полягає в тому, що втрата на веб сайт Уповноваженого органу річного плану в якості наслідку може мати недійсність вже проведених торгів.

Цивілістичні відносини в закупівлях продовжуються безпосередньо з закупівлі. Мета закупівлі – здійснити акцепт пропозиції закупівель. Акцепт пропозиції хоча і має традиційну цивілістичну назву, але для нього характерні певні особливості. Оскільки законодавець навмисно ігнорує п. 1 ст. 642 ЦК України, відповідно до якого відповідь особи, котрій адресована пропозиція укласти договір, про її прийняття (акцепт) повинна бути повною і безумовною. Акцептування в закупівлях здійснюється не шляхом підписання договору, а оприлюдненням наміру «За результатами розгляду та оцінки тендерної пропозиції замовник визначає переможця та приймає рішення про намір укласти договір». Таким чином акцептування не обов'язково тягне наслідком укладання та підписання договору. Порушення правил публікації або нездійснення публікації перерахованої інформації тягне відповідальність за ст. 164-14 Кодексу України про адміністративні правопорушення. Тому на цієї стадії можливі кіберзлочини як з боку третіх осіб, так і з боку замовника з метою уникнення від відповідальності.

Договір про закупівлю - договір, який укладається між замовником і учасником за результатами процедури закупівлі та передбачає надання послуг, виконання робіт або набуття права власності на товари за державні кошти. Договір про закупівлю укладається в письмовій формі. Але навіть незахищеність від кібер атак є головним недоліком цих правовідносин. Тому що:

По-перше, договір про закупівлю не є «результатом процедури закупівлі» тому, що Держказначейство до здійснення оплати за договорами про закупівлю перевіряє наявність та відповідність укладеного договору про закупівлю звіту про результати проведення процедури закупівлі та річному плану закупівель. Тобто договір про закупівлі повинен відповідати звіту про закупівлі, а не навпаки. А звіт і буде «результатом процедури закупівлі».

По-друге, в законодавстві про закупівлі не коректно використовуються конструкції з «умовами договору». Так, умови договору про закупівлю не повинні відрізнятися від змісту пропозиції конкурсних торгів або цінової пропозиції (у тому числі ціни за одиницю товару) переможця процедури закупівлі. Істотні умови договору про закупівлю не можуть змінюватися після його підписання до виконання зобов'язань сторонами у повному обсязі, крім випадків прямо передбачених. Тобто у всіх договорах на закупівлю до істотних умов законодавець відніс лише умови про предмет та ціну. Як бути с іншими умовами, віднести їх до звичайних? Ми можемо вказати на те, що в пропозиції конкурсних торгів (цінової пропозиції) містяться не умови договору, а виключно інформація про предмет закупівлі (лоти) та ціну пропозиції.

По-третє, нова для цивілістів правова конструкція «строк на укладання договору». Так, наприклад у відкритих торгах, замовник укладає договір про закупівлю з учасником, пропозицію конкурсних торгів якого було акцептовано, не пізніше ніж через 20 днів з дня акцепту пропозиції відповідно до вимог документації конкурсних торгів та акцептованої пропозиції. З метою забезпечення права на оскарження рішень замовника договір про закупівлю не може бути укладеним раніше ніж через 10 днів з дати публікації у державному офіційному друкованому виданні з питань державних закупівель повідомлення про акцепт пропозиції конкурсних торгів. Цей безпідставно скорочений строк фактично обмежує сторони в часі та правовому просторі та не має прямих аналогів в цивільному та адміністративному праві.

Як висновок можемо зазначити таке:

- по-перше, необхідно розробити методичні вказівки щодо розслідування кіберзлочинів у сфері державних закупівель;

- по-друге, автор вважає, що природа відносин із закупівлі – цивільно–правова, відповідно Цивільний та Господарський кодекси України повинні бути загальними нормативними ак-

тами до наказів та інструкцій Міністерства економічного розвитку і торгівлі з означених питань;

- законодавство з державних закупівель потребує уніфікації та удосконалення.

Одержано 25.10.2017

УДК 341.1.8

Микола Іванович МАРЧУК,
кандидат юридичних наук, доцент, завідувач кафедри конституційного і міжнародного права факультету № 4 Харківського національного університету внутрішніх справ

ІНФОРМАЦІЙНА БЕЗПЕКА ПРАВООХОРОННОЇ СФЕРИ УКРАЇНИ

У сьогоднішніх реаліях в Україні назріла нагальна потреба у формуванні нової, цілісної, науково обґрунтованої системи гарантування інформаційної безпеки, котра має реалізовуватися не тільки на зовнішньополітичній арені та протидіяти таким сучасним викликам як гібридна війна, транснаціональна злочинність, міжнародний тероризм та ін., але й забезпечувати функціонування корпоративних організацій публічно-правового та приватно-правового характеру на загальнодержавному та локальному рівнях.

Особливості реалізації інформаційної безпеки обумовлюються специфікою конкретної сфери суспільного життя. Наприклад, в економічній сфері це протидія промисловому шпіонажу чи банківська таємниця, у політичній – це питання національної безпеки та дипломатичні місії, у військовій сфері – інформація про нові типи озброєння та військову інфраструктуру. Свої особливості має й процес досягнення стану інформаційної безпеки й у правоохоронній сфері і, в тому числі, й у діяльності Національної Поліції України.

Правоохоронні органи, зокрема Національна Поліція України, є складовою частиною системи інформаційної безпеки держави. Вони мають специфічні особливості функціонування в інформаційному середовищі як організація та орган охорони інформаційних прав особистості. Кожен вид інформаційної діяльності працівників правоохоронних органів вирізняється специфічними правилами та порядком їх здійснення, які встановлюються спеціальними правовими нормами. Визначення конкретного змісту правової норми, яка регламентує діяльність суб'єктів інформаційних правовідносин є складним

з огляду на їх різноплановість та нерівноправність (ієрархічність) і, як правило, визначається правовими нормами, що регулюють кожний конкретний вид інформаційної діяльності. Так обсяг прав і обов'язків правоохоронних органів щодо здійснення діяльності, спрямованої на охорону і захист життєво важливих інтересів особи, суспільства і держави від загроз в інформаційній сфері, встановлено Конституцією, законами та підзаконними нормативно¬-правовими актами України.

Специфіка діяльності правоохоронних органів за сучасних умов, а також неординарність завдань, виконання яких покладають на ці органи, обумовлюють особливі вимоги до їхнього інформаційного забезпечення і системи захисту інформації. Інформаційна безпека правоохоронних органів відображає стан захищеності прав та інтересів держави, суспільства, окремих фізичних і юридичних осіб, що стосуються збирання, обробки, зберігання, поширення інформації та доступу до неї.

Однак захист інформації не належить до основних функцій правоохоронних органів України, тому їхню діяльність не сконцентровано на забезпеченні власної інформаційної безпеки. Такий стан зумовлений відсутністю єдиної системи служб і підрозділів, робота яких базувалася б на забезпеченні захисту інформації на різних рівнях. Адже важливість інформації, котра потребує належного убезпечення під час роботи правоохоронних органів, вимірюється за шкалою «від особи – до держави».

На думку Д. О. Красікова, забезпечення інформаційної безпеки правоохоронних органів України здійснюють за двома формами:

– організаційною (організація роботи правоохоронних органів, роботи, пов'язаної з обігом, збиранням, обробкою, зберіганням та використанням інформації, взаємодія працівників правоохоронних органів щодо забезпечення інформаційної безпеки);

– правовою (видання наказів та розпоряджень, розроблення положень, інструкцій, складання планів тощо) [1].

Проаналізувавши практичну діяльність правоохоронних органів, уважаємо за доцільне розмежувати форми гарантування їхньої інформаційної безпеки на:

– законодавчу – ухвалення нормативно¬правових актів, які встановлюють правила використання й обробки інформації, доступ до якої обмежено, та визначають ступінь відповідальності за порушення цих правил;

– технічну – регулювання доступу до всіх ресурсів інформаційної системи (технічних, програмних, елементів баз даних), регламентація порядку роботи користувачів і персоналу, обмеження права доступу до окремих файлів тощо.

Водночас процедура застосування механізмів забезпечення інформаційної безпеки діяльності правоохоронних органів України не може обмежувати права і свободи людини та громадянина в інформаційні сфері. Ці питання має бути збалансовано на основі прийняття нормативно¬правових актів, де чітко було б визначено обов'язки та повноваження правоохоронних органів України щодо застосування заходів інформаційної безпеки та надання доступу до певних видів інформації (або відмови в ньому) фізичним і юридичним особам.

Досвід роботи поліції зарубіжних країн стосовно забезпечення інформаційної безпеки дає змогу виокремити два напрями діяльності вітчизняних правоохоронних органів. Перший – полягає в удосконаленні діяльності правоохоронних органів щодо гарантування власної інформаційної безпеки зсередини, тобто, так званої внутрішньої реформи. Другий – у поліпшенні правового забезпечення інформаційної безпеки на державному рівні, тобто в імплементації своєрідної зовнішньої реформи.

Задіюючи такі механізми вдосконалення процесу забезпечення інформаційної безпеки, слід пам'ятати про їхній взаємозв'язок. Адже задля досягнення вищого рівня забезпечення інформаційної безпеки правоохоронних органів необхідна не тільки трансформація чинного законодавства, а й навички його реалізації. Такий комплекс заходів спроможний, на нашу думку, активізувати всі чинники, необхідні для гарантування інформаційної безпеки нашої держави.

Список використаних джерел:

1. Красіков Д. О. Правове забезпечення інформаційної безпеки в діяльності органів внутрішніх справ України: автореф. дис. ... канд. юрид. наук: 12.00.07. К., 2012. 20 с.

Одержано 30.10.2017

УДК 341.1.8

Ірина Миколаївна МЕЛЬНИК,
слухач магістратури факультету №1 Харківського національного університету внутрішніх справ

Андрій Васильович ВОЙЦІХОВСЬКИЙ,
кандидат юридичних наук, доцент, професор кафедри конституційного і міжнародного права факультету № 4 Харківського національного університету внутрішніх справ

ПОШИРЕННЯ ДИТЯЧОЇ ПОРНОГРАФІЇ В ІНТЕРНЕТІ ЯК ЗАГРОЗА ДЛЯ УКРАЇНСЬКОГО СУСПІЛЬСТВА

У процесі розвитку комп'ютерних технологій, особливо мережі Інтернет, з'явились можливості передачі рухомого зображення і звуку, що стало для сучасного суспільства великим досягненням. Однак, завдяки цьому, суспільство також зіткнулось з проблемою розповсюдження порнографії, у тому числі дитячої. Передача її по мережі Інтернет, так би мовити, забезпечує розповсюджувачам та споживачам анонімність і ускладнює задачу державним органам в боротьбі з цим видом злочинності.

Нині не існує єдиного центру для збереження і поширення інформації. У зв'язку з чим жодна установа з технічної точки зору не здатна контролювати всю інформацію, що передається через Інтернет. Ряд інтернет-ресурсів, до яких відносяться й такі, що містять дитячу порнографію, викликають серйозне занепокоєння в суспільстві.

Суспільна небезпека цих злочинів полягає в тому, що дані злочинні дії порушують духовні принципи людського буття, є антиморальними та неприпустимими в сучасному суспільстві, адже вони несуть небезпеку й для самих дітей. Це стосується тих випадків, коли дітей в цілях виготовлення дитячої порнографії знімають відеокамерою або, коли вони отримують такий матеріал як глядачі, чим завдають велику шкоду власному психологічному розвитку.

За даними Міжнародної правозахисної організації «End Child Prostitution Child Pornography & Trafficking of Children for Sexual Purposes» (ECPAT International) найчастіше об'єктами злочину стають саме російські, білоруські і українські діти. Це здебільшого діти віком від 10 до 14 років, які є безпритульними або з неблагополучних сімей. У 80% випадків дитяча порнографія поширюється через мережу Інтернет. Це стало свого роду бізнесом на чорному ринку. За оцінками МВС України,

вітчизняна порноіндустрія приносить залученим у неї людям близько 100 мільйонів доларів США щорічно.

Кожна країна світу намагається протидіяти цьому негативному явищу. Наприклад, у США дитяча порнографія вважається кримінальним злочином, який відноситься до категорії насильницьких, тобто найбільш тяжких злочинів. Пункт 2252 глави 110 Кримінального кодексу США забороняє перевезення, відправку чи отримання дитячої порнографії по каналах зв'язку між штатами, включаючи поштові та комп'ютерні засоби зв'язку. Боротьба з цими злочинами покладається на Федеральне бюро розслідувань США, яке тісно співпрацює з Митною та поштовою службами. Також ці служби спільно проводять спецоперації щодо виявлення фактів розповсюдження дитячої порнографії і доволі часто ці спецоперації є успішними.

Канада ухвалила закон, згідно з яким навіть пошук дитячої порнографії у світовій мережі Інтернет є кримінально караним діянням, навіть якщо обвинувачений нічого не знайшов. Такі, можливо, жорсткі заходи можуть хоча б якось зменшити ризик подальшого розповсюдження дитячої порнографії.

20 січня 2010 року був прийнятий Закон України № 1819-VI «Про внесення змін до деяких законодавчих актів України щодо протидії розповсюдженню дитячої порнографії», який пропонує системний підхід у боротьбі з таким ганебним явищем, як дитяча порнографія. Зміни внесено до законів України «Про захист суспільної моралі», «Про телекомунікації» та Кримінального кодексу України.

Змінами до ст. 301 Кримінального кодексу України посилено відповідальність за поширення порнографічної продукції за допомогою комп'ютерних програм, за що передбачено покарання позбавленням волі на строк до 12 років.

В Україні профілактикою сексуальної експлуатації дітей займаються: Уповноважений Верховної Ради України з прав людини; Уповноважений Президента України з прав дитини; Міністерство соціальної політики України; Служби у справах дітей; Центри соціальних служб для сім'ї, дітей та молоді; Національна поліція України; Міністерство освіти і науки України, навчальні заклади; громадські організації та ін.

Стрімкий розвиток сучасних інформаційних технологій ставить перед правоохоронними органами все нові проблеми у сфері протидії розповсюдженню порнографії. Зокрема, висо-

кими темпами розробляються зручні в застосуванні кодовані комп'ютерні програми, якими часто користуються особи, що займаються розповсюдженням дитячої порнографії.

Сьогодні однозначно можна сказати, що ні держави, ні інші міжнародні спеціалізовані інституції не можуть самостійно боротися в повній мірі з тими викликами, які постали у зв'язку із розвитком мережі Інтернет. До них, в першу чергу, слід віднести й поширення в Інтернеті дитячої порнографії, що є свідченням потреби співпраці держав і громадянського суспільства в пошуку вирішення даних викликів та вироблення міжнародних стандартів у зазначеній сфері [1].

Список використаних джерел:

1. Плахотнюк Н. В. Міжнародно-правові аспекти боротьби з торгівлею жінками та дітьми: дис. … канд. юрид. наук: 12.00.11. К. 2002. 219 с.

Одержано 30.10.2017

УДК 342.98:343.43

Ольга Миколаївна МЕРДОВА,
кандидат юридичних наук, завідувач кафедри адміністративно-правових дисциплін Донецького юридичного інституту МВС України

РОЛЬ ДЕПАРТАМЕНТУ ПРЕВЕНТИВНОЇ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ У ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ

Проблема протидії торгівлі людьми в останні роки привертає велику увагу державних органів всіх рівнів, зокрема, правоохоронних органів, неурядових громадських організацій та всіх небайдужих до цього негативного явища сьогодення.

Протягом останніх десятиріч зусилля розбудови спроможності у боротьбі з торгівлею людьми скеровувалися майже виключно до спеціалізованих підрозділів органів внутрішніх справ. Так, у системі Міністерства внутрішніх справ України ще з 2000-х років почали створюватися перші спеціалізовані підрозділи, діяльність яких полягала у протидії торгівлі людьми, що передбачалося державною Комплексною програмою дій із запобігання торгівлі жінками та дітьми на 1999-2001рр, а на сьогодні це підрозділи боротьби зі злочинами, пов'язаними з торгівлею людьми. Однак, казати про те, що тільки ці підрозділи повинні протидіяти цьому негативному явищу, є безпідставним. У протидії торгівлі людьми повинен застосовуватися комплексний підхід із застосуванням всіх можливих сил і засобів, який передбачає попередження торгівлі людьми, переслідування осіб, які вчиняють такі злочини

або сприяють їх вчиненню, а також зміцнення захисту постраждалих. Отже, цілком доречно стверджувати про певну роль у боротьбі з торгівлею людьми всіх підрозділів Національної поліції.

На сьогоднішній день роль Департаменту превентивної діяльності Національної поліції у протидії торгівлі людьми полягає у реалізації поліцейської превенції, яка здійснюється шляхом виявлення, попередження, недопущення і припинення злочинів, що готуються, виявлення і проведення необхідної роботи з особами, схильними до скоєння таких злочинів, наданні допомоги спеціалізованим підрозділам поліції у розслідуванні злочинів, пов'язаних з торгівлею людьми, розшуку і затриманні злочинців, здійсненні юрисдикційної діяльності.

Слід відзначити, що практичні працівники поліції наголошують на тому, що доволі часто при виявленні злочинів, пов'язаних з торгівлею людьми, які відзначаються підвищеною латентністю, ключову роль відіграють поліцейські, які працюють «на землі» і є найбільш наближеними до населення – служба дільничних офіцерів поліції, за умов належного виконання її працівниками повсякденних обов'язків на адміністративній дільниці, вмілого використання своїх зв'язків. Дільничні офіцери поліції мають можливість, як ніхто інший, виявляти осіб, що мають відношення до вчинення злочинів, пов'язаних із торгівлею людьми, та своєчасно інформувати зацікавлені спеціалізовані підрозділи поліції, а також вживати у встановленому порядку і в межах своєї компетенції заходи з протидії зазначеній категорії злочинів. Саме ці підрозділи, враховуючи їх максимальне наближення до населення, мають змогу здійснювати оцінку імовірності потрапляння осіб із уразливих категорій населення у ситуації пов'язані із торгівлею людьми. Особливу увагу дільничні офіцери поліції приділяють здійсненню індивідуально-профілактичній роботі з особами, які були засуджені за вчинення торгівлі людьми за ст. 149 КК України, та з особами, що були причетні до зазначеної категорії злочинів.

Особливу роль у попередженні злочинів, пов'язаних із торгівлею людьми, щодо неповнолітніх осіб відводиться підрозділам ювенальної превенції, працівники яких здійснюють комплекс заходів серед неповнолітніх у питаннях недопущення фактів їх експлуатації, а також виявлення осіб, які вчиняють відносно неповнолітніх, злочини передбачені ст. 149 КК України.

Недостатня або викривлена поінформованість населення про причини торгівлі людьми та про те, яким чином убезпечити себе від потрапляння до тенет торгівців людьми, є одним із важливих чинників поширення цього явища. Через підвищення поінформованості населення про можливі небезпеки та шляхи їх уникнення працівники Департаменту превентивної діяльності Національної поліції суттєво впливають на зменшення таких ризиків. Така превентивна робота здійснюється із застосуванням різних форм:

- поширення листівок, брошур та інших інформаційних матеріалів серед громадян, які входять до групи ризику;
- проведення бесід з громадянами, які планують виїзд за кордон чи до інших регіонів України з різних причин, особливо у пошуках роботи;
- проведення лекцій для різних категорій громадян із залученням спеціально підготовлених фахівців, у тому числі з неурядових організацій;
- звернення до громадськості через засоби масової інформації (газети, радіо, телебачення) [1, с. 25].

Підсумовуючи зазначу, що на сьогоднішній день вкрай актуальними питаннями є удосконалення нормативно-правової основи превентивної діяльності як підрозділів Національної поліції, так й інших правоохоронних структур, а також створення оптимальної системи науково-методичного і інформаційного забезпечення превентивної діяльності у сфері протидії торгівлі людьми, адаптованої до особливостей сьогодення, пов'язаних з існуванням збройного конфлікту на сході нашої країни.

Список використаних джерел:

1. Протидія торгівлі людьми : посібник для дільничних інспекторів міліції. К., 2012. 40 с.

Одержано 25.10.2017

УДК 351.74 (477)

Вадим Олександрович НЕГОДЧЕНКО,
доктор юридичних наук, доцент, заступник начальника Управління поліції охорони в Дніпропетровській області

НАПРЯМИ УДОСКОНАЛЕННЯ ОРГАНІЗАЦІЙНО-ПРАВОВИХ ЗАСАД ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ ОРГАНАМИ ПОЛІЦІЇ УКРАЇНИ

Особливості сучасного розвитку суспільства зумовлюють постійне підвищення ролі інформації у сфері державного управління. Не є виключенням і діяльність органів поліції, що обумовлює нові виклики та можливості в інформаційній сфері, до яких даний орган має адаптуватися з метою ефективного виконання покладених на нього завдань в умовах, що змінюються.

Суттєвим недоліком сучасного стану реалізації державної інформаційної політики держави є фактична відсутність стратегічних програмних документів у цій сфері. Так, у 2015 р. сплив термін дії Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки». При цьому за результатами парламентських слухань «Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України» 31 березня 2016 р. констатовано, що план дій щодо його реалізації не було виконано. Відповідно сьогодні існує потреба в прийнятті нового програмного законодавчого акта у сфері розвитку інформаційного суспільства в Україні, який би враховував сучасний рівень розвитку інформаційних технологій.

Національна поліція – це, передусім, правоохоронний орган, а її діяльність, у першу чергу, має спрямовуватися на забезпечення безпеки, захист прав і свобод людини, інтересів суспільства та держави в усіх сферах суспільного життя, зокрема в інформаційній. Даний аспект діяльності Національної поліції відображено, зокрема, в Стратегії кібербезпеки України, затвердженій указом Президента України від 15.03.2016 р. № 96/2016. Документ визначає такі завдання Національної поліції у розглядуваній сфері, як: забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі.

У структурі Національної поліції виконання наведених завдань покладено, у першу чергу, на Департамент кіберполіції. Аналіз функцій даного департаменту дозволяє свідчити, що вони, в цілому, повною мірою закріплюють та конкретизують завдання, поставлені перед Національною поліцією у сфері забезпечення кібербезпеки. Однак слід мати на увазі, що вказаний підрозділ є відносно новим, що потребує проведення значної роботи стосовно нормативно-правового та організаційного забезпечення його діяльності. Передусім, це має стосуватися налагодження взаємодії з іншими органами та підрозділами поліції та правоохоронними органами України. Необхідність забезпечення взаємодії з іншими підрозділами поліції посилюється з огляду на особливості організації Департаменту кіберполіції як міжрегіонального територіального органу поліції, що безпосередньо не підпорядкований головним управлінням Національної поліції на місцях.

Не менш важливим є забезпечення ефективної міжнародної співпраці у галузі протидії злочинам у сфері високих технологій. Так, Стратегія кібербезпеки України прямо визначає необхідність досягнення сумісності кіберполіції з відповідними підрозділами держав – членів НАТО.

Зауважимо, що абз. 4 п. 2 р. 1 Рішення РНБО України «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» від 28.04.2014 р. додатково передбачає необхідність прийняття Закону України «Про кібернетичну безпеку України». Даний законодавчий акт має визначити основні засади державної політики, спрямованої на захист життєво важливих інтересів особи, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем. Зокрема, вважаємо за доцільне серед основних суб'єктів забезпечення кібернетичної безпеки окремо закріпити Міністерство внутрішніх справ України та Національну поліцію. Якщо на Міністерство внутрішніх справ України доцільно покласти функцію з участі у формуванні та реалізації державної політики з питань боротьби з кіберзлочинами, у тому числі такими, що вчиняються з терористичною метою, то на органи Національної поліції вважаємо за необхідне покласти наступні функції у даній сфері: а) забезпечення у межах своєї компетенції безпеки громадян у національному сегменті кіберпростору; б) вжиття необхідних заходів щодо попередження, своєчасного виявлення, припи-

нення і розкриття кіберзлочинів; в) забезпечення належного функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні кіберзлочинів; г) забезпечення взаємодії з операторами та провайдерами телекомунікацій з питань попередження кіберінцидентів кримінального характеру; д) взаємодія з компетентними органами інших країн в рамках надання міжнародно-правової допомоги у протидії кіберзлочинам тощо.

Сьогодні можна визначити наступні ключові напрями удосконалення забезпечення державної інформаційної політики в органах поліції. По-перше, необхідним є забезпечення подальшого розвитку кіберполіції як органу, який покликаний забезпечувати виконання завдань щодо протидії злочинності у сфері інформаційних технологій. Украй необхідним є вироблення механізму взаємодії даних підрозділів як з іншими підрозділами поліції, так і з іншими правоохоронними органами як України, так і зарубіжних держав. По-друге, важливим є запровадження механізму електронного урядування в органах поліції. По-третє, необхідним є розширення практики використання інформаційних технологій у службовій діяльності, в тому числі шляхом максимального використання можливостей систем «CrimeMapping», у тому числі з використанням американського досвіду функціонування системи «Compstat». По-четверте, суттєвого удосконалення потребує такий напрям роботи, як налагодження інформаційних каналів з громадськістю, зокрема щодо інформування органів державної влади та органів місцевого самоврядування, а також громадськості про діяльність органів та підрозділів поліції.

Одержано 30.10.2017

УДК 342.9

Євгеній Костятинович ПАНІОТОВ,
аспірант Міжнародного економіко-гуманітарного університету імені академіка Степана Дем'янчука; заступник начальника Департаменту міжнародного поліцейського співробітництва Національної поліції України

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ СИСТЕМ ІНТЕРПОЛУ ДЛЯ ПРОТИДІЇ ЗЛОЧИННОСТІ

Міжнародне правоохоронне співтовариство, у тому числі правоохоронці практики, науковці – розглядають Міжнародну організацію кримінальної поліції – Інтерпол як, по-перше, сві-

товий інформаційно-аналітичний центр з питань боротьби зі злочинністю, а по-друге, як практичний інструмент міжнародного поліцейського співробітництва у цій сфері.

Наряду із правовими та організаційними механізмами, що дозволяють Інтерполу багато десятиріч зберігати за собою статус чи не основного засобу міжнародного поліцейського співробітництва у правоохоронній галузі, неабияку важливість для підтримання такого реноме відіграє саме технологічна складова діяльності цієї Організації.

Основними технічними інструментами Інтерполу, завдяки яким забезпечується міжнародне співробітництво правоохоронних органів під час протидії злочинності, є його інформаційно-пошукова система I-24/7 та банки даних.

Інформаційно-пошукова система I-24/7 – це глобальна телекомунікаційна система Міжнародної організації кримінальної поліції – Інтерпол, яка побудована з урахуванням новітніх інформаційних технологій та надає якісний та конфіденційний цілодобовий безпосередній доступ до інформаційних ресурсів Генерального секретаріату Інтерполу, а також дозволяє здійснювати обмін інформацією між національними центральними бюро Інтерполу.

За період використання система I-24/7 зарекомендувала себе як ефективний інструмент міжнародного співробітництва в боротьбі зі злочинністю, у тому числі у сфері забезпечення безпеки кордонів.

У системі I-24/7 забезпечується захист інформації від несанкціонованого та неконтрольованого ознайомлення, модифікації, знищення, копіювання, поширення. Доступ до інформації надається тільки ідентифікованим та автентифікованим користувачам. У системі також здійснюється реєстрація результатів ідентифікації та автентифікації користувачів, результатів виконання користувачем операцій з обробки інформації, спроб несанкціонованих дій з інформацією, фактів надання та позбавлення користувачів права доступу до інформації та її обробки, а також результатів перевірки цілісності засобів захисту інформації.

Банки даних Генерального секретаріату Інтерполу – це система програмно-апаратних, мовних та організаційних засобів Генерального секретаріату Інтерполу, призначених для централізованого накопичення та колективного використання інформації, а також сама інформація про розшукувані, викрадені, втрачені або виявлені предмети, осіб, які перехову-

ються від правоохоронних органів, зникли безвісти або не можуть повідомити про себе ніяких відомостей тощо.

Система I-24/7 використовується правоохоронними органами України з 2003 року. Упродовж 2003-2006 років робочі станції системи були встановлені в Робочому апараті Укрбюро Інтерполу і його територіальних підрозділах. Крім того, поетапно робочі станції мережі I-24/7 встановлювались в окремих структурних підрозділах центрального апарату МВС і в інших правоохоронних органах, наприклад в підрозділах ДАІ, пізніше – міграційної служби тощо. Однак, оскільки технологія підключення через окремі робочі станції є достатньо коштовною, значного розширення мережі доступу до банків даних Інтерполу в Україні тривалий час не відбувалось.

У 2015 році в Україні була впроваджена технологія підключення до комунікаційної системи Інтерполу FIND (Fixed INTERPOL Network Database – фіксована мережна бази даних Інтерполу), що передбачає інтеграцію комунікаційної мережі Інтерполу з комунікаційними системами національних правоохоронних органів. Уперше в Україні цю технологію було застосовано для підключення до банків даних Інтерполу Державної прикордонної служби України. Так, унаслідок запровадження в Україні обов'язкових перевірок за банками даних Інтерполу осіб, які перетинають державний кордон, стало можливим виявляти осіб, які переховуються від кримінального переслідування та оголошені в міжнародний розшук каналами Інтерполу. Згідно із наявною статистикою, у 2012 році на території України було встановлено 57 осіб, які значились в міжнародному розшуку згідно з банками даних Інтерполу, у 2013 – 40 осіб, у 2014 – 44 особи. Але внаслідок впровадження новітніх технологій Інтерполу, вже у 2015 році кількість таких осіб встановлених в Україні сягнула – 131, а у 2016 – 312 осіб – тобто збільшення порівняно з 2012-2014 роками в шість разів. Згідно останніх статистичних даних Департаменту міжнародного поліцейського співробітництва за 9 місяців 2017 року, в Україні було встановлено місцезнаходження вже 366 осіб, розшукуваних за вчинення злочинів іноземними правоохоронними органами на міжнародному рівні.

Слід також відзначити, що у даний час Національною поліцією України за підтримки Консультативної місії Європейського Союзу в Україні реалізовується проект міжнародної технічної допомоги в рамках якого здійснюється розроблення програмного забезпечення та закупівля обладнання, що дозво-

лить вже у поточному 2017 році впровадити технологію FIND в Національній поліції і надавати доступ до комунікаційної системи Інтерполу всім підрозділам поліції, що мають потребу використовувати банки даних Інтерполу у повсякденній роботі.

У зв'язку із цим відзначаємо неабияку актуальність питання щодо навчання поліцейських-практиків роботі з інформаційними ресурсами Інтерполу, що у свою чергу, на наш погляд, вимагає уваги і з боку навчальних закладів, які здійснюють підготовку відповідних фахівців.

Одержано 31.10.2017

УДК 343.9 : 004 : 343.3/7

Олександр Сергійович ПИРОЖЕНКО,
кандидат юридичних наук, доцент, професор кафедри соціально-економічних дисциплін Комунального закладу «Харківська гуманітарно-педагогічна академія» Харківської обласної ради, адвокат

ДО ПИТАННЯ ПРО НАПРЯМИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

На сучасному етапі розвитку людської цивілізації інформаційна сфера є системоутворюючим фактором життя суспільства, безпосереднім чинником економічного зростання. Розвиток інформаційних та телекомунікаційних технологій сприяє розширенню можливостей управління різними процесами, що впливає на забезпечення соціально-економічної стабільності й обороноздатності країни.

Комплексне і широкомасштабне використання персональних комп'ютерів, інформаційно-обчислювальних мереж і комп'ютеризованих комунікаційних систем призвело до появи нового стратегічно важливого ресурсу, що потребує всебічної охорони, – інформації. У зв'язку з цим інформаційна безпека є однією зі складових національної безпеки держави.

Одним із негативних наслідків науково-технічного прогресу безумовно стало виникнення нових видів суспільно небезпечних діянь – «кіберзлочинів», які проявляються у багатьох сферах життєдіяльності людини (від викрадення коштів з банківського рахунку потерпілого до отримання контролю над транспортним засобом чи повітряним судном).

У науковій юридичній літературі справедливо відмічається, що основною проблемою боротьби зі злочинністю в мережі Інтернет є транснаціональність самої мережі і відсутність механізмів контролю. Відтак, світова спільнота перебуває у пос-

тійному пошуку дієвих способів та засобів протидії кіберзлочинності, іноді нехтуючи природними правами і свободами конкретної людини з метою «забезпечення загального блага».

Відмітимо, що функції з протидії кіберзлочинам покладають на поліцію, органи державної безпеки, спеціальні служби захисту інформації тощо. При цьому нерідко створюються спеціальні підрозділи, головним завданням яких є:

– моніторинг кіберпростору з метою виявлення кіберзлочинів, вірусів або шкідливого програмного забезпечення;

– здійснення оперативно-розшукових та розвідувальних заходів з метою фіксування протиправної діяльності кіберзлочинців;

– розслідування кіберзлочинів, надання методичної та практичної допомоги іншим галузевим службам і правоохоронним органам у межах своєї компетенції;

– накопичення, узагальнення та аналіз інформації про кіберзлочинність;

– профілактику кіберзлочинів за допомогою громадськості та засобів масової інформації тощо [1, с. 109].

Ефективність виконання згаданими вище органами завдань у сфері інформаційної безпеки істотно залежить від якості підготовки персоналу. В цьому вагоме слово повинні промовляти заклади із специфічними умовами навчання, які здійснюють підготовку фахівців по боротьбі з кіберзлочинністю. Погоджуючись з колегами з Національної академії прокуратури України слід відмітити, що, окрім підготовки поліцейських, важливою складовою у протидії злочинам, що вчинюються з використанням інформаційних та інформаційно-телекомунікаційних технологій, є відповідна підготовка прокурорів (державних обвинувачів) та суддів [2].

Важливим елементом у системі заходів боротьби з кіберзлочинністю є створення захищеної інформаційної інфраструктури. Своєчасне удосконалення комплексів програмно-технічних засобів, організаційних систем та нормативних баз забезпечить швидку організацію взаємодії інформаційних потоків, якісне функціонування та всебічний розвиток засобів інформаційної взаємодії та інформаційного простору. Цікавим прикладом такої взаємодії є проект протидії кіберзлочинності, що з 2013 року реалізовується спільними зусиллями Національної асоціації банків України, Національного банку України, Департаменту кіберполіції та банками-членами НАБУ. Головна мета проекту – створення Єдиної інформаційної бази банків

для запобігання кібершахрайству на загальнодержавному рівні [3].

Досягнення позитивних результатів у сфері протидії кіберзлочинності є абсолютно неможливим без відповідної профілактичної роботи серед населення та інформування суспільства про нові види кіберзагроз. При цьому вказані функції повинні реалізовуватися не тільки правоохоронними органами, а й громадськими організаціями масштабу Transparency International, Greenpeace, Amnesty International тощо.

Наостанок відмітимо, що кіберзлочинність – проблема XXI століття, яка невпинно зростає та поглинає все більше фінансових ресурсів. Незважаючи на заходи, що вживаються окремими особами, як фізичними, так і юридичними, державою, це явище продовжує існувати та розширює масштаби своєї діяльності, збільшуючи прибутки правопорушників. Тому на сьогодні особливо важливим питанням є усвідомлення глибини даної проблеми, прогнозування подальших напрямів її розвитку та дія на випередження.

Список використаних джерел:

1. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і безпека.* 2015. № 2. С. 107-113.
2. До питання протидії кіберзлочинності в Україні. URL: http://www.akademia.gp.gov.ua/userfiles/file/Academia2016/Akt_schema/123441234524.pdf. (дата звернення: 28.10.2017).
3. Протидія кіберзлочинності. URL: https://nabu.ua/ua/protidiya-kiberzlochinnosti.html (дата звернення: 28.10.2017).

Одержано 30.10.2017

УДК 342.98

Віктор Миколайович ПЛЕТЕНЕЦЬ,
кандидат юридичних наук, доцент кафедри криміналістики, судової медицини та психіатрії факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ

Катерина Вікторівна КАРАБУТА,
курсант КМ-443 факультету підготовки фахівців для підрозділів кримінальної поліції Дніпропетровського державного університету внутрішніх справ

ШАХРАЙСТВО У КІБЕРПРОСТОРІ: ОКРЕМІ АСПЕКТИ ПРОТИДІЇ

На сучасному етапі розвитку інформаційних технологій шахрайство посідає особливе місце. Це пов'язано з тим, що з

кожним роком інформаційні технології все більше проникають в наше повсякденне життя. Останнім кроком буде перехід на електронні гроші. Це ми можемо побачити, з сучасної політики передових країн світу.

Однак дане положення провокує появу інтелектуальних правопорушників «хакерів». Дана ситуація виходить з того, що вислідити правопорушників дуже складно, бо вони працюють дистанційно.

Згідно тлумачення видатного криміналіста Р. С. Бєлкіна комп'ютерна інформація – інформація на машинному носії, в ЕОМ, системі або мережі ЕОМ – також може бути криміналістично значимою, при розслідуванні і комп'ютерних злочинів, і посягань, де ЕОМ виступає як об'єкт (крадіжка комп'ютера, незаконне використання машинного часу) або засіб скоєння злочину (використання ЕОМ для накопичення інформації, підробки документів і ін.). Програмні продукти теж можуть використовуватися і в якості об'єкту злочину (незаконне копіювання, спричинення збитку застосуванням руйнівних програм - вірусів), і в якості інструменту скоєння злочину (несанкціоноване проникнення в комп'ютерну систему, спотворення і підробки інформації) [1, с. 945].

Необхідно відзначити, що підвищення ефективності попереднього розслідування у кримінальних справах про кіберзлочинність неможливе без визначення чинників, які здатні робити помітний негативний вплив на якість процедури розслідування кримінального провадження. По-перше, це стосується недосконалості норм вітчизняного кримінального права, що передбачають відповідальність за кіберзлочинності. Ця проблема зумовлює неминуче виникнення труднощів в правильній кваліфікації даного різновиду шахрайства. По-друге, відсутнє повною мірою адекватне криміногенній ситуації, що склалася, криміналістичне забезпечення процедури розслідування цієї категорії кримінальних справ (як на рівні криміналістичної методики, так і на рівнях криміналістичної тактики і техніки). По-третє, міра професійної кваліфікації суб'єктів розслідування не завжди повною мірою відповідає сучасним вимогам, що, безумовно, не може не позначитися на якості. По-четверте, негативне дію чинить недостатня координація спільних зусиль правоохоронних органів з державними і недержавними структурами, що спеціалізуються на забезпеченні безпеки у сфері телекомунікації і комп'ютерній інформації [2, с. 213].

Інтернет шахраї є вигадливими не тільки у способах вчинення, й маскування свої дій. Так, 30 вересня 2017 року працівниками кіберполіції було затримано інтернет-шахрая, який ретельно конспірував свою злочинну діяльність: розміщував оголошення на сайті, знаходячись у громадських місцях, де є вільний доступ до мережі Інтернет, аби ускладнити пошук його місцезнаходження. У знайомого він придбав банківські картки, на які отримував гроші від потерпілих. А знімав гроші з банкоматів у медичній масці, аби камери терміналів не зафіксували його обличчя [3]. І подібні випадки є непоодинокими.

Однак, як відзначає Шапочка С. В. [4, с. 227] з'явилося і нове явище, що виникло в мережі Інтернет менше п'яти років тому. Йдеться про широке розповсюдження і популяризацію використання децентралізованих віртуальних криптовалют (Bitcoin, Litecoin, Namecoin, Zerocoin, Quark, Megacoin, Peercoin, Worldcoin, тощо), темпи приросту капіталу їх власників склали 100 %, 200 % і навіть 1000 % на день. Криптовалюта стала одним із видів електронних платіжних засобів для оплати товарів і послуг в мережі Інтернет, яку також можна обміняти на реальні гроші. На даний час, нерегульована сфера віртуальних валют, користується великою популярністю серед організованих злочинних угруповань, що вже приймають оплату за свої послуги в віртуальній валюті, використовуючи альтернативний Інтернет – DarkNet, що функціонує на основі системи TOR (The Onion Router) [4, с. 227]. В таких країнах, як Росія, Тайланд та Китай Bitcoin фактично поза законом. Взяти наприклад Національний банк Китайської Народної Республіки, який наклав заборону на кредитно-фінансові установи проводити будь-які операції із використанням крипто валюти Bitcoin.

В Україні, жорстка реакція з боку влади, щодо здійснення банківських операцій з використанням криптовалюти відсутня. Ми можемо погодитися з думкою Шапочки С. В., що це пов’язано з недооцінкою рівня можливого негативного впливу криптовалюти на економіку, стан злочинності та функціонування кредитно-банківської системи держави.

З огляду на вище викладене, ми можемо дійти висновку, що даний напрям наукового дослідження дуже актуальний в наш час, і відкритий для подальшого вивчення та вдосконалення.

Список використаних джерел:

1. Криминалистика: учебник для вузов / под ред. Р. С. Белкина. – М. : НОРМА, 2001. – С. 990.
2. Антонов И. О., Шилимов А. Н. Актуальные проблемы расследования мошенничетсва с исмользованием компьютерной информации. *Ученые записки Казанского университета.* 2015. Том 157, Кн. 6. С. 212–220.
3. Працівники кіберполіції затримали інтернет-шахрая, який переховувався від органів слідства. URL: https://cyberpolice.gov.ua/news/praczivnyky-kiberpolicziyi-zatrymaly-internet-shaxraya-yakyj-perexovuvavsya-vid-organiv-slidstva-637/ (дата звернення: 25.10.2017).
4. Шапочка С. В. Щодо шахрайства, що вчиняється з використанням можливостей мережі інтернет // Збірник науково-практичної конференції «Актуальні проблеми управління інформаційною безпекою держави» (20.03.2014 р., м. Київ,) у 2-х частинах. Ч. 1. С. 226-230.

Одержано 25.10.2017

УДК 343.9 : [343.431 : 061.2] (477)

Максим Юрійович ПОГУЦА,
курсант факультету № 2 Харківського національного університету внутрішніх справ

ЩОДО СУБ'ЄКТІВ ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ В УКРАЇНІ

Свобода людини є однією з головних цінностей сучасного цивілізованого суспільства, а забезпечення недоторканності свободи особи – одна з головних функцій держави. Відповідно до норм міжнародного законодавства, кожна країна, що поважає права людини, повинна гарантувати їх виконання, зокрема запобігання насильству, покарання злочинців, забезпечення компетентного розслідування актів насильства і надання компенсації людині, що постраждала. Однак, за останні роки в умовах глобалізації суспільства набула особливої актуальності проблема торгівлі людьми. Вона охопила всі регіони та країни і стала глобальною.

На сьогоднішній день протидію торгівлі людьми простежуємо на всіх рівнях: глобальному (ООН, Інтерпол), регіональному (ОБСЄ, Рада Європи, ЄС) та державному (державні механізми протидії) [1, с.83].

Протидія торгівлі людьми є одним із пріоритетних напрямів діяльності у сфері захисту прав людини органів законодавчої і виконавчої влади нашої країни. Адже Україна в міжнародній системі ідентифікована як країна – постачальниця

живого товару на ринки Європи, Азії, США та інших країн. Так, за 6 місяців 2017 року Національною поліцією встановлено та надано допомогу 156 потерпілим від злочинів у сфері торгівлі людьми. Про це повідомляє прес-служба Нацполіції, зазначивши, що це більш ніж удвічі більше, ніж упродовж минулого року.

Законом України «Про протидію торгівлі людьми» визначено основні напрями реалізації державної політики, спрямованої на протидію торгівлі людьми. Цим же законом було визначено чітке коло суб'єктів протидії торгівлі людьми, до яких відносяться : 1) Президент України; 2) Кабінет Міністрів України; 3) центральні органи виконавчої влади; 4) місцеві органи виконавчої влади; 5) закордонні дипломатичні установи України; 6) заклади допомоги особам, які постраждали від торгівлі людьми. 2. У здійсненні заходів, спрямованих на попередження протидії торгівлі людьми, беруть участь органи місцевого самоврядування, а також, за згодою, підприємства, установи, організації незалежно від форми власності, громадські організації та окремі громадяни [2].

Для одних із суб'єктів ця діяльність є основною або однією з основних функцій; для інших – однією із функцій у межах організаційно-управлінської діяльності; або однією із функцій у межах правоохоронної діяльності; чи однією із функцій у межах державного управління та іншої загально-соціальної діяльності; неформальною організацією громадського обов'язку.

Розкриємо зміст діяльності основних з них:

Департамент боротьби зі злочинами, пов'язаними з торгівлею людьми, Національної поліції України є структурним підрозділом Національної поліції України, який функціонує у складі кримінальної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері протидії торгівлі людьми, запобігання вчиненню, виявлення, припинення та розкриття кримінальних правопорушень, пов'язаних з нелегальною міграцією, а також правопорушень у сфері суспільної моралі.

Міністерство молоді та спорту України, до функцій якого належать координація заходів органів виконавчої влади щодо протидії торгівлі людьми, реалізація інформаційно-просвітницьких програм у цій сфері, забезпечення координації роботи зі створення центрів реабілітації для осіб, потерпілих від торгівлі людьми.

Міністерство закордонних справ України покликане захищати права та інтереси громадян і юридичних осіб України за кордоном та вести облік громадян України, які постійно або тимчасово проживають за кордоном.

Міністерство соціальної політики України, на яке покладено превентивні функції: надання профорієнтаційних послуг, вирішення питань зайнятості випускників ПТУ й вищих навчальних закладів, сприяння працевлаштуванню молоді, здійснення контролю за посередницькою діяльністю суб'єктів підприємницької діяльності із працевлаштування за кордоном.

Міністерство освіти і науки України залучається до запобігання торгівлі людьми шляхом участі у вирішенні питань зайнятості молоді, проведення серед представників групи ризику роз'яснювальної роботи, видання інформаційних матеріалів щодо означеної проблеми [3, 60-63].

Уповноважений Верховної Ради України з прав людини, метою діяльності якого є, зокрема, захист основних свобод людини й громадянина України, запобігання порушень прав і свобод людини і громадянина або сприяння їх відновленню, сприяння приведенню законодавства України про права та свободи людини і громадянина у відповідність до Конституції України та міжнародних стандартів у цій сфері, запобігання дискримінації стосовно реалізації людиною своїх прав і свобод, сприяння правовій інформованості населення.

Державна прикордонна служба України надає інформацію про нові тенденції, способи та шляхи вивезення людей у тому числі й про способи нелегального вивезення мігрантів із метою подальшої торгівлі ними.

Міжнародні організації (Міжнародна організація з міграції, міжнародна організація праці, ООН, ОБСЄ, та ін.), які надають консультативну допомогу, сприяють в обміні досвідом і кращими міжнародними практиками щодо протидії торгівлі людьми.

Засоби масової інформації. Завданням ЗМІ є інформування суспільства про найболючіші проблеми сьогодення, однією з яких є торгівля людьми, а також проведення активної пропагандистської діяльності попереджувального характеру, надання експертних оцінок і оприлюднення даних, які допомагають людям довідатися про проблему й усвідомити її значущість.

Громадські організації, (22 червня 2011 року в місті Києві створено Всеукраїнську коаліцію громадських організацій

щодо протидії торгівлі людьми) серед основних напрямів діяльності яких є превентивна діяльність, співробітництво із засобами масової інформації, робота «гарячих ліній», надання допомоги мігрантам, які опинилися у скрутному становищі, і зокрема, постраждалим від торгівлі людьми.

Підводячи підсумок викладеному, слід сказати, що вельми широке коло суб'єктів державної та громадської спрямованості в справі протидії торгівлі людьми свідчить про підвищену суспільну небезпечність цього явища. Факт значного поширення в XXI торгівлі людьми, кинув виклик усій світовій спільноті, нівелюючи основні права і свободи людини та загальноприйняті норми і принципи міжнародного права.

Заходи протидії цьому явищу мають базуватися на комплексному системному підході та реалізовуватися шляхом консолідації зусиль як урядових структур, міжнародних організацій, так і кожного члена суспільства.

Список використаних джерел:

1. Краєвська О., Лукач Н. Міжнародний досвід протидії глобальній проблемі торгівлі людьми. Вісник Львівського університету. 2015. Вип. 37. ч. 3. С. 82-89.
2. Про протидію торгівлі людьми : закон України від 09.12.2015 № 3739-17 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/3739-17 (дата звернення: 26.10.2017).
3. Висвітлення у засобах масової інформації проблеми торгівлі людьми : посібник для журналістів : сайт. URL: http://dnipr.kievcity.gov.ua/files/2015/4/27/zmi.pdf.

Одержано 01.11.2017

УДК 342

Вікторія Миколаївна ПРЕОБРАЖЕНСЬКА,
голова благодійної організації «Благодійний фонд «Добробут України»

ВИКОРИСТАННЯ ІНТЕРНЕТ РЕСУРСІВ ДЛЯ ТОРГІВЛІ ЛЮДЬМИ: МАРКЕРИ НЕБЕЗПЕЧНОСТІ

Одним з найбільш негативних явищ сучасного суспільства продовжує бути проблема торгівлі людьми. Торгівля людьми посідає одне з перших міст по прибутковості на рівні з торгівлею наркотиками та є одним з найстрашніших порушень прав людини.

Актуальність теми підтверджується тим, що з появою інтернету, вебкамер, можливостей здійснювати відеодзвінки

з'явилися нові форми вербування, втягування та незаконної експлуатації людей з метою отримання прибутку.

Згідно з Протоколом про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї, що доповнює Конвенцію Організації Об'єднаних Націй проти транснаціональної організованої злочинності: a) «торгівля людьми» означає здійснювані з метою експлуатації вербування, перевезення, передачу, приховування або одержання людей шляхом загрози силою або її застосування або інших форм примусу, викрадення, шахрайства, обману, зловживання владою або уразливістю положення, або шляхом підкупу, у вигляді платежів або вигод, для одержання згоди особи, яка контролює іншу особу. Експлуатація включає, як мінімум, експлуатацію проституції інших осіб або інші форми сексуальної експлуатації, примусову працю або послуги, рабство або звичаї, подібні з рабством, підневільний стан або вилучення органів; b) згода жертви торгівлі людьми на заплановану експлуатацію, про яку йдеться в підпункті (a) цієї статті, не береться до уваги, якщо було використано будь-який із заходів впливу, зазначених у підпункті (a).

Торгівля людьми є бізнесом і як весь сучасний бізнес все більше у своїй діяльності використовує новітні технології, насамперед інтернет ресурси. Наразі, існує велика кількість сайтів знайомств, чатів та месенджерів для спілкування, а також соціальних мереж, які використовуються з метою вербування та надання послуг близьких до проституції та порнографії.

Дівчата та жінки, які досягли 18 річного віку, в пошуках роботи на сайтах в інтернеті натрапляють на об'яви з пропозицією працевлаштування, які не містять ніякої попередньої інформації про справжню роботу. Подібні студії на початку можуть виглядати офіційними і визивати довіру. Зазвичай, в них при працевлаштуванні просять зробити фотографію з власними паспортом, щоб мати впевненість в віці того хто «працевлаштовується». Потім відбувається реєстрація на спеціальних сайтах, що є провайдерами зазначених послуг. Здебільшого з початку дівчатам пропонують спілкування в чаті з «клієнтами» з використанням вебкамери, але з тих чи інших причин таке спілкування не приносить дівчатам заробітку, на який вони розраховували. І тоді надходить пропозиція, щодо демонстрування свого тіла. Як правило, спочатку в білизні, а потім і без. За таке спілкування вони отримують від 30 до 50% від тих грошей, які «клієнт» сплачує за подібне дозвілля. Про-

позиції щодо подібної роботи є на сайтах з пошуку роботи, широко розповсюджуються через соціальні мережі.

Не всі «роботодавці» є справними платниками «заробітної платні». В сфері, яка є на межі з конфліктом з законодавством дуже складно довести трудові стосунки з «роботодавцем» та відпрацьований час. Не одній з дівчат не прийшло на думку звернутися за допомогою в отримані своїх грошей. Такий прибутковий бізнес стає ще більш прибутковим коли відеозапис такого сеансу «розмови» з дівчиною потрапляє до людей, що пропонують їй угоду: або вона сплачує певну суму грошей, або родичі та близькі побачать це відео. Також варіантом угоди можуть бути надання інших послуг інтимного характеру. На цьому не закінчується небезпека подібного роду занять. Є випадки психологічного та сексуального насильства від «роботодавців», які також залишаються замовчуваними.

Професія «веб-модель» тільки звучить красиво, насправді, це шлях до проституції та торгівлі людьми. Виходячи з вищесказаного, єдине що можна порадити тим хто опинився в скрутному становищі і має потребу в швидкому заробітку – це бути дуже пильними при працевлаштуванні. При виявлені подібних сайтів та об'яв інформувати поліцію та уповноважені органи влади з метою припинення протиправної діяльності. Важлива роль громадських активістів щодо виявлення таких сайтів і проведення роз'яснювальної роботи серед груп ризику. Лише об'єднуючи зусилля громадськості, науково-освітнього середовища та правозахисних органів є шанс протидіяти торгівлі людьми, особливо в разі використання інтернет ресурсів.

Приклади об'яв в соціальних мережах:

1. Работа в Харькове: Требуются девушки желающие хорошо заработать (от 18 лет). Сотрудничество на очень выгодных условиях: - достойная зарплата, - удобный график работы, - Регистрируем девушек с любой точки Украины. Вы всегда сможете следить за своим заработком, так как в любой день сможете просматривать заработанные деньги, это очень удобно. Выплаты каждые две недели! У нас самый высокий процент. У нас самые лучшие условия и возможность зарабатывать реально. Пишите в личку, буду рада ответить на все интересующие Вас вопросы. Писать только заинтересованным лицам старше 18 лет.

2. Приглашаем современных, целеустремлённых девушек от 18 лет для работы webcam-моделью. Достойная заработная плата (от 20-100$ за смену), первые 8 смен оплачиваются сра-

зу после смены, мы несем полную ответственность за своих сотрудников! Без начальника (ваш чат, вам решать как работать, но мы всегда рады помочь и подсказать если возникнут вопросы во время работы), график работы есть разный (три смены - утро, день, ночь), зарплата по курсу доллара (Можно получать в гривнах и в долларах зп, как удобно), мощный ПК, качественная камера, комфортная, современная студия.

У нас хороший коллектив, всегда можно пообщаться с девчонками на перерывах. Пишите мне, спрашивайте. Мы ценим ответственных, пунктуальных и жизнерадостных сотрудников) ХАРЬКОВ. ДНЕПР.

Одержано 01.11.2017

УДК 327.84 : 004

Анатолій Анатолійович РУСЕЦЬКИЙ,
кандидат юридичних наук, депутат Харківської обласної ради VII скликання

КІБЕРРОЗВІДКА В ПОЛІТИЧНІЙ ДІЯЛЬНОСТІ

Останнім часом майже усі політичні процеси стають тісно пов'язаними з інформаційним простором та інформаційними технологіями. Таким чином, зараз майже не зустрінеш політичного діяча або політичну партію, які б не мали власного сайту, або акантів в соціальних мережах для висвітлення результатів власної діяльності, програм та звернень до громадян.

Поняття кіберрозвідки необхідно розглядати у двох аспектах: як пошук інформації з відкритих джерел інформації (використання методології пошуку OSINT) та як несанкціоноване збирання інформації (кібершпигунство).

В першому випадку - використання методології пошуку OSINT, яка включає в себе пошук, вибір і збір інформації, отриманої із відкритих джерел і її аналіз. Така діяльність не містить ознак кримінального правопорушення, так як термін «відкритий» вказує на загальнодоступність джерела.

Процес збору інформації з відритих джерел інформації нажаль не врегульовано в національному законодавстві України, проте існує роз'яснення даного права Європейського суду з прав людини.

Таким чином, права на отримання інформації з відкритих джерел глобальної мережі Інтернет роз'яснено Європейським судом з прав людини, який у своїх постановах постійно підкреслює, що стаття 10 (1) Європейської конвенції з прав людини надає право на отримання тільки тієї інформації, яку особа

бажає передати. Виходячи з цього, особа, яка розміщує персональні дані в соціальних мережах, погоджуючись з Політикою конфіденційності такої соціальної мережі, розміщує відомості про себе у відкритому доступі глобальної мережі Інтернет, усвідомлюючи, що такі дані можуть бути використані іншими особами, для її персоніфікації.

Якщо розглядати другий випадок, то дана діяльність передбачає, несанкціоноване отримання будь-якої інформації з метою отримання особистої, економічної, політичної чи військової переваги, здійснюваний з використанням обходу (злому) систем комп'ютерної безпеки, з застосуванням шкідливого програмного забезпечення, включаючи вірусні програми і шпигунських програмне забезпчення . Кібершпигунство може здійснюватися як дистанційно, за допомогою глобальної мережі Інтернет, так і шляхом проникнення в комп'ютери і комп'ютерні мережі підприємств за допомогою працівників-інсайдерів, а також хакерами. В багатьох країнах Європейського союзу на даний час встановлено кримінальну відповідальність саме за кібершпигунство.

Підсумовуючи вищевикладене необхідно зауважити наступне:

1. Політичні діячі повинні забезпечити неперервний процес захисту інформації, яка є досить важливою для забезпечення максимального захисту організації (установи) від внутрішнього і зовнішнього, випадкового і навмисного деструктивного впливу.

2. Привертання уваги персоналу до питань безпеки, додержання персоналом вимог впровадженої в організації (установі) політики безпеки та застосування персоналом у роботі низки методів і дій, необхідних для підвищення захисту інформаційного забезпечення.

3. Введення кримінальної діяльності за ведення кібершпигунства.

Список використаних джерел:

1. Базенков Н. И., Губанов Д. А. Обзор информационных систем анализа социальных сетей. *Управление большими системами*: *сб. трудов*. 2013. № 41. С. 357-394.
2. Присяжнюк М. Жарков Я. Аналіз засобів ведення інформаційної боротьби з використанням інформаційних технологій, форм і способів їх застосування. URL: http://defpol.org.ua/site/index.php/uk/ (дата звернення: 18.10.2017).

Одержано 30.10.2017

Актуальні питання протидії кіберзлочинності та торгівлі людьми. Харків, 2017

УДК 34:004-049.(477)

Маріям Рзаївна ЧАЛАБІЄВА,
аспірант Харківського національного університету внутрішніх справ

ПРОБЛЕМИ ПРАВОВОГО РЕГУЛЮВАННЯ СФЕРИ КІБЕРБЕЗПЕКИ У НАЦІОНАЛЬНОМУ ЗАКОНОДАВСТВІ УКРАЇНИ

Ми живемо в той час, коли науково-технічний прогрес захопив усі сфери життя населення, коли інформаційні технології керують не тільки людиною, як суспільною одиницею, а й цілими країнами, визначаючи їх рівень життя та розвитку. Нові можливості несуть з собою нову специфіку проблем, які торкнулися України – кібернетичні злочини різного масштабу. Вони зазіхають не тільки на безпеку кожного з нас, але й на цілісність та безпеку нашої країни.

Наразі, у світі розробляється розгалужена система засобів по захисту від подібних правопорушень. Україна намагається не відставати, запозичуючи методи протидії вчиненню злочинів у віртуальному просторі. Він, на відміну від реального, не має фактичного обмеження, а це дуже зручно для здійснення протиправної поведінки у кібер-сфері.

Ця сучасна проблематика у теоретичних та практичних аспектах цікавила таких науковців, як: В. М. Богуш, В. М. Бутузов, К. Ю. Галинська, Н. В. Коваленко, Л. П. Коваленко та інші. Аналізуючи їх наукові доробки та національне законодавство, можна дійти до сумного висновку – наявна нормативно-правова база у сфері кібербезпеки в Україні не відповідає існуючому «європейському вектору розвитку», відверто не дотягуючи до бажаного міжнародного рівня.

Основним ратифікованим Україною міжнародно-правовим актом, що передбачає співробітництво і загальну кримінальну політику держав у даній сфері є Конвенція Ради Європи про кіберзлочинність. До протиправних кібер-діянь дана конвенція відносить шахрайство та підробку; діяння пов'язані зі змістом продукції (дитяча порнографія), захист авторських та суміжних прав тощо.

Розвиток положень Конвенції Ради Європи про кіберзлочинність ми можемо спостерігати й у національному законодавстві України. Так, Закон України «Про інформацію» визначає можливість встановлення певних інформаційних обмежень. Зокрема, оприлюднювана інформація у будь-якому

просторі (навіть віртуальному) не може бути використана як заклик для повалення конституційного ладу, порушення територіальної цілісності України, пропаганди війни, насильства, жорстокості; розпалювання міжетнічної, міжрасової, релігійної ворожнечі, вчинення терористичних актів, посягання на права і свободи людини [2]. Закон України «Про доступ до публічної інформації» також встановлює аналогічне обмеження щодо доступу до інформації, але в цьому випадку до публічної [5]. Закон України «Про телекомунікації» встановлює для провайдерів/операторів можливість і право відключення обладнання абонента на основі рішення суду, якщо воно використовується для здійснення протиправних діянь проти безпеки держави [3]. Закон України "Про основи Національної безпеки України" розлягає поняття комп'ютерний тероризм та злочинність, як найголовніші загрози національній безпеці України [4]. У Законі України «Про оборону України» зазначається, що Генеральний штаб Збройних Сил України бере участь в організації використання і контролю не тільки за повітряним та водними просторами, а й за державним інформаційним простором [6]. Закон України «Про засади внутрішньої та зовнішньо політики» регулює можливість запобігання і нейтралізації реальних та потенційних загроз національним інтересам у зовнішньополітичній, оборонній, соціально-економічній, енергетичній, продовольчій, екологічній та інформаційних сферах [7]. Закон «Про захист інформації в інформаційно-телекомунікаційних системах» тлумачить поняття «несанкціонованих дій щодо інформації в системі», як дії, що проводяться з порушенням порядку доступу до інформації, установленого відповідно до норм законодавства [8]. Закон «Про Державну службу спеціального зв'язку та захисту інформації України» визначає правові основи функціонування Державної служби спеціального зв'язку, та спеціальної програми реагування на комп'ютерні надзвичайній події – CERT-UA, що аналізує дані про спроби та факти вчинення протиправної поведінки стосовно інформаційних ресурсів у кібернетичній сфері [9].

Відповідно до Указу Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України», визначені основні завдання та цілі на період до 2020 року. Так, основними пріоритетами Стратегії є: розвиток інформаційної інфраструктури держави, створення системи кібербезпеки і безпеки інформаційних ресурсів, розвиток спеціальної мережі

реагування на комп'ютерні надзвичайні події CERT, цілодобовий моніторинг кіберпростору з метою своєчасного виявлення та запобігання кіберзагрозам, відмова від програмного забезпечення, зокрема антивірусного, яке було розроблено у Російській Федерації [11]. Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України», затверджує Доктрину інформаційної безпеки України, яка є концептуальним документом, який протидіє російським кібератакам та загрозам. Вона є гостро необхідним механізмом боротьби з гібридною інформаційною війною, оскільки Україна досі має велику кількість суб'єктивних медіа, які безвідповідально публікують неправдиві факти [10].

Розпорядження Кабінету Міністрів України «Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України містить у собі 19 завдань за напрямами: нормативно-правове забезпечення діяльності у сфері кібербезпеки; створення технологічної складової національної системи кібербезпеки; налагодження більш тісного співробітництва з міжнародними партнерами України; налагодження процесу підготовки кадрів у сфері кібербезпеки [12].

Аналізуючи вищезазначену нормативно-правову базу, можна дійти до висновку, що її головними цілями з урахуванням останніх подій в Україні, є забезпечення державної безпеки, протидія протиправній агресивній поведінці зі сторони Росії у віртуальному просторі. Гостро необхідним видається прийняття окремого спеціалізованого Закону, який би врегулював відносини у кіберпросторі. Запозичення міжнародного досвіду, міжнародне співробітництво у сфері кібернетичної безпеки держави – це важливі елементи у процесі формування безпечного українського віртуального простору, але без вдосконалення національної нормативної бази, казати про ефективне функціонування міжнародних актів в межах України зарано.

Список використаних джерел:

1. Конвенція про кіберзлочинність : Конвенція від 7 вересня 2005 року № 2824-IV URL: http://zakon3.rada.gov.ua/laws/show/994_575 (дата звернення: 23.10.2017).
2. Про інформацію : Закон України від 2 жовтня 1992 року № 2657-XII URL: http://zakon3.rada.gov.ua/laws/show/2657-12 (дата звернення: 23.10.2017).
3. Про телекомунікації : Закон України від 18 листопада 2003 року № 1280-IV URL:

http://zakon5.rada.gov.ua/laws/show/1280-15 (дата звернення: 23.10.2017).
4. Про основи національної безпеки : Закон України від 19 червня 2003 року № 964-IV URL: http://zakon3.rada.gov.ua/laws/show/964-15 (дата звернення: 23.10.2017).
5. Про доступ до публічної інформації : Закон України від 13 січня 2011 № 2939-VI URL: http://zakon2.rada.gov.ua/laws/show/2939-17 (дата звернення: 23.10.2017).
6. Про оборону України : Закон України від 06 грудня 1991 року № 1932-XII URL: http://zakon2.rada.gov.ua/laws/show/1932-12 (дата звернення: 23.10.2017).
7. Про засади внутрішньо та зовнішньої політики : Закон України від 1 липня 2010 року № 2411-VI URL: http://zakon3.rada.gov.ua/laws/show/2411-17 (дата звернення: 23.10.2017).
8. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 року № 80/94-ВР URL: http://zakon3.rada.gov.ua/laws/show/80/94-вр (дата звернення: 23.10.2017).
9. Про Державну службу спеціального зв'язку : Закон України від 23 лютого 2006 року № 3475-IV URL: http://zakon5.rada.gov.ua/laws/show/3475-15 (дата звернення: 23.10.2017).
10. Про Доктрину інформаційної безпеки України : Указ Президента України «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року» : від 25 лютого 2017 № 47/2017 URL: http://zakon3.rada.gov.ua/laws/show/47/2017 (дата звернення: 23.10.2017).
11. Про Стратегію національної безпеки України : Указ Президента України «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року » : від 26 травня 2015 року №287/2015 URL: http://zakon5.rada.gov.ua/laws/show/287/2015 (дата звернення: 23.10.2017).
12. Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України : Розпорядження Кабінету Міністрів України від 10 березня 2017 р. № 155-р URL: http://www.kmu.gov.ua/control/uk/cardnpd?docid=249807504 (дата звернення: 23.10.2017).

Одержано 25.10.2017

Актуальні питання протидії кіберзлочинності та торгівлі людьми. Харків, 2017

УДК 343.98

Дмитро Володимирович ШВЕЦЬ,
кандидат педагогічних наук, перший проректор Харківського національного університету внутрішніх справ

ДЕРЖАВНІ МЕХАНІЗМИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

На сучасному етапі розвитку суспільства все більше відчувається значущість інноваційних процесів, що відбуваються в нашому суспільстві у зв'язку з глобальною інформатизацією. Але разом з позитивними досягненнями, інформатизація супроводжується побічними, негативними явищами криміногенного характеру, до яких відносять комп'ютерну злочинність. Це, безумовно, вимагає негайного створення системи протидії даному різновиду злочинності на державному рівні. Для сучасного суспільства (в період його переходу від індустріального етапу розвитку до нового – постіндустріального, інформаційного) актуальність цієї проблеми не викликає сумнівів. За різними експертними оцінками у всьому світі втрати від діяльності кіберзлочинців складають щорічно від 300 до 800 млрд євро.

На міжнародному рівні у ряді нормативно-правових актів визнано, що кіберзлочинність погрожує не лише національній безпеці окремих країн, але і безпеці людства та міжнародному правопорядку. Стратегія державних підходів та механізмів з поліпшення інформаційних систем повинна сприяти скороченню масштабів кіберзлочинності та створити основні принципи національної політики протидії кіберзлочинності в міжнародному кіберпросторі. Протидія кіберзлочинності в широкому розумінні включає у себе загальнодержавні заходи економічного, політичного, виховного та іншого характеру, а також комплекс спеціальних заходів, спрямованих на безпосереднє подолання злочинності.

Враховуючи міжнародний характер кіберзлочинності, у боротьбі з нею життєво важливе значення має гармонізація національних законодавств. Проте, гармонізація повинна враховувати регіональні вимоги і можливості. Велике значення регіональних аспектів в здійсненні стратегій боротьби з кіберзлочинністю підкреслює той факт, що багато правових і технічних стандартів було погоджено між країнами світу.

Глобальна програма кібербезпеки заснована на п'яти основних принципах: 1) правові заходи; 2) технічні й процедурні заходи; 3) організаційні структури; 4) створення потенціалу; 5)

міжнародна співпраця. Зрозуміло, що українська система державних механізмів боротьби з кіберзлочинністю повинна використовувати всі ці принципи.

Серед п'яти принципів, при розгляді стратегії боротьби з кіберзлочинністю, ймовірно, правові заходи є найбільш важливими. По-перше, ці заходи вимагають прийняття основних положень кримінального законодавства, що передбачають кримінальну відповідальність за такі дії, як комп'ютерне шахрайство, незаконний доступ, спотворення даних, порушення авторських прав, розповсюдження дитячої порнографії тощо. Механізми й інструменти, необхідні для розслідування кіберзлочинів, можуть істотно відрізнятися від тих, що використовуються для розслідування загальних злочинів. У зв'язку з міжнародним масштабом кіберзлочинності необхідно додатково доробити основи національного законодавства, з тим, щоб мати можливість спільної співпраці з правоохоронними органами за кордоном.

Ефективна боротьба з кіберзлочинністю вимагає розвиненої організаційної структури. Не маючи правильно створеної системи відповідних органів, яка дозволяє уникнути дублювання та чітко розподіляє повноваження, навряд чи можна чекати на комплексне вирішення юридичних, технічних та соціальних аспектів даної проблеми. Кіберзлочинність є глобальним явищем. Для того, щоб мати можливість ефективно розслідувати кіберзлочини, необхідно не тільки гармонізувати законодавство, але й розробити відповідні механізми міжнародної співпраці.

Рівень довіри повинен зрости не лише між державами, але й між приватним і державним секторами. Одним з найбільш важливих елементів в попередженні кіберзлочинів є навчання користувача. Деякі кіберзлочини, особливо ті, які пов'язані з шахрайством типу «спуфінг», як правило, обумовлені не відсутністю засобів технічного захисту, а непоінформованістю або простою безвідповідальністю. Існують різні програмні продукти, що дозволяють автоматично визначати деякі шахрайські веб-сайти, хоча, на жаль, не всі. Попри те, що засоби технічного захисту продовжуватимуть розвиватися і доступні програмні продукти регулярно оновлюватимуться, такі продукти поки ще не можуть замінити інші підходи. Стратегія захисту користувача, що заснована тільки на програмних продуктах, ще не дає гарантії повного захисту користувачів.

Важливу роль відіграє також беззаперечне дотримання встановлених правил і процедур інформаційної безпеки. Наприклад, якщо користувачі знають, що їх фінансові установи ніколи не зв'язуватимуться з ними по електронній пошті з проханням повідомити пароль або деталі банківського рахунку, вони не стануть жертвами фішингу або атаки з метою крадіжки ідентифікації. Навчання користувачів Інтернету скорочує кількість потенційних жертв кіберінцидентів. Держава повинна розробити відповідну інформаційну програму розумної поведінки щодо попередження кіберзлочинності. До її поширення слід долучити громадські кампанії, школи, інформаційні центри і ВНЗ, реалізовуючи приватно-державні партнерства.

Проблема протидії комп'ютерної злочинності – це комплексна проблема. Закони України та інші нормативні документи у сфері кібербезпеки повинні відповідати сучасному рівню розвитку інформаційних технологій. З цією метою необхідно проводити цілеспрямовану роботу з гармонізації й удосконалення законодавства, що регулює поширення інформації в телекомунікаційних мережах. Одним з пріоритетних напрямків є також організація взаємодії і координації зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою, а також розвиток державно-приватного партнерства.

Одержано 01.11.2017

УДК [343.9 : 343.431] 477

Тетяна Анатоліївна ШЕВЧУК,
кандидат юридичних наук, викладач кафедри кримінального права і кримінології факультету № 1 Харківського національного університету внутрішніх справ

РОЛЬ ГРОМАДСЬКИХ ОРГАНІЗАЦІЙ У ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ

Торгівля людьми є однією з найжорстокіших форм порушення основних прав і свобод людини. Незалежно від виду експлуатаційної мети, торгівля людьми має тяжкі, а часом фатальні наслідки для постраждалих осіб. Злочин торгівлі людьми постійно еволюціонує услід за прагненнями злочинців отримати щонайвищі прибутки від експлуатації постраждалих та протистояти зусиллям правоохоронних органів з протидії їхній злочинній діяльності [1, с. 6].

Згідно з даними соціологічних опитувань, населення все більше схиляється до хибної думки, ніби протидія злочинності – справа винятково правоохоронних органів. Кримінологи ж, у свою чергу, справедливо вважають, що протидія злочинності як загальносуспільне завдання повинна здійснюватися зусиллями всього суспільства, а створена цим суспільством система правоохоронних органів – лише один з інструментів, хоча й найбільш специфічних.

Важливу роль у розв'язанні багатьох соціальних завдань, пов'язаних із торгівлею людьми, в тому числі, відіграють неурядові організації. У сучасних міжнародних документах із проблем протидії торгівлі людьми вони перебувають у центрі уваги як організації, котрі захищають права особи, надають соціальну і психологічну допомогу, а також ініціюють прийняття державними органами рішень, законів і розроблення механізмів запобігання правопорушенням [2, 97].

Визначальне місце серед неурядових організацій з протидії торгівлі людьми посідає громадська організація «Ла Страда Україна», серед основних завдань діяльності якої є сприяння запобіганню торгівлі людьми, інших проявів насильства, жорстокого поводження, особливо по відношенню до дітей; сприяння дотриманню прав українських громадян, які перебувають за кордоном та недопущення потрапляння їх до ситуації торгівлі людьми; сприяння більш глибокому розумінню умов і причин, що породжують проблеми насильства, дискримінації, торгівлі людьми, насильству та дискримінації в суспільстві; сприяння проведенню досліджень з зазначеної проблематики, організації конференцій, форумів, громадських акцій.

Крім того, у 2011 році було створено Всеукраїнську коаліцію громадських організацій щодо протидії торгівлі людьми, до якої долучились громадські організації, які працюють в сфері захисту прав потерпілих від торгівлі людьми в Україні, зокрема : Миколаївський фонд «Любисток», Громадський Рух «Віра, Надія, Любов» м. Одеси, Харківська міська організація Міжнародної організації «Жіноча громада», Закарпатська громадська жіноча організація «Веста», Дніпропетровська обласна громадська організація «Промінь», Західноукраїнський центр «Жіночі перспективи», Міжнародний благодійний фонд «Карітас України» та багато інших.

За результатами оцінки діяльності громадських організацій з протидії торгівлі людьми можна виділити наступні форми їх діяльності:

- удосконалення вітчизняного законодавства про громадські організації з визначенням ефективного механізму, їх залучення до формування державної політики у сфері протидії торгівлі людьми;

- участь у розробленні та впровадженні національних та місцевих програм із протидії та захисту жертв торгівлі людьми;

- моніторинг діяльності владних органів, перш за все, здійснення контролю за ходом реалізації державних програм із протидії та захисту жертв торгівлі людьми;

- організація і проведення різноманітних заходів (тренінги, семінари, круглі столи, брифінги, масові акції, інформаційні кампанії) та ін., а також участь у форумах, спільних проектах з міжнародними громадськими організаціями;

- налагодження зв'язків з міжнародними організаціями, розповсюдження в Україні змісту та основних положень міжнародно-правових документів з прав людини та протидії торгівлі людьми;

- створення та подальше забезпечення діяльності «гарячих ліній» з питань торгівлі людьми;

- створення мережі організацій, які б надавали соціальну допомогу потерпілим, що постраждали від торгівлі людьми за місцем їхнього проживання (реабілітаційних центрів, притулків);

- сприяння підвищенню рівня правової грамотності населення та захист прав громадян, які стали жертвами торгівлі людьми;

- здійснення інформаційно - пропагандистської діяльності (особливо серед молоді) з метою інформування про масштаби торгівлі людьми, основні причини цього явища, та алгоритм дій у разі перетворення на жертву цього злочину;

- створення інтернет – центрів для громадських організацій з метою їх інтернаціоналізації;

- організація інформаційних і тренінгових центрів.

Проаналізувавши основні форми діяльності громадських організацій щодо протидії торгівлі людьми, слід зазначити, що їх основна перевага в тому, що вони можуть інтегруватися, вони більш гнучкі, ніж державні органи, і це дає їм можливість швидко реагувати на зміну ситуації у суспільстві. Громадські організації вільні у виборі форм та методів роботи, вони не зарегламентовані певними нормами, і не обмежені функціями та рамками [3, с. 127].

Таким чином, можна з впевненістю констатувати, що громадські організації становлять значний масовий досить ефективний та інтенсивний потенціал протидії злочинності в цілому, та злочинам, пов'язаним з торгівлею людьми, зокрема. Саме їх активність в політичному та соціальному житті країни привертає увагу всього суспільства до появи та розповсюдження торгівлі людьми. Якщо це злочинне явище соціально обумовлене, то протидіяти йому повинен саме соціум в особі об'єднання громадян на основі росту його національної свідомості та в тісній взаємодії з міжнародною спільнотою, що буде запорукою зміцнення гарантій прав людини на міжнародному рівні.

Список використаних джерел:

1. Васильєва М. О., Касько В. В., Орлеан А. М., Пустова О. В. Україна як країна призначення для торгівлі людьми : матеріали для практичного використання працівниками прикордонної служби, правоохоронних органів та суддями. Київ, 2012. 120 с.
2. Іващенко В. О. Торгівля жінками та дітьми:кримінологічні та кримінально – правові аспекти боротьби : монографія. Київ : Атіка, 2004. 112 с.
3. Балакірєва О. М., Бондар Т. В., Галустян Ю. М., Горбунова О. Г. Секс бізнес в Україні: спроба соціального аналізу. Київ : Український інститут соціальних досліджень, 2001. 159 с.

Одержано 01.11.2017

УДК 343.98

Наталія Василівна ЮРКОВИЧ,
кандидат фізико-математичних наук, доцент, доцент кафедри твердотільної електроніки та інформаційної безпеки ДВНЗ «Ужгородський національний університет»

Василь Петрович САВЧИН,
головний спеціаліст відділу сім'ї, оздоровлення дітей та запобігання сімейного неблагополуччя департаменту соціального захисту населення Закарпатської обласної державної адміністрації

Інна Василівна САБАДОШ,
голова Закарпатської громадської жіночої організації «Веста»

Василь Михайлович РІЗАК,
доктор фізико-математичних наук, професор, завідувач кафедри твердотільної електроніки та інформаційної безпеки ДВНЗ «Ужгородський національний університет»

РЕАЛІЗАЦІЯ МЕХАНІЗМУ ВЗАЄМОДІЇ СУБ'ЄКТІВ ПРИ ЗДІЙСНЕННІ ЗАХОДІВ У СФЕРІ ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ В ЗАКАРПАТСЬКІЙ ОБЛАСТІ

Сьогодні торгівля людьми з використанням інформаційних технологій набула транснаціональний характер та створює реальні загрози національній безпеці нашої держави. Якщо досі Україна була переважно країною постачання і транзиту живого товару, то на сьогоднішній день спостерігається стрімкий розвиток експлуатації дорослої та дитячої праці, продаж дітей, людських органів за кордон тощо. Тому актуальність питання протидії торгівлі людьми є гострим, а аналіз підходів у забезпеченні вирішення вказаних глобальних проблем є невідкладним.

Незважаючи на велику кількість наукових праць з цієї проблематики [1, с.41; 2, с.182], з потужним розвитком інформаційних технологій, де тісно переплелася кіберзлочинність і торгівля людьми (технології забезпечення анонімності за захищеної передачі інформації у мережі, мережні сховища, сайти з надання послуг, пов'язаних з торгівлею людьми, електронні гроші та платіжні системи і т.д.) форми торгівлі людьми і незаконні угоди проти особи постійно трансформуються. Це потребує наукових пошуків боротьби з кіберзлочинністю і торгівлею людьми в Україні.

Закарпатська область украй вразлива до такого виду злочинів (один з видів цих злочинів - вербування та незаконне переміщення людей) у зв'язку із «зручним» географічним розміщенням на кордонах із Словаччиною, Угорщиною, Румунією та Польщею. Тому, особлива увага у нашій області приділяється освітній та превентивній діяльності з цієї проблеми. На протязі 2015-2017 років в області реалізовано проект Представництва Міжнародної організації з міграції (МОМ) в Україні «Впровадження національного механізму взаємодії суб'єктів, які здійснюють заходи у сфері протидії торгівлі людьми, в тому числі і дітьми, у Закарпатській області» за підтримки Агентства США з міжнародного розвитку, Канадського Міністерства закордонних справ, торгівлі і розвитку DFATD [3; 4]. Виконавчим партнером цього проекту була Закарпатська громадська жіноча організація «Веста» у партнерстві з Департаментом соціального захисту населення облдержадміністрації, Головним Управлінням Національної поліції в Закарпатській області та іншими суб'єктами, які здійснюють заходи з протидії торгівлі людьми в Закарпатській області. Проектом було визначено чотири ключові напрями [4]: координація зусиль та прийняття місцевого нормативного документу; навчання фахівців державних установ, правоохоронних органів та громадського сектору з надання допомоги постраждалим особам; інформаційна кампанія для населення області з проблеми торгівлі людьми та можливості отримання допомоги для постраждалих; виявлення, перенаправлення та надання допомоги постраждалим від торгівлі людьми.

Під час реалізації проекту було продовжено надання допомоги постраждалим від торгівлі людьми, які вже отримали статус. Кількість осіб, яким Міністерство соціальної політики України встановило статус особи, яка постраждала від торгівлі людьми в Закарпатській області у період 2015-2017 років склало 10 осіб, з яких 9 жінок, 1 чоловік. Загалом, по Закарпатській області за 2013 - 2017 роки 23 особи отримали статус особи, постраждалої від торгівлі людьми [5]. Всі заходи проекту сприяли підвищенню спроможності та професійної компетентності суб'єктів взаємодії щодо проведення ідентифікації та ефективності надання допомоги особам, які постраждали від торгівлі людьми. Це забезпечило надання належної комплексної допомоги відповідно до вимог чинного законодавства суб'єктами національного механізму взаємодії в Закарпатській області [6].

Підсумовуючи вищевикладене, слід наголосити, що тільки у тісній співпраці наукових установ, державних органів влади, громадських організацій, Національної поліції буде забезпечено удосконалення системи підготовки фахівців у сфері протидії торгівлі людьми, а проведення комплексних досліджень виявлення, попередження та розслідування злочинів пов'язаних з торгівлею людьми, є гарантією ефективності практичної діяльності у цьому напрямку.

Список використаних джерел:

1. Орел Ю. С. Актуальні проблеми боротьби з торгівлею людьми в Україні. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2014. №1. Вип. 32. С.41-44.
2. Хахановський В. Г. Запобігання та протидія торгівлі людьми в мережі інтернет. Інформація і право. 2012. №2. Вип. 5. С. 182-185.
3. Протидія торгівлі людьми: Офіційний сайт Представництва Міжнародної організації з міграції в Україні. URL: http://iom.org.ua/ua/protidiya-torgivli-lyudmi (дата звернення: 10.10.2017).
4. Офіційна сторінка Закарпатської громадської жіночої організації «Веста» у Фейсбуці URL: https://www.facebook.com/officiaVESTA.uzhgorod/ (дата звернення: 10.10.2017).
5. Офіційний сайт Департаменту соціального захисту населення Закарпатської ОДА. URL: http://www.zaksoc.gov.ua/index.php/2017-01-27-12-57-20/2017-02-06-14-45-48. (дата звернення: 10.10.2017).
6. Про протидію торгівлі людьми: Закон України від 20 вересня 2011 року № 3739-VI (в редакції від 9 грудня 2015 року № 3739-17). URL: http://zakon5.rada.gov.ua/laws/show/3739-17. (дата звернення: 10.10.2017).

Одержано 25.10.2017

РОЗДІЛ 2.
КРИМІНАЛЬНО-ПРАВОВІ, ПРОЦЕСУАЛЬНІ ТА КРИМІНАЛІСТИЧНІ АСПЕКТИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 343.13

Олександр Вячеславович АМЕЛІН,
головний науковий співробітник відділу науково-методичного забезпечення участі прокурорів у кримінальному провадженні НДІ Національної академії прокуратури України

ПРОБЛЕМИ ОБЛІКУ КІБЕРЗЛОЧИНІВ В УКРАЇНІ

Згідно із статистичними даними частка злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, що передбачені у розділі XVI Кримінального кодексу України, в загальній структурі злочинності є незначною й становить менше 1%. Водночас більшість кримінальних правопорушень, що вчиняються з використанням комп'ютерних (інформаційних) технологій, розміщені в інших розділах КК України, що унеможливлює об'єктивну оцінку їх рівня з урахуванням встановлених форм і методів державної статистичної звітності [1]. Крім того, через відсутність у чинному законодавстві базового поняття «кіберзлочини» ускладнено й проведення класифікації вказаних кримінальних правопорушень.

У зв'язку з викладеним реальну «картину» злочинності у сфері інформаційних (комп'ютерних) відносин на даний час визначити неможливо.

Аналіз статистичних даних свідчить, що в нашій державі динаміка злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку є несталою. Так з 2010 року розпочалася тенденція щодо їх зменшення (12,4% порівняно з 2009 роком). Ця тенденція посилилася у 2011 році, оскільки було зареєстровано 131 злочин на відміну від 190 злочинів, які обліковано в 2010-му. В 2012 році зареєстровано 138 злочинів, що свідчить про їх незначне збільшення (7%). У 2013 році кількість зареєстрованих злочинів вказаної категорії досягла 595, однак у 2014 році їх чисельність вже становила 443. У 2015-му кількість зареєстрованих злочинів

знову зросла до 598. Вказана тенденція продовжилась у 2016 році, оскільки кількість облікованих злочинів становила 818.

Незначна питома вага злочинів у вказаній сфері в загальній структурі злочинності на думку наукової спільноти серед іншого обумовлена високою латентністю, яка за підрахунками вчених становить до 99,9%.

Не сприяє вирішенню зазначених проблем специфіка джерел інформації, у яких містяться відомості про вчинення кримінальних правопорушень, оскільки тактика та методика розслідування кримінальних проваджень у сфері інформаційних (комп'ютерних) відносин залежать від вихідних даних, які утворюють змістовне наповнення елементів криміналістичної характеристики злочинів (спосіб, місце, обстановка, особа злочинця, особа потерпілого тощо).

Чи не найважливішою проблемою, яка стоїть на заваді достовірного обліку кримінальних правопорушень у сфері інформаційної (комп'ютерної) злочинності є правильність кримінально-правової кваліфікації. Практика показує, що правоохоронними органами, судами та науковцями досліджувані кримінальні правопорушення кваліфікуються не однаково, а іноді діаметрально протилежно.

Зазначені кримінальні правопорушення можуть бути вчинені різними способами. Зокрема, шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК України), використання підроблених електронних засобів доступу до банківських рахунків (ст. 200 КК України), збут і розповсюдження порнографічних предметів з використанням електронно-обчислювальної техніки (ч. 4 ст. 301 КК України), вилучення посадовою особою фінансової установи з банківських рахунків клієнтів електронних коштів, які перебували у правомірному володінні цієї особи (ч. 2 ст. 191 КК України) тощо.

З огляду на викладене, проаналізувавши кількісні та якісні показники можна дійти висновку, що кваліфікація кіберзлочинів за статтями, які не містяться в розділі XVI КК України, призводить до викривлення статистичної звітності та є однією з причин неможливості встановлення реальної «картини» злочинності в цій сфері.

Аналогічна ситуація складається і під час обліку вказаних правопорушень судами. Зокрема, відповідно до офіційних даних судової статистики у 2010 році за вчинення злочинів, передбачених розділом XVI Кримінального кодексу України, за-

суджено 69 осіб. У 2011 році кількість засуджених дещо зменшилась – до 56. Водночас у 2012 році законної сили набрали обвинувальні вироки відносно 80 осіб. Починаючи з 2013 року, позначилася тенденція до зменшення кількості засуджених осіб – до 49. Вказана закономірність посилилася протягом наступних трьох років: 2014 рік – 37 осіб, 2015 – 31 особа, 2016 – 24 особи. Таким чином, протягом останніх шести років правоохоронними органами здійснювалось розслідування 2913 злочинів вказаної категорії, за результатами судового розгляду яких обвинувальні вироки набрали законної сили щодо 346 осіб, 1 особу виправдано [2].

Усе вищезазначене свідчить, що розв'язання окресленої проблематики потребує вдосконалення нормативно-правових актів, у яких необхідно класифікувати кримінальні правопорушення в цій сфері та доповнити розділ XVI КК України спеціальними нормами, які передбачатимуть кримінальну відповідальність за кримінальні правопорушення у сфері комп'ютерної інформації (крадіжка, шахрайство), узгодивши їх з Конвенцією Ради Європи про кіберзлочинність. Це дозволить відмежувати вказані злочини від загальнокримінальних. Крім того необхідно внести відповідні зміни до статистичної звітності правоохоронних органів та суду.

Наведене надасть можливість ґрунтовно підвищити достовірність відображення реального стану злочинності по державі.

Список використаних джерел:

1. Єдиний звіт про кримінальні правопорушення. Форма № 1, затверджена Наказом ГПУ від 23 жовтня 2012 року № 100, за погодженням з Держстатом України.
2. Звіт про кількість осіб, засуджених, виправданих, справи щодо яких закрито, неосудних, до яких застосовано примусові заходи медичного характеру та види кримінального покарання. Форма № 6, затверджена наказом Державної судової адміністрації України від 21.11.2012 року № 153.

Одержано 01.11.2017

УДК 343.98 (477)

Богдан Анатолійович БУРБЕЛО,
викладач кафедри криміналістики та судової експертології факультету № 1 Харківського національного університету внутрішніх справ

КРИМІНАЛІСТИЧНІ АСПЕКТИ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ З ТОРГІВЛЕЮ ЛЮДЬМИ

Людина, її життя і здоров'я, честь і гідність, недоторканність і безпека визнаються в Україні найвищою соціальною цінністю.

Успішне розслідування і попередження злочинів у сфері торгівлі людьми значною мірою залежить від належної професійної підготовки працівників поліції.

Аналіз слідчої практики свідчить, що розслідування торгівлі людьми в Україні викликає певні труднощі пов'язаних з недостатнім міжвідомчим співробітництвом на національному та міжнародному рівнях і відсутність пропозицій для покращення діяльності по боротьбі з цими злочинами. Також під час розслідування слідчими не завжди всебічно і повно оцінюються слідчі ситуації на різних етапах розслідування, не проводиться весь комплекс необхідних слідчих, оперативно-розшукових заходів, спрямованих на встановлення місця знаходження потерпілого, до кримінальної відповідальності притягуються лише рядові виконавці, тоді як організатори і керівники злочинних груп залишаються поза полем впливу правоохоронних органів.

Таким чином, вважаємо, що в юридичній науці сформувалася потреба в комплексному дослідженні проблеми розслідування злочинів, пов'язаних з торгівлею людьми, інтегровано включаючи, як кримінально-процесуальні, так і криміналістичні аспекти.

До основ криміналістичного забезпечення діяльності по виявленню торгівлі людьми, на наш погляд, повинні входити: способи та прийоми виявлення ознак торгівлі людьми; технічко-криміналістичні засоби діяльності по їх виявленню; засоби та прийоми оперативно-розшукової діяльності для виявлення ознак торгівлі людьми; особливості взаємодії правоохоронних органів різних держав по виявленню ознак цих злочинів; основні напрямки підвищення ефективності роботи по виявленню торгівлі людьми тощо.

На нашу думку, криміналістична характеристика торгівлі людьми повинна включати такі елементи: а) способи вчинення торгівлі людьми; б) відомості про особу злочинця; в) відомості про особу потерпілого; г) «слідова картина» торгівлі людьми. Необхідність включення до методики розслідування торгівлі людьми етапу виявлення ознак злочину обумовлена перш за все специфікою механізму вчинення торгівлі людьми та особливостями одержання первісної інформації, підвищеною латентністю даного виду злочину і складністю виявлення його ознак.

Для вчинення вказаних злочинів також характерні наявність декількох взаємопов'язаних між собою етапів злочинної діяльності та їх ретельне планування, обов'язковими елементами якого, як правило, є:

- створення різноманітних фірм, які, прикриваючись підприємницькою діяльністю, фактично займаються вербуванням та вивезенням за кордон жінок під виглядом їх подальшого працевлаштування;
- підшукування поза межами України «ринків збуту» для продажу потерпілих з метою їх подальшої експлуатації;
- вибір способів для переміщення потерпілих через державний кордон України.

Певні криміналістичні особливості має торгівля людьми, в зв'язку з тим, що цей злочин вчиняється злочинними групами. Для криміналістичної характеристики таких злочинів суттєве значення мають дані про формування таких груп. Існування родинних зв'язків в злочинній ланці є дуже характерним для даного виду злочинів. Така родинність підвищує рівень організованості цих груп, придає їм більшу оперативність у вирішенні поточних питань і збільшує рівень конспірації. При вчиненні злочинів у сфері торгівлі людьми організованими злочинними групами, злочинці наполегливо здійснюють заходи з протидії розслідуванню.

Типові сліди торгівлі людьми доцільніше досліджувати, поділяючи їх за способами вербування потерпілих та способами переміщення їх через державний кордон України. Це дозволить виявити типові сліди протиправної діяльності в сфері торгівлі людьми: сліди-відображення; сліди-предмети, що належать злочинцю або потерпілому, що локалізуються в певних типових для даного злочину місцях і свідчать про вчинення злочинцями певної сукупності дій; сліди на тілі потерпілого чи

злочинця; інформаційні сліди у вигляді аудіо-відео записів, що мають відношення до справи.

Ефективність розслідування залежить від того, наскільки діяльність слідчого та взаємодіючих з ним органів дізнання відповідає особливостям злочину та обстановки, що складається під час розслідування. Така відповідність насамперед багато в чому визначається чітким уявленням про предмет доказування.

Вважаємо, що для підвищення ефективності розслідування торгівлі людьми є дослідження і подальша розробка типових слідчих ситуацій і розробка на цій основі рекомендацій з методики розслідування торгівлі людьми необхідні для правильної побудови слідчих версій, визначення напрямку розслідування, виявлення обставин, що мають значення для справи.

Одержано 30.10.2017

УДК 343.38

Андрій Анатолійович ВАСИЛЬЄВ,
кандидат юридичних наук, доцент, професор кафедри кримінального права і кримінології факультету № 1 Харківського національного університету внутрішніх справ

ДО ПИТАННЯ ПРО ПОСИЛЕННЯ ВІДПОВІДАЛЬНОСТІ ЗА ВЧИНЕННЯ ЗЛОЧИНУ З ВИКОРИСТАННЯМ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Інформаційно-телекомунікаційні, інформаційні та телекомунікаційні системи як засоби або способи для з'єднання окремих користувачів у мережі Інтернет, а також соціальні служби (мережі) чи відеохостінги, настільки глибоко проникли у наше повсякденне життя, що ігнорування тих загроз, які існують поряд із безумовно позитивними їх якостями вже не тільки помилково, а у окремих випадках навіть злочинно. Мова йде про використання указаних систем як для вчинення явно злочинних діянь (наприклад, шахрайства, збуту наркотичних засобів та психотропних речовин, а в окремих випадках зброї та небезпечних матеріалів), так і для поширення закликів до вчинення протиправних діянь, схиляння до розпалювання ненависті чи розбрату, поширення неправдивої інформації, яка містить відомості, що ганьблять конкретну особу чи групу осіб тощо. Інформація, що поширюється мережею Інтернет, користувачем, нажаль, не завжди сприймається критично, що використовується автором або «власником» цієї інфо-

рмації у корисливих чи інших цілях, іноді злочинних. Указане свідчить про необхідність перегляду норм чинного законодавства, перш за все кримінального, в частині врегулювання указаних проблем.

Питання врегулювання сфери Інтернет-відносин, упорядкування того масиву інформації, яка поширюється в цій мережі, у тому числі кримінальної відповідальності за порушення у цій сфері не є новим для нашої країни, так, зокрема, воно було предметом дискусій на інформаційних форумах, розглядалося на сторінках друкованих видань. Так, спроби вирішити окремі питання відповідальності за кіберзлочини та злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку розглядалися в роботах Д. С. Азарова, Ю. М. Батуріна, П. Д. Біленчука, М. В. Карчевського, М. О. Кравцової, В. В. Крилова, Ю. І. Ляпунова, О. В. Манжая, А. А. Музики, П. І. Орлова, С. О. Орлова, Д. В. Пашнєва, Н. А. Розенфельда та інших науковців.

Однак, навіть ураховуючи внесок указаних науковців у вирішення питання протидії кіберзлочинності на сьогодні, нажаль, доводиться констатувати як підвищення кримінального комп'ютерного професіоналізму, високу мобільність злочинців при недостатній кількості фахівців-правоохоронців, так і відсутність законодавчо врегульованого механізму забезпечення протидії поширенню кіберзагроз.

Безумовно, окремі кроки у напрямі врегулювання обігу потенційно шкідливого контенту здійснені і на державному рівні, так, указом Президента від 15 травня 2017 року № 133/2017 було введено в дію рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» [1], яким, зокрема, було обмежено доступ до російських інформаційних ресурсів в Інтернеті: Yandex, соцмереж «ВКонтакте» та «Одноклассники», а також заборонено використання бухгалтерського програмного продукту 1С. Не вдаючись до оціночних суджень щодо необхідності саме такого способу протидії потенційним небезпекам, які поширюються в інформаційному просторі, слід зазначити, що це лише незначний крок на шляху упорядкування обігу шкідливих даних, адже існує безліч способів оминути таке блокування. Потребує вироблення цілий комплекс заходів, спрямованих на убезпечення безпеки як держави в цілому,

так і окремих громадян. Одним із найбільш дієвих способів запобігання вчиненню правопорушень залишається криміналізація окремих форм вчинення діяння або посилення (введення додаткових умов) відповідальності за використання деяких способів вчинення діяння. Однак, як слушно зазначають І. В. Владленова та Е. А. Кальницький, «у формуванні політики і засобів боротьби з проблемою кіберзлочинності необхідно уникати надмірного регулювання при збереженні відкритості Інтернету і захисту прав людини, як-то: право на приватне життя і інформаційне самовизначення, свободу слова, інформації та комунікації» [2].

Використання мережі Інтернет чи інших систем або мереж, по-перше, полегшує вчинення окремих злочинів через свою доступність, по друге, через можливість анонімності є привабливим способом вчинення злочину та породжує «ілюзію уседозволеності», і, нарешті – спосіб спрямований на невизначене коло осіб, що створює небезпеку як для осіб, які розуміють протиправність посягання, так і для неповнолітніх чи малолітніх, які не здатні усвідомлювати небезпеки.

Слід вказати, що у чинному КК України вже передбачено у якості кваліфікуючої ознаки для окремих складів злочинів їх вчинення «з використанням засобів масової інформації». Однак, згідно закону, під засобами масової інформації розуміються газети, журнали, теле- і радіопрограми, кінодокументалістика, інші періодичні форми публічного розповсюдження масової інформації, які відповідним чином зареєстровані. До них не можна відносити, зокрема, блогерів, які мають акаунти на відеохостінгу «Youtube», осіб, які створюють і модерують групи у соціальних мережах чи месенджерах.

Використання ж можливостей указаних мереж або систем дає змогу звертатися до невизначеної кількості осіб і розповсюдження інформації, поширення якої створює певні умови (обставини), наявність яких ставить у небезпеку певні суспільні відносини (наприклад, поширення у соціальних мережах реклами щодо придбання наркотичних засобів, реклама «ескорт» послуг тощо).

Зазначене дозволяє зробити висновок про необхідність урахування розвитку інформаційних технологій і сфер використання інформаційно-телекомунікаційних систем, зокрема, при внесення змін у кримінальне законодавство. Зміни, спрямовані на посилення відповідальності за вчинення злочину з використанням інформаційно-телекомунікаційних систем,

можливі у таких формах: введення кваліфікуючої ознаки та утворення кваліфікованого складу злочину (наприклад, у ч. 3 ст. 109, ст. 113, ч. 2 статей 161, 182, ч. 3 ст. 190, ч. 2 статей 258, 258-2 КК України тощо) або введення такого «використання» в якості обставини, що обтяжує покарання (наприклад, у ст. 67 КК України). Однак, такі істотні нововведення потребують подальших наукових досліджень та додаткового обґрунтування підстав криміналізації.

Список використаних джерел:

1. Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій): Указ Президента України від 15.05.2017 р. № 133/2017. URL: http://zakon3.rada.gov.ua/laws/show/n0004525-17 (дата звернення: 26.10.2017).
2. Владленова І. В., Кальницький Е. А. Кіберзлочинність як виклик інформаційному суспільству. *Гілея: науковий вісник.* 2013. № 77. С. 142–146. URL: http://nbuv.gov.ua/UJRN/gileya_2013_77_45 (дата звернення: 26.10.2017).

Одержано 30.10.2017

УДК 343.1 + 004

Андрій Вікторович ВІНАКОВ,
кандидат юридичних наук, керуючий партнер компанії ILP

Ірина Андріївна МАНЖАЙ,
завідувач навчального відділу Харківського економіко-правового університету

ОКРЕМІ ПИТАННЯ ФІКСАЦІЇ ЕЛЕКТРОННИХ ДОКАЗІВ

На теперішній час в Україні нема єдиної сталої термінології, яка б визначала докази, одержані з носіїв цифрових даних, а також чітко не визначено порядок роботи з ними. Тому на практиці нерідко виникають питання щодо правильного оформлення таких доказів та їх представлення в суді.

20.06.2017 року Верховна Рада України в першому читанні прийняла проект закону № 6232 «Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів». У даному документі пропонується розуміти під електронними доказами інформацію в електронній (цифровій) формі, що містить дані про обставини, що мають значення для справи, зокрема, елек-

тронні документи (в тому числі текстові документи, графічні зображення, плани, фотографії, відео- та звукозаписи тощо), веб-сайти (сторінки), текстові, мультимедійні та голосові повідомлення, метадані, бази даних та інші дані в електронній формі. Такі дані можуть зберігатись, зокрема на портативних пристроях (картах пам'яті, мобільних телефонах та ін.), серверах, системах резервного копіювання, інших місцях збереження даних в електронній формі (в тому числі в мережі Інтернет).

Докази, одержані в рамках розслідування, повинні відповідати вимогам достовірності, належності і допустимості. Вказані вимоги висуваються як до форми одержаних відомостей, так і їх змісту. Ці вимоги є справедливими і для електронних доказів. Для того, щоб грамотно задокументувати відомості з цифрових джерел, потрібно враховувати функціональні особливості технологій, з використанням яких їх було створено, збережено, передано тощо.

Закріплення електронних доказів, одержаних в результаті передбачених Кримінальним процесуальним кодексом, слідчих чи негласних слідчих (розшукових) дій здійснюється з дотриманням декількох вимог до форми і змісту. Перша група вимог передбачає процесуальне оформлення відповідних протоколів, залучення у разі необхідності спеціаліста та понятих, вжиття заходів із належного збереження цифрових носіїв даних, важливих для кримінального процесу. Друга група вимог висувається до змістовного наповнення інформації, її якісної та кількісної складової. В останньому випадку слід особливу увагу звернути на повноту одержаних відомостей, для того, щоб вони у подальшому могли бути представлені як в судовому засіданні, так і передані на дослідження експерту.

Слід пам'ятати, що хоча в окремих слідчих діях участь понятих не є обов'язковою, але з іншого боку вона надає більшої вагомості одержаним доказам. При цьому поняті мають бути обізнаними, хоча б на базовому рівні, в інформаційних технологіях, а мова протоколювання повинна бути максимально зрозумілою для пересічної особи.

У рамках фіксації електронних доказів також слід орієнтувати слідчого на застосування носіїв інформації, які не можуть бути повторно перезаписані, для того щоб у подальшому обвинувачений або сторона захисту не могли стверджувати про створення дописів в електронних носіях з боку правоохоронців. Також для уникнення суперечок можна додатково вино-

сити на експертизу питання про наявність в електронних доказах ознак стороннього втручання, зокрема монтажу.

Самі носії інформації, а також інші докази, одержані в результаті проведення слідчих та негласних слідчих (розшукових) дій, повинні належним чином описуватися, упаковуватися та опечатуватися, щоб убезпечити їх від пошкодження і втрати доказових властивостей.

Крім того хотілося б відмітити, що на теперішній час в правоохоронних органах існує серйозна проблема проведення експертних досліджень електронних доказів у розумні строки. Недостатня кількість експертів, які мають право проводити комп'ютерно-технічні експертизи, сприяє створенню кількамісячних, а у деяких випадках кількарічних черг на проведення означеного виду експертиз. З урахуванням наведеного вбачається доречним розширення практики дослідження відповідних електронних доказів безпосередньо слідчим із залученням спеціаліста (за необхідності) з подальшим оформленням проведеного дослідження протоколом огляду. Така практика вже існує в регіонах, проте вона все ще не є поширеною, зважаючи на недостатні знання слідчих (у переважній більшості) в сфері інформаційних технологій.

Одержано 30.10.2017

УДК 343.98.06 (477)

Іван Андрійович ГРАБАЗІЙ,
кандидат юридичних наук, доцент кафедри оперативно-розшукової діяльності та розкриття злочинів факультету № 2 Харківського національного університету внутрішніх справ

ОКРЕМІ ЕЛЕМЕНТИ МОДЕЛІ ЗЛОЧИННОЇ ДІЯЛЬНОСТІ ОРГАНІЗОВАНИХ ЗЛОЧИННИХ ГРУП, ЯКІ ЗАЙМАЮТЬСЯ ТОРГІВЛЕЮ ЛЮДЬМИ

Враховуючи вимоги світової спільноти щодо перебудови та модернізації поліцейської діяльності у бік проактивної позиції, вважаємо, що структурно модель злочинної діяльності повинна складається з відомостей: про ознаки та механізм злочинної діяльності; причетність до злочинної діяльності (не карне сприяння, використання злочинних добутків, участь у проведені вільного часу злочинців, медичного та організаційного забезпечення злочинної діяльності); схильності до злочинної діяльності; «ділові» контакти зі злочинцями та обізнаність

про них; пошукові ознаки об'єктів, що становлять оперативний інтерес щодо запобігання конкретному виду злочинів.

Таким чином змістовна сторона оперативно-розшукової моделі злочинної діяльності містить дійову складову, та складається з наступних фаз:

- інформаційно-пошукова (розвідувальна) фаза;
- активна фаза: побудова схеми та механізму злочинної діяльності;
- реалізація злочинного задуму;
- відтворення та розширення злочинної діяльності.

Кожній фазі розвитку кримінальної активності відповідають певні завдання по реалізації злочинного задуму.

Для визначення оптимальної моделі оперативної розробки оперативні працівники повинні знати зміст кожної фази.

Інформаційно-пошукова та активна фаза.

Ці фази складаються з низки заходів щодо пошуку інформації, необхідної для успішної підготовки, здійснення й приховання злочину.

Загальна структура ОЗГ включає в себе декілька ланок. Кожна з них виконує певні функції: організаторів, вербувальників, провідників, переправників, корумпованих чиновників, інформаторів та ін. Невід'ємною складовою їх злочинної діяльності є підшукування та переправлення живого товару за кордон.

Аналіз оперативно-розшукових справ та кримінальних проваджень, аналітичних матеріалів міністерства юстиції, правоохоронних та громадських організацій, думок практичних працівників, наукових праць, дозволяє визначити види трафіків торгівлі людьми:

1. Працевлаштування за кордоном - надання через ЗМІ рекламних оголошень, в яких пропонується високооплачувана праця українських громадян за кордоном.

2. Туристичні послуги - через турфірми пропонуються послуги з отримання туристичних віз, оформлення закордонних паспортів, придбання туристичних путівок та запрошень у місця відпочинку інших країн.

3. Шлюбні агентства - через ЗМІ здійснюється пошук бажаючих вийти заміж за кордоном, друкуючи оголошення на зразок "Багатий самотній англієць шукає симпатичну молоду слов'янку для шлюбу".

4. Через мережу Internet - як відомо, 80% комерційних прибутків з функціонування мережі Internet приносять так

звані "порно-сайти". Також існують сайти, які пропонують працевлаштування за кордоном, туристичні послуги чи інформацію про так звану ескорт-проституцію, яка проявляється у сексуальному супроводженні багатих зарубіжних клієнтів проститутками, які не знають мови замовника, а тому гарантується відносна анонімність та конфіденційність особи клієнта.

5. Через інфраструктуру фіктивних рекрутських та кадрових агентств.

Реалізація злочинного задуму.

Способи, які використовують злочинці, можна розділити на дві групи:

1. Способи вербувальників і кур'єрів, що використовуються на першому етапі, тобто для отримання згоди особи виїхати за кордон. Зазвичай, жертва сама приймає рішення виїхати з України, але її до цього «психологічно обробляють», використовують обман і зловживання довірою, надаючи недостовірну інформацію щодо характеру та умов роботи і проживання;

2. Способи організаторів. Серед цих способів виділяють насильство як психологічне, так і фізичне (борг, кабала, шантаж, погроза розправою над родичами).

Відтворення та розширення злочинної діяльності.

Ця фаза складається з процесу відмивання отриманих грошей через економічну інфраструктуру ОЗУ, використання коштів для розширення злочинної діяльності та визначення її нових напрямків.

Підводячи підсумки, вважаємо, що на підставі такої моделі оперативний працівник може визначити способи запобігання даному виду злочинів, та режим оперативного обслуговування імовірних об'єктів вчинення злочинів, а також конкретних осіб-об'єктів оперативно-профілактичної діяльності.

Одержано 30.10.2017

УДК 343.98

Вадим Анатолійович КОРШЕНКО,
завідувач науково-дослідної лабораторії захисту інформації та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

РОЛЬ ТЕЛЕКОМУНІКАЦІЙНОЇ ЕКСПЕРТИЗИ ПРИ РОЗСЛІДУВАННІ ЗЛОЧИНІВ, ВЧИНЕНИХ З ВИКОРИСТАННЯМ КРИПТОВАЛЮТ

Тема криптовалют на сьогодні є мегаактуальною. Останні декілька років інформація про них мусується у засобах інформації. Мільйони людей по всьому світу використовують криптовалюти для різних цілей: як об'єкт для інвестицій, платіжний засіб, джерело фінансування проекту тощо. Однак, не дивлячись на актуальність теми у більшості населення криптовалюти асоціюються з фінансовими пірамідами і незаконними угодами в інтернеті та в його «темній» зоні - даркнеті.

Криптовалюта за своєю суттю це цифрові гроші, випуск та облік яких заснований на технології блокчейн, яка являє собою вибудований за певними правилами безперервний послідовний ланцюг блоків що містять інформацію. Тобто вся інформація зберігається не в одному централізованому місці а на безлічі електронних засобів, сполучених мережею інтернет. Історія транзакцій в блокчейні відкрита всім учасникам системи і незмінна, всі користувачі залишаються анонімними і мають рівні статуси. Блокчейн можна представити у вигляді облікової книги записів про події у цифровому світі, єдиним способом змінити стан реєстру в якій - зробити транзакцію. При цьому записи в журнал транзакцій можуть вноситися тільки з відома більшості учасників мережі. Це означає, що не можна непомітно видалити транзакцію з журналу або додати нову в його середину. Технологія блокчейну базується на спеціальних алгоритмах шифрування, що потребує відповідного програмного забезпечення та комп'ютерного обладнання.

Станом на сьогодні в світі існує більше тисячі криптовалют. Наразі самою популярною криптовалютою є біткоін. Популярність біткоіну можна пояснити тим, що це перша подібна валюта у своєму роді. Стрімкий ріст курсу біткоіну спровокував появу величезної кількості аналогів, які існують на даний момент.

В Україні статус криптовалют до теперішнього часу залишається не визначеним. Національний банк України офіційно розглядає криптовалюту як грошовий сурогат, що не має забезпечення реальною вартістю. Звідси витікає неможливість її використання фізичними і юридичними особами на території України як засоби платежу.

Незважаючи на чітку позицію національного регулювальника економіки заперечувати світовий досвід і розвиток криптовалюти в практиці міжнародних валютних розрахунків вважаємо недоцільним. Відмовлятися від використання криптовалюти зважаючи на її потенційну небезпеку і можливість шахрайських дій також не розумно. Єдиним рішенням проблеми, на наш погляд, являється створення ефективної системи контролю обігу криптовалюти в Україні. Технології сьогодні розвиваються швидше, ніж держава встигає адаптувати законодавство щодо їх регулювання. Зміни світу технологій, фінансів та інвестицій породжують нові фінансові інструменти та принципово інші бізнес-моделі в тому числі на основі технологій блокчейн і вимагають від держави відповідної реакції.

Станом на сьогодні в Верховну Раду України внесений проект Закону «Про стимулювання ринку криптовалют та їх похідних в Україні» [1] яким пропонується створити передумови для розвитку економіки на базі новітніх технологій в Україні.

Вказаний законопроект вважаємо актуальним, адже на сьогоднішній день всі операції з криптовалютами в України проводяться за межами правового поля. Слід зазначити, що при операціях з криптовалютами існують суттєві ризики. Доступ до криптовалютного гаманця може буде скомпрометовано, а операція із переказу криптовалюти є неповоротною. Відсутність прямої вказівки держави на закон, який потрібно застосовувати до операцій з криптовалютами створює дуже високі ризики їх використання. Правоохоронні органи завдяки невизначеності статусу криптовалют в Україні істотно обмежені у виборі засобів і методів протидії злочинам які вчиняються з використанням криптовалют та злочинів де криптовалюта є об'єктом протиправного посягання. Зловмисникам поточний стан справ навпаки розв'язує руки і надає безліч можливостей, особливо в незаконному заволодінні криптовалютою. Існує велика кількість шахрайських схем щодо незаконного заволодіння криптовалютою такі як фейкові сайти відомих

ресурсів, піраміди, онлайн казино, фішингові інструменти, продаж неіснуючих товарів та послуг тощо.

На сьогодні єдиним дієвим способом пошуку слідів злочину скоєного з використанням криптовалют і злочинів де криптовалюта є об'єктом протиправного посягання та перетворення потенційної інформації що знаходиться в цих слідах злочину в доказову інформацію є проведення телекомунікаційної експертизи, а в деяких випадках – комплексної телекомунікаційної та комп'ютерно-технічної експертизи. Адже сліди злочинів у сфері використання інформаційних технологій утворюються в результаті зовнішнього або внутрішнього неправомірного впливу на телекомунікаційну систему, окремий електронний пристрій, програму чи на комп'ютерну інформацію і являють собою будь-які зміни комп'ютерної інформації, які відбулися в результаті вчинення злочину із застосуванням комп'ютерних технологій [1, с. 62].

Телекомунікаційна експертиза є досить молодим, але дуже сучасним і прогресивним родом судових експертиз. Ефективність розслідування злочинів, вчинених з використанням криптовалют, та злочинів, де криптовалюта є об'єктом протиправного посягання безпосередньо залежить від сучасних можливостей та якості проведення судових експертиз, зокрема судової телекомунікаційної експертизи.

Список використаних джерел:

1. Про стимулювання ринку криптовалют та їх похідних в Україні: проект закону 7183-1 від 10.10.2017. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=62710&pf35401=436015 (дата звернення: 30.10.2017).
2. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : дис. ... канд. юрид. наук: 12.00.09. Х., 2007. 228 с.

Одержано 30.10.2017

УДК 343.1

Андрій Ігорович КУНТІЙ,
кандидат юридичних наук, доцент кафедри кримінального процесу факультету №1 Львівського державного університету внутрішніх справ

ЩОДО ДЕЯКИХ СУБ'ЄКТІВ ВЗАЄМОДІЇ ЗІ СЛІДЧИМ ПІД ЧАС РОЗСЛІДУВАННЯ ТОРГІВЛІ ЛЮДЬМИ

Важливою умовою розслідування кримінального проваджень, пов'язаних з торгівлею людьми, а також належної про-

тидії торгівлі людьми є налагодження дієвої взаємодії з усіма суб'єктами, які здійснюють заходи в цій сфері.

Дослідженню питання взаємодії органів досудового розслідування та інших підрозділів, що залучалися до цієї сфери, приділялась певна увага у працях вітчизняних учених: О.М. Бандурки, В.В. Голіни, Л.М. Давиденко, І.М. Даньшина, О.М. Джужи, А.П. Закалюка, В.С. Зеленецького, О.Г. Кальмана, О.М. Костенка, М.В. Костицького, О.М. Литвака, М.І. Мельника, В.А. Мисливого, В.М. Поповича, Б.Г. Розовського, В.І. Шакуна та інших. Важливі теоретичні питання протидії торгівлі людьми розкрито у працях С.Р. Абрамової, В.І. Василинчука, Г.П. Власової, В.І. Дубини, О.В. Святуна, І.В. Буреша, О.В. Іляшенка, А.А. Нєбитова, В.В. Турока, Є.Д. Скулиша та інших. Як свідчить статистика, на протязі 2013 р. було зареєстровано 131 кримінальне провадження за ст. 149 КК України, у яких 79 особами вручено повідомлення про підозру та 58 обвинувальних актів скеровано до суду; у 2014 р.- 118 (повідомлення про підозру – 77; обвинувальні акти – 55); у 2015 – 110 (повідомлення про підозру – 79; обвинувальні акти – 59); у 2016 р. – 115 (повідомлення про підозру – 59; обвинувальні акти – 45); протягом січня - березня 2017 р. – 79 (повідомлення про підозру – 29; обвинувальні акти – 16) [1].

На нашу думку, взаємодія органів досудового слідства з іншими органами та підрозділами Національної поліції, що залучаються до сфери розслідування злочинів, пов'язаних з протидією торгівлі людьми являє собою засновану на законі, узгоджену за цілями, місцем і часом, діяльність даних суб'єктів, здійснювана з метою попередження, розкриття і розслідування кримінальних правопорушень, пов'язаних з торгівлею людьми, а також розшуку злочинців, що їх вчинили.

Існують різні форми взаємодії слідчого та інших органів і підрозділів, у зв'язку з чим виникає питання їх класифікації, проте більшість вчених-криміналістів і процесуалістів розрізняють процесуальні (засновані на нормах КПК та Законів України, що регламентують діяльність органів, що перебувають у взаємодії) і непроцесуальні (організаційні) форми взаємодії. Якщо в першому випадку взаємодія може протікати лише у формах, передбачених кримінально-процесуальним законом, вони тією чи іншою мірою врегульовані ним, характеризуються наявністю певних процесуальних відносин і на практиці не виникає особливих проблем в їх реалізації, то непроцесуальні

форми необхідно систематизувати в контексті розслідування торгівлі людьми.

Законодавчими актами, на підставі яких будується процесуальна форма взаємодії у категорії досліджуваних нами злочинів є: Постанова Кабінету Міністрів України від 18 квітня 2012 року № 303 «Про затвердження Положення про створення та функціонування Єдиного державного реєстру злочинів торгівлі людьми»; Постанова Кабінету Міністрів України від 23 травня 2012 року № 417 «Про затвердження Порядку встановлення статусу особи, яка постраждала від торгівлі людьми»; Наказ Міністерства соціальної політики України № 366 від 18.06.2012; Постанова «Про затвердження Порядку виплати одноразової матеріальної допомоги особам, які постраждали від торгівлі людьми»; Постанова «Про затвердження Порядку взаємодії суб'єктів, які здійснюють заходи у сфері протидії торгівлі людьми»; наказ Міністерства соціальної політики України від 14 вересня 2012 року № 578 «Про затвердження форм оцінки потреб особи, яка постраждала від торгівлі людьми; плану реабілітації особи, яка постраждала від торгівлі людьми; обліку осіб, які постраждали від торгівлі людьми; звіту щодо осіб, які постраждали від торгівлі людьми»; розпорядження Кабінету Міністрів України від 07 жовтня 2015 року № 1053-р «Про схвалення Концепції Державної соціальної програми протидії торгівлі людьми на період до 2020 року»; наказ Міністерства соціальної політики України від 18 червня 2012 року № 366 «Про затвердження форм заяв про встановлення статусу особи, яка постраждала від торгівлі людьми, журналу реєстрації заяв осіб, які мають намір отримати статус особи, яка постраждала від торгівлі людьми, розписки про нерозголошення відомостей, облікової картки особи, яка вважає себе постраждалою від торгівлі людьми, журналу реєстрації видачі довідок про встановлення статусу особи, яка постраждала від торгівлі людьми» та ряд інших актів.

Порядок взаємодії суб'єктів, які здійснюють заходи у сфері протидії торгівлі людьми, затверджено Постановою Кабінету Міністрів України від 22 серпня 2012 р. № 783. Згідно із зазначеним актом, Міністерство соціальної політики є Національним координатором, що, відповідно, координує діяльність центральних і місцевих органів виконавчої влади.

Проаналізувавши наведені законодавчі акти, ми виділили суб'єктів, що можуть взаємодіяти зі слідчим під час розслідування злочинів, пов'язаних з торгівлею людьми: 1) державні

органи; 2) органи місцевого самоврядування; 3) громадські організації; 4) міжнародні організації.

На нашу думку, загалом, до таких органів та організацій відносяться: управління у справах сім'ї та молоді облдержадміністрацій та відповідні виконавчі органи міських рад; центри соціальних служб для сім'ї, дітей та молоді; служби у справах дітей; управління освіти і науки облдержадміністрацій та відповідні виконавчі органи міських рад; управління охорони здоров'я облдержадміністрацій та відповідні виконавчі органи міських рад; управління праці та соціального захисту населення облдержадміністрації та відповідні виконавчі органи міських рад; центри зайнятості; підрозділи Національної поліції України; підрозділи Служби безпеки України; підрозділи Державної прикордонної служби України; заклади охорони здоров'я; дошкільні, загальноосвітні, професійно-технічні, вищі та позашкільні навчальні заклади; громадські організації, що працюють у сфері надання допомоги особам, які постраждали від торгівлі людьми; міжнародні організації.

Підсумовуючи, слід зауважити, що ефективність розслідування кримінального провадження загалом, залежить від того, наскільки діяльність слідчого та взаємодіючих з ним органів відповідає особливостям злочину та обстановки, що складається під час розслідування. Така відповідність насамперед багато в чому визначається чітким уявленням про предмет доказування, встановлення якого, в свою чергу, є кінцевою метою розслідування.

Список використаних джерел:

1. Єдині звіти про кримінальні правопорушення за 2013-березень 2017 року. URL: http://www.gp.gov.ua (дата звернення 17.10.2017).

Одержано 24.10.2017

УДК 65.012.8 + 004

Олександр Володимирович МАНЖАЙ,
кандидат юридичних наук, доцент, доцент кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ДИТЯЧИЙ ҐРУМІНГ ТА ОКРЕМІ АСПЕКТИ ЙОГО ДОКУМЕНТУВАННЯ

Одним з негативних явищ застосування інформаційних технологій з протиправною метою є дитячий ґрумінг, який може використовуватись для залучення неповнолітніх до тор-

гівлі дітьми, нелегальних оборудок, таких як дитяча проституція або виробництво дитячої порнографії. Це поведінка характерна для педофілії [1, с. 49].

Онлайн ґрумери можуть бут розділені на дві групи. До першої належать ті, які працюють «виключно онлайн», у той час як друга група має на меті вчинення сексуального насильства не стільки в кіберпросторі як у фізичному світі. Працівники поліції нерідко використовують легендовані профілі дітей для приваблювання потенційних педофілів. При цьому аналіз відповідних поліцейських профілів засвідчив, що вони не містили стереотипних ознак вразливих до насильства дітей. Це вказує на те, що будь-яка дитина може стати жертвою онлайн-ґрумінга [2, с. 111, 117].

У 2017 році британського педофіла Пола Лейтона (Paul Leighton) було засуджено до 16 років позбавлення волі за зґвалтування в режимі онлайн. Він створив 30-40 несправжніх облікових записів Facebook для знайомства з дітьми. За допомогою соціальної мережі зловмисник спочатку вмовляв дітей надіслати йому фотографії інтимного характеру, після отримання яких шантажував дітей, змушуючи їх до вчинення сексуальних дій насильницького характеру. Так, 14-річного хлопця з Флориди (США) Лейтон змусив зґвалтувати 12 річну племінницю, 14-річну дівчину з Південної Дакоти (США) примусив до статевих актів зі своїм братом, які вони знімали для зловмисника на відео. В аналогічній ситуації опинилась і 13-річна дівчина з Теннессі (США). Загалом жертвами серійного педофіла стали більше ста осіб з різних країн [3].

З технічної точки зору під час документування ґрумінгу можна здійснювати:

- огляд веб-сайту;
- контроль за вчиненням злочину у формі спеціального слідчого експерименту із використанням апаратних та програмних засобів фіксації;
- тимчасовий доступ до речей і документів;
- зняття інформації з транспортних телекомунікаційних мереж;
- зняття інформації з електронних інформаційних систем.

Аналіз форм документування процесу огляду інформації, яка не має обмеження доступу встановленого її володільцем та зберігається в електронному вигляді, в різних регіонах України засвідчує, що існують два головних підходи в цьому питанні. Перший полягає у відповідному документуванні з викорис-

танням протоколу огляду. У другому випадку процес документування оформлюється протоколом негласної слідчої (розшукової) дії щодо зняття інформації з електронних інформаційних систем, доступ до яких не обмежується її власником, володільцем або утримувачем або не пов'язаний з подоланням системи логічного захисту, а тому не потребує дозволу слідчого судді (ч. 2 ст. 264 Кримінального процесуального кодексу України). Різниця в підходах пояснюється суперечностями щодо належності інформації в електронній формі до місцевості, приміщення, речей або документів, щодо яких можна здійснювати огляд (ч. 1 ст. 237 Кримінального процесуального кодексу України). Водночас більшість правоохоронних органів в регіонах все ж тяжіють до використання першого підходу – оформлення електронних доказів протоколом огляду.

Список використаних джерел:

1. Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій (Проект): навчальний курс / [В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков]. К., 2015. 158 с.
2. Cybercrime and its victims / Edited by Elena Martellozzo, Emma A Jane. 2017. Routledge. 230 p.
3. British paedophile Paul Leighton jailed for 16 years for rape. URL: https://www.theguardian.com/uk-news/2017/sep/04/british-paedophile-paul-leighton-jailed-for-16-years-for-rape (дата звернення: 22.09.2017).

Одержано 30.10.2017

УДК 343.13

Євгеній Олександрович НАЛИВАЙКО,
кандидат юридичних наук, викладач відділу підготовки прокурорів з нагляду за додержанням законів органами, які проводять оперативно-розшукову діяльність, дізнання та досудове слідство Національної академії прокуратури України

КРИМІНАЛІСТИЧНІ ТА ПРОЦЕСУАЛЬНІ ОСОБЛИВОСТІ У ЗЛОЧИНАХ ПОВ'ЯЗАНИХ ІЗ КІБЕРЗЛОЧИННІСТЮ

На актуальність та необхідність теми вдосконалення боротьби з кіберзлочинністю вказує кількість злочинів у даній сфері яка постійно зростає.

Відповідно до принципів сучасного міжнародного кримінального права злочини з використанням комп'ютерних технологій (інакше «кіберзлочини») віднесені до злочинів міжнародного характеру. Перелік видів кіберзлочинів визначається

Конвенцією про кіберзлочинність (2001 р.), яка називає серед інших наступні склади: незаконний доступ до комп'ютерної системи, нелегальне перехоплення технічними засобами комп'ютерних даних, втручання у комп'ютерні данні, втручання у функціонування комп'ютерної системи, підробку та шахрайство пов'язане з комп'ютерами.

На сучасному етапі, в Україні, до найбільш актуальних схем кіберзлочинів можливо віднести – фішинг, вішинг, соцінженерія та злочини у банкоматній мережі. З цього приводу навіть є «Методичні рекомендації МВС України щодо виявлення та документування злочинів пов'язаних з несанкціонованим використанням пристроїв - ,,скіммерів", для отримання інформації про банківські платіжні картки Управління боротьби з кіберзлочинністю МВС України» 2013 року.

Одним з проблемних питань є те, що діючий Кримінальний процесуальний кодекс фактично не містить положення, які дають змогу використовувати докази в електронній формі. Таким чином, значно ускладнюється можливість доказування наявності того чи іншого протиправного діяння, пов'язаного з рухом інформації в електронному вигляді в реальному масштабі часу. Саме рух інформації в цифровому вигляді є об'єктом протиправних діянь, які кваліфікуються як кіберзлочини. Разом із тим особливості слідоутворення та збору доказової бази залежить від середовища їх скоєння.

Згідно зі ст. 84 КПК доказами в кримінальному провадженні є фактичні дані, отримані у передбаченому КПК порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Особливою формою є електронні докази. Процесуальними джерелами доказів є: показання, речові докази, документи, висновки експертів. Зазначений перелік є вичерпним.

Поряд із цим можливо вказати на позитивну норму в контексті означеної проблеми, а саме: ч. 2 ст. 8 Закону України «Про електронні документи та електронний документообіг», відповідно до якої допустимість електронного документа як доказу не може бути спростована лише на підставі того, що він має електронну форму.

Наразі фактично єдиним способом використання електронної інформації як доказів у суді є висновок експерта. Таким чином, доказами у кримінальній справі можуть бути ви-

користанні висновки комп'ютерно-технічної експертизи, виконаної відповідно до Закону «Про судову експертизу». Позитивним в цьому аспекті є можливість здійснення експертизи не тільки в державних спеціалізованих установах, а й у незалежних експертів, які атестовані в порядку, визначеному законодавством України.

На даний час проаналізувавши експертну практику можливо пересвідчитися у постійному збільшенні кількості експертних завдань щодо пошуку на комп'ютерних носіях інформації, яка стосується роботи користувача персонального комп'ютера (ПК) у глобальній мережі Інтернет, тобто звернення його на конкретні сайти, хронології чи історії звернень тощо. Це зумовлено збільшенням кількості кримінальних проваджень, пов'язаних з противоправним поширенням у глобальній мережі певної інформації, у тому числі кримінального характеру (щодо торгівлі людьми, розповсюдження порнографічних зображень тощо).

Вважаємо за необхідне наголосити на невідповідність тяжкості покарання передбаченому у законодавстві України у вказаній категорії злочинів, що також не є стримуючим фактором у діях злочинців, тобто міра покарання практично усіх злочинах не перевищую середню тяжкість, а отже не завжди можливо застосування НСРД.

Як приклад у Іспанії лише за перетинання границі з фальшивими кредитними карточками, борговими картками чи акредитивами передбачене покарання від восьми до десяті років позбавлення волі та штрафу у десятикратному розмірі підроблених грошей.

Ще одним проблемним питанням у злочинах пов'язаних із кіберзлочинністю можна назвати відсутність можливості дослідження електронних доказів, котрі зберігаються на віддалених серверах. На даний час ними можуть бути сервіси зберігання інформації в мережі Інтернет (Adrive, Box.net, Clip2Net, DropBoks, SkyDrive, MediaMax та ін.), електронні скриньки, системи інтернет-банкінгу та ін. Натомість відбувається дослідження їх паперових аналогів. Однак завдяки порівняно нескладному обладнанню, дослідження таких доказів може вийти на якісно новий рівень. Це також могло б суттєво підвищити ефективність дослідження не лише електронних, а й інших доказів (фотоілюстрацій висновків експертів, протоколів слідчих дій, інших додатків).

З огляду на викладене, з метою покращення можливостей розслідування даної категорії злочинів необхідне вдосконалення як процесуального законодавства так і криміналістичного (постійної розробки новітньої методиці збирання та дослідження електронних доказів на досудовому провадженні, та методика дослідження цих доказів у судовому засіданні). З урахуванням сучасних можливостей криміналістики необхідно підвищити принаймні базовий рівень знань у галузі ІТ технологій усіх осіб, які здійснюватимуть пошук і фіксацію та досліджуватимуть електронні докази.

Одержано 01.11.2017

УДК 343.1 + 004

Віталій Вікторович НОСОВ,
кандидат технічних наук, доцент, професор кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ДЕЯКІ ПРАКТИКИ ЗАБЕЗПЕЧЕННЯ НАЛЕЖНОСТІ ДОКАЗІВ, ОТРИМАНИХ З ОНЛАЙН РЕСУРСІВ

Злочини, що пов'язані із торгівлею людьми, широко застосовують інформаційні технології шляхом: організації в онлайн-режимі секс-чатів, відео трансляцій сексуальних дій; вербування жертв через веб-сайти з оголошеннями про працевлаштування; публікації на різноманітних ресурсах в Інтернеті пропозицій щодо надання сексуальних послуг; і таке інше.

При розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій, здійснюється пошук доказів, на підставі яких суд буде вирішувати питання про вину підозрюваних в учиненні кримінального злочину. Онлайн-ресурси в Інтернеті, пов'язані із торгівлею людьми, можна розглядати як цифрові джерела речових доказів, які мають певні унікальні характеристики порівняно із традиційними доказами.

Відповідно до ст. 94 Кримінального процесуального кодексу України кожен доказ у кримінальному провадженні має оцінюватися з точки зору належності, допустимості, достовірності. При оцінці належності доказів із цифрових джерел інформації можуть використовуватися критерії: справжності, повноти, надійності, переконливості.

Для забезпечення належності доказів, отриманих з онлайн ресурсів в Інтернеті, представляється доцільним використання

поряд із традиційними методами специфічних практик документування, що наводяться нижче.

Відео захоплення екрану (video screen capture). Доцільно разом із записом на відеокамеру процесу огляду онлайн ресурсів використовувати спеціальні програми цифрового відеозапису інформації, яка виводиться на екран. Доречним є використання безкоштовних програм з відкритим вихідним кодом, наприклад, ShareX (https://getsharex.com/).

Підтвердження справжності веб-сторінки. Для визначення справжності веб-сторінки, що буде оглядатися, по-перше, доцільно за допомогою утиліт командного рядка типу tracert (traceroute) зафіксувати маршрут прямування даних до сервера, на якому розміщено веб-сайт. По-друге, зафіксувати процес отримання непрямого доступу (через проксі) до веб-сторінки, наприклад через сервіс Google Translate. Для цього в адресному рядку браузеру потрібно ввести адресу цільового сайту (xxxx.xxx):

https://translate.google.com/translate?sl=en&tl=ru&u=http://xxxx.xxx,

де виставити напрям перекладу на оригінальну мову веб-сторінки. В цьому випадку сервер Google підключається до серверу, де знаходиться потрібна веб-сторінка, запитує зазначений веб-ресурс і передає отримані дані. Якщо записати процес перевірки на відео, то можна підтвердити, що здійснюється огляд справжньої веб-сторінки, при цьому час і дата відвідування Google Translate, IP-адреса і URL будуть відображені в журналах серверів Google.

Збереження вихідного HTML-коду веб-сторінки. Для збереження вихідного HTML-коду веб-сторінки достатньо у браузері вибрати опцію «Зберегти сторінку як» або «Файл - Зберегти як». Також у контекстному меню є опція «Подивитися вихідний код», який можна зберегти як текстовий файл.

Створення повної копії веб-сайту. В деяких випадках у судовому процесі потрібно демонструвати повний вміст веб-сайту. З метою фіксації вмісту усього веб-сайту, а не окремої веб-сторінки, можна створити копію сайту для перегляду в автономному режимі, наприклад, за допомогою програми HTTrack Website Copier (http://www.httrack.com), яка завантажує пов'язані веб-об'єкти за визначеною глибиною і дозволяє відкрити веб-сайт з усіма зображеннями в автономному режимі.

Фіксація метаданих об'єктів веб-сторінки. Розширення HttpFox для браузеру Mozilla Firefox дозволяє вибрати будь-який елемент веб-сторінки і зафіксувати метадані, наприклад, час і дату останньої модифікації.

Фіксація стороннім сервісом дати і локального часу веб-серверу, на якому розміщений веб-ресурс. Щоб збільшити доказову силу відеозапису, можна продемонструвати додаткові технічні дані досліджуваної веб-сторінки, які надає сторонній сервіс, наприклад, http://www.webconfs.com/http-header-check.php, який відображає HTTP-заголовки заданого домену. Як правило, заголовок містить поле «дата», в якому міститься дата і локальний час наданий веб-сервером, де розміщений сайт.

Встановлення внутрішнього ідентифікатора об'єкту соціальної мережі. Соціальні мережі широко використовують внутрішні ідентифікатори (ID) для відстеження будь-якої активності на сайті (користувачі, фотографії, чати, сеанси, групи, позначки «мені подобається» і т.д.). Наприклад, Facebook використовує ідентифікатор «fbid» (https://www.facebook.com/photo.php?fbid=10103832396388711). Поряд із отриманням скріншоту профіля, зображення і т.п. підозрюваного доцільно встановити його внутрішній ідентифікатор в базі даних соціальної мережі.

Ідентифікатори встановлюються або в адресному рядку браузера або через їх пошук у вихідному коді веб-сторінки. Для Facebook ідентифікатор профілю у вихідному коді можна знайти за запитом ?id=, а для Twitter – за запитом data-user-id. Для перевірки правильності знайденого значення внутрішнього ідентифікатору можна скористуватися сторонніми сервісами, наприклад, https://findmyfbid.in/.

Після збереження відповідних файлів на підготовлений цифровий носій (наприклад, DVD-R) з метою подальшого контролю цілісності отриманої інформації потрібно обчислити їх дайджест (хеш-функцію). На сьогодні безпечним алгоритмом з найменшим розміром дайджесту визнаний алгоритм хешування SHA-2, який, наприклад, реалізований у програмі з відкритим вихідним кодом QuickHash (https://quickhash-gui.org).

Розглянуті практики забезпечення належності доказів, отриманих з онлайн ресурсів, не є вичерпними і можуть змінюватися разом із зміною інформаційних технологій.

Одержано 18.10.2017

Актуальні питання протидії кіберзлочинності та торгівлі людьми. Харків, 2017

УДК 343.1 : 65.012.8 + 004

Іван Вікторович ПАНАСЮК,
аспірант Харківського національного університету внутрішніх справ

НЕГЛАСНА ДІЯЛЬНІСТЬ ПІДРОЗДІЛІВ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ ЩОДО ПОШУКУ ТА ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ

В умовах сьогодення збирання цифрових даних та їх використання правоохоронними органами набуло системного характеру. Вказана діяльність вже активно розвивається не лише у країнах умовного «Заходу», але і у більш технічно відсталих, малорозвинених державах. Резонансні викриття високотехнологічних негласних методів і засобів роботи правоохоронних органів та спеціальних служб США, зроблені останніми роками, лише засвідчили, що інноваційна технічна складова здатна надати неоцінені переваги державним органам як у розвідувальній діяльності, так і під час вирішення завдань протидії злочинності. Останній напрям все частіше привертає увагу вітчизняних правоохоронних органів, зокрема Національної поліції України. Серед іншого в державі було прийнято низку ключових актів у сфері забезпечення кібербезпеки, реформовано кіберполіцію, значно посилено технічний потенціал та аналітичну складову в роботі поліції.

Слід відмітити, що в Україні постійно зростає кількість зареєстрованих високотехнологічних правопорушень. Так, лише по злочинах у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку в 2016 році відбулося збільшення в 1,4 рази порівняно з попереднім 2015 роком. Причому, переважну більшість цих злочинів було кваліфіковано як тяжкі. У той же час цифрові носії все частіше стають доказами не лише по кіберзлочинах, але й у інших більш класичних випадках. За 2012-2016 рр. лише підрозділами Експертної служби МВС України було проведено 15529 комп'ютерно-технічних експертиз та досліджено 88791 об'єкт. Крім того, за цей саме період цією ж службою було здійснено 1154 комп'ютерно-технічних досліджень та досліджено 11890 об'єктів. Поряд з цим протягом 2012-2016 рр. було проведено 8880 комп'ютерно-технічних експертиз та експертних досліджень силами науково-дослідних установ судових експертиз Міністерства юстиції України.

З метою ефективного збирання цифрових даних під час протидії злочинності поліції часто доводиться залучати відповідних спеціалістів. Так, наприклад, представники Експертної служби МВС України у 2014 році взяли участь у 13656 оперативно-розшукових заходах, у 2015 році таких випадків було 9380. У 2016 році працівники експертної служби 190 раз брали участь у здійсненні негласних слідчих (розшукових) дій.

Вказана ситуація свідчить на користь збільшення ролі цифрових даних, зібраних під час негласної роботи, для вирішення завдань ефективної протидії злочинності. Водночас брак фахівців з комп'ютерно-технічної експертизи викликає нагальну потребу у підвищенні рівня знань та вмінь у сфері збирання та використання цифрових даних саме пересічних оперативних працівників та слідчих. Наразі в Україні підвищення кваліфікації щодо застосування високих технологій у протидії злочинності переважно ведеться у кіберполіції, при цьому інші підрозділи нерідко залишаються поза увагою науковців та інших фахівців під час розробки відповідних рекомендацій та надання практичної допомоги. Вказане зумовлює необхідність опрацювання теоретичних та практичних особливостей негласної діяльності підрозділів національної поліції щодо пошуку та використання цифрових доказів.

Одержано 14.10.2017

УДК 343.98

Яна Анатоліївна СОКОЛОВА-ВИСОЧИНА,
кандидат юридичних наук, доцент, старший викладач відділу підготовки прокурорів з нагляду за додержанням законів органами, які проводять оперативно-розшукову діяльність, дізнання та досудове слідство Національної академії прокуратури України

АКТУАЛЬНІ ПИТАННЯ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

Розвиток та впровадження сучасних інформаційних технологій у всі сфери суспільного життя та економіки в Україні дає можливість використовувати їх, зокрема, й з корисливих та інших мотивів. Інформаційні технології також надають нові можливості для злочинної діяльності, комп'ютер «забезпечує» і нові види злочинів, і нові способи вчинення вже звичних протиправних діянь. Протидія злочинам, вчиненим із застосуванням інформаційних технологій, є новим викликом для правоохоронних органів [1, с. 6, 143].

Підвищений інтерес злочинців до Інтернету не випадковий. Унікальність глобальної мережі полягає в тому, що вона не перебуває у віданні конкретної фізичної особи, приватної компанії, державної або громадської організації чи навіть окремої держави. Використання телекомунікаційних мереж дає можливість вчинити злочин, не виходячи з дому, офісу, не покидаючи межі своєї країни, або одночасно з території декількох держав. Відсутні будь-які форми контролю за інформацією, що відкриває необмежені можливості для доступу до неї та її використання злочинцями. Зазначене обумовлює транснаціональний, організований, груповий характер багатьох кіберзлочинів [2, с. 15].

Кіберзлочинність є явищем міжнародного значення, рівень якого перебуває у прямій залежності від рівня розвитку та впровадження сучасних інформаційних технологій. Відбувається консолідація ІТ-злочинців у групи з подальшим їх укрупненням до злочинних угруповань, злочинних організацій, що діють на постійній основі – «професійна кіберзлочинність». Також має місце швидке налагодження та зміцнення зв'язків між злочинними угрупованнями, що дає змогу забезпечити оперативний обмін інформацією, здійснення обміну прийомами та способами вчинення злочинів, способами переведення електронних коштів у готівку тощо [3, с. 93].

У науковій літературі зазначається, що з'явився новий напрям науково-практичної діяльності – інформаційні технології процесуального доказування, що виник в умовах інформаційного суспільства на стику правових та природничо-технічних наук. Він покликаний забезпечити ефективність правосуддя шляхом включення у процедуру його здійснення найбільш ефективних сучасних інформаційних технологій. Не лише злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, але й багато «традиційних» суспільно небезпечних діянь залишають після себе електронні сліди у комп'ютерних мережах, на магнітних чи оптичних носіях, екранах моніторів. У зв'язку з цим виникає практична проблема використання зазначених слідів під час досудового розслідування [4, с. 313].

Розслідування кіберзлочинів також ускладнене певними особливостями: латентністю; можливістю знищення або зміни комп'ютерної інформації, що є доказом вчинення злочину; виникненням проблеми під час огляду комп'ютерних систем, ви-

лучення та дослідження слідів, які зберігаються в пам'яті технічних пристроїв, в електромагнітному полі, на машинних носіях комп'ютерної інформації; короткочасністю зберігання інформації, здатної виступити як доказ на серверах компаній – операторів телекомунікаційних мереж тощо [5, с. 180].

Саме тому викликом сучасності, що постав перед криміналістичною теорією і практикою, є необхідність вивчення електронних слідів як явища об'єктивної дійсності й розроблення криміналістичних рекомендацій щодо найбільш ефективного їх виявлення, дослідження, фіксації, вилучення й використання у діяльності з розслідування й попередження злочинів. Адже потенціал використання електронних слідів у діяльності органів кримінальної юстиції з розшуку та ідентифікації осіб, запобігання правопорушенням тощо, залишається на неприпустимо низькому рівні [6, с. 426].

Список використаних джерел:

1. Болгов В. М., Гадіон Н. М., Гладун О. З. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій : наук.-практ. посібник. Київ: НАПУ, 2015. 202 с.
2. Гусаров С. М. Розслідування кіберзлочинів органами внутрішніх справ України: наукове та кадрове забезпечення // Актуальні питання розслідування кіберзлочинів : матеріали міжнародної науково-практичної конференції, м. Харків, 10 грудня 2013 року. Харків: ХНУВС, 2013. С. 14-18.
3. Шапочка С. В. До питання боротьби з шахрайством, яке вчиняється з використанням можливостей мережі Інтернет. Правова інформатика. 2014. № 3(43). С. 89–95..
4. Мурадов В. В. Електронні докази: криміналістичний аспект використання. Порівняльно-аналітичне право. 2013. № 3-2. С. 313–315.
5. Бурбело Б.А. Криміналістичні основи протидії кіберзлочинності // Актуальні питання розслідування кіберзлочинів: матеріали міжнародної науково-практичної конференції, м. Харків, 10 грудня 2013 року. Харків: ХНУВС, 2013. С. 179–182.
6. Білоус В.В. Електронні сліди як актуальний напрямок криміналістичних досліджень // Правове життя сучасної України : матеріали міжнародної наукової конференції, м. Одеса, 20–21 квітня 2012 р. Т. 2. Одеса: Фенікс, 2012. С. 425–427.

Одержано 01.11.2017

УДК 343.9 : 004

Валерія Сергіївна ЧЕРНОВОЛ,
курсант факультету № 4 Харківського національного університету внутрішніх справ

Віталій Вікторович НОСОВ,
кандидат технічних наук, доцент, професор кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ДЛЯ ВСТАНОВЛЕННЯ ФАКТУ ПЕРЕБУВАННЯ ПІДОЗРЮВАНИХ ОСІБ НА МІСЦІ ПОДІЇ

Використання електронних засобів спілкування, приладів передавання інформації (мобільний телефон, електронна пошта, соціальні мережі тощо), певною мірою, пов'язують конкретну особу з індивідуальними технічними засобами спілкування.

Інформаційні сліди використання таких технічних засобів, при належному їх аналізі, дозволяють правоохоронним органам ідентифікувати певну особу та визначити її конкретне місцезнаходження. Останнім часом зазначений напрям є надзвичайно актуальним та перспективним для діяльності правоохоронних органів з протидії злочинності, зокрема, щодо встановлення факту перебування підозрюваної особи на місці події [1, С. 15-18].

Яскравим прикладом є застосування утиліт під операційну систему «Android», за допомогою яких можна встановити наступні відомості: Provader Code (код оператора стільникового зв'язку), LAC (Location Area Code), CID (Cell ID), рівень сигналу, тип мережі.

Щодо дзвінків з мобільного телефону для аналітичної роботи може бути отримана така інформація: кількість абонентів, серійний номер телефону, серійний номер сім карти, час та тривалість дзвінка, місцеперебування абонента [3]. Таку інформацію, в першу чергу, можна отримати, звернувшись з запитом до операторів мобільного зв'язку, в порядку передбаченому Главою 15 «Тимчасовий доступ до речей і документів» Кримінального процесуального кодексу України [2].

Інформаційно-аналітична робота, в правоохоронних органах, яка здійснюється щодо підозрюваних осіб - користувачів соціальних мереж, дозволяє отримати наступні відомості: в соціальній мережі «Facebook» – ім'я користувача, унікальний

код (ID), підписки, локація (місцезнаходження), пристрій з якого заходив користувач на сайт, час та дата його активності; із соціальної мережі «Twitter» – ім'я користувача, мова, дата створення облікового запису, ім'я користувача комп'ютера (username), унікальний код (ID), місцезнаходження користувача, з якого зроблено твіт, дата та час, унікальний код (ID) твіту, кількість та імена підписників сторінки, верифікаційний статус. Майже аналогічні дані можна отримати про користувачів інших соціальних мереж.

За наявності MAC-адреси та ESSID точок безпровідного доступу до Інтернет за допомогою сервісу WiGLE можна знайти місцезнаходження більшості точок безпровідного доступу до Інтернет.

За допомогою сервісу 2ip (посилання https://2ip.ua), за першими трьома парами MAC-адрес пристрою працівники правоохоронних органів можуть встановити більш детальну інформацію про пристрій.

Таким чином, вищевказана інформація наочно демонструє можливості використання відкритих джерел інформації та інформаційних слідів, що створює умови для ефективної роботи правоохоронних органів для здійснення аналітичної роботи щодо встановлення перебування підозрюваних осіб на місці події під час вчинення кримінального правопорушення.

Список використаних джерел:

1. Ковальова О. В. Використання науково-технічних засобів та методів у розшуковій роботі слідчого автореф. дис. на здобуття наук. ступеня канд. юрид. наук: спец. 12.00.09. К., 2014. 20 с.
2. Кримінальний кодекс України: закон України від 05.04.2001 № 2341-III // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon3.rada.gov.ua/laws/show/2341-14 (дата звернення: 20.10.2017).
3. Verizon forced to hand over telephone data – full court ruling // База даних «Public Information» / National Security Agency. URL: https://www.theguardian.com/world/interactive/2013/jun/06/verizon-telephone-data-court-order (дата звернення: 25.10.2017).

Одержано -01.11.2017

УДК 343.985

Ганна Володимирівна ЩЕРБАКОВА,
кандидат юридичних наук, доцент, головний науковий співробітник відділу науково-методичного забезпечення участі прокурорів у кримінальному провадженні НДІ Національної академії прокуратури України

ОСОБЛИВОСТІ ПІДГОТОВКИ ТА ПРОВЕДЕННЯ ОБШУКУ ПІД ЧАС РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ З ТОРГІВЛЕЮ ЛЮДЬМИ

Обшук є однією з процесуальних дій, що суттєво впливає на формування доказової бази під час розслідування різних видів злочинів, у тому числі таких, що пов'язані з торгівлею людьми.

Обшук проводиться на підставі ухвали слідчого судді, як того вимагає ч. 2 ст. 234 КПК України. Ухвала слідчого судді про дозвіл на обшук житла чи іншого володіння особи з підстав, зазначених у клопотанні прокурора, слідчого, надає право проникнути до житла чи іншого володіння особи лише один раз.

Фактичною підставою для проведення вказаної слідчої (розшукової) дії є наявність достатніх відомостей, що вказують на те, що знаряддя кримінального правопорушення або майно (речі й цінності), здобуті в результаті його вчинення, а також інші предмети та документи, які мають значення для розкриття цього правопорушення чи забезпечення цивільного позову, відомості про обставини вчинення торгівлі людьми або іншої незаконної угоди щодо людини знаходяться у певному приміщенні або місці чи в якої-небудь особи.

Відповідно до ч. 2 ст. 235 КПК ухвала про дозвіл на обшук повинна містити відомості про речі, документи або осіб, для виявлення яких проводиться обшук.

На практиці непоодинокими є випадки відмови слідчим суддею, судом у задоволенні клопотання про проведення обшуку, зокрема, у ході розслідування злочинів пов'язаних з торгівлею людьми. Підставою для цього слугує недотримання слідчими та прокурорами вимог ч. 3 ст. 234 КПК України при оформленні клопотань про надання дозволу на проведення обшуку житла чи іншого володіння особи. Зважаючи на це, важливо щоб слідчий, процесуальний керівник забезпечували належну якість підготовлених клопотань про надання дозволу на проведення обшуку.

З тактичних міркувань важливою вбачається система заходів, що забезпечує ретельну підготовку до проведення обшуку, зокрема:

1. Вивчення матеріалів кримінального провадження та збір орієнтуючої інформації, що характеризує особу, яку планують обшукувати; місце обшуку; предмети і документи, які слід шукати.

2. Визначення інших осіб, які підлягають обшуку по даному кримінальному провадженню. У випадку вчинення кримінального правопорушення групою осіб, обшук слід проводити одночасно у всіх осіб, що входять в таку групу [1, с. 56].

3. Вирішення питання щодо: часу проведення обшуку; кола учасників; способу проникнення в помешкання, що підлягає обшуку; заходів безпеки (інструктаж учасників); забезпечення охорони місця обшуку та інші питання організаційно-тактичного та прогностичного характеру залежно від ситуації.

4. Підготовка науково технічних засобів фіксації проведення цієї С(Р)Д.

Проведення обшуків доречно планувати одночасно із затриманням, в ситуаціях, коли особа підозрюваного встановлена до його затримання, це дозволить використати фактор раптовості і забезпечить виявлення важливих доказів. Якщо дані стосовно підозрюваних у вчиненні торгівлі людьми отримані тільки після їх затримання, насамперед слід вжити заходів по встановленню місця постійного чи тимчасового проживання (роботи) осіб, їх співучасників, знайомих та родичів, після чого невідкладно і по можливості одночасно організувати проведення там обшуків [2, с. 103].

Слідчий, прокурор повинні враховувати те, що найчастіше злочинці використовують в злочинній діяльності комп'ютери, комп'ютерні мережи, у тому числі й електронну пошту через мережу Інтернету, у пам'яті яких можуть зберігатися дані, що стосуються злочинної діяльності (облік жінок, отриманих за їх продаж грошей і т. ін.). Тому під час обшуків обов'язково слід з'ясувати наявність у підозрюваних комп'ютерів, електронних органайзерів, факсимільних апаратів, мобільних телефонів, електронних записників, касет до автовідповідачів тощо.

Важливо щоб після прибуття на місце проведення обшуку слідчий, прокурор видалили з місця проведення С(Р)Д сторонніх осіб та забезпечили його охорону, якщо це не було зроблено раніше. Якщо слідчому, прокурору відомо про використання злочинцями ЕОМ, комп'ютерів, комп'ютерних мереж, слід за-

безпечити охорону ЕОМ, у якій було виявлено сліди злочину, сервер, пункти вимкнення живлення, якщо техніка знаходиться у ввімкненому стані, тощо; забезпечити неможливість вчинення сторонніми особами будь-яких дій з комп'ютерною технікою, їх користування іншими технічними засобами, що можуть за допомогою бездротових технологій вносити зміни в інформацію (видаляти її).

Особлива увага під час проведення обшуку повинна звертатися на виявлення: записних книжок, мобільних телефонів, документів про надходження та одержання грошових переказів, інших цінностей, анкет для отримання закордонних паспортів; митних декларацій; трудових договорів; копій квитанцій на міжнародні поштові відправлення та переводи; установчих документів, що підтверджують право на заняття туристичною діяльністю, діяльністю з працевлаштування (в тому числі і за кордоном); проїзних квитків та ін.

Список використаних джерел:

1. Весельський В. К., Пясковский В. В. Торгівля людьми в Україні (Проблеми розслідування) : навчальний посібник. К. : КНТ, 2007. 268 с.
2. Діяльність прокурора з протидії злочинам, пов'язаним з торгівлею людьми та незаконною трансплантацією органів і тканин : навч. посіб. / І. М. Козьяков, О. М. Толочко, В. М. Куц, А. М. Орлеан, І. П. Ковтун та ін.; Нац. акад. прокуратури України. Кам'янець-Подільський : Буйницький О. А., 2014. 166 с.

Одержано 01.11.2017

УДК 343.3

Ксенія Володимирівна ЮРТАЄВА,
кандидат юридичних наук, старший викладач кафедри кримінального права і кримінології факультету № 1 Харківського національного університету внутрішніх справ

КРИМІНАЛЬНО-ПРАВОВІ АСПЕКТИ ПРОТИДІЇ НЕЗАКОННОМУ ВИКОРИСТАННЮ КОМП'ЮТЕРНИХ ПАРОЛІВ ТА КОДІВ ДОСТУПУ, ЯКІ НАДАЮТЬ ДОСТУП ДО КОМП'ЮТЕРНИХ СИСТЕМ АБО ЇХ ЧАСТИН

Останнім часом в Україні почастішали випадки незаконного використання комп'ютерних паролів, кодів доступу та подібних даних, які надають доступ до комп'ютерних систем або їх частин. Зазначені діяння вчиняються для отримання доступу до банківський рахунків, конфіденційної інформації, що зберігається в комп'ютері або в комп'ютерній системі, до

приватних акаунтів користувачів комп'ютерних мереж тощо. Іноді комп'ютерні шахраї займаються незаконним збором подібних даних з метою їх продажу й подальшого незаконного використання.

На теперішній час КК України не містить окремих норм щодо кримінальної відповідальності за незаконне використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин [1]. Ратифікована Україною Конвенція Ради Європи про кіберзлочинність 2001 р. передбачає встановлення відповідальності за виготовлення, продаж, придбання для використання, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення злочинів, передбачених статтями 2-5 Конвенції [2]. Проте Україна реалізувала зазначену вимогу лише частково, зробивши відповідне застереження під час ратифікації вказаної угоди.

Провівши аналіз положень чинного КК України, приходимо до висновку, що притягнення до кримінальної відповідальності за продаж, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин, на теперішній час є практично неможливим. Так, наприклад, деякі фахівці пропонують кваліфікувати розповсюдження кодів доступу до комп'ютерної системи як пособництво у вчиненні інших комп'ютерних злочинів. У такому випадку слідчим має бути доведено усвідомлення особи хоча б у загальних рисах, що розповсюдження або продаж комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин, є частиною конкретного комп'ютерного злочину та сприяє його вчиненню, що на практиці здійснити вкрай складно. Вбачається, що незаконне, без права на це розповсюдження конфіденційної інформації як-от комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин, є самостійною, ізольованою діяльністю особи, яка зазвичай спрямована на невизначене та не персоніфіковане коло осіб. Умисел особи зазвичай обмежуються збутом (розповсюдженням) зазначених предметів з отримання матеріальної винагороди або без такої, тому подібну діяльність

вбачається недоцільним розглядати як співучасть у вчиненні інших комп'ютерних злочинів.

Окремо слід розглянути випадки, коли особа будь-яким чином без право на це умисно отримує комп'ютерний пароль, код доступу або подібні дані, які надають доступ до комп'ютерної системи або її частини, для подальшого їх використання для вчинення інших комп'ютерних злочинів самостійно, без залучення інших осіб. Прикладом цього можуть бути фішинг, вішинг, смішинг та інші види комп'ютерного шахрайства. Вбачається, що незаконне отримання комп'ютерних паролів, кодів доступу або подібних даних, за наявності необхідних підстав можливо кваліфікувати як готування до вчинення комп'ютерного злочину. Проте у деяких випадках притягнення до кримінальної відповідальності стає неможливим, наприклад, за готування до злочину, передбаченого ст. 163 КК України (порушення таємниці кореспонденції, що передається через комп'ютер), оскільки останній є злочином невеликої тяжкості, готування до яких не тягне за собою кримінальної відповідальності. Крім того умисел на вчинення подальших комп'ютерних злочинів не завжди можливо довести. Утім, слід зазначити, що фішинг-шахраї часто збирають та накопичують конфіденційну інформацію з метою передачі (збуту) іншим особам, що знову повертає нас до вже аналізованих проблем співучасті у вчиненні подібних злочинів.

Підсумовуючи, можна зробити висновок, що чинний КК України на теперішній час не передбачає ефективних можливостей притягнення до кримінальної відповідальності за дії, пов'язані з незаконним використання комп'ютерних паролів, кодів доступу або подібних даних, які надають доступ до комп'ютерних систем або їх частин. До Верховної Ради України було подано декілька законопроектів щодо встановлення відповідальність за вказане діяння, однак жодний з них не був прийнятий. Відповідальність за незаконне використання комп'ютерних паролів, кодів доступу або подібних даних передбачена в ст. 285 КК Грузії, ст. 216 КК Естонської Республіки, ст. 260-4 КК Республіки Молдови, ст. 46 Антикорупційного закону Румунії, §1028A(6) Титулу 18 США. Враховуючи негативну динаміку розповсюдження суспільно небезпечних діянь, пов'язаних з протиправними діями з комп'ютерними паролями, кодами доступу або подібними даними, вбачається обґрунтованим передбачення кримінальної відповідальності за вказані діяння у Розділі XVI Особливої частини КК України

«Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку».

Список використаних джерел:

1. Кримінальний кодекс України URL: http://zakon3.rada.gov.ua/laws/show/2341-14 (дата звернення: 01.10.2017).
2. Конвенція про кіберзлочинність 2001 р. URL: http://zakon3.rada.gov.ua/laws/show/994_575 (дата звернення: 01.10.2017).

Одержано 01.11.2017

РОЗДІЛ 3.
ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ І ТЕХНІЧНИХ ЗАСОБІВ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 004.056.53

Василий Александрович АЛЕКСЕЕВ,
аспирант кафедры компьютерной радиоинженерии и систем технической защи-ты информации Харьковского национального университета радиоэлектроники

Денис Юрьевич ГОРЕЛОВ,
кандидат технических наук, доцент, доцент кафедры компьютерной радиоинженерии и систем технической защиты информации Харьковского национального университета радиоэлектроники

СБОР И АНАЛИЗ ХАРАКТЕРИСТИК КЛАВИАТУРНОГО ПОЧЕРКА ПОЛЬЗОВАТЕЛЕЙ С ЦЕЛЬЮ ОТСЛЕЖИВАНИЯ И ПРЕДОТВРАЩЕНИЯ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОМПЬЮТЕРИЗИРОВАННЫМ СИСТЕМАМ

Задачи, связанные с защитой персональных и корпоративных данных в наши дни приобретают первоочередное значение и привлекают внимание большого числа специалистов по всему миру [1]. Непрерывно растущая сложность программно-аппаратных приложений и сервисов работающих на их основе, требует более новых и эффективных подходов в обеспечении безопасности при получении прав на доступ к ресурсам системы, т.е. в момент аутентификации. В тоже время, аутентификация является одним из наиболее приоритетных механизмов, позволяющих как предотвращать, так и оперативно отслеживать попытки несанкционированного доступа к данным. В качестве основы реализации такого рода механизма аутентификации достаточно эффективно [2] может быть использован анализ динамических биометрических характеристик пользователя, которые в отличие от традиционных (идентификатор, логин, пароль, токен), как правило, трудно воспроизвести и они не могут быть утеряны или забыты.

Клавиатурный почерк характеризует стиль работы человека с клавиатурой посредством вычисления и обработки временных параметров нажатий клавиш. При этом основу мате-

матической модели почерка субъекта составляет анализ двух последовательных событий или диграфов – время между нажатиями соседних клавиш (ВСК) и время удержания единичной клавиши (ВУК), которые могут быть измерены с точностью до единиц миллисекунд (см. рис. 1).

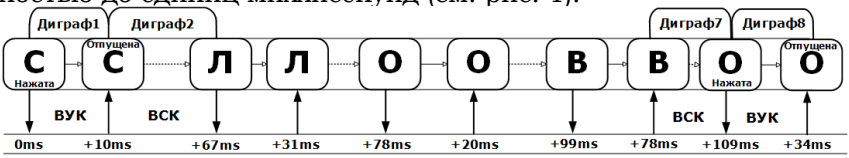

Рис. 1. Основные временные характеристики диграфов клавиатуры

В качестве базового алгоритма для обработки полученных данных и построения модели аутентификации авторами использовался вероятностно-статистический подход с использованием статистических параметров диграфов [3], а также его модификация, учитывающая динамические свойства диграфов (переход от временных параметров диграфов к их отношениям) и раздельный функциональный анализ зон клавиатуры, как признак несущий дополнительные информативные свойства [4]. В рамках предложенного алгоритма клавиши клавиатуры делились на четыре группы: блок алфавитно-цифровых клавиш, блок клавиш-модификаторов, блок функциональных клавиш и зона клавиш из дополнительного цифрового блока. Конечное решение об аутентификации пользователя принималось на основании всех данных со всех функциональных зон клавиатуры.

Задача аутентификации пользователя состоит из 2 основных этапов: обучение системы и распознавание. На этапе обучения системы создаются эталонные профили зарегистрированных пользователей, которые состоят из идентификаторов диграфов и соответствующих им статистических параметров. На этапе распознавания формируемые профили сравниваются с эталонными и на основе статистических правил принимается решение об идентификации пользователя [4].

Для апробации различных алгоритмов, лежащих в основе процедуры идентификации по клавиатурному почерку, разработано клиент-серверное WEB-приложение [http://biokey.tech/]. На рис. 2 приведены профили, построенные по алгоритму из [4], 2-х пользователей с различными навыками работы на клавиатуре. Как видно из графиков, профили пользователей достаточно сильно различаются и мо-

гут быть использованы для повышения информационной безопасности компьютеризированных систем.

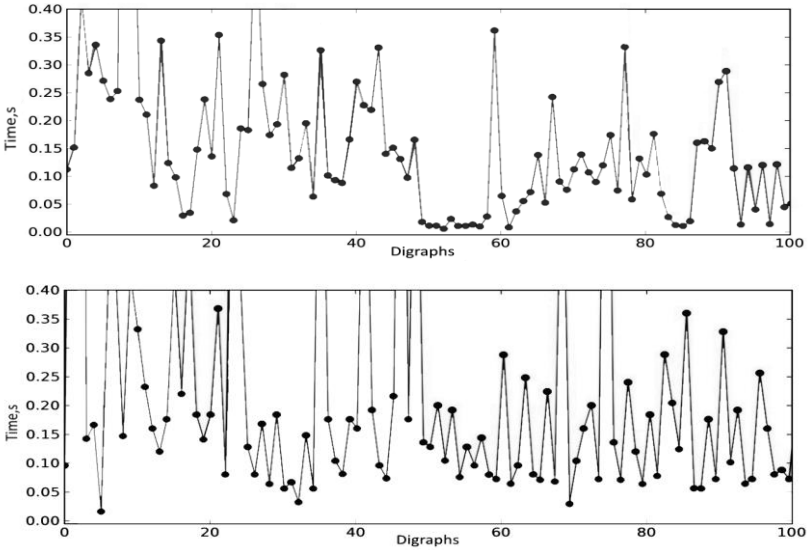

Рис. 2. Примеры клавиатурных профилей пользователей

Изучение свойств клавиатурного почерка имеет потенциал для применения в различных приложениях как дополнительная мера, повышающая общий уровень безопасности при аутентификации. Отсутствие необходимости внедрения дополнительного оборудования, а также возможность продолжительного сбора статистики во время всего сеанса работы пользователя с клавиатурой (скрытое наблюдение) делают данный подход интересным для изучения.

Список використаних джерел:

1. Zhong Y., Deng Y. Recent Advances in User Authentication Using Keystroke Dynamics Biometrics. Science Gate Publishing, 2015. Chapter 2. pp. 23-40.
2. Draffin, B., Zhu, J., & Zhang, J. KeySens: passive user authentication through micro-behavior modeling of soft keyboard interaction // Mobile Computing, Applications, and Services: International Conference on Mobile Computing, Applications, and Services. 2013. pp 184-201.
3. Синиця Ю. О. Автентифікація суб'єктів за клавіатурним почерком з використанням диграфів // Международная кон-

ференция "Интернет-технологии и программирование компьютерных мобильных систем": Материалы XVII Международного молодежного форума "Радиоэлектроника и молодежь в XXI веке ". Т. 5. Х., 2013. С. 167-168.
4. Алексеев В., Синица Ю., Горелов Д. Модифицированный метод диграфов в задаче аутентификации пользователей по клавиатурному почерку. *Защита информации.* 2017. Вып. 4. С. 252-261.

Одержано 27.10.2017

УДК 004.9

Роман Васильович БАРАНЕНКО,
кандидат технічних наук, доцент, професор кафедри професійних та спеціальних дисциплін Херсонського факультету Одеського державного університету внутрішніх справ

ЗАХИСТ КРИТИЧНОЇ ІНФРАСТРУКТУРИ В КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ДЕРЖАВИ

Інформаційна безпека відіграє важливу роль у забезпеченні інтересів будь-якої держави. Створення розвиненого й захищеного інформаційного середовища є неодмінною умовою розвитку суспільства та держави [1].

Найнебезпечнішими загрозами державним інтересам в інформаційному суспільстві є неконтрольоване розповсюдження інформаційної зброї. Інформаційна зброя є сукупністю засобів, методів і технологій, що забезпечують можливість силового впливу на інформаційну сферу супротивника з метою руйнування його інформаційної та управлінської інфраструктури. Інформаційна зброя не знає географічних відстаней, підриває традиційне поняття державних кордонів, роблячи їх технологічно проникними. Використання цієї зброї може відбуватися досить приховано («буденно»), не доводячи справу до оголошення «гарячої» війни; не потребує великої й видимої підготовки. До того ж, у зв'язку з відсутністю систем і методик, що оцінюють загрозу і заздалегідь попереджають про підготовлюваний напад, ускладнюється можливість протидіяти такій агресії [2].

Під життєво важливою критичною інфраструктурою розуміються «системи та об’єкти, фізичні чи віртуальні, настільки життєво важливі для держави, що недієздатність або знищення таких систем або об’єктів підриває національну безпеку, економіку, здоров’я або безпеку населення, або має своїм результатом будь-яку комбінацію з перерахованого вище» [3].

З-поміж загроз критичній інфраструктурі називають пандемії, промислові аварії, терористичну та злочинну діяльності, кібератаки, стихійні лиха тощо [4].

Прикладом кібератаки на критичну інфраструктуру держави є вірус Stuxnet, головною метою якого стало ураження програмованих логічних контролерів, які використовуються для автоматизації технологічних процесів на заводі зі збагачення урану у місті Нетенз в Ірані. За деякими версіями вірус Stuxnet на підприємство приніс один з контрактних робітників використовуючи USB-флешку.

Код Stuxnet інфікував програмовані логічні контролери центрифуг для збагачення урану трьома послідовностями атак A, B і C. Послідовності A і B виконували свої атаки запуску роторів центрифуг при дуже низьких і високих частотах (таких, як 2 і 1410 Гц, відповідно). Періоди, в який вони передавали команди центрифугам для обертання на цих швидкостях, досить короткий (50 і 15 хвилин, відповідно), і відокремлені один від одного: близько 27 днів між атаками. Це, можливо, вказує на те, що архітектори кібератаки хотіли якомога довше залишатися не поміченими.

Хоча часу, протягом якого центрифуги сповільнювалися або прискорювалися, ймовірно, не було достатньо для того, щоб реально досягти мінімального й максимального значень, вони як і раніше призводили до значних уповільнень і швидкісних злетів. Повільної швидкості достатньо, щоб призвести до неефективно переробленого урану, а високі швидкості, можуть призвести центрифуги до фактичного знищення, так як вони працювали на межі максимальної швидкості.

Stuxnet приховував шкідливі коди, записані на програмовані логічні контролери для саботажу центрифуг, а також захищав ці шкідливі коди від перезапису. Перед тим як шкідлива програма запускає процедуру атаки, вірус записував нормальні робочі частоти центрифуг і передавав ці записані дані до програми-монітору під час атаки. Результатом було те, що система показувала нормальну роботу замість оповіщення персоналу про аномальні частоти, на яких центрифуги насправді працюють. Stuxnet також змінив деякі процедури на програмованих логічних контролерах, запобігаючи безпечному завершенню роботи системи, навіть якщо оператор виявить, що система не працює в нормальному режимі.

Однак на практиці практично неможливо довести, що такі дії відповідають критеріям кібертероризму, хоча й діяльність

вірусу Stuxnet дійсно могла створити небезпеку для життя працівників ядерних об'єктів. Але без добровільного зізнання про політичні мотиви організаторів дану дію вкрай складно класифікувати як кібертероризм, швидше, як кібердиверсію [5].

Список використаних джерел:

1. Степко О. М. Аналіз головних складових інформаційної безпеки держави. *Науковий вісник Інституту міжнародних відносин НАУ*. Сер. : Економіка, право, політологія, туризм. 2011. Вип. 1(3). С.90-99.
2. Крутских А. В. Война или мир: международные аспекты информационной безопасности // Научные и методологические проблемы информационной безопасности (сборник статей); под ред. В. П. Шерстюка. М.: МЦНМО, 2004. С.85-96.
3. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism : USA PATRIOT ACT. 2001. URL: http://frwebgate.access.gpo.gov (дата звернення: 13.10.2017).
4. Critical Infrastructure Resilience Strategy / Australian Government URL: http://www.tisn.gov.au/. (дата звернення: 13.10.2017).
5. Дубов Д. В., Ожеван М. А. Кібербезпека: світові тенденції та виклики для України. К .: НІСД, 2011. 30 с.

Одержано 30.10.2017

УДК 004.056.5:343.34

Єлизавета Георгіївна БЄЛЯЄВА,
курсант 2-го курсу факультету № 4 Харківського національного університету внутрішніх справ

Олексій Михайлович РВАЧОВ,
старший викладач кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ВІРУСИ-ШИФРУВАЛЬНИКИ, ЯК ГОЛОВНА ЗБРОЯ КІБЕРТЕРОРИСТІВ

Проблема поширення світом кібертероризму з кожним роком набуває все більшого значення, а отже питання протидії кібертероризму стає ще більш актуальнішим. Кібератаки складають велику загрозу, як суто національній, так і міжнародній безпеці країн.

На теперішній час в законодавстві України визначення поняття «кібертероризм» не наведено в жодному з нормативно-правових документів, хоча цей термін і вживається в деяких нормативних документах та законодавчих актах.

В Законі України «Про боротьбу з тероризмом» від 20.03.2003 дане визначення терміну «технологічний тероризм – злочини, що вчиняються з терористичною метою із застосуванням ядерної, хімічної, бактеріологічної (біологічної) та іншої зброї масового ураження або її компонентів, інших шкідливих для здоров'я людей речовин, засобів електромагнітної дії, комп'ютерних систем та комунікаційних мереж, включаючи захоплення, виведення з ладу і руйнування потенційно небезпечних об'єктів, які прямо чи опосередковано створили або загрожують виникненням загрози надзвичайної ситуації внаслідок цих дій та становлять небезпеку для персоналу, населення та довкілля; створюють умови для аварій і катастроф техногенного характеру» [1].

З цього визначення можна припустити, що технологічний тероризм включає в себе й так званий кібертероризм.

Цілями для кібертероризму є: незаконне втручання в роботу комп'ютерних систем і отримання доступу до особистої та банківської інформації, військовим та державним конфіденційним даним; виведення з ладу обладнання та програмного забезпечення, створення перешкод, порушення мереж електроживлення; крадіжка цифрових даних; витік секретної інформації у відкритий доступ; поширення дезінформації за допомогою захоплених каналів засобів масової інформації; порушення роботи каналів зв'язку [2].

Найпопулярнішим методом кібертероризму є ураження комп'ютерних систем та пристроїв шкідливим програмним забезпеченням шляхом використання: вразливостей операційних систем та програмного забезпечення; методів соціального інжинірінгу; незаконне втручання в роботу популярних інформаційних ресурсів (вебсайти та сервери оновлення для програмних продуктів).

В ст. 361-1 Кримінального Кодексу України використовується термін «шкідливі програмні засоби», але в національному законодавстві не наведено визначення цього терміну [3]. За результатами аналізу визначень цього терміну від провідних антивірусних компанії, можна сформулювати наступне визначення: «шкідливе програмне забезпечення – це програма, яка була навмисно створена для виконання несанкціонованих, часто шкідливих дій, на електронному пристрою без відома його власника» [4, 5].

Виділяють кілька типів шкідливого програмного забезпечення: шпигунські, рекламні, фішингові, троянські, здирниць-

кі програми, віруси, черв'яки, руткіти та програми, націлені на захоплення контролю над браузером [5].

До одних з наймасштабніших кібертеракт 2017 року, на теперішній час, можна віднести ураження соціального, економічного та державного секторів шкідливим програмним забезпеченням з сімейства «Petya». А за цей рік ще стали відомими такі віруси як «WannaCry», «EternalRocks» (також відомий як MicroBotMassiveNet).

Події, які сталися у червні 2017 року показали світу усю небезпечність вірусів-шифрувальщиків та незахищеність комп'ютерів користувачів. Вірусні атаки торкнулися соціального сектору, енергетичних компаній, державних інтернет-ресурсів та локальних мереж, укрмедіа та ряд інших великих підприємств, що в результаті призвело до величезних збитків. Станом на 28 червня 2017 року вірус заразив 12 500 ПК у 64 країнах світу.

Як встановили спеціалісти, зараження вірусом відбувалося через оновлення української програмного забезпечення для подачі бухгалтерської звітності «M.E.Doc», а також під час відкриття користувачами фішингових листів електронної пошти, що містили файли із вірусом.

Після свого запуску вірус шифрує файли на жорсткому диску комп'ютера-жертви, а також перезаписує і шифрує головний завантажувальний запис (MBR) – дані, необхідні для завантаження операційної системи і проводить перезавантаження комп'ютер, та під виглядом перевірки жорсткого диску починає шифрувати файли на ньому. В результаті всі файли, що зберігаються на комп'ютері, стають недоступними. Потім програма вимагає грошовий викуп у біткоїнах за розшифровку і відновлення доступу до файлів.

Систему можливо запустити навіть після її компрометації, якщо встигнути запустити команду «bootrec/fixMbr» для відновлення MBR, а також працездатності ОС. Але розшифрувати файли вже не вдасться («зловред» шифрує файли максимум на 15 піддиректорії, тобто файли вкладені на більшу глибину, знаходяться в безпеці).

Експерти «Positive Technologies» виявли «kill-switch» – можливість локально вимкнути шифрувальщик. Для запобігання зараженню треба зробити вигляд наче комп'ютер вже є зараженим. Якщо процес має адміністративні привілегії ОС, то перед підміною MBR шифровальщик перевіряє наявність файлу «perfc» без розширення в директорії «C:\Windows\». Для захис-

ту лише потрібно створити файл під назвою «perfc.dll» та зробити його доступним лише для читання аби вірус не зміг внести в нього будь-які зміни. Наявність такого файлу в директорії може бути одним з індикаторів компрометації. Якщо файл у наявності в даній директорії, то процес виконання вірусного програмного забезпечення завершується таким чином.

Але найпростішим способом не дати вірусу поширити шкідливий код це заблокувати у фаєрволі операційній системи доступ до 135, 139, 445 TCP-портів, саме які він використовує для свого розповсюдження [6].

Президент компанії «InfoWatch» Наталія Касперська вважає, що останні вірусні атаки, в тому числі атака вірусу-шифрувальника «Bad Rabbit», організовані з метою кібертероризму, а не заробітку [7]. Ми згодні з даною думкою.

На сьогодні в України існує потреба чіткого визначення на законодавчому рівні значень таких термінів як «кібертероризм» та «шкідливе програмне забезпечення».

Список використаних джерел:

1. Про боротьбу з тероризмом: Закон України від 20.03.2003 № 638-IV, редакція від 07.05.2017. URL: http://zakon.rada.gov.ua/laws/show/638-15 (дата звернення: 25.10.2017).
2. Угрозы информационной безопасности. Кибервойны. Кибертерроризм // Аналитический центр «Anti-Malware.ru». URL: https://www.anti-malware.ru/threats/cyberterrorism (дата звернення: 25.10.2017).
3. Кримінальний Кодекс України: Закон України від 05.04.2001 № 2341-III, редакція від 03.09.2017 // База даних «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 26.10.2017).
4. Вредоносная программа // Энциклопедия / АО «Лаборатория Касперского». URL: https://securelist.ru/threats/malware-glossary/ (дата звернення: 26.10.2017).
5. Что такое вредоносная программа и как от нее избавиться // Компания AVAST Software. URL: https://www.avast.ru/c-malware (дата звернення: 28.10.2017).
6. Как победить вирус Petya // Хабрахабр / Компания «Positive Technologies». 28 июня 2017 года. URL: https://habrahabr.ru/company/ pt/blog/331858/ (дата звернення: 25.10.2017).
7. Наталья Касперская о последних вирусных атаках: «Это кибертерроризм в чистом виде» // «БИЗНЕС Online»: Деловая электронная газета Татарстана. 26 октября 2017 года. URL:

https://www.business-gazeta.ru/news/362049 (дата звернення: 27.10.2017).

Одержано 30.10.2017

УДК 004.93

Владислав Вячеславович БОРОДАВКА,
студент Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ»

Михайло Віталійович ЦУРАНОВ,
старший викладач кафедри комп'ютерних систем та мереж Національного аерокосмічного університету ім. М. Є. Жуковського «ХАІ»

ВИКОРИСТАННЯ БІОМЕТРИЧНОГО КОНТРОЛЮ ДОСТУПУ ДО LINUX СЕРВЕРІВ ДЛЯ ПРОТИДІЇ НЕСАНКЦІОНОВАНОМУ ДОСТУПУ

З розвитком інформаційних технологій все більша кількість сервісів переноситься на хмарні платформи і використовує технологію клієнт-сервер для забезпечення безпечної обробки і зберігання даних. Для забезпечення контролю доступу до серверів і серверних приміщень використовуються різні СКУД (Системи контролю управлінням доступом). У цих системах використовуються різні токени для автентифікації користувачів: RFID мітки, смарт-карти, uaTocken і т.д.

Останнім часом все більшого поширення в СКУД отримують системи біометричної автентифікації (БА) користувача. Системи БА – системи, що використовують для ідентифікації особи людей їх біометричні дані [1]. Біометрія передбачає систему розпізнавання людей по одній або кільком фізичним, або поведінковим характеристикам людини. В даний час методи БА стали більш досконалими, а надійна авторизація та автентифікація стають важливими атрибутами повсякденного життя [2, с. 18]. Широке застосування біометричних технологій (БТ) призводить до появи принципово нових видів загроз. Зараз БТ трансформувалися в повноцінний компонент систем захисту, інтеграція яких вимагає продуманого підходу.

Стрімкий розвиток технології клієнт-сервер призвело до виникнення значної кількості нових загроз, багато з яких отримали подальший розвиток в середовищі ОС Linux. Це стало можливим в результаті того, що Linux використовується в якості серверної ОС і за даними компанії Netcraft на вересень 2017 року, вісім з десяти найбільш надійних інтернет-

компаній, що надають хостинг, використовують Linux на своїх веб-серверах [3]. Linux є ключовим компонентом комплексу, що поставляється з серверним комплектом ПЗ LAMP (Linux, Apache, MariaDB / MySQL, Perl / PHP / Python), а також для управління суперкомп'ютерами, за даними на червень 2017, 99,6% комп'ютерів зі списку 500 найпотужніших працювали під управлінням Linux [4].

Метою даної роботи є аналіз особливостей методів і алгоритмів БА, можливості їх застосування в різних промислових системах безпеки та операційних системах, розгляд вразливостей біометричних систем, а також розробка програмного засобу БА для ОС Linux.

Результатом роботи є модель загроз для БА, матриця аналізу методів і алгоритмів БА, а також готовий програмний засіб БА для ОС Linux. Наведені результати дозволять підвищити безпеку і ефективність автентифікації в серверах на базі Linux, а також зменшити ризики обходу СКУД.

Список використаних джерел:

1. Wikipedia: Биометрические системы аутентификации URL: https://ru.wikipedia.org/wiki/Биометрические_системы_аутентификации (дата звернення: 24.10.2017).
2. Каклаускас А. Биометрическая и интеллектуальная поддержка решений. Вильнюс: Техника, 2012. с. 344.
3. Most Reliable Hosting Company Sites in September 2017 Netcraft. URL: https://news.netcraft.com/archives/2017/ (дата звернення: 24.10.2017).
4. Operating system family/Linux URL: https://www.top500.org/statistics/details/osfam/1. (дата звернення: 24.10.2017).

Одержано 25.10.2017

УДК 004.056

Олександр Юрійович ГОРЕЛОВ,
студент факультету комп'ютерних наук Харківського національного університету радіоелектроніки

ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ОДНОГО КЛАСУ ВЕБ-ДОДАТКІВ

Однією з актуальних проблем кібербезпеки є забезпечення безпеки веб-додатків і хмарних додатків, які дуже активно розвиваються в останні роки. З огляду на те, що величезне число додатків цих класів розробляються з використанням мови Java, особливу актуальність здобуває завдання забезпечення безпеки саме додатків цього класу.

Першим рубежем захисту будь-якої програмної системи є автентифікація та авторизація користувача. Його інфраструктура може бути спроектована на основі централізованої або розподіленої моделі. Централізована модель автентифікації дозволяє підтримувати розподілений каталог, інформація в якому може бути розділена на розділи. Одним з варіантів реалізації централізованої системи автентифікації є використання фреймворку Spring Security та засобів створення й ведення реєстру користувачів і маршрутизації.

Фреймворк Spring Security є інструментом, який найбільш часто використовується для реалізації цього рівня захисту Java-додатків зазначених класів. Він надає засоби побудови систем автентифікації та авторизації, та інші можливості забезпечення безпеки додатків, створених за допомогою Spring Framework.

Інфраструктура Spring Security надає високий рівень абстракції, що дозволяє застосовувати різні моделі автентифікації й авторизації, і забезпечує високу переносимість між різними серверами додатків. Серед основних її можливостей: декларативна безпека, підтримка різних схем автентифікації й авторизації, підтримка однократного пред'явлення пароля, підтримка інтеграції контейнерів, анонімних сеансів, одночасних сеансів, безпеки на рівні каналу та інше.

До ключових об'єктів контексту Spring Security відносяться [1]:

- SecurityContextHolder - містить інформацію про поточний контекст безпеки додатка;
- SecurityContext - містить об'єкт Authentication та при необхідності інформацію системи безпеки, пов'язану із запитом від користувача.
- Authentication - представляє користувача з погляду Spring Security.
- GrantedAuthority - відбиває дозволи, видані користувачеві в масштабі всього додатка (ролі).
- UserDetails - надає необхідну інформацію для побудови об'єкта Authentication із джерел даних системи безпеки.

Для створення й ведення каталогу та реалізації маршрутизації можна використати сервер Apache DS [2] та LDAP. Apache DS - це відкритий LDAP-сервер із гнучкою й розширюваною структурою, розроблений мовою Java. Важливою його особливістю є те, що він дозволяє застосовувати різні протоколи в службі каталогу. Найбільш важливим протоколом,

реалізованим за допомогою ApacheDS є LDAP. LDAP — відносно простий протокол, що використовує TCP/IP і дозволяє проводити операції авторизації, пошуку та порівняння, а також операції додавання, зміни або видалення записів. ApacheDS виступає як LDAP-сервер, очікує запити та координується із внутрішнім стрижнем служби каталогу для відповіді на запити LDAP. При використанні LDAP відпадає необхідність у використанні спеціальних драйверів, можна реалізувати гнучку схему обробки, орієнтуватися на користувача (аутентіфикація, аудит, створення груп, паролі, сертифікати тощо) і ефективно визначати його контекст безпеки. Інтеграцію у веб-додаток можна здійснити у вигляді сервлета, що витягає з веб-запиту необхідну інформацію.

Список використаних джерел:

1. Краткий обзор Spring Security. URL: https://habrahabr.ru/post/203318/ (дата звернення: 18.10.2017).
2. ApacheDS-official site. URL: http://directory.apache.org/ (дата звернення: 28.12.2016).

Одержано 27.10.2017

УДК 004.056

Юрій Петрович ГОРЕЛОВ,
кандидат технічних наук,доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

ЗАХОДИ ПРОТИДІЇ АТАКАМ З ВИКОРИСТАННЯМ ВРАЗЛИВОСТЕЙ АРХІТЕКТУРИ HTTP- ПОВІДОМЛЕНЬ

Однією з актуальних завдань забезпечення кібербезпеки є захист веб-серверів і веб-додатків. Серед десятків видів атак на веб-сервери та додатки високий пріоритет мають атаки, у ході яких відбувається експлуатація вразливостей архітектури повідомлень HTTP при роботі за схемою клієнт-проксі-сервер. Наявність проміжних вузлів, таких, як кешуючий сервер, міжмережних екранів або проксі серверів, що працюють у режимі «reverse proxy», робить обмін даними небезпечним.

Різні види атак цього класу мають свої особливості, але їхньою загальною рисою є порушення структури http-запитів або http-відповідей, що дозволяє втручатися в роботу веб-серверів або додатків.

До основних заходів протидії даним видам атак можна віднести:

- установка екранів для веб-додатків;
- застосування стійких технік керування сесіями та завершення сесій після кожного запиту;
- відключення розподілу TCP-з'єднань на проміжних пристроях;
- активізація заборони на кешування всіх сторінок;
- використання технології SSL для захисту сайтів;
- повне усунення XSS-вразливостей;
- блокування запитів по протоколі HTTP/1.0 на рівні веб-сервера;
- фільтрація уведених користувачем даних з метою видалення послідовностей CRLF.

Одержано 27.10.2017

УДК 651. 34

Світлана Юріївна ГАВРИЛЕНКО,
кандидат технічних наук, доцент кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

Ілля Валентинович ШЕВЕРДІН,
аспірант кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

РОЗРОБКА ЕКСПЕРТНОЇ СИСТЕМИ ВИЯВЛЕННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА БАЗІ АНАЛІЗУ ВІРУСУ PETYA

Найпомітнішою подією першого літнього місяця 2017 року на Україні стала епідемія вірусу-шифрувальника Trojan.Encoder.12544, що згадується в ЗМІ як Petya.A або mbr locker 256. Під удар «вірусу-вимагача» потрапили українські державні структури і приватні компанії: Кабінет Міністрів, «Ощадбанк», «Укренерго», «Нова пошта», аеропорт Бориспіль, Чорнобильська АЕС та інші організації. Ця шкідлива програма заразила комп'ютери безліч організацій і приватних осіб в 60 країнах світу.

В роботі проаналізовано даний вірус та описано етапи поширення, а саме встановлено наступні шляхи зараження:

1) шляхом експлуатації вразливості в SMB MS17-010 (аналогічно вірусу Wanna Cry);

2) шляхом спрямованої відправки шкідливого програмного забезпечення за електронною поштою;

3) шляхом використання вразливості для виконання шкідливого коду: CVE-2017-0199;

4) шляхом використання вразливості для поширення і зараження в EternalBlue.

Першим етапом є впровадження, воно здійснюється шляхом скачування шкідливого контенту з заражених веб-сайтів, через ботнет, через ігрові сервери або за рахунок використання вразливості різних компонентів системи, а саме:

- вразливості веб-браузерів (експлойти iframe, XSS);
- вразливості клієнтів електронної пошти;
- вразливості операційної системи.

Другий етап, це безпосередній запуск вірусу, що являє собою шифрування інформації. Як правило користувач запускає вірус сам, при цьому не здогадуючись про фатальну помилку, тому що вірус захований шляхом впровадження в стороннє програмне забезпечення або плагін для веб-браузера.

Розшифрувати файли, зашифровані вірусом шляхом підбору ключа неможливо, тому що вірус Petya використовує асиметричну криптографію RSA, тобто для кожного зараженого комп'ютера існує персональний ключ (private key) RSA. Для підбору ключа потрібно дуже великий обчислювальний потенціал, який в звичайних умовах неможливо відтворити.

Наступним етапом роботи вірусу Petya буде перезавантаження системи, в окремих випадках воно здійснюється автоматично, шляхом створення завдання на перезавантаження в системному планувальнику завдань. Після перезавантаження, на екран виводитися банер з вимогою перевести гроші за розшифрування, в якому пропонується перерахувати $300 шляхом використання піринговой платіжної системи Bitcoin. Використання даної платіжної системи дозволяє зловмисникам залишатися анонімними. Оплативши послугу, виводиться повідомлення про те, що необхідно надати ідентифікатор гаманця Bitcoin і згенерований ідентифікатор системи на електронну пошту вимагачів. Гарантії відновлення файлів немає, так як на той час, в більшості випадків, вже будуть заблоковані рахунки і поштовий ящики зловмисників. Так само немає доказів, що окремий подібний вірус створений тільки з метою вимагання. Подібні віруси також можуть створюватися з метою тільки шкідливого впливу, блокуючи роботу державних організацій.

Результатом аналізу вірусу у віртуальній операційній системі є збір системних звітів і подій та формування бази послі-

довності системних команд, котрі мають зловмисну дію. В якості команд будо виділено ключи реєстру, зміна MBR та зміни файлової системи, а саме створення файлів, шифрування та видалення. Отримано, що в заражених системах зазначені файли розташовуються в файловій системі в таких папках:

1) C: \ Windows \ perfc.dat;
2) % APPDATA% \ 10807.exe;
3) C: \ myguy.xls.hta.

Виявлено наступні шкідливі файли та їх хеш-суми:

1) файл myguy.xls, розмір 13893 байт,
SHA1: 736752744122A0B5EE4B95DDAD634DD225DC0F73
MD5:0487382A4DAF8EB9660F1C67E30F8B25;

2) файл BCA9D6.exe, розмір 275968 байт
SHA1: 9288FB8E96D419586FC8C595DD95353D48E8A060,
MD5: A1D5895F85751DFE67D19CCCB51B051A.

Отримана інформація дозволила побудувати антивірусний програмний додаток на базі нейронної мережі типу АРТ-1, що надалі дозволить виявляти модифікації даного вірусу.

Одержано 24.10.2017

УДК 004.056.53

Захар Георгійович ДЕМИДОВ,
науковий співробітник науково-дослідної лабораторії захисту інформації та кібербезпеки Харківського національного університету внутрішніх справ

ОСНОВНІ ВИДИ КІБЕРАТАК НА WEB-САЙТИ

Основне правило при створенні web-ресурсу - ніколи не довіряти даним, введеним користувачем. Про це знають багато web-програмістів, але не всі до кінця дотримуються цього, з думкою: "Що там на цьому сайті ламати, та кому це потрібно". Але найчастіше на таких сайтах і вчаться зламувати адмінку й бази даних. Винятки становлять сайти, зроблені на основі якогось сучасного фреймворку (Наприклад: LARAVEL, SYMFONY, YII 2.0), бо там система безпеки вже протестована досвідченими фахівцями в цьому напрямку [1].

У інтернет-мережі зараз маса інформації щодо різних видів хакерських атак на web-сайти, але давайте їх ще раз узагальнимо, пояснимо та визначимо способи боротьби та запобігання.

SQL ін'єкція (англ. SQL injection) - один з найпоширеніших способів злому web-ресурсів, програм, які працюють з даними. Його мета - впровадити в запит сторонній, чужий SQL-код.

Впровадження SQL запитів, в залежності від виду використовуваної СУБД і умов, дає можливість хакерам виконати сторонній запит до бази даних (наприклад, видалити, прочитати, додати або змінити дані з будь-яких таблиць бази), отримати можливість працювати з локальними файлами і виконання своїх команд на сервері, що атакується.

Здебільшого, такий вид нападу можна бачити на прикладі сайтів, де використовуються параметри командного рядка (змінні URL), щоб побудувати SQL-запити до баз даних, без відповідної перевірки.

Для виключення таких випадків потрібно фільтрувати лапки та інші спецсимволи, вони можуть порушити логіку вашого запиту. Також, коли у вас є число, обов'язково явно приводити його до числового типу.

Деякі фахівці радять застосовувати для цього спеціальні конструктори SQL-запитів, які самі забезпечують необхідний поділ запиту і даних.

PHP ін'єкція – теж спосіб злому веб-сайтів, які написані на PHP. Основна думка - впровадження свого розробленого сценарію в код на серверній стороні ресурсу, що призводить до виконання сторонніх команд. Відомо - в багатьох розповсюджених движках та на форумах, які працюють на PHP (найчастіше це застарілі версії), є не зовсім продумані модулі та конструкції з уразливими місцями. Хакери шукають ці уразливості, аналізують їх, та користуються ними.

XSS (Cross Site Scripting, "міжсайтовий скриптинг") являє собою атаку, при якій зловмисник публікує на сайті, що атакується, скрипт, який виконується у користувачів при відкритті ними сторінок. Оскільки цей скрипт виконується в браузері у користувача, то він має доступ до інформації в його cookie, й може виробляти дії на сайті від імені користувача (якщо той "залогінився"), наприклад, писати, читати та видаляти повідомлення.

Розрізняють активні та пасивні XSS атаки. При першому типі нападу шкідливий скрипт зберігається на сервері та починає свою діяльність при завантаженні сторінки сайту в браузері клієнта. При другому виді атаки скрипт не зберігається на сервері, а шкідливий вплив починає виконуватися тільки в

разі будь-якого дії користувача, наприклад, при натисканні на сформоване посилання.

Основним способом протидії XSS-атак є фільтрація надходячих ззовні та публікуємих на сайті даних. Як правило, достатньо замінювати символи "<" та ">" на "& lt;" та "& gt;" відповідно (php-функція htmlspecialchars), при цьому введений відвідувачем текст втрачає HTML-оформлення, а скрипти, що містяться в ньому, втрачають шкідливість.

CSRF (англ. Cross Site Request Forgery - «міжсайтова підробка запиту», також відома як XSRF) - вид атак на відвідувачів веб-сайтів, який використовує недоліки протоколу HTTP. Коли користувач заходить на сайт, який створив зловмисник, від користувача таємно відправляється запит на інший сервер (наприклад, на сервер платіжної системи), який здійснює якусь шкідливу операцію (наприклад, переказ грошей на рахунок зловмисника). Для здійснення даної атаки жертва повинна бути автентифікована на тому сервері, на який відправляється запит, і цей запит не повинен вимагати будь-якого підтвердження з боку користувача, яке не може бути проігноровано або підроблено атакуючим скриптом.

На відміну від інших вразливостей CSRF виникає не в результаті помилок програмування, а є нормальною поведінкою Web-сервера і браузера. Тобто більшість сайтів, які використовують стандартну архітектуру, уразливі «за замовчуванням».

Спосіб боротьби - питати введення CAPTCHA при здійсненні критичних дій на зразок зміни пароля або переказу грошей (як зроблено в WebMoney).

DOS

Відокремлено в ряду загроз безпеки стоять вразливості DOS - Denial Of Service (відмова в обслуговуванні). Як правило, до цього класу нападів належать події, описувані в новинах "Хакери атакували сайт X, порушивши його роботу. Сайт не працював протягом Y годин". Тобто це саме "атака", а не "злом". На сервер виробляються запити, які він не може (не встигає) обробити, в результаті чого він не встигає обробити запити звичайних відвідувачів і виглядає для них як непрацюючий.

Ці атаки не мають на меті викрасти дані з бази, але можуть допомогти почати інші види атак, тобто звільнити шлях. Наприклад, деякі програми через помилки в своєму коді можуть викликати виняткові ситуації, і при відключенні сервісів здатні виконувати код, наданий зловмисником. Або атаки ла-

винного типу, коли сервер не може обробити величезну кількість вхідних пакетів.

При бажанні (бюджеті) можна «завалити» будь-який сервер. Обмежили кількість звернень з однієї IP-адреси? Отримайте DDOS (distributed - розподілений), коли звернення проводяться не з одного комп'ютера. DDoS використовується там, де звичайний DoS неефективний. Для цього кілька комп'ютерів об'єднуються, далі кожен створює DoS атаку на систему жертви.

Проти DOS атаки неможливо захиститися на 100%, але можна зробити обмеження на кількість спроб логіна з однієї IP-адреси в деяку кількість часу. Наприклад - не більше 5 в 10 хвилин. При вичерпанні показувати повідомлення "почекайте" або пропонувати ввести CAPTCHA. Деякі системи просять ввести CAPTCHA взагалі при кожній спробі логіна.

Список використаних джерел:

1. Лучшие PHP фреймворки в 2017 году. URL: blog.liveedu.tv/список-лучших-php-фреймворков/ (дата звернення: 21.10.2017).
2. Виды взломов сайтов и их предотвращение. URL: http://captcha.ru/articles/antihack/ (дата звернення: 10.10.2017).
3. Виды хакерских атак. URL: https://sites.google.com/site/hakerskieataki/home/vidy-hakerskih-atak (дата звернення: 10.10.2017).

Одержано 27.10.2017

УДК 343.9 : 004

Ян Андреевич ИЖБОЛДИН,
курсант факультета № 4 Харьковского национального университета внутренних дел

ОТДЕЛЬНЫЕ УЯЗВИМОСТИ В ЯДРЕ ОПЕРАЦИОННОЙ СИСТЕМЫ LINUX

Уязвимость Dirty COW (CVE-2016-5195) - серьезная программная уязвимость в ядре Linux, существующая с 2007 года и исправленная в октябре 2016 года. С её помощью локальный пользователь может повысить свои права и получить привилегии из-за ошибки состязания в реализации механизма копирования при записи для страниц памяти «dirty bit», помеченных флагом dirty.

Проблема возникает при многочисленном одновременном вызове системной функции «madvise» (MADV_DONTNEED) и

записи в страницу памяти, относительно которой пользователь не имеет права доступа и внесения изменений. Эти вызовы осуществляются из разных потоков одновременно. При попытке записи в read-only COW - страницу памяти, ядро автоматически создаёт её копию, после чего записывает данные в созданную копию. Исходная страница памяти при этом остаётся нетронутой. Код уязвимого ядра Linux не осуществляет проверку, завершен ли процесс создания копии и существует ли данная копия, прежде чем начать запись по запрашиваемому адресу памяти. Поскольку это две последующие операции, считалось, что несанкционированный доступ к ним – маловероятен.

Для реализации возможностей данной уязвимости используется эксплойт «Dirty COW», при активизации которого создаются два потока: поток A и поток B. Системный вызов madvise (MADV_DONTNEED) в потоке A сообщает ядру о том, что исполняемая программа больше не нуждается в использовании указанной страницы памяти, поэтому ядро сразу же удаляет все копии данной страницы, но оставляет доступ к ней, не внося изменений в путь к прежнему адресу.

Запись в эту же страницу из потока B приводит к необходимости создания новых копий указанной страницы памяти. При одновременном выполнении описанных выше операций, с очень малой вероятностью может произойти ситуация, когда копия страницы удаляется сразу же после её создания, но перед операцией записи. В случае возникновения неблагоприятной ситуации, ядро может сохранить данные в исходную read-only страницу памяти, а не в её копию. При многочисленном повторении запросов из разных потоков происходит перенагрузка на сервер и маловероятное событие обязательно произойдёт, в результате чего эксплойт получает право на изменение исходной read-only страницы. Обычно процесс занимает не более нескольких секунд. Необходимым условием для использования уязвимости является доступ на чтение к файлу или участку памяти.

Это означает, что локальный пользователь не может напрямую перезаписать системные файлы, которые не доступны для чтения, как например /etc/shadow, что позволило бы сменить пароль суперпользователя. Однако уязвимость позволяет записать произвольный код в любой исполняемый файл, в том числе любой suid-файл.

Таким образом, пользователь получает возможность вносить изменения в системные файлы, запускаемые им от имени суперпользователя (обладателя root прав). Например, становится возможным заменить suid-файл ping на системный терминал, который запустится от имени суперпользователя. Несмотря на то, что ошибка повышения привилегий реализуется исключительно среди локальных пользователей. Злоумышленники, не имеющие доступа к локальной сети, могут использовать уязвимость в сочетании с другими эксплойтами, которые предоставляют возможность удаленного управления и выполнение непривилегированного кода.

Использование такого сочетания инструментов не оставляет цифровых следов в системных журналах и приводит к полному взлому удаленной системы.

Список використаних джерел:

1. Linux Kernel 2.6.22 < 3.9 (x86/x64) - 'Dirty COW /proc/self/mem' Race Condition Privilege Escalation (SUID Method). URL: https://www.exploit-db.com/exploits/40616/ (дата звернення: 23.10.2017).

Одержано 30.10.2017

УДК 004.492.2

Ігор Володимирович КОБЗЕВ,
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій і систем управління Харківського регіонального інституту державного управління Національної академії державного управління при Президентові України

Вікторія Анатоліївна ЛУК'ЯНОВА,
кандидат педагогічних наук, завідувач кафедри природознавчих наук Харківського національного університету радіоелектроніки

МЕТОДИ ЗАХИСТУ САЙТУ НА CMS WORDPRESS

Сфера інформаційної безпеки – актуальне питання сучасності. Захист сайтів від «хакерів» стає глобальною проблемою, над вирішенням якої працюють фахівці всього світу. Бізнес, побудований в агресивному середовищі Інтернет, уразливий і схильний до нападів з боку конкурентів і недоброзичливців. Єдиного інструменту для усунення усіх загроз несанкціонованого доступу до сайтів просто не існує [1].

WordPress є популярною безкоштовною системою управління контентом для сайтів. Відкрита форма WordPress використовується вже на 28,7 % світових сайтів. При цьому на ринку систем управління контентом (CMS) WordPress є

безперечним лідером за даними W3Techs web technologies з рейтингом 59,5 % [2]. На даний момент актуальною версією CMS WordPress є версія 4.8.2. Зокрема на WordPress працюють сайти освітніх установ та навчальних закладів, таких як Харківській національний університет радіоелектроніки (http://nure.ua/), Харківській політехнічний інститут (http://www.kpi.kharkov.ua/), Державний університет телекомунікацій (http://www.dut.edu.ua/), Академія Державної пенітенціарної служби (http://academy.kvs.gov.ua/), Міжнародний університет фінансів (http://iuf.edu.ua/) тощо.

Системи управління контентом (CMS), як і багато інших видів програмного забезпечення, досить уразливі. При цьому, чим поширенішою є система і чим частіше вона застосовується на популярних сайтах, тим більше грошей і зусиль зловмисники інвестують в пошук її проблемних місць. Крім того, більшість сучасних CMS складаються з безлічі модулів, і більшість уразливих місць пов'язані з плагінами, які зазвичай написані та протестовані на безпеку гірше, ніж основний код системи.

Основним недоліком WordPress, як і будь-якої іншої відкритої безкоштовної платформи для блогів, є її доступність для зловмисників.

Розглянемо декілька простих засобів захисту сайтів, які побудовано на CMS WordPress. Необхідно видалити користувача з логіном Admin. Зловмисникам набагато легше отримати доступ до вашого сайту за допомогою брут-форс атаки, особливо, якщо логін вже відомий. Найлегше зламати сайти, якщо використовується стандартний логін «admin» для адміністрування сайту.

Приховуємо версію Wordpress. Система автоматично вставляє номер поточної версії CMS в код кожної сторінки. Необхідно прибрати додавання в початковий код версії CMS WordPress. У файлі functions.php необхідно додати наступний код remove_action ('wp_head', 'wp_generator'). Також бажано видалити файл readme.html в кореневій теці сайту або можна використати плагін Remove WP version and shortlink.

Використовуємо файл .htaccess для захисту файлу wp-config (файл конфігурації сайту). .htaccess – це головний конфігураційний файл веб-сервера.

wp-config.php містить абсолютно усі дані, які потрібні для підключення до сервера MySQL, а також до бази даних. Необхідно знайти або створити файл .htaccess в корені сайту, та додати наступні рядки:

order allow, deny
deny from all

Необхідно обмежити кількість спроб доступу. Найчастіше зловмисники роблять величезну кількість спроб входу на сайт, підбираючи пароль. Можна налаштувати систему так, щоб IP-адреса була заблокована на декілька годин після певної кількості невдалих спроб входу. Для цього можна використати додаткові плагіни, наприклад, Login LockDown або Limit Login Attempts. У налаштуваннях цих плагінів, можна самостійно встановити кількість спроб входу і час блокування.

Додатково існує можливість прибрати відображення повідомлення про те, що введений логін і пароль невірні, адже це інформація також може допомогти зловмисникові.

Декілька складнішими є наступні засоби захисту:

– зміна префіксу таблиць баз даних за допомогою SQL-запиту PhpMyAdmin;

– використання SSL-сертифікату. Для передачі захищеної інформації і конфіденційності обміну даними рекомендується використовувати SSL-протокол. Необхідно придбати SSL-сертифікат і встановити його для доменного імені;

– використання двохфакторної автентифікації облікових записів. Після того, як ви вводите пароль на сайті, вам надсилається запит на новий одноразовий пароль, який ви отримуєте на контактний номер телефону або електронну пошту. Найпопулярніші плагіни двохфакторної верифікації WordPress – це Google Authenticator і Clef Two – Factor Authentication.

Отже можна зробити висновок, що забезпечення захисту сайту – це комплексне завдання, яке потребую чимало зусиль, і в умовах сьогодення є важливим та актуальним.

Список використаних джерел:

1. Кобзев И. В., Петров К. Е., Калякин С. В. Обеспечение безопасности сайта, построенного на системе управления контентом WordPress. *Системи обробки інформації.* 2012. Вип. 4(2). С. 37-41.
2. Usage Statistics and Market Share of Content Management Systems for Websites, October 2017. *W3Techs web technologies surveys.* URL: https://w3techs.com/technologies/overview/content_management/all (дата звернення: 10.10.2017).

Одержано 17.10.2017

УДК 65.012.8 + 004

Тетяна Петрівна КОЛІСНИК,
кандидат педагогічних наук, доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

Володимир Володимирович ТУЛУПОВ,
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

ОСОБЛИВІ ПИТАННЯ ЗБОРУ ТА ОБРОБКИ ІНФОРМАЦІЇ

На теперішній час мало хто із користувачів знає, що тільки 15-20 % Інтернету доступні. Інша частина таємна і називається глибинним Інтернетом.

Тому якщо розглянути видиму частину, то можна зробити простий висновок, що кожна підключена до Інтернет система ненавмисно просочує внутрішню інформацію про свою організацію, яка може бути використана для розробки цільової атаки. Залежно від джерела цього витоку, інформація може відноситися до компонентів, які використовуються у фізичній інфраструктурі, активів організації, процесів управління тощо.

Велика частина цієї інформації у більшості випадків, відноситься до топології мережі організації та видів сервісів у ній. Це дозволяє зловмисникові намітити цілі для подальших атак.

Збір інформації, що стосується конкретних осіб може бути активно використаний в атаках соціальної інженерії – можливо, через оману, підкуп або шантаж. Також важливим аспектом цього витоку інформації є її відкритий доступ через Інтернет, і, ймовірно, те, що вона може міститись у системах, не пов'язаних з організацією. Тому, доступ до інформації стає незалежним від ресурсів організації і, отже, до неї може «анонімно» звернутися будь-хто.

Як правило процеси виявлення цього витоку інформації дуже прості і існує безліч легко доступних інструментів та сервісів, які дозволяють зробити їх ще простішими. Але, багато з інструментів або вже вбудовані в найпопулярніші операційні системи, або знаходяться у вільному доступі на різних Інтернет ресурсах.

Методи, що використовуються для виявлення витоку інформації, як правило, називають «пасивним або активним збором інформації» – і вони грають життєво важливу роль (яка часто упускається з виду) в будь-якому тесті на проникнення (пентест) або оцінці безпеки інформаційних ресурсів.

Фахівці стверджують, що пасивна розвідка може включати переглядання цільових веб-сайтів, щоб переглянути та завантажити публічно доступний контент, в той час як інші стверджують, що пасивна розвідка не припускає відправку будь-яких пакетів взагалі на цільовий сайт.

Багато важливої інформації може бути зібрано пасивно, а потім використано в прямій атаці або для зміцнення інших від нападів. Залежно від джерела, легко може бути отримана така інформація, як - поточний рівень встановлених оновлень та патчів, топологія внутрішньої мережі або дані щодо облікових записів.

Виходячи з вищевказаного основні процеси пошуку та обробки інформації передбачають використання таких Інтернет-ресурсів та джерел як:

1. Бази даних Інтернет – інформація щодо IP-адрес.
2. Доменна система імен – інформація щодо вузлів.
3. Пошукові системи – інформація, що стосуються організації або її співробітників.
4. Системи електронної пошти – інформація, що міститься в кожному процесі доставки пошти.
5. Угоди про присвоєння імен – спосіб, у який організація кодує або класифікує сервісі, які працюють на її вузлах.
6. Аналіз сайту – публічно доступна інформація, що може становити ризик для безпеки.

Слід важливо зрозуміти де отримують цю інформацію і рівень деталізації інформації, бо тоді організація зможе припинити цей витік інформації просто і швидко.

Якщо розглядати основний сегмент збору інформації, то слід виділити більш увагу питанням отримання інформації про організацію, її мережу, вузли та сервіси з відкритих джерел використовуючи такі, а іноді вони стають нажаль основними, можливими методами як:

- оголошення про пошук роботи, каталоги пропозицій, прохідні сторінки та інші підказки, інший вміст сайту;
- пошук документів та визначення цікавого контенту;
- веб-портали, веб-пошта та адміністративні консолі;
- тестові сторінки, лог-файли та сторінки статусу сервера;

- резервні копії, застарілі файли, і на код стороні сервера;
- файли конфігурації та дамп бази даних файлів;
- спеціалізовані форуми;
- файли користувачів і паролів;
- клієнтський код;
- виявлення вразливостей;
- дослідження програмного забезпечення відомих вразливостей на основі виявлених технологій;
- перевірка URL та пасивне сканування через перехоплюючий проксі;
- інші документи, що представляють інтерес.

Одержано 30.10.2017

УДК 004.89

Олексій Феліксович ЛАНОВИЙ,
кандидат технічних наук, доцент, доцент кафедри програмної інженерії Харківського національного університету радіоелектроніки

ВИКОРИСТАННЯ МЕТОДІВ ІНТЕЛЕКТУАЛЬНОЇ ОБРОБКИ ІНФОРМАЦІЇ В МЕРЕЖІ DARKNET ДЛЯ ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ

Серед основних тенденцій розвитку інформатизації суспільства, що стосується практично всіх сфер життєдіяльності слід відзначити стрімкий розвиток інформаційної мережі Інтернет. Розвиток інформаційних технологій сприяв виникненню нового виду злочинності – комп'ютерної, а перехід на цифрові технології, методи електронного управління технологічними процесами, конвергенція і глобалізація комп'ютерних мереж стали передумовою появи кіберзлочинності. Фахівці зазначають, що загроза поширення кіберзлочинності та кібертероризму за рівнем негативного впливу може бути порівняна з реальними бойовими діями. Водночас, розвиток інтернету призводить до виникнення низки проблем: соціальних, організаційних, юридичних тощо, але найгострішою є активне використання мережі злочинним світом. Міжнародним суспільством кіберзлочинність визнано загрозою не тільки національній безпеці окремих держав, а й людству та міжнародному порядку в цілому [1].

Тіньовий або глибинний Інтернет («Deep Web») – величезна частина Інтернету, яка знаходиться за межами стандартних методів пошуку. Значна частина тіньового Інтернету – це сай-

ти, які недоступні для пошуку за допомогою звичайних пошукових систем або захищені паролем. Частина глибинного Інтернету, відома також під назвою Даркнет («DarkNet»), доступна тільки за допомогою спеціальних програм, що відкривають доступ до напівлегальних і нелегальних товарів або послуг. Інтернет, і особливо Dark Web, зробили торгівлю людьми більш легкою для розповсюдження та приховування. Інтернет-реклама використовується, щоб заманити потенційних жертв торгівлі людьми, на закритих форумах обговорюють різні аспекти торгівлі людьми та послуги, що приховані в Dark Web [2]. Для більш ефективної боротьби з торгівлею людьми Агентство передових оборонних дослідницьких проектів (також відоме як DARPA), що входить до складу Міністерства оборони США, у 2014 році запустило програму Memex [3].

Законодавство України не забороняє використання програмного забезпечення і технічних засобів забезпечення зв'язку, що надають повну анонімність користувача для доступу в Даркнет, а також технічно не вирішено питання можливого блокування функціонування подібного роду програмних продуктів і технічних рішень. Тому суттєвими стають питання, пов’язані з можливістю одночасної ідентифікації осіб в мережах Інтернет та Даркнет.

В основу сучасної технології Data Mining (discovery-driven data mining) покладено концепцію шаблонів (патернів), що відображають фрагменти багатоаспектних взаємовідносин у даних. Ці шаблони містять закономірності, що властиві вибірках даних, які можуть бути виражені у зрозумілій формі. Пошук шаблонів в інформаційному просторі Даркнет у цьому випадку проводиться методами, що не обмежені рамками апріорних припущень про структуру вибірки.

Інформація, що знайдена в процесі використання методів Data Mining під час дослідження Даркнет, повинна описувати нові зв'язки між властивостями, передбачати значення одних ознак на основі інших тощо. Завдання, які вирішуються методами Data Mining, включають:

- класифікацію та віднесення об'єктів (спостережень, подій) до одного із заздалегідь визначених класів;
- прогнозування та встановлення залежності вихідних змінних від вхідних;
- кластеризацію – угруповання об'єктів (спостережень, подій) на основі даних або властивостей, що описують сутність цих об'єктів;

- асоціацію – виявлення асоціативних закономірностей;
- послідовні шаблони – встановлення закономірностей між пов'язаними в часі подіями, тобто виявлення залежності, згідно до якої якщо відбудеться подія X, то через заданий час відбудеться подія Y.

У зв'язку з неможливістю проведення контекстного пошуку та застосування методів Data Mining одночасно в мережах Інтернет та Даркнет, результати обробки інформації повинні зберігатися в окремих базах даних, які і будуть опрацьовуватись. З цією метою інформаційна система повинна:

- в режимі реального часу здійснювати збір та збереження інформації з тіньових форумів;
- визначати псевдоніми («ніки») зловмисників.

На підставі отриманих даних інформаційна система повинна надавати можливість проведення пошуку за патернами збережених об'єктів серед форумів мережі Даркнет та в соціальних мережах Інтернет з метою знаходження можливих збігів.

Список використаних джерел:

1. Lacey D., Salmon P. M. It's dark in there: Using systems analysis to investigate trust and engagement in dark web forums. *Engineering Psychology and Cognitive Ergonomics.* Vol. 9174 of Lecture Notes in Computer Science. 2015 PP. 117–128. URL: https://link.springer.com/chapter/10.1007/978-3-319-20373-7_12 (дата звернення: 22.10.2017).
2. Rathod Digvijaysinh. Darknet Forensics. *International Journal of Emerging Trends&Technology in Computer Science.* 2017. Vol. 6. Issue 4. PP. 77–79. URL: http://www.ijettcs.org/Volume6Issue4/ IJETTCS-2017-07-24-29.pdf (дата звернення: 22.10.2017).
3. Pellerin Cheryl DARPA Program Helps to Fight Human Trafficking URL: https://www.defense.gov/News/Article/Article/1041509/darpa-program-helps-to-fight-human-trafficking/ (дата звернення: 22.10.2017).

Одержано 27.10.2017

УДК 004.728 : 519.87

Александр Александрович МОЖАЕВ,
доктор технических наук, профессор, профессор кафедры информационных технологий факультета № 4 Харьковского национального университета внутренних дел

Хазим Рахим НАЕМ,
аспирант кафедры мультимедийных информационных технологий и систем Национального технического университета «Харьковский политехнический институт»

ОСОБЕННОСТИ ТРАФИКА ПЕРЕДАЧИ ИНФОРМАЦИИ ГИБРИДНОЙ КОМПЬЮТЕРНОЙ СЕТИ КРИМИНОГЕННОГО МОНИТОРИНГА УКРАИНЫ

Современный уровень развития систем мониторинга чрезвычайных ситуаций, экологической обстановки в Украине, а также достаточно сложная криминогенная и политическая ситуация в стране требуют создания и дальнейшего развития системы криминогенного мониторинга Украины. Эта система должна включать в себя подсистему сбора первичной информации в Украине (соответствующие стационарные и мобильные посты, узлы и центры), подсистему передачи информации как в рамках подсистемы сбора информации, так и в основной системе криминогенного мониторинга, а также оперативно-аналитический центр, в который поступает наиболее важная первичная информация из локальных и региональных центров сбора и обработки информации. Рекомендации оперативно-аналитического центра позволят силовым органам Украины применить соответствующие средства и методы для преодоления соответствующих выявленных эксцессов, что в итоге позволит снизить уровень криминогенной обстановки.

Одной из основных проблем, связанных с качеством функционирования системы мониторинга, является неоднородный характер сети передачи информации системы, что может существенно снизить реальную эффективность системы мониторинга по сравнению с показателями, которые закладывались ее проектировщиками. Используемая сеть передачи данных является гибридной, т.е. включает в себя элементы: проводной инфраструктуры, которая достаточно развита в крупных городах, экономически развитых районах; беспроводной инфраструктуры, разнообразных методов и

принципов доступа к сети, а также элементов инфраструктуры спутниковой связи, необходимость использования которой возникает в труднодоступных удаленных территориях. Все эти составные элементы сети присутствуют и в сетях передачи информации криминогенного мониторинга Украины.

Но известно, что трафик в сети, характеризующийся высокой степенью гетерогенности, обладает свойством самоподобия, т.е. масштабной инвариантности [1, с. 57]. Моделирования трафика такой сети достаточно сложный процесс и классические модели, использующие Марковские процессы не позволяют создать модель, адекватную исследуемому процессу.

В докладе предлагается рассмотреть модель трафика гибридной сети как совокупность трафиков независимых источников, которые передают информацию заданным узлам через операционный центр (NOC). Для работы необходимо оценить количество источников, которые могут передавать данные, не перегружая NOC. Источники независимы и работают по принципу ON/OFF. В определенный момент времени источник должен быть занятым или свободным. Последовательность событий (занятый, свободный) представляет операционный цикл. Под операционным циклом будем понимать случайную величину:

$$\Theta^{(i)} = \left\{\Theta_k^{(i)} \middle| k \in Z\right\},\ i \in \{1, \dots, M\};\ \ \Theta^i = B_k^{(i)} + I_k^{(i)}, \qquad (1)$$

где $B_k^{(i)}$ и $I_k^{(i)}$ - случайные величины, характеризующие занятый и свободный периоды k-го интервала i- го источника передачи информации.

Для простоты будем считать, что интенсивность генерирования пакетов источником i в момент времени k одинакова. Совокупный процесс является результатом сложения трафика отдельных источников:

$$\left(\alpha(M); B(M)\right) = \left\{\left(\alpha_k(M), B_k(M)\right) \middle| k \in Z\right\}. \qquad (2)$$

Для каждого приема осуществляется определенное обслуживание, обозначенное случайной переменной γ_k , которая не зависит от процесса. $X = \{X_{k_i} | k_i \in Z\}$- совокупность состояний, которая отображает количество источников за время t_i. Процесс приема - это совокупный процесс λ, интенсивность приема - ξ_{k_i}.

Процесс обслуживания имеет распределение с "тяжелым хвостом". В этом случае рассматривается распределение Парето с параметрами, которые оцениваются по экспериментальным данным. Полученная марковская цепь является стационарной, если $p = \lambda\mu_B < 1$.

Таким образом, в докладе предложена модель трафика гибридной компьютерной сети передачи информации системы криминогенного мониторинга Украины, которая учитывает гетерогенный характер сети, особенности слияния трафика от нескольких независимых источников и интегральный трафик обладает распределением с «тяжелым» хвостом, таким как, распределение Паретто.

Список використаних джерел:

1. Можаєв О. О. Передача інформації у гетерогенних комп'ютерних мережах: монографія. Х. : НТУ «ХПІ», 2012. 220 с.

Одержано 17.10.2017

УДК 004.056.53

Юрій Миколайович ОНИЩЕНКО,
кандидат наук з державного управління, доцент кафедри кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Катерина Костянтинівна ПЕТРОВА,
студентка групи факультету комп'ютерних наук Харківського національного університету радіоелектроніки

ДВОФАКТОРНА АВТЕНТИФІКАЦІЯ, ЯК ЗАСІБ ЗАХИСТУ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ

Двофакторна автентифікація – це метод ідентифікації користувача в якому-небудь сервісі за допомогою запиту автентифікаційних даних двох різних типів, що забезпечує двошаровий, тобто більш ефективний захист акаунта від несанкціонованого доступу.

Двофакторна автентифікація вже сьогодні застосовується у сфері фінансів при створенні сервісів Internet-банкінгу, мобільного банкінгу і тому подібних рішень для кінцевих користувачів. Вона заснована на спільному використанні декількох чинників автентифікації, що значно підвищує безпеку використання інформації, щонайменше, з боку користувачів, що

підключаються до інформаційних систем по захищених і незахищених каналах комунікацій.

Розглянемо сильні й слабкі сторони двофакторної автентифікації. До переваг можна віднести її здатність захистити інформацію від зовнішніх і внутрішніх загроз, наявних при використанні парольної або однофакторної автентифікації. Додавання другого чинника значно мінімізує вірогідність злому: шанси виникнення ситуації, при якій зловмисник окрім логіна і пароля також оволодів іншим чинником, досить малі, і такий спосіб авторизації є досить надійним. При цьому для забезпечення такого захисту необхідно використовувати додаткові програмно-апаратні комплекси, облаштування зчитування даних, їх зберігання, що вимагає певних витрат на їх придбання, впровадження і обслуговування. Безумовно, для того, щоб автентифікація була насправді надійною, важлива не кількість типів ознак, а й якість реалізації механізму на обох сторонах взаємодії як в частині, що знаходиться у користувача, так і в частині, що знаходиться у перевіряючої сторони. Тому, особливу увагу треба приділити способу зберігання ідентифікаційних даних.

Сьогодні використовуються декілька способів реалізації двофакторної автентифікації. Кожен з них передбачає наявність чинника знання, тобто паролів, які користувачі зберігають у своїй пам'яті, і одного з наступних чинників:

– речовий чинник. В першу чергу, під цим розуміються апаратно-програмні системи ідентифікації і автентифікації. До них належать: токени (електронний (USB) ключ, автономний генератор OTP – One Time Password Token Generator); смарт-карти; телефони/смартфони (відправка SMS з OTP, генератори OTP);

– біометричний чинник (включає біометричні дані, для зняття яких, як правило, потрібні спеціальні програмно-апаратні засоби – так звані, біометричні сканери, які розрізняються за характером даних, що зчитуються. До них належать: відбитки пальців; геометрія рук; райдужна оболонка ока; розпізнавання голосу тощо).

Перш ніж приступити до порівняння систем двофакторної автентифікації, необхідно сформувати вимоги безпеки, яким вони повинні відповідати: безпечно зберігати ідентифікаційну інформацію; забезпечити гарантований захист від крадіжки ідентифікаційних даних через Internet; використовувати одноразові паролі при роботі в не довіреному середовищі; вико-

ристовувати криптографічну стійку автентифікацію при доступі до робочих станцій, веб-порталів, електронної пошти.

Перш ніж зробити вибір методу автентифікації, необхідно зрозуміти принципові відмінності технологій і їх реалізацій в плані адекватності вирішуваної задачі. Так, автономні генератори OTP, генератори OTP в смартфонах найчастіше використовуються для віддаленого доступу до сервісів, додатків, VPN і Web-порталів. Смарт-карти і USB-токени добре себе зарекомендували в шифруванні та підписі пошти, документообігу, корпоративних single-sing-on (технологія єдиного входу) або VPN-доступі. Передача OTP по мобільному зв'язку частіше використовується для віддаленого доступу на платіжні портали і банківські акаунти.

Для того, щоб остаточно визначитися з вибором, необхідно ввести якісні критерії оцінки, що відбивають вимоги безпеки, вимоги до вартості і простоти використання. Загальна вартість складається з вартості придбання і впровадження, а також подальшої підтримки інфраструктури. Вимоги безпеки складаються з вимог до суворості автентифікації, можливості інтеграції з існуючими застосуваннями, надійності засобу в перспективі найближчих років. Безпосередні користувачі системи зацікавлені в простоті використовуваного засобу.

Мають перевагу два методи: USB-ключі і OTP-генератори на смартфоні. Тепер необхідно зробити вибір між ними. Важливо відмітити основні переваги двофакторної автентифікації з використанням OTP. До них належать: застосування одноразових паролів замість статичних; відсутність необхідності встановлювати яке-небудь додаткове програмне забезпечення на клієнтській частині комп'ютерної системи, оскільки користувач вводить пароль вручну, використовуючи ті ж програмні інтерфейси, що і при застосуванні статичних паролів; низька вартість; застосування генераторів OTP можливе в тих випадках, коли користувач не має можливості використовувати USB-порт або він просто відсутній.

Зважаючи на те, що кількість користувачів об'єкту захисту сягає тисяч, недоцільно використовувати USB-ключ з точки зору витрат і умов використання. Таким чином, виходячи з характеристик об'єкту захисту, основних критеріїв вибору, переваг кожного з методів, доцільно зробити вибір на користь OTP-генератора як додатка для смартфону.

Одержано 17.10.2017

УДК 651. 34

Сергій Геннадійович СЕМЕНОВ,
доктор технічних наук, старший науковий співробітник, завідувач кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

Кассем ХАЛИФЕ,
аспірант кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

Віталіна Миколаївна ЗМІЇВСЬКА,
завідувач навчальної лабораторії кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

СПОСІБ ОЦІНКИ ВРАЗЛИВОСТІ СИСТЕМНОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Спосіб оцінки вразливості системного програмного забезпечення (ПЗ) включає в себе наступні кроки.

Крок 1. Аналіз ймовірних загроз системного ПЗ. Змістовна постановка задачі дослідження.

Крок 2. Розробка операційної схеми для дослідження динамічної системи «ПЗ - ЗЛОВМИСНИК».

Блок 3. Складання рівнянь для численностей станів в диференціальної формі відповідно до методу динаміки середніх.

Крок 4. Завдання вихідних даних, початкових і додаткових умов для вирішення завдання.

Крок 5. Чисельне рішення задачі, фіксація і апроксимація результатів моделювання.

Крок 6. Обчислення показників ефективності методу розробки системного ПЗ.

Кількісно оцінити вразливість можна за допомогою показника втрат ΔZ_i по кожному засобу z_i. Цей показник визначає величину відносного збитку, нанесеного засобу z_i в результаті злочинних атак на ПЗ. При цьому, відповідно до робот [1, с. 50; 3, с. 82], показник відносної шкоди може бути обчислений за формулою:

$$\Delta Z_i\left(t^*\right) = \frac{z_i(t_0) - z_i\left(t^*\right)}{z_i(t_0)} \cdot 100\%, \quad i = 1\ldots n, \qquad (1)$$

де t* – поточний момент часу (момент виходу з циклу моделювання процесу); $\Delta Z_i(t^*)$ – відносний збиток для засобу z_i на момент часу t*; $z_i(t_0)$ – вихідний потенціал засобу z_i в момент часу t_0; n – число фазових координат (розмірність вектора z) динамічної системи «ПЗ - Зловмисник».

Крок 7. Аналіз та узагальнення результатів моделювання і підготовка рекомендацій щодо вибору структури методології розробки системного ПЗ [2, с. 20] і стратегії її використання в фірмах.

Обчислювальний експеримент з розробленою в середовищі MathCad програмою дозволяє для заданих умов реалізувати імітаційну модель процесу взаємодії системного ПЗ, як об'єкту нападу, і зловмисника і оцінити вразливості ПЗ.

Значення ймовірностей виведення з ладу однієї одиниці ПЗ або коштів зловмисники приймемо відповідно до даних табл. 1.

Табл. 1. Значення ймовірностей виведення з ладу однієї одиниці ПЗ і засобів зловмисників

ПЗ				**Зловмисник**		
p_{14}	p_{16}	p_{26}	p_{36}	p_{43}	p_{53}	p_{63}
0,1	0,08	0,09	0,03	0,08	0,125	0,06

Моделювання (чисельне рішення) диференціальних рівнянь (4.2) виконано в циклі на інтервалі часу від 0 до 180 год., з кроком 0,1 год.

Обмеженнями моделювання, при якому неможливо продовження заданої програми є випадки коли: $z_1 \le 1$; $z_2 \le 1$; $z_3 \le 10\%$; $z_4 \le 1$; $z_5 \le 10\%$; $z_6 \le 1$.

Обчислимо відносний збиток $\Delta Z_i(t^*)$ для всіх z_i де i = 1,...,6.

Результати обчислень представлені в табл. 2.

Табл. 2. Відносний збиток $\Delta Z_i(t^*)$ для всіх z_i для t^* = 120 год.

ПЗ			**Зловмисник**		
$\Delta Z_1(t^*)$	$\Delta Z_2(t^*)$	$\Delta Z_3(t^*)$	$\Delta Z_4(t^*)$	$\Delta Z_5(t^*)$	$\Delta Z_6(t^*)$
29,57	18,31	11,99	64,57	50,45	40,36

Таким чином, удосконалено спосіб оцінки вразливості системного ПО. Його відмінною рисою є облік можливості масштабування процесу розробки програмного забезпечення шляхом впровадження фахівців безпеки (PersonNon, SecDev).

Список використаних джерел:

1. Надеждин Е. Н. Оценка эффективности механизма защиты сетевых ресурсов на основе игровой модели информационного противоборства. *Научный вестник: ООО "Консалтинговая компания Юком"*. 2015. №2(4). С. 49-58.
2. Семенов С. Г., Халифе Кассем, Захарченко М. М. Усовершенствованный способ масштабирования гибкой методологии разработки программного обеспечения. *Сучасні інформаційні системи*. 2017. № 1. С. 19-24.
3. Семенов С. Г., Лисица Д. А. Модель оценки риска разработки программного обеспечения // Матеріали XV Міжнародної НТК «Проблеми інформатики і моделювання». Х: НТУ «ХПІ», 2015. С. 82.

Одержано 24.10.2017

УДК 651. 34

Сергій Геннадійович СЕМЕНОВ,
доктор технічних наук, старший науковий співробітник, завідувач кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

Тетяна Миколаївна ШИПОВА,
аспірант кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

АНАЛІЗ ВИМОГ ЯКОСТІ ПЕРЕДАЧІ ТА ОБРОБКИ ДАНИХ В КОМП'ЮТЕРНИХ СИСТЕМАХ В УМОВАХ ЗОВНІШНІХ ВПЛИВІВ

Розвиток комп'ютерних систем та мереж вимагає розробки якомога точних та детальних способів математичного моделювання, а також відповідного розвитку теоретичних основ дослідження процесів функціонування та проектування комп'ютерних мереж, включаючи забезпечення [1 стр.19, 2 стр.29, 3 стр.76]:

- якості обслуговування при передачі різнорідного трафіку з вимогами, що відрізняються, до робочих характеристик ме-

режі (у тому числі з самоподібною структурою та в умовах обмежених мережних ресурсів);

- надійності функціонування (життєздатності);
- безпеки від шкідливих впливів будь-якого походження.

Процес технічного проектування мереж є найбільш важкою науково-технічною задачею, що ґрунтується на використанні результатів теорії систем, графів, ефективності, черг, математичного програмування та передбачає рішення комплексу взаємопов'язаних задач.

Відповідно до теорії систем, мережі володіють сукупністю властивостей, кожна з яких може бути кількісно описана за допомогою деякої змінної (показника якості), яка характеризує її якість відносно обраної властивості. Показник якості можна записати у вигляді функціонала: $\Phi = \Phi(W, U)$, де U – умови функціонування, що визначаються зовнішнім середовищем.

Для кількісної характеристики властивостей якості мережі вводяться відповідні показники. При цьому глобальна система показників якості Y_Φ включає векторні показники якості, що характеризують оцінку найбільш істотних властивостей процесу інформаційного обміну $Y_{ИО}$ і управління $Y_У$, а також системи інформаційного обміну $Y_{СИО}$ і системи управління $Y_{СУ}$:

$$Y_\Phi = \left[Y_{ІО}, Y_У, Y_{СІО}, Y_{СУ}\right]^T = \left[t_{ДС}, P\left(t_{ДС} \le t_{ДС\,ТР}\right), P_Д, P_б, C\right]^T,$$

де $t_{ДС}$, $P\left(t_{ДС} \le t_{ДС\,ТР}\right)$ – середній час та ймовірність своєчасної доставки повідомлень; $P_Д, P_б$ – показники, що характеризують достовірність передачі повідомлень та виконання вимог інформаційної безпеки; С – вектор затрат ресурсів на доставку повідомлень. При цьому складові системи показників якості мають наступний вигляд:

а) система показників якості процесів інформаційного обміну:

$$Y_{ИО} = \left[t_{ДС}(r), P\left(t_{ДС}(r) \le t_{ДС\,ТР}(r)\right), P_{Д_{ІО}}(r), P_{б_{ІО}}(r), C_{ІО}(r)\right]^T$$

де $r = \overline{1, R}$ – пріоритет повідомлень (даних), визначених за класами якості послуг і категоріям користувачів, в тому числі і для повідомлень підсистем сигналізації, управління, інформа-

ційної безпеки; $t_{ДС}(r), P\left(t_{ДС}(r) \le t_{ДС\,ТР}(r)\right)$ – середній час і ймовірність своєчасної доставки повідомлень (даних) різних пріоритетів $r = \overline{1,R}$ в нормальних умовах функціонування; $P_{Д_{ІО}}(r), P_{б_{ІО}}(r)$ – показники, що характеризують достовірність інформаційного обміну і виконання вимог інформаційної безпеки при забезпеченні інформаційного обміну (за видами послуг і підсистем); $C_{ІО}(r)$ – вектор витрат ресурсів на забезпечення інформаційного обміну;

б) система показників якості процесів управління:

$$Y_У = \left[T_{ЦУ}, P\left(t_{ДС_У} \le t_{ДС_У\ ТР}\right), P_{Д_{ИО}}(r), P_{б_У}, C_У\right]^T$$

де $T_{ЦУ}$ – середній час доставки повідомлень (даних) управління, який визначає середню тривалість циклу управління параметрами мережі зв'язку (здійснюється при порушенні нормального режиму її функціонування і визначає оперативність, безперервність і стійкість управління); $P\left(t_{ДС_У} \le t_{ДС_У\ ТР}\right)$ – ймовірність своєчасної доставки повідомлень керування; $P_{б_У}$ – показник, що характеризує виконання вимог інформаційної безпеки при забезпеченні управління; $C_У$ – вектор затрат ресурсів на забезпечення управління;

в) система показників якості систем інформаційного обміну та управління:

$$Y_{СІО} = \left[V, H_{СІО}, C_{СІО}\right]^T;\ Y_{СУ} = \left[V_{СУ}, H_{СУ}, C_{СУ}\right]^T,$$

де $V, V_{СУ}$ – вектор пропускної продуктивності елементів систем інформаційного обміну та управління; $H_{СІО}, H_{СУ}$ – вектор показників стійкості (надійності, живучості, завадостійкості/ перешкодозахищеності)) елементів системи інформаційного обміну і системи управління; $C_{СІО}, C_{СУ}$ – вектор витрат ресурсів на побудову та експлуатацію систем інформаційного обміну та управління.

Таким чином розроблено узагальнену систему показників якості передачі та обробки даних в комп'ютерних системах в умовах зовнішніх впливів. Це дозволяє провести синтез систем

захисту даних з врахуванням сучасних вимог, щодо балансу існуючих показників.

Список використаних джерел:

1. Семенов С. Г., Подорожняк А. А., Баленко А. И. Анализ и синтез защищенных компьютерных систем и сетей. Х : НТУ«ХПІ», 2012. 204 с.
2. Семенов С. Г., Ільїна І. В., Загайнов С. О. Аналіз вимог до якості зв'язку у комп'ютерних мережах систем критичного застосування // Інформаційні технології в навігації і управлінні: стан та перспективи розвитку: мат. наук.-техн. конф. К. : ДП «ЦНДІ НіУ», 2010. С. 29.
3. Семенов С. Г., Босько В. В., Березюк І. А. Выбор критерия параметрической идентификации информационной системы // Інформаційні технології: наука, техніка, технологія, освіта, здоров'я: мат. наук.-техн. конф. Х: НТУ «ХПІ». 2011. С. 76.

Одержано 24.10.2017

УДК 651. 34

Анна Сергіївна СЕМЕНОВА,
студентка Національного технічного університету «Харківський політехнічний інститут»

Максим Володимирович БАРТОШ,
студент Національного технічного університету «Харківський політехнічний інститут»

АНАЛІЗ ПОКАЗНИКІВ ЦЕНТРАЛІЗАЦІЇ ЗВ'ЯЗКІВ ДЛЯ ОЦІНКИ БЕЗПЕКИ МЕРЕЖІ INTERNET OF THINGS

Проведений аналіз [1, с. 161; 2, с. 1120; 3] показав, що одним з недоліків і чинників, що знижують ефективність (в тому числі і безпеку) функціонування комп'ютерних мереж IoT є стратегія на централізованого управління хмарними ресурсами. Це підтверджується фактами успішно проведених зловмисних атак на ключові вузли комутації IoT.

Слід зауважити, що створення децентралізованого IoT – складне завдання. Необхідно розробити протоколи виявлення пристроїв, безпеки та управління ідентичністю, реалізувати схеми довіри, інтегрувати в мережу криптовалюту і вирішити багато інших завдань.

Проведені дослідження показали, що однією з первинних завдань в переліку є розробка оптимальної топологічної струк-

тури комп'ютерної мережі IoT. Для її вирішення необхідно попередньо провести аналіз і дослідження існуючих показників централізації (децентралізації) вузлів мережі і ступінь впливу їх можливого виходу з ладу на загальний показник безпеки комп'ютерної мережі IoT.

Розглянемо більш докладно дані показники:

Ступінь зв'язності (degree centrality) – історично перша і концептуально проста міра C_0 важливості вузлів в мережі. Цей захід визначається як кількість зв'язків deg (v), інцидентних даного вузла v:

$$C_0(v) = \deg(v),$$

Ступінь зв'язності вузлів комп'ютерної мережі IoT можна інтерпретувати як міру активності вузлів в процесі виконання різних завдань, характерних даному виду IoT.

Ступінь близькості до інших вузлів (closeness centrality) $C_c(v)$ – зворотна величина суми найкоротших шляхів $d(v_i, w_i)$ від вузла v до інших вузлів w_i: $C_{\tilde{n}}(v) = 1 \Big/ \sum_{i=1}^{|V|} d(v, w_i)$ де $|V|$ – число всіх вузлів мережі.

Таким чином, чим більше важливим є вузол відповідно до зазначеного показником, тим менше сума найкоротших шляхів від нього до інших вузлів.

Ступінь посередництва (betweenness centrality) – характеристика вузла, що показує, наскільки часто цей вузол лежить на найкоротших шляхах між іншими вузлами.

Цей параметр обчислюється таким чином $C_b(v) = \sum_{k \neq i} \sum_{j \neq i,\ j > k} \frac{\sigma_{kj}(v)}{\sigma_{kj}}$, де σ_{kj} - кількість найкоротших шляхів з вузла k в вузол j, а $\sigma_{kj}(v)$ - кількість цих шляхів, що проходять через вузол. Через вузол з високим ступенем посередництва буде проходити великий обсяг даних, за умови що передача буде здійснюватися по найкоротших шляхах. Це має на увазі велику вразливість таких вузлів до атак зловмисників.

Впливовість (eigenvector centrality) - рекурсивна міра $C_e(v)$ важливості вузла, заснованої на важливості сусідніх вузлів. Чим більше впливові вузли, з якими пов'язаний вузол, тим більше впливовість самого вузла: $C_e(v) = \frac{1}{\lambda} \sum_{i \in M(v)} C_e(t) = \frac{1}{\lambda} \sum_{i \in G} A_{v,t} C_e(t)$ де $M(v)$ – множина сусідніх вузлу v вузлів; λ – константа; $A_{v,t}$ – елемент матриці суміжності (задається на основі зв'язності вузлів мережі).

$C_{LVC}(i)$ (Local Vector Centrality (LVC)) – це показник, що характеризує вразливість комп'ютерної мережі IoT до видалення вузлів. Вузол з більш високим LVC важливіший для структури мережного з'єднання.

Нехай y – власний вектор, пов'язаний з другим найменшим власним $\mu(L)$ значенням матриці Лапласса L. Тоді $C_{LVC}(i)$ можна розрахувати як $C_{LVC}(i) = \sum_{j \in N_i} (y_i - y_j)^2$.

Слід зауважити, що хоч $C_{LVC}(i)$ – це і узагальнена центральна міра, її можна точно апроксимувати локальними обчисленнями і передачею повідомлень з використанням методу розподіленої потужності для обчислення вектора у.

В результаті проведених аналізу літератури і досліджень були визначені найбільш інформативні показники централізації мережі IoT. Проведено дослідження можливості їх використання для аналізу стійкості комп'ютерної мережі IoT до атак зловмисників, спрямованих на виведення з ладу центральних, найбільш ванних вузлів. Результати показали в цілому порівнянність результатів в розглянутому конкретному випадку, і перевагу до 20% показника Local Vector Centrality при видаленні 10 вузлів.

Список використаних джерел:

1. Юдина М. Н. Узлы в социальных сетях: меры центральности и роль в сетевых процесах. *Омский научный вестник.* 2016. № 4(148). С. 161-165.
2. Pin-Yu Chen Hero A. O. Local Fiedler vector centrality for detection of deep and overlapping communities in networks // IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2014. P. 1120–1124.

3. Rethinking a Secure Internet of Things. URL: http://iot.stanford.edu (дата звернення: 12.10.2017).

Одержано 24.10.2017

УДК 327.84 : 004

Руслан Юрійович СЕНЬ,
провідний фахівець факультету № 4 Харківського національного університету внутрішніх справ

Валерія Сергіївна ЧЕРНОВОЛ,
курсант факультету № 4 Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ЗЛОЧИНАХ ПОВ'ЯЗАНИХ З ТОРГІВЛЕЮ ЛЮДЬМИ

Феномен торгівлі людьми піддається постійному аналізу і є предметом багатьох суперечок і дискусій.

Жертвами торгівлі людьми можуть стати чоловіки, жінки, діти, – з метою примусової праці, сексуальної експлуатації, жебрацтва та/або отримання біологічного трансплантаційного матеріалу (органів).

На даний час, за даними звіту Державного департаменту США про торгівлю людьми у світі в 2016 році Україну помістили в другу групу, як «країну походження, транзиту й призначення для чоловіків, жінок та дітей, які зазнають примусової праці та сексуальної експлуатації» [1].

Кількість випадків торгівлі людьми та рабства в Україні почастішали. І це зумовлено не лише перманентною кризою та низьким рівнем життя, – нині через неконтрольовані ділянки кордонів України, окрім зброї та боєприпасів, переміщаються жертви та злочинці торгівлі людьми.

Необхідно зауважити, що глобальна інформатизація та глобалізація усіх ланок суспільного життя спонукає до інтеграції традиційних злочинів до кіберпростору.

Таким виключенням не стала торгівля людьми, враховуючи той факт, що у 2009 році в обіг було введено першу криптовалюту «bitcoin», використання якої гарантує майже повну анонімність. Завдяки використанню технології P2P, біткоін, як криптовалюта функціонує без будь-якого контролюючого органу чи центрального банку. Обробка транзакцій та емісія здійснюється колективно лише учасниками мережі [2].

Цікаво, що біткоін має відкритий вихідний код, його архітектура відома усьому світу, але ніхто не в змозі контролювати його та володіти ним.

Правоохоронним органам вже відомо декілька випадків спроб продажу людини за криптовалюту. Одним із них є інцидент, коли жінку виставили на продаж на Інтернет-аукціоні та вимагали за неї біткоїни в еквіваленті рівні сумі в 300 тисяч євро.

Міжнародна практика свідчить, що на даний час все дедалі частіше використовуються інформаційні технології при готуванні та здійсненні кримінального правопорушення щодо продажу людини.

Необхідно зазначити, що в Україні інформаційні технології виступають у якості допоміжних засобів, які використовуються безпосередньо для вчинення злочину: зазвичай для вербування жертв використовують особисті зв'язки або фальшиві рекламні оголошення розміщенні на веб-сайтах з працевлаштування, або на будь-яких інших сайтах, форумах, у якості рекламних банерів. Нелегальні кадрові агенції, які здійснюють роботу в режимі online. Умови, що пропонують вербувальники, є зазвичай дуже привабливими та можуть здатися правдоподібними, наприклад фінансова допомога та підтримка в організації поїздки, оформлення всіх необхідних документів тощо [3].

Траплялись випадки, коли недосить «досвідчені» злочинці розміщували повідомлення про продаж людини, або її органів на платформах безкоштовних повідомлень.

Таким чином можна зробити висновок: головна проблема протидії торгівлі людьми полягає в тому, що досить важко виявляти та розслідувати такі злочини, а з використанням передових інформаційних технологій - практично неможливе. Транснаціональна злочинність виробила добре відпрацьований механізм здійснення торгівлі людьми, при якому відслідкувати рух "живого товару" надзвичайно важко.

Проте, слід зазначити, що останнім часом запроваджено певні позитивні зміни у ставленні до проблеми торгівлі в Україні. Існує правова база для боротьби з торгівлею людьми: Кримінальний Кодекс України в ст. 149 встановлює відповідальність за цей вид злочину, розроблено урядову програму щодо запобігання торгівлі жінками і дітьми. До речі, Україна стала третьою державою Європи, поряд з Бельгією і Німеччиною,

які на законодавчому рівні визнали торгівлю людьми тяжким злочином.

Список використаних джерел:

1. Палажій Г. В Україні почастішали випадки торгівлі людьми та рабства. Як не стати жертвою? URL: http://zik.ua/news/2017/03/28/v_ukraini_pochastishaly_vypadky_torgivli_lyudmy_ta_rabstva_yak_ne_staty_1069197 (дата звернення: 13.10.2017).
2. Биткойн - это инновационная сеть платежей и новый вид денег! URL: https://bitcoin.org/ru/ (дата звернення: 15.10.2017).
3. Торгівля людьми в Україні. Актуальні ризики та вразливі групи. URL: http://pidmoga.info/torgivlya-lyud-my-v-ukrayini-aktual-ni-ry-zy-ky-ta-vrazly-vi-grupy/ (дата звернення: 15.10.2017).
4. Кримінальний кодекс України: закон України від 05.04.2001 № 2341-III. URL: http://zakon3.rada.gov.ua/laws/show/2341-14 (дата звернення: 08.10.2017).

Одержано 30.10.2017

УДК 004.056.57

Віталій Анатолійович СВІТЛИЧНИЙ,
кандидат технічних наук, доцент кафедри кібербезпеки факультету №4 Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ МЕТОДІВ СОЦІАЛЬНОГО ІНЖИНІРИНГУ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

Інформаційний простір давно став безпосередньою і невід'ємною частиною нашого життя, але незважаючи на усі заходи, що приймають окремі особи, установи, держава, кіберзлочинність продовжує свою діяльність. Тому сьогодні особливо важливо переглянути усі існуючі заходи та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців. Будь-який зловмисник перш за все – людина, отже має певні вразливості психіки, які можливо використовувати при проведенні розслідування. В залежності від психологічних особливостей кіберзлочинця, можливо виділити певні вразливості його психіки та ефективно впливати методами і прийомами соціальної інженерії на нього.

Кіберзлочинець, який скоїв злочин, розуміє, що він порушив закон, тому в більшості випадків не виключено, що на підсвідомому рівні він боїться свого викриття, тому він більшу частину часу перебуває в страху. Це призводить до втрати

уваги та сконцентрованості, що, при правильному застосуванні техніки соціального інжинірингу, можливо використати на користь оперативного працівника, який розслідує даний злочин. Беручи до уваги той факт, що більшість кібезлочинів здійснюються з метою самоствердження, то цілком природно буде вважати, що такого кіберзлочинця будуть обурювати почуття марнославства та бажання того, що б про його діяння стало відомо щонайбільшій кількості людей. Така поведінка дуже розповсюджена серед молодих та недосвідчених представників хакерської спільноти, особливо серед тих, хто до цього не зіткався з представниками кіберполіції і не потрапляв у ситуації, коли до нього застосовується судове переслідування. В такому випадку правильно організований пошук інформації в мережі Інтернет може допомогти при встановленні особи порушника або пошуку його реквізитів, таких, як IP і MAC адреси, або контактні дані для ведення листування. У ході листування можливе застосування технік соціального інжинірингу з метою отримання інформації щодо причетності особи до вчинення певного злочину. Також для можливості стеження за кіберзлочинами, що скоєні або плануються, працівник поліції може впроваджуватися в спільноти хакерів під виглядом такого ж хакера з метою отримання довіри до себе. В результаті такий працівник може мати доступ до найсвіжішої та актуальної інформації щодо кібезлочинів, які скоюються цією спільнотою з наступною реалізацією цієї інформації, розслідування кібезлочинів, пошуку та відстеження контактних даних та реальних імен та адрес хакерів, притягнення їх до відповідальності за вчинені злочини. Така методика може мати характер інсайдерінгу в цілях недопущення та попередження кіберзлочинів. При впровадженні працівника в хакерську спільноту для розслідування кіберзлочинів, він може для встановлення особи зловмисника, застосовувати прийом провокації та дезінформації. Крім того для ефективного розслідування або недопущення кіберзлочінів цілком обґрунтовано використання метода «подвійній агент». Як відомо, подвійним агентом називається особа, яка одночасно співпрацює з двома різними організаціями (службами, спільнотами), які, зазвичай, протиборствують. Подвійний агент, який систематично веде роботу в осередку злочинців та направляє їм різного роду дезінформацію, проводить провокаційну діяльність під легендою – прикриттям, тобто здійснює оперативну гру. Подвійних аге-

нтів можливо розділити за декількома категоріями в залежності від особливостей їх роботи:

- «торговець» – агент, який доставляє інформацію одній стороні в обмінна отримання інформації про другу сторону;
- «кріт» – працівник однієї сторони, який потайки співпрацює з другою;
- «лжекріт» – працівник однієї сторони, який за завданням свого керівництва пропонує свої послуги другій стороні або дозволяє себе завербувати;
- «перевертень» – працівник однієї сторони, якого було розкрито і який погодився на співпрацю з іншою з метою уникнення покарання або іншою.

Природно, що методи соціального інжинірингу для розслідування кіберзлочинів можуть застосовуватись кіберполіцією у всіх випадках та порядку, коли вони відповідають вимогам чинного законодавства, діючих підзаконних актів та міжнародних законодавчим документам. Здійснивши аналіз вразливості людської психіки, можливо виявити вразливості кіберзлочинця та можливості використання їх для розслідування кіберзлочинів. На основі цих вразливостей слід взяти до уваги інші базові методи соціального інжинірингу, які потрібно застосовувати для розслідування кіберзлочинів, а саме:

- використання бренда відомої корпорації;
- підроблена лотерея;
- фальшиві антивіруси і програми для забезпечення безпеки (scareware);
- фішинг і його різновиди;
- фрікінг;
- претекстінг;
- quid pro quo;
- «дорожнє яблуко»;
- збір інформації з відкритих джерел головним чином з соціальних мереж;
- плечовий серфінг (shoulder surfing);
- зворотна соціальна інженерія.

Крім того, на нашу думку, працівник кіберполіції може для розслідування кіберзлочинів використовувати спільно з методами соціального інжинірингу відомі методи оперативно-розшукової діяльності, але інтерпретовані під використання в кіберпросторі.

Одержано 25.10.2017

УДК 343.346.8 : 004.056.53

Володимир Михайлович СТРУКОВ,
кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

МОДИФІКАЦІЯ АЛГОРИТМУ КЛАСТЕРИЗАЦІЇ K-MEANS

В даний час спостерігається тенденція все більш частого використовування кримінальними елементами Інтернету для злочинних цілей - розповсюдження порнографії, наркотиків, зброї, втягнення неповнолітніх у сферу своєї діяльності тощо. У постійно зростаючому потоці даних шукати кримінально значиму інформацію вручну неефективно та й недоцільно.

У зв'язку з стрімким наростанням потоків неструктурованої інформації у віртуальному просторі і неможливістю накопичувати і зберігати всі дані, що поступають, в пам'яті, все більш актуальним є застосування методів аналітичної обробки потоків даних Data Mining, Text Mining, Web Mining. В основі цих наукоємних технологій лежать методи класифікації-кластеризації.

Існує досить велика кількість різних підходів, методів та алгоритмів кластеризації [1], які застосовуються і ефективні в різних конкретних ситуаціях. Розглянемо випадок, коли передбачається, що кластери добре виражені, тобто є угрупування даних, які досить чітко відокремлені одне від одного. Крім того, дані мають велику розмірність (тисячі і мільйони записів) і вимірюються у числовій шкалі.

Одними з простих та широко використовуваних алгоритмів кластеризації є алгоритми K- means і C- means [1]. Їх основними перевагами є простота реалізації, результативність і висока швидкодія. Головний недолік – заздалегідь задана кількість кластерів, на які необхідно розбити вихідний набір об'єктів. Крім того, в алгоритмах цього класу на першій стадії при визначенні первинних центрів шуканих кластерів, як правило, випадковим чином обираються K об'єктів. При певних обставинах це певною мірою прийнятно - наприклад, при відносно невеликій кількості вихідних об'єктів (до декількох сотень) і передбаченої в подальшому процедурі оптимізації знайденого рішення. Однак у тих випадках, коли кількість досліджуваних об'єктів досягає сотень тисяч і мільйонів записів, такий підхід є завідомо неприйнятним. У цьому випадку є доцільним мати

досить "хорошу" початкову вибірку первинних центрів, яка в подальшому забезпечить рішення, близьке до локального (або глобального) екстремуму.

Пропонується підзадачу визначення первинних центрів кластерів вирішувати як задачу оптимізації деякого критерію, що забезпечує максимальне розсіювання первинних центрів кластерів. Обґрунтуванням вибору такого критерію є припущення про те, що кластери добре виражені (виділені і відокремлені), отже, їх центри розташовані в такий спосіб, що вони доставляють екстремум функції розсіювання деяких параметрів первинних центрів кластерів. В якості такого параметру пропонується використовувати показник середньоквадратичного відхилення від середньої відстані між первинними центрами.

Для формалізації задачі введемо наступні позначення:

X={xij} ∈ Rmxn - матриця «об'єкт-властивість», де xij – значення j-ї властивості i-го об'єкта a, i=1,2, …, m; j=1,2, …, n, при цьому кожний об'єкт може бути описаний вектором-рядком властивостей xi = (xi1, xi2, …, xin) ∈ Rn. Вважатимемо, що значення всіх n ознак задані у звичайній числовій шкалі, хоча, як показано в [2], до такого випадку можна звести і ситуацію, коли значення ознак об'єктів задані в інших шкалах.

K – кількість кластерів у задачі;

Xc={x_i^c}, i=1, 2, …, K – множина шуканих центрів кластерів.

Нехай також у просторі Rn об'єктів задана відстань між ними у звичайній евклідовій метриці:

$$d_{il} = \sqrt{\sum_{j=1}^{n} (x_{ij} - x_{lj})^2}. \qquad (1)$$

Тоді через d_{ij}^c позначимо відстань між центрами кластерів x_i^c і x_j^c. Відповідно, середня відстань від об'єкта x_i^c до усіх інших центрів (об'єктів множини Xc) може бути записана у вигляді:

$$d_i^c = \frac{1}{K-1} \sum_{x_j^c \in X^c; x_j^c \neq x_i^c} d_{ij}^c. \qquad (2)$$

Таким чином, цільова функція у підзадачі пошуку первинних центрів K кластерів буде мати наступний вигляд:

$$f^c = \sum_{j=1}^{K} (d_j^c - \frac{1}{K} \sum_{i=1}^{K} d_i^c)^2 \to \min. \qquad (3)$$

Експериментальне дослідження програмної реалізації запропонованого підходу на тестових прикладах підтвердило його ефективність.

Список використаних джерел:

1. Aggarwal C.C., Reddy C.K. Data clustering. Algorithms and Applications. Cham: Springer Ltd. Publ., Switzerland, 2015. 734 p.
2. Бодянский Е.В., Струков В.М., Узлов Д.Ю. Задача оценки близости многомерных объектов анализа данных. *Управляющие системы и машины.* 2016. № 6. С. 67-72.

Одержано 19.10.2017

УДК 004.658.6

Юлія Володимирівна ТРЕГУБ,
студентка Національного аерокосмічного університету ім. Н. Є. Жуковского «ХАІ»

ВИКОРИСТАННЯ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ У СФЕРІ ДЕРЖАВНОГО УПРАВЛІННЯ

З розвитком інформаційного суспільства, державні послуги зазнають великих змін і переходять до обслуговування за допомогою мережі Інтернет. Саме тому, наша держава пропонує велику кількість онлайн послуг, а саме: електронний уряд, послуги центру державного земельного кадастру, тощо. Цим державним сервісам приділяють велику увагу кіберзлочинці. Тому постає питання про адекватний захист інтересів держави у кіберспросторі.

5-го жовтня 2017 року у Верховній Раді України був прийнятий законопроект №2126а від 19.06.2015 «Про основні засади забезпечення кібербезпеки в території України».

Згідно з Законом в Україні створюється національна система кібербезпеки, як "сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів політичного, науково-технічного, інформаційного характеру, організаційних, правових, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури."[1].

Основними суб'єктами національної системи кібербезпеки є Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, Національний банк України, які відпо-

відно до Конституції і законів України виконують в установленому порядку основні завдання з забезпечення надійної передачі, збереження та обробки інформації.

Саме на ці структури Законом покладено забезпечення, розвиток та стале функціонування державних послуг в умовах протидії кіберзлочинцям. Одним із методів захисту даних в державних інфраструктурах є технологія блокчейн.

Блокчейн – це розподілена база даних, яка представляє собою один із способів зберігання, обробки та захисту даних і транзакцій користувача. Організована вона у вигляді ланцюга блоків інформації, у кожен з яких записана певна кількість операцій і даних з попереднього блоку [2].

Існує два види блокчейну: приватні та публічні. Приватні блокчейни - це блокчейни, в яких створення блоків централізовано, використовується технологія «докази роботи» (proof-of-work), і всі права на зчитування/запис належать одній організації. Публічні блокчейни можуть бути прочитані будь-яким користувачем, при цьому операції захищаються механізмами кри1птографічного верифікації, такими як доказ виконання роботи або підтвердження частки (proof-of-stake). Права тут у всіх учасників однакові, що не гарантує повноцінну конфіденційність даних [3].

Сполучення блокчейну з реальним світом забезпечується за допомогою заздалегідь запрограмованих умов і їх передачі до всіх вузлів - розумних контрактів. Звідси випливає, що необхідність в будь-якій іншій уповноваженій особі, визнаній обома сторонами, відпадає. Смарт-контракти, засновані на криптографії, забезпечують кращу безпеку, ніж традиційні контракти, засновані на праві, і зменшують ймовірність транзакційних витрат, пов'язаних з укладанням договорів і можливих судових витрат [4].

Починаючи з 2017-го року, в Україні, розвивається проект застосування блокчейну у системі державного управління на сайтах оренди та продажу державного майна, електронному самоврядуванні та земельному кадастрі. Це дозволяє підвищити ефективність державного управління; забезпечити конфіденційність даних; зробити взаємодію з державними органами простішою, швидшою та ефективнішою.

Згідно з постановою Кабінету Міністрів України від 21 червня 2017 року №688 Міністерство аграрної політики та продовольства і Державне агентство електронного урядування та Transparency International Україна розробили Державний зе-

мельний кадастр, який відтепер працюватиме на технології Blockchain [5]. Впровадження цієї технології дозволить забезпечити надійну синхронізацію даних, що унеможливить їх підміну в результаті зовнішнього втручання, гарантує прозорість, а також дасть можливість здійснювати суспільний контроль за системою.

Застосування технології блокчейн у державних установах дозволяє наблизити онлайн сервіси нашої держави до найвищих стандартів інформаційного суспільства. Наша країна активно впроваджує вказані технології. Завдяки цьому дані користувачів будуть надійно захищені від фальсифікації та несанкційного доступу зловмисника. В результаті проведеного аналізу були запропоновані шляхи впровадження технології BlockChain 2.0 для державних установ України з використанням відкритих крипто валют. Виявлені недоліки в реалізації технології блокчейн для державного земельного кадастру України, та запропоновані шляхи їх вирішення.

Список використаних джерел:

1. Конституція України: Закон від 19.06.2015 №2126а // База даних «Законодавство України»/ВР України. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657. (дата звернення 23.10.17).
2. Wikipedia.org: Блокчейн. URL: https://uk.wikipedia.org/wiki/%D0%91%D0%BB%D0%BE%D0%BA%D1%87%D0%B5%D0%B9%D0%BD. (дата звернення 23.10.17).
3. Profitgid.ru: «Разница между приватными и публичными блокчейнами». URL: https://profitgid.ru/raznica-mezhdu-publichnymi-i-privatnymi-blokchejnami.html. (дата звернення 23.10.17).
4. Wikipedia.org: Смарт контракт. URL: https://ru.wikipedia.org/wiki/Смарт_контракт. (дата звернення 23.10.17).
5. TI-Ukraine: «Державний земельний кадастр перейшов на технологію блокчейн». URL: https://ti-ukraine.org/news/derzhavnyi-zemelnyi-kadastr-pereishov-na-tekhnolohiiu-blokchein/. (дата звернення 23.10.17).

Одержано 01.11.2017

УДК 65.012.8 + 004

Володимир Володимирович ТУЛУПОВ,
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

Валерій Миколайович ПЕРЕСІЧАНСЬКИЙ,
старший викладач кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

ДЕЯКІ ОСОБЛИВОСТІ ПОШУКУ ТА ВСТАНОВЛЕННЯ ОСОБИ ПРИ РОЗСЛІДУВАННІ КІБЕРЗЛОЧИНІВ

У сучасній методиці боротьби з кіберзлочинністю одним із проблемних питань залишається встановлення та визначення місцезнаходження особи за її мережними ідентифікаторами, тобто за тими обліковими даними, яка особа залишила або надала інформацію про себе.

Одним із способів встановлення особи може виступати пошук інформації за певним ідентифікатором за допомогою різного роду сервісів та ресурсів [1, с. 256].

Знаючи наприклад IP-адресу комп'ютера або мережного обладнання особи та розуміючи правила надання доменних імен і закріплення їх за зонами, працівник правоохоронного органу здебільшого має змогу самостійно визначити фізичне місцезнаходження комп'ютера, за яким дана адреса закріплена.

Місцезнаходження програмно-технічних засобів у мережі Інтернет визначається також за IP - адресою, яка належить певному провайдеру і є взаємопов'язаною з номером телефону користувача послуг доступу до мережі (наприклад провайдера ВАТ «Укртелеком» за стандартом доступу ADSL) . Але цей спосіб пошуку та встановлення особи за допомогою офіційного запиту до власника ресурсу часто не дає бажаних результатів.

Тому, сьогодні існує декілька методів пасивного та активного збору інформації, програмних продуктів та утиліт за допомогою яких можна отримати відомості щодо власника домену (сайту), його IP-адреси та дізнатися, де розміщено сам сервер із сайтом (хостінг або Colocation) [2, с. 68].

Частіше використовують пасивний метод збору інформації який характерний тим, що його етапи неможливо виявити, тому що на практиці вони не викликають ніяких підозр, при

цьому фактично неможливо визначення вузла, з якого проводиться пасивний збір інформації.

За допомогою пасивного методу збору інформації в більшості випадків можна скласти приблизну карту вузлів зовнішнього периметра з припущеннями про їх роль, зібрати додаткову інформацію про організацію, контактну інформацію про особу та багато іншої корисної інформації. Одним із програмних продуктів, що допомагає при визначенні інформації різного виду в мережі Інтернет, є програма IP-Tools, що містить такі корисні утиліти як:

- Ping- Skanner – ping за діапазоном адрес або за списком адрес;
- Trace–показує маршрут, яким проходять IP-пакети між комп'ютерами;
- Whois–одержання реєстраційної інформації про домени з офіційних Whois серверів;
- Finger –одержання інформації про користувачів певного хоста;
- LookUp –визначає IP-адресу хоста або розташування самого сервера за іменем або навпаки.

Також у мережі Інтернет існують інші безкоштовні сервіси, за допомогою яких можна отримати ту чи іншу інформацію щодо ресурсів мережі (сайтів) (наприклад, SmartWhois, Mod IP, City тощо). За допомогою вказаних сервісів отримують інформацію про:

- належність конкретної IP-адреси до сегмента Інтернет певної країни, провайдера, хост-провайдера, їх контакти;
- IP-адресу певного сайту (ресурсу);
- реєстратора доменного імені певного сайту;
- технічну площадку (фізичне розташування) проксісервера;
- історію сайту, ресурс, який ним використовується, розрахунок трафіку, посилання на сайт тощо [2, с. 69].

Також слід використовувати сайти та програмні продукти які теж корисні при проведенні певного збору інформації наприклад:

- www.kali.org - Kali Linux продукт для пентесту тощо;
- www.edge-security.com/metagoofil.php - інструмент для збору інформації з документів які знаходяться в публічному доступі (Metagoofil використовує Google);
- www.archive.org - містить архів веб-сайтів;
- www.domaintools.com - розвідка доменних імен;

- www.alexa.com - база даних інформації про веб-сайти;
- www.serversniff.net - безкоштовні онлайн утиліти;
- www.centralops.net - безкоштовні онлайн утиліти;
- www.pipl.com - пошук людей;
- www.yoname.com - пошук людей в соціальних мережах і блогах;
- www.tineye.com - можна використовувати для визначення звідки зображення, чи є модифіковані версії;
- www.2ip.com.ua - безкоштовні онлайн утиліти.

Список використаних джерел:

1. Манжай О. В., Осятинська І. А. Встановлення та визначення місцезнаходження особи за її мережними ідентифікаторами // Актуальні питання розслідування кіберзлочинів : матеріали Міжнар. наук.-практ. конф., м. Харків, 10 груд. 2013 р. / МВС України, Харк. нац. ун-т внутр. справ. Х.: ХНУВС, 2013. С. 256.
2. Протидія кіберзлочинам: кримінально-правові та криміналістичні аспекти: посібник / [Р. І. Благута, О. В. Захарова, О. І. Зачек, М. Ю. Літвінов, Т. І. Созанський, І. А. Федчак]. Київ, 2012.

Одержано 17.10.2017

РОЗДІЛ 4.
КАДРОВЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 159.922

Вадим Іванович БАРКО,
доктор психологічних наук, професор, головний науковий співробітник лабораторії психологічного забезпечення Державного науково-дослідного інституту МВС України

ПСИХОЛОГІЧНІ ПРИНЦИПИ ОТРИМАННЯ ДОСТОВІРНОЇ ІНФОРМАЦІЇ В ПРОЦЕСІ ПРОВЕДЕННЯ СПІВБЕСІДИ З КАНДИДАТОМ НА ПОСАДУ В ПОЛІЦІЇ

У зв'язку з реформування Міністерства внутрішніх справ України в частині створення Національної поліції України, виникла потреба у забезпеченні новостворених підрозділів (кіберполіції, кримінального аналізу, патрульної та дорожньої поліції тощо) кваліфікованими кадрами шляхом прийняттям на службу цивільних осіб з відповідним фахом або атестації осіб, які працювали в ОВС України.

Під час відбору кадрів необхідно приділяти важливу увагу дослідженню професійної придатності кандидата на службу. Вивчення досвіду розвинутих зарубіжних країн світу свідчить про те, що процедура дослідження професійної придатності поліцейських є досить складним процесом, який включає в себе низку соціально-психологічних методів, у тому числі, співбесіду з кандидатом [2, с. 40; 3, с. 150; 7, с. 243].

У ході співбесіди (інтерв'ю), можуть бути отримані дані про комунікативні здібності, загальноосвітній рівень, «сумісність» кандидата з корпоративним середовищем, лояльність тощо. Технологія інтерв'ю широко застосовується в процесі оцінки кандидатів на посаду в поліції та під час атестації працівників поліції, причому така оцінка здійснюється на основі моделей компетенцій.

Співбесіда, як правило, проводиться при вирішенні питання про висунення поліцейських на посади різного рівня [4, с.310; 5, с. 20; 6, с. 55].

В ході інтерв'ю кандидат у вільній формі відповідає на різноманітні питання, що в основному стосуються досвіду у подоланні або вирішенні тих або інших службових і життєвих ситуацій. На підставі аналізу змісту його розповіді, психолог

або фахівець кадрового підрозділу, робить висновок про наявність і міру розвитку тих або інших компетенцій, істотних для ефективного виконання службової діяльності.

Правильно побудоване інтерв'ю будується на припущенні, згідно з яким надійнішою основою для висновків є інформація про реальні дії людини, які вона здійснювала в різних умовах і ситуаціях, а не її думки і припущення про те, якими якостями зумовлювалися ці дії. Зрозуміло, що неправдивий кандидат може спотворювати інформацію також стосовно реальних фактів свого життя, проте така брехня досить легко може бути виявлена за допомогою психофізіологічних методів оцінки достовірності інформації.

Основною метою інтерв'ю для отримання «поведінкових прикладів», є отримання детальних відомостей про те, як кандидату вдається упоратись зі службовими функціями в різних ситуаціях. В ході цього інтерв'ю кандидат не дає оцінок своїм діям, а просто описує свою поведінку, переживання і вчинки в різних обставинах, про які його запитує інтерв'юер, і які мають відношення до компетенцій, що вивчаються.

У процесі проведення інтерв'ю виникає питання щодо можливості оцінки достовірності інформації, що повідомляється. На сьогодні цю оцінку можливо зробити за рахунок використання розробленої групи методів, об'єднаних назвою «Методи оцінки достовірності інформації». В основі цих методів лежать різні способи оцінки та інтерпретації змін психофізіологічного стану людини.

Розглянемо деякі принципи побудови інтерв'ю з урахуванням аналізу невербальних ознак. Численні дослідження показують, що між ефективним і неефективним способом проведення співбесіди у формі структурованого опитування, існують очевидні відмінності, обумовлені тактикою поведінки особи, що веде бесіду (інтерв'юера). Перша відмінність полягає в тому, що «правильний інтерв'юер» ставить переважно широкі запитання, спонукаючи опитуваного говорити більшу частину часу. При непрофесійному проведенні структурованого інтерв'ю зустрічаються три основні види типових помилок: а) інтерв'юер без необхідності часто перериває співрозмовника; б) опитуваному задається надмірно велика кількість вузьких і навідних запитань, що призводять до менш детальних відповідей; в) послідовність запитань часто буває заздалегідь не продумана, трапляються недоречні і несподівані запитання,

що є перешкодою для нормальної роботи пам'яті і відтворення матеріалу.

Розглянемо загальні психологічні принципи і прийоми проведення співбесіди, націлені на поліпшення якості інформації і погіршення умов для особи, яка бреше у відповідь. Співбесіду, що проводиться з використанням перерахованих нижче принципів і підходів іноді ще називають «когнітивним інтерв'ю». До таких принципів і прийомів належать:

1. Схожість ситуації до реальної події – інтерв'юер повинен постаратися відновити в пам'яті співрозмовника усі можливі зовнішні атрибути події (включаючи обстановку, погодні умови, емоційні переживання, супутні думки).

2. Фокусованість відтворення – відтворення в пам'яті, як і будь-яка психічна активність, потребує певної концентрації зусиль, тому одне із завдань інтерв'юера полягає в тому, щоб допомогти опитуваному сконцентрувати свої зусилля на відтворенні потрібної інформації.

3. Екстенсивність відтворення – чим більше спроб робить опитуваний для пригадування конкретного епізоду, тим більш істотну інформацію він відтворює, тому його треба постійно спонукати до того, щоб він робив якомога більше спроб згадувати певну подію.

4. Підлаштування питань під співрозмовника – успішне відтворення деталей з пам'яті залежить від того, наскільки зміст питань і форма, в якій вони ставляться, відповідають особливостям запам'ятовування, тому важливо, щоб інтерв'юер максимально підлаштовував свої запитання під співрозмовника.

Перш ніж запропонувати опитуваному викласти у вільній формі сутність фактів і подій, йому слід дати наступний алгоритм: 1. Відновлення обставин. «Постарайтеся відновити в пам'яті усю обстановку, що супроводжувала подію». 2. Виклад деталей. «Іноді люди не повідомляють усю інформацію, що цікавить, тому що вони не вважають її важливою. Будь ласка, не опускайте ніяких дрібниць». 3. Зміна порядку. «Зазвичай вважають, що найбільш зручною є хронологічна послідовність викладу. Проте спробуйте розповісти усе в іншому порядку». 4. Зміна перспективи. «Уявіть себе на місці інших учасників і постарайтеся відтворити все ще раз так, як вони могли б усе це бачити і чути».

В ході співбесіди можна використати низку специфічних запитань, які сприятимуть поліпшенню відновлення з пам'яті

елементів інформації, що повідомляється. Сфери, що охоплюються цими питаннями, зокрема, включають: а) опис фізичних характеристик; б) імена; в) числа; г) особливості мовлення; д) зміст розмов.

Дослідження показують, що використання перелічених вище психологічних принципів і прийомів проведення співбесіди (інтерв'ю) у процесі вивчення особистості кандидата на посаду працівника поліції значно підвищує якість і кількість корисної інформації, отримуваної від щирого співрозмовника. В той же час якість викладу відомостей нещирим працівником в таких умовах значно погіршується і супроводжується появою значної кількості невербальних ознак, що дозволяють упевнено діагностувати ці висловлювання як неправдиві. Тому подібні інтерв'ю є цінним психологічним засобом перевірки професійної придатності поліцейського при проведенні конкурсу на службу або зайняття кандидатом вакантної посади в поліції, у тому числі у новостворених підрозділах кіберполіції, кримінального аналізу, патрульної та дорожньої поліції Національної поліції України.

Список використаних джерел:

1. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. *Відомості Верховної Ради України.* 2015. № 40-41 (9 жовтня). Стор. 1970. Ст. 379.
2. Барко В. І., Зелений В. І., Ірхін Ю. Б. Робоча книга керівника органу внутрішніх справ (психолого-педагогічний аспект) : навч. посіб. Вінниця : Книга-Вега ; Вінниц. обл. друк., 2009. 248 с.
3. Мучински П. Психология, профессия, карьера. 7-е изд. СПб. : Питер, 2004. 539 с.
4. Мескон М.Х., Альберт М., Хедоури Ф. Основы менеджмента: пер. с англ. М.: Дело, 1992. 702 с.
5. Сошников А., Пеленицын А. Оценка персонала : психологические и психофизиологические методы. М.: Эксмо, 2009. 240 с.
6. Чарльз М. Т. Современное состояние и перспективы профессиональной подготовки сотрудников полиции (милиции) США и России. СПб. : Алетейя, 2000. 268 с.

Одержано 31.10.2017

УДК 343.1

Віта Петрівна КОНОНЕЦЬ,
кандидат юридичних наук, старший викладач кафедри адміністративного права, процесу, адміністративної діяльності Дніпропетровського державного університету внутрішніх справ

Владислав Олександрович ХИТРОВ,
слухач магістратури факультету підготовки фахівців для підрозділів превентивної діяльності Дніпропетровського державного університету внутрішніх справ

ЕФЕКТИВНІСТЬ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОГО АНТИКОРУПЦІЙНОГО БЮРО УКРАЇНИ

Корупція як негативне соціальне явище міцно увійшло в життя нашої держави. Про причини і наслідки такої суспільної хвороби сказано багато, проте дієвого механізму профілактики і боротьби з нею допоки вироблено не було. Володіння адміністративною владою відкриває широкі можливості для зловживання нею, будь то у формі протекціонізму, незаконного придбання різних соціальних благ і різного роду привілеїв, корупції тощо. Це випливає з самої суті адміністративної влади, анонімності, що характеризується, безособовістю, величезним впливом майже у всіх галузях суспільного життя, часто зрощенням з економічною владою, володінням інформацією з найбільш важливих проблем, що стоять перед суспільством, арсеналом примусових засобів [1, с. 19].

Проблемами антикорупційної діяльності держави займались ряд вчених з аміністративного права України та зарубіжжя, фахівці з державного управління та кримінального права, зокрема праці В. Б. Авер'янова, Д. М. Бахраха, Ю. П. Битяка, І. Л. Бородіна, І. П. Голосніченка, Є. В. Додіна, М. С. Кельмана, Л. В. Коваля, Ю. М. Козлова, та інших вчених.

Заборона здійснення корупційних діянь в Україні передбачена Законом «Про запобігання корупції». Згідно зі ст. 1 цього закону, корупційне правопорушення - умисне діяння, що містить ознаки корупції, за яке законом передбачено кримінальну, адміністративну, цивільно-правову та дисциплінарну відповідальність. Під корупцією закон розуміє використання суб'єктами відповідальності їх службових повноважень та пов'язаних із цим можливостей з метою одержання неправомірної вигоди або прийняття обіцянки (пропозиції) такої вигоди

для себе чи інших осіб. Неправомірною вигодою є грошові кошти або інші переваги, пільги, послуги, нематеріальні активи, які обіцяють, пропонують, надають або одержують без законних на те підстав.

Відповідно до Закону «Про запобігання корупції», суб'єктами відповідальності за корупційні правопорушення в Україні є: особи, уповноважені на виконання функцій держави або місцевого самоврядування (у тому числі Президент України, народні депутати, урядовці, судді); посадові особи юридичних осіб публічного права, які одержують заробітну плату за рахунок державного чи місцевого бюджету; особи, які надають публічні послуги (аудитори, нотаріуси, експерти, арбітражні керуючі, третейські судді тощо); посадові особи іноземних держав, міжнародних організацій; посадові особи і працівники юридичних осіб (у разі одержання ними неправомірної вигоди або надання ними такої вигоди особам, зазначеним вище) тощо. Досить широке коло суб'єктів правопорушення вимагає прискіпливого аналізу та контролю за діяльністю правоохоронних органів як в середини держави, так і за її межами.

Наразі створено цілий ряд органів державної влади, які покликані зробити наше суспільство і державу вільними від корупції: центральний орган виконавчої влади України зі спеціальним статусом - Національне агентство з питань запобігання корупції [2]; Урядовий уповноважений з питань антикорупційної політики [3] - посадова особа Кабінету Міністрів України, яка забезпечує підготовку і подання пропозицій щодо спрямування і координації роботи органів виконавчої влади із запобігання і протидії корупції тощо.

Національне антикорупційне бюро України створено відповідно до Закону України «Про Національне антикорупційне бюро» 2014 року. Цим Законом визначно, що воно є державним правоохоронним органом, на який покладається попередження, виявлення, припинення, розслідування та розкриття корупційних правопорушень, віднесених до його підслідності, а також запобігання вчиненню нових.

Головне завдання Національного антикорупційного бюро вже дещо звужує коло корупційних деліктів, говорячи про протидію суто кримінальним корупційним правопорушенням, які вчинені вищими посадовими особами, уповноваженими на виконання функцій держави або місцевого самоврядування, та становлять загрозу національній безпеці [4].

Компетенцією Національного антикорупційного бюро України є широкий спектр повноважень щодо запобігання, припинення та розслідування кримінальних корупційних правопорушень, зокрема:1) здійснення оперативно-розшукових заходів з метою попередження, виявлення, припинення та розкриття кримінальних правопорушень, віднесених законом до його підслідності, а також в оперативно-розшукових справах, витребуваних від інших правоохоронних органів; 2) здійснення досудового розслідування кримінальних правопорушень, віднесених законом до його підслідності, а також проводення досудового розслідування інших кримінальних правопорушень у випадках, визначених законом; 3) вжиття заходів щодо розшуку та арешту коштів та іншого майна, які можуть бути предметом конфіскації або спеціальної конфіскації у кримінальних правопорушеннях, віднесених до підслідності Національного бюро, здійснення діяльності щодо зберігання коштів та іншого майна, на яке накладено арешт; 4) взаємодія з іншими державними органами, органами місцевого самоврядування та іншими суб'єктами для виконання своїх обов'язків; 5) здійснення інформаційно-аналітичної роботи з метою виявлення та усунення причин і умов, що сприяють вчиненню кримінальних правопорушень, віднесених до підслідності Національного бюро; 6) забезпечення особистої безпеки працівників Національного бюро та інших визначених законом осіб, захист від протиправних посягань на осіб, які беруть участь у кримінальному судочинстві, у підслідних йому кримінальних правопорушеннях; 7) забезпечення на умовах конфіденційності та добровільності співпраці з особами, які повідомляють про корупційні правопорушення.

Також до їх повноважень відносять і кадрові питання. Адже від нього залежить ефективність діяльності і органу, і системи, і держави. Вдосконалення публічної служби, забезпечення більш прозорої процедури, що стосуються допуску до публічної служби, просування по службі, звільнення з неї, оцінка діяльності публічних службовців, впровадження системи обертання на публічну службу - такі кроки наближають суспільство до без корупційної дійсності. Інституціональні механізми і правила, що регулюють вступ на публічну службу повинні бути поліпшені, і допуск до будь-яких сфер публічної служби має бути є прозорим, проведеним на основі конкурсу.

Паралельно слід приділити увагу здійснення заходів, спрямованих на підвищення авторитету публічної служби,

здійсненні спеціальних програм для підтримки та стимулювання публічних службовців. Але соціальні та трудові гарантії повинні корелюватись з вимогою підвищення професійних знань і навичок співробітників Національного антикорупційного бюро України щодо виявлення, розслідування і кримінального переслідування корупціонерів. Відтак, проведення оперативно - розшукових заходів, спрямованих на виявлення корупційних злочинів буде більш ефективним. Вважається, що забезпечення співробітників правоохоронних органів високими зарплатами є одним з основних факторів у боротьбі з корупцією. Проте і контроль за їх діяльністю, а відтак і небезпека втрати посади публічним службовцем Національного антикорупційного бюро України має бути реальною. Тоді можна казати про таку пряму залежність.

Заходи Національного антикорупційнго бюро України у сфері боротьби з корупцією, а також обов'язки та повноваження державних органів у цій сфері здійснюється відповідно до принципів верховенства права, поваги до прав і свобод людини і громадянина. Основними напрямами подальшого удосконалення роботи системи антикорупційних державних органів мають стати: надання громадськості інформацію про свою діяльність.

Таким чином, корупція завжди залишалася однією з найсерйозніших проблем України. Після Революції гідності Україна залишалася найбільш корумпованою країною Європи: за результатами глобального Індексу сприйняття корупції 2016 (Corruption Perceptions Index) країна посідає 131 місце зі 176. Отже, Україна залишається тотально корумпованою державою. Існуючий механізм протидії корупційним проявам в Україні є неефективним.

Список використаних джерел:

1. Настюк В. Я Корупція, відповідальність, компроміс: адміністративні та кримінально-правові аспекти : монографія. Х. : Право, 2010. 152 с.
2. Про утворення Національного агентства з питань запобігання корупції : Постанова Кабінету Міністрів України від 18 березня 2015 р. № 118. URL: http://zakon2.rada.gov.ua/laws/show/118-2015-%D0%BF (дата звернення 12.10.2017).
3. Про затвердження структури Секретаріату Кабінету Міністрів України Постанова Кабінету Міністрів України від 23.08.2016 № 564. URL: http://zakon3.rada.gov.ua/laws/show/564-2016-%D0%BF (дата звернення 12.10.2017).

4. Про Національне антикорупційне бюро України Верховна Рада України; Закон від 14.10.2014 № 1698-VII. URL: http://zakon2.rada.gov.ua/laws/show/1698-18 (дата звернення 12.10.2017).

Одержано 19.10.2017

УДК 343.9 : 681.142 + 351.745.5(477)

Вадим Анатолійович КУДІНОВ,
кандидат фізико-математичних наук, доцент, професор кафедри інформаційних технологій та кібернетичної безпеки Національної академії внутрішніх справ

ЩОДО МОЖЛИВОСТІ ПІДГОТОВКИ В НАЦІОНАЛЬНІЙ АКАДЕМІЇ ВНУТРІШНІХ СПРАВ ФАХІВЦІВ З ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Сьогодні комп'ютерні та телекомунікаційні технології охопили майже всі сфери життєдіяльності суспільства і держави. Але становлення інформаційного суспільства відбувається не без проблем, найсуттєвішою з яких слід вважати кіберзлочинність. Спектр кіберзлочинів різноманітний – від створення комп'ютерних вірусів, вчинення крадіжок, різних видів шахрайства, комп'ютерних підробок до порушення авторських прав та розповсюдження дитячої порнографії. Зазвичай кіберзлочини мають корисливу спрямованість й відрізняються високим рівнем латентності й анонімності.

Сьогодні жертвами осіб, які вчиняють злочини у віртуальному просторі, можуть стати не лише окремі люди чи юридичні особи, а й цілі відомства і навіть держави. Зареєстровані випадки так званого кібертероризму, коли комп'ютер використовувався для блокування важливих систем життєзабезпечення та створення загрози для цілих груп населення. Для України, як однієї з найбільших європейських держав, де у повсякденне життя стрімко входять нові комунікативні технології, зокрема, ті, що розширюють можливості реалізації товарів і послуг за допомогою мережі Інтернет, проблема кіберзлочинності не обходить жодним чином.

Таким чином, для України проблема поширення кіберзлочинності сьогодні є вельми актуальною й такою, що вимагає невідкладного вирішення. Кіберзлочинність, без перебільшення, стала одним з основних викликів, що постають перед сучасним суспільством. Тому нагальними є питання щодо якісної підготовки фахівців-правоохоронців з протидії кіберзлочинності [1; 2].

В Національній академії внутрішніх справ є досвід підготовки таких фахівців [3]. Протягом 2011-2014 років в академії було підготовлено належним чином понад 80 спеціалістів (4 навчальні групи) у сфері протидії кіберзлочинності. Станом на сьогодні більшість з них працює за фахом.

Після незначної перерви, що пов'язана з питаннями реформування вишу у відповідності до вимог сьогодення, в Національній академії внутрішніх справ відновлюється підготовка фахівців-правоохоронців з поглибленим вивченням інформаційно-комунікаційних технологій, питань кібербезпеки та протидії кіберзлочинності. Так, зокрема, для спеціально відібраних за конкурсом курсантів 4-х курсів планується викладання таких навчальних дисциплін: «Сучасні комп'ютерні системи та інформаційні технології», «Основи побудови телекомунікаційних систем та мереж», «Основи забезпечення кібербезпеки, захисту інформації та протидії кіберзлочинності», «Основи інформаційно-аналітичної підтримки діяльності органів та підрозділів поліції». Низка провідних Департаментів, Управлінь Національної поліції, МВС України вже сьогодні виявили зацікавленість в отриманні даних фахівців у свої підрозділи.

На сьогодні Національна академія внутрішніх справ може бути одним з провідних навчальних закладів системи МВС України щодо підготовки фахівців-правоохоронців у галузі інформаційно-комунікаційних технологій, протидії кіберзлочинності та торгівлі людьми. Це пов'язано з багатьма факторами, зокрема: 1) наявністю в академії науково-педагогічного складу високої кваліфікації; 2) наявністю вагомих наукових та навчально-методичних доробок працівників вишу з зазначеної тематики; 3) наявністю потужної матеріально-технічної бази, що відповідає сучасним вимогам для якісної підготовки фахівців-правоохоронців; 4) наявністю в м. Києві безпосередніх замовників зазначених фахівців-правоохоронців – Департаментів, Управлінь Національної поліції, МВС України, представники яких будуть залучатися до освітнього процесу в академії; 5) наявністю в м. Києві низки провідних вишів, фахівці яких також планується залучати до проведення бінарних занять з курсантами в рамках спільних угод; 6) тісна співпраця академії з Міжвідомчим науково-дослідним центром з проблем боротьби з організованою злочинністю при РНБО України та Державним науково-дослідним інститутом МВС України, працівники яких мають значні успіхи в дослідженні зазначеної тематики; 7) значної кількості міжнародних, міжвідомчих та

міжвузівських заходів (науково-практичних конференцій, семінарів, круглих столів, тощо) в м. Києві з цієї тематики; 8) інші підстави.

Отже, на часі в академії: популяризація ідей і методів ІТ-безпеки як складової національної безпеки; розробка та впровадження в освітній процес нових спеціальних дисциплін та спецкурсів з протидії кіберзлочинності; взаємозв'язок освітнього процесу з науковими дослідженнями; спрямованість навчання на поглиблену теоретичну підготовку ІТ-фахівців з найбільш загальних аспектів безпеки поряд із акцентом на практичне застосування; орієнтація на вивчення конкретних програмно-технічних засобів протидії кіберзлочинності та торгівлі людьми; розширення міжнародних та міжвузівських зв'язків у сфері протидії кіберзлочинності та торгівлі людьми.

Список використаних джерел:

1. Кудінов В. А., Орлов Ю. Ю. Підготовка фахівців з протидії кіберзлочинності. *Бюлетень з обміну досвідом роботи МВС України.* 2011. № 188. С. 23-34.
2. Кудінов В.А. Вирішення проблем добору та підготовки кадрів правоохоронців щодо протидії кіберзлочинам. *Кадровий вісник, науково-виробничий журнал.* 2011. № 1(1). С. 51-68.
3. Кудінов В. А. Організація підготовки фахівців із розслідування кіберзлочинів в Україні в Національній академії внутрішніх справ // Актуальні питання підготовки фахівців із розслідування кіберзлочинів: збірник матеріалів «круглого столу» (Київ, 25 листопада 2011 р.). К. : Наук.-вид. відділ Нац. акад. СБ України, 2012. С. 101-107.

Одержано 01.11.2017

УДК 159.922

Павло Валентинович МАКАРЕНКО,
кандидат психологічних наук, доцент, заступник декана з навчально-методичної роботи факультету № 4 Харківського національного університету внутрішніх справ

Станіслав Олександрович ЛАРІОНОВ,
кандидат психологічних наук, доцент, доцент кафедри педагогіки та психології факультету № 3 Харківського національного університету внутрішніх справ

ПСИХОЛОГІЧНІ АСПЕКТИ СТАВЛЕНЬ МАЙБУТНІХ ПРАЦІВНИКІВ КІБЕРПОЛІЦІЇ ДО ЯВИЩ СОЦІАЛЬНО-ПРОФЕСІЙНОГО ОТОЧЕННЯ

Кіберполіція в Україні є новою правоохоронною службою, професійна діяльність працівників якої є ще недостатньо вивченою в науковому плані. Підготовка працівників кіберполіції здійснюється у відомчих вишах МВС України двома шляхами: перепідготовки фахівців ІТ-сфери з наявною вищою освітою та підготовки курсантів за першим рівнем вищої освіти в умовах специфічного навчального середовища.

Обидва шляхи є перспективними і доцільними, але мають і певні недоліки. Так, щодо ІТ-фахівців, складно прогнозованою є їх професійна надійність, яка ґрунтується в основному на мотивації служіння і пошуку нових вражень, адже вони обрали професію із явно нижчою оплатою праці, ніж це можливо для кваліфікованого спеціаліста у цивільних фірмах. Стійкість такої мотивації незначна, а отже прогноз стабільності і надійності їх праці – сумнівний. Професійна надійність курсантів ВНЗ МВС, принаймні перші роки після випуску, не викликає сумнівів. Але, їх професійна готовність явно поступається «дорослим» колегам, тобто їх необхідно доучувати вже на робочому місці. Для успіху цього процесу неабияке значення має те, як саме майбутні кіберполіцейські ставляться до важливих об'єктів і явищ соціально-професійного оточення: до громадян, законів, злочинців, своїх прав і обов'язків, врешті решт до себе самих. Ці ставлення, разом з іншими, утворюють цілісну систему ставлень курсанта, яка багато в чому визначає його професійне мислення, готовність до певної поведінки у професійній площині.

У дослідженні взяли участь 40 курсантів 3 курсу Харківського національного університету внутрішніх справ, які навчаються за спеціальністю «Протидія кіберзлочинності» з них 10

дівчат та 30 юнаків віком 19-21 років. Групи дослідження були сформовані за статтю.

Емпіричне дослідження ставлень курсантів здійснювалось з використанням методів суб'єктивного шкалювання та колірного тесту ставлень Бажина-Еткінда.

На першому етапі було складено контрольний список понять, що позначають окремі об'єкти і явища соціально-професійного оточення (загалом 64 поняття, далі в тексті). Вказані поняття були оцінені досліджуваними за низкою семибальних шкал: «Важливі / не важливі», ««Позитивні / негативні», «Приємні / не неприємні», «Звичні / не звичні», «Прості / складні» та ін.

На другому етапі емпіричного дослідження, зазначений список понять був оцінений досліджуваними за допомогою процедури колірного тесту ставлень. Отримана в результаті прямокутна матриця рангових позицій понять була піддана процедурі багатовимірного шкалювання.

Аналіз результатів дослідження базувався на припущенні про те, що самооцінка ставлень відбувається на двох рівнях: свідомому, декларативному, на якому «працює» суб'єктивне шкалювання; неусвідомленому, емоційному, на якому через стимул-колір «працює» колірний тест ставлень (КТС).

За таких умов існують три ймовірні ситуації відносно кожного окремого ставлення:

а) несуперечливе ставлення, при якому свідома, декларативна оцінка важливості явища, отримана за допомогою суб'єктивного шкалювання не суперечить емоційній оцінці явища, отриманій за допомогою колірного тесту ставлень;

б) суперечливе ставлення, при якому явище декларується як важливе, але виявляється неважливим в КТС;

в) суперечливе ставлення, при якому явище декларується як неважливе, але виявляється важливим в КТС.

Несуперечливі, узгоджені ставлення можна вважати стійкими, усталеними, вони не викликають внутрішнього напруження, а отже – не схильні змінюватись. Суперечливі ставлення, навпаки, є нестійкими, адже характеризуються протиріччями між знаннями про об'єкт та його емоційною оцінкою («знаю, що погано, але подобається», або «знаю, що добре, але не подобається»).

Найбільш стійкими, внутрішньо несуперечливими є ставлення дівчат до (ранг шкалювання / ранг КТС): життя в цілому (6/3); невдача (56/60); здоров'я (5/6); успіх (12/11); Я-

ідеальна (24/22); алкоголь (64/51); паління (62/56); правопорушники (58/61); злочинці (59/64); батько (15/17); мати (4/5); працівники поліції (50/53); курсові офіцери (55/54); навчальна література (46/49); агресія (61/62); брехня (60/63); гаджети і техніка (32/33); розумова праця (27/23); інтернет (31/35); громадянські обов'язки (34/31). Можна вважати, що за умови того, що ці ставлення не отримають свого розвитку у нових ситуаціях життя, вони будуть незмінними, і будь-які виховні й інші дії не матимуть на них впливу. Деяка частина ставлень звичайно зміниться, як це відбудеться, наприклад, зі злочинцями і правопорушниками, коли курсанти почнуть стажування на посадах в підрозділах поліції та «познайомляться» з ними.

Аналізуючи наявність суперечливих ставлень у групі дівчат, визначена група об'єктів, які декларуються важливими, але не є такими насправді, використовуються для підтримки «соціального обличчя». Серед них: теперішнє (9/25); майбутнє (1/10); майбутній чоловік (2/9); діти (3/18); відпочинок (10/21); самоосвіта (8/14).

Також існує група понять, які декларуються дівчатами як неважливі, але виявляються такими щодо емоційної оцінки, тобто їх значимість не усвідомлюється або приховується досліджуваними. Це: минуле (48/19); власна зовнішність (14/1); власні розумові здібності (17/8); друзі (16/2); майбутня професія (13/4); прикраси, предмети розкоші (35/15); національні традиції (42/20); українська мова (41/27). Саме в межах цих явищ здається доцільною і перспективною будь-яка просвітницька, виховна, психологічна та інші види соціальної роботи з курсантами-дівчатами.

Найбільш стійкими, усталеними у групі юнаків є ставлення до (ранг шкалювання / ранг КТС): життя в цілому (8/6); теперішнього (11/7); невдач (61/62); успіху (4/1); власної зовнішності (23/21); алкоголю (63/50); паління (64/63); людей (45/48); правопорушників (60/55); майбутньої дружини (18/22); агресії (57/56); їжі (13/16); фізичної праці (41/45); розумової праці (24/29); відпочинку (15/18). Таких понять значно менше, ніж у групі дівчат, загалом система ставлень юнаків відрізняється значно більшою неузгодженістю, внутрішньою суперечливістю, напруженістю.

Аналізуючи наявність суперечливих ставлень у групі юнаків, визначена група об'єктів, які декларуються важливими, але не є такими насправді, використовуються для підтримки

«соціального обличчя». Серед них окремо слід виділити такі, розбіжність між якими дуже велика, це: майбутнє (1/61); власні розумові здібності (10/36); особи протилежної статі (12/34); закони (25/59); служба (27/64); викладачі (29/60); українська мова (26/44). Ставлення до цих явищ у юнаків напружене, ймовірно вони знаходяться в процесі кризи їх переоцінки, оцінюють їх негативно, але не можуть цього показати.

Серед явищ соціально-професійного оточення, що характеризуються суперечливим ставленням, але не настільки напруженим, слід вказати: майбутню професію (9/23); практику (7/19); вищу освіту (5/14); самоосвіту (16/24); громадянські обов'язки (32/47). Важливість і значимість цих речей юнаками декларується більшою мірою, ніж воно є насправді.

Визначено групу явищ, які декларуються юнаками як неважливі, але виявляються такими щодо емоційної оцінки, тобто їх значимість не усвідомлюється або приховується досліджуваними. Такими є: Я-ідеальний (39/17); батько (2/17); діти (4/19); одяг і взуття (3/42); прикраси і предмети розкоші (30/50); дозвілля і хобі (9/21). Викликає занепокоєння, що і цьому переліку знаходяться явища, які мають високі рангові позиції за емоційною оцінкою. Виявляється, що у досліджених юнаків-курсантів лише успіх і декларується важливим і є таким насправді, а ось особистісну значимість решти трьох найважливіших явищ (батько, одяг і взуття, діти), вони чомусь приховують.

Проведене дослідження гендерних особливостей ставлень курсантів поліції до явищ соціально-професійного оточення засвідчило принципову можливість оцінки, кількісного і якісного аналізу особливостей системи ставлень курсантів поліції засобами психологічної діагностики. Воно дозволило сформулювати найбільш істотні, на нашу думку, аспекти систем ставлень курсантів поліції різної статі:

1. Система ставлень дівчат курсантів третього курсу навчання вирізняється більшою, ніж у юнаків стійкістю і внутрішньою узгодженістю. Важливість і значимість більшої частини досліджуваних об'єктів і явищ соціально-професійного оточення однаковою мірою і декларується дівчатами і сприймається на рівні особистих переконань.

У юнаків-курсантів, навпаки, система ставлень більш мінлива, неузгоджена. Більша частина об'єктів і явищ соціально-професійної дійсності сприймається ними суперечливо, ви-

кликаючи внутрішню напруженість і незадоволеність собою і оточенням.

2. Дівчата-курсанти виявляються більш незрілими у сфері професійних ставлень, очікування від майбутньої професії у них не сформовані. При цьому вони переважно орієнтовані на здійснення сімейних ролей, задоволені собою, що звужує перспективи саморозвитку.

Юнаки-курсанти, навпаки, незадоволені собою і більш націлені на досягнення життєвого й професійного успіху, а ставлення до професійної сфери у них є більш зрілими.

Список використаних джерел:

1. Гіренко С. П., Ларіонов С. О. Стан, перспективи та досвід формування конфліктологічної культури майбутніх працівників патрульної та кіберполіції. *Право і безпека.* 2016. №4(63). С. 121-127.
2. Кузнецов М. А., Ларионов С. А, Макаренко П. В. Эмпирические методы исследования системы отношений личности. В*існик ХНПУ імені Г.С. Сковороди.* Сер. Психологія. Вип. 51. 2015. С. 128-140.
3. Ларіонов С. О., Гончарова Г. О. Система ставлень особистості: теоретичні аспекти дослідження. *Право і безпека.* 2017. №1(64). С. 130-134.
4. Ломов Б. Ф. Психическая регуляция деятельности : избранные труды. М. : Ин-т психол. РАН, 2006. 624 с.
5. Мясищев В. Н. Психология отношений : избр. психол. тр. М. : Ин-т практ. психологии, 1995. 356 с.

Одержано 30.10.2017

Актуальні питання протидії кіберзлочинності та торгівлі людьми.
Харків, 2017

РОЗДІЛ 5.
МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 341.1.8

Вікторія Володимирівна АРЕНДАР,
слухач магістратури факультету № 3 Харківського національного університету внутрішніх справ

Андрій Васильович ВОЙЦІХОВСЬКИЙ,
кандидат юридичних наук, доцент, професор кафедри конституційного і міжнародного права факультету № 4 Харківського національного університету внутрішніх справ

КІБЕРТЕРОРИЗМ ЯК ЗАГРОЗА МІЖНАРОДНІЙ БЕЗПЕЦІ

Розвиток інформаційних технологій призвів до масового використання у всьому світі мережі Інтернет. Остання є не тільки важливою сполучною ланкою між різними світовими культурами, але й важливим інструментом для обміну політичної, економічної, торгової, споживчої інформації.

Число активних користувачів Інтернету невпинно зростає, чим користуються різні злочинні елементи з метою розширення свого впливу на суспільну свідомість, поширення насильницької інформації, провокаційних заяв і т.п. Тому, з появою мережі Інтернет виникла одна з найбільш небезпечних різновидів кіберзлочинності – кібертероризм.

Що стосується визначення кібертероризму, то міжнародна спільнота ще не сформувала єдиного розуміння. Баррі Коллін, старший науковий співробітник Каліфорнійського інституту безпеки та розвідки, в 1980 році вперше вжив термін «кібертероризм». Відтоді учені стали аналізувати його як явище. Представник ФБР США, агент М. Поллітт, визначив цей вид тероризму як «навмисні політично мотивовані атаки на інформаційні комп'ютерні системи, комп'ютерні програми і дані, виражені в застосуванні насильства по відношенню до цивільних цілей з боку субнаціональних груп або таємних агентів».

Кібертероризм представляє велику загрозу інформаційній безпеці держави. Адже кібератаки націлені не тільки на пасивний збір даних, але й на незаконне заволодіння фінансовою і секретною інформацією, на отримання несанкціонованого доступу до апаратури контролю над космічними приладами, си-

стемами водопостачання та розподілу електроенергії, ядерними електростанціями, воєнними комплексами та ін.

На сьогодні протидією кібертероризму на міжнародному рівні займаються окремі міжнародні організації. Це Підрозділ по боротьбі з тероризмом ОБСЄ і Інтерпол. У рамках у ЄС розпочав роботу Центр по боротьбі з кіберзлочинністю. Країничлени ЄС і європейські інституції мають намір підтримувати Центр по боротьбі з кіберзлочинністю для створення оперативних і аналітичних можливостей її розслідування і для співпраці з міжнародними партнерами [1, с.58].

Крім того, задля протидії різним проявам кіберзлочинності, НАТО створив Технічний центр Сил реагування на комп'ютерні інциденти (NCIRC). NCIRC розробляють умови співробітництва, які зрештою відкриють доступ до спеціальних знань в усіх сферах кібербезпеки, а також рекомендації щодо реагування НАТО на прохання країн Альянсу і партнерів про допомогу в захисті їхніх інформаційних і комунікаційних систем [2, с.182].

Для більш ефективної протидії кібертероризму Єврокомісія пропонує створити нове відомство ЄС з кібербезпеки, а також розробити і ввести в Європі єдину систему сертифікації, яка дозволить гарантувати безпеку використання товарів і послуг у цифровому середовищі. Нове відомство пропонується створити на основі вже наявного і розташованого в Афінах Європейського агентства мережної та інформаційної безпеки (Enisa), розширивши його і наділивши новими повноваженнями. «Кібератаки стали все частішими, більш глобальними, витонченими, і Європа має бути спроможною протистояти цим атакам цілодобово у всіх країнах ЄС», - комісар ЄС з цифрової економіки та суспільства Андрус Ансіп.

Єдину систему сертифікації пропонують поширити на побутові прилади, автомобілі та будь-які пристрої, здатні підключатися до Інтернету. Сертифікати допоможуть споживачам у Європі розпізнавати, чи відповідають товари, які вони планують придбати, європейським стандартам безпеки [3].

Таким чином, потрібно усвідомити, що для ефективної протидії кібертероризму потрібна плідна міжнародна співпраця багатьох країн світу як на державному рівні, так і на рівні співробітництва між урядовими організаціями та представниками бізнесу у сфері розповсюдження ІТ-технологій.

Першочерговими завданнями для світової спільноти ми вбачаємо в: постійному удосконаленні законодавства у сфері

інформаційної безпеки держав; систематичному збирання та аналізі даних про потенційні кібертерористичні загрози; розробці якісних технологій захисту від кібернападів; встановлення заборон на використання у різних сферах не захищеного належним чином програмного забезпечення; введення єдиної системи сертифікації на побутові прилади, автомобілі та будь-які пристрої, здатні підключатися до мережі Інтернет.

Список використаних джерел:

1. Яцик Т. П. Особливості інформаційного тероризму як одного із способів інформаційної війни *Науковий вісник Національного університету державної податкової служби України (економіка, право)*. 2014. № 2. С.55-60.
2. Войціховський А. В. Діяльність НАТО у боротьбі з кіберзлочинністю // Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності: матеріали міжн. наук.-практ. конф. (Харків, 12 лист. 2014 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків: Права людини, 2014. С. 181-184.
3. 3. В Євросоюзі створять відомство з кібербезпеки // Корреспондент.net. 19.09.2017. URL: http://ua.korrespondent.net/world/3887910-v-yevrosouizi-stvoriat-vidomstvo-z-kiberbezpeky (дата звернення: 28.10.2017).

Одержано 30.10.2017

УДК 343.1

Тетяна Юріївна БУНДЮК,
студентка 10 факультету 4 курсу 1 групи Національного юридичного університету імені Ярослава Мудрого

ПРОТИДІЯ ТОРГІВЛІ ЛЮДЬМИ: МІЖНАРОДНИЙ ДОСВІД ТА УКРАЇНСЬКІ РЕАЛІЇ

Україна стала третьою в світі державою (після Німеччини та Бельгії) та першою на пострадянському просторі, яка криміналізувала торгівлю людьми.

На сьогодні, диспозиція статті 149 Кримінального кодексу України передбачає кримінальну відповідальність за торгівлю людьми або здійснення іншої незаконної угоди, об'єктом якої є людина, а так само вербування, переміщення, переховування, передача або одержання людини, вчинені з метою експлуатації шляхом обману, шантажу чи уразливого стану особи [1].

У вересні 2011 року було прийнято Закон України «Про протидію торгівлі людьми», який суттєво наблизив українське законодавство до міжнародних стандартів в сфері протидії торгівлі людьми. Ним визначаються організаційно-правові засади протидії торгівлі людьми, основні напрями державної політики та засади міжнародного співробітництва у цій сфері, повноваження органів виконавчої влади, порядок встановлення статусу осіб, які постраждали від торгівлі людьми, та порядок надання їм допомоги [2].

Однак, незважаючи на позитивні зміни законодавства України у сфері протидії торгівлі людьми, проблемні аспекти правового регулювання цього питання так і не вичерпано.

Зокрема, у Законі України «Про протидію торгівлі людьми» не відображені усі положення Конвенції Ради Європи про заходи щодо протидії торгівлі людьми. Так, наприклад, не застосовується термін «встановлення періоду реабілітації та обмірковування» для осіб, стосовно яких є підстави вважати, що вони є жертвами торгівлі людьми, не встановлено механізм з'ясування безпечності повернення особи до країни походження та не сформульовані положення щодо виплати компенсацій постраждалим від торгівлі людьми, формування спеціального фонду компенсації особам, постраждалим від торгівлі людьми, як того вимагає ст. 15 Конвенції.

Також Законом не передбачено можливості притягнення юридичної особи до кримінальної відповідальності за торгівлю людьми. Більше того, вчинення юридичною особою такого злочину не є підставою для позбавлення такої юридичної особи ліцензії на здійснення зазначеного в ній виду діяльності.

Отже, ці та інші суперечності українського законодавства потребують подальшого дослідження та опрацювання [3].

З приводу цього, доцільним для України є застосування зарубіжного досвіду імплементації міжнародних стандартів у національне законодавство.

Так, ми вважаємо, що цікавим для України є досвід Німеччини з використання чотирьох стандартних баз даних, у яких міститься інформація щодо фактів торгівлі людьми: статистика злочинів, куди вносяться дані поліцейських розслідувань; звіти щодо ситуації у зв'язку з існуванням явища торгівлі людьми, які складаються Федеральним бюро кримінальних розслідувань Німеччини; статистика по справах, що передані до суду; центральний реєстр кримінальних справ, що містить інформацію щодо стосовно розглядів.

Здійснення такої чіткої фіксації усієї інформації у сфері протидії торгівлі людьми дає змогу не лише швидко знаходити потрібну інформацію, а й усунути безліч зайвих дій, що здійснюються працівниками правоохоронних органів нашої держави у пошуку прецедентних кримінальних справ, осіб, причетних до скоєння таких злочинів, а також розгляду зазначеної категорії справ у судах.

Для України створення таких баз даних є необхідністю, оскільки судовий розгляд багатьох справ затягується, а вироки часто не відповідають реальному ступеню завданої злочином шкоди та наслідків, і довести таку невідповідність стає дуже складно. До того ж існування таких баз суттєво спрощує процедуру пошуку й фіксації речових доказів та в цілому підвищує рівень можливостей у протидії торгівлі людьми.

Також, актуальною, для перейняття Україною, вважаємо політику Білорусі, яка полягає в підвищенні ефективності протидії торгівлі людьми шляхом комплексного й скоординованого запровадження необхідних заходів як на міжнародному, так і на національному рівні. Завдяки чому торгівля людьми у Білорусі не отримує значних масштабів [4].

Але, як відомо, у боротьбі з торгівлею людьми досить часто традиційні засоби безсилі або малоефективні. Для України однією зі складних проблем є використання оперативно-розшукових даних у викритті трафікерів, хоча за кордоном (Німеччина, США) давно застосовують порядок проведення "особливих" слідчих дій (використання агентів під прикриттям тощо), що здійснюються лише за дорученням прокурора або слідчого судді й органом, який не бере участі у розслідуванні конкретної справи.

Отже, зважаючи на вищевикладене, з огляду на умови складної воєнної обстановки та проведення в Україні антитерористичної операції, досить повільні темпи реформування системи соціального захисту, значна частина людей залишається під загрозою потенційної підвищеної віктимності. Тому нашій державі необхідним є виділення протидії торгівлі людьми як одного із пріоритетних напрямів державної політики, а також запозичення зарубіжного досвіду створення реально діючої та ефективної системи протидії цьому явищу.

Список використаних джерел:

1. Кримінальний кодекс України від 5 квітня 2001 року. URL: http://zakon5.rada.gov.ua/laws/show/2341-14. (дата звернення: 10.10.2017).

2. Про протидію торгівлі людьми. Закон України від 20.09.2011 № 3739-VI. URL: http://zakon5.rada.gov.ua/laws/show/3739-17. (дата звернення: 10.10.2017).
3. Наскільки законодавство України у сфері протидії торгівлі людьми відповідає міжнародним стандартам? URL: http://www.lastrada.org.ua/ucp_mod_news_list_show_274.html. (дата звернення: 10.10.2017).
4. Кушнір О. Міжнародні стандарти протидії торгівлі людьми. URL: http://goal-int.org/mizhnarodni-standarti-protidii-torgivli-lyudmi/. (дата звернення: 10.10.2017).

Одержано 17.10.2017

УДК 351.74

Олексій Олександрович ДЕРЕВЯГІН,
кандидат юридичних наук, старший науковий співробітник, доцент кафедри оперативно-розшукової діяльності та розкриття злочинів факультету № 2 Харківського національного університету внутрішніх справ

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ, ЯК СКЛАДОВА ЗАБЕЗПЕЧЕННЯ МІЖНАРОДНОЇ БЕЗПЕКИ

Питання пошуку шляхів протидії злочинам з використанням інформаційно-комунікаційних систем уже тривалий час знаходиться у сфері уваги як державних правоохоронних органів, так й міжнародної спільноти. Беручи до уваги, що розвиток інформаційних технологій йде швидше ніж приймаються нормативно-правові акти, якими вони регулюються, а об'єми незаконно одержаних коштів кіберзлочинцями зростають, необхідно на постійній основі знаходити шляхи вирішення нових задач, пов'язаних з такими сферами, як захист даних, транскордонний доступ правоохоронних служб до даних та обмін інформацією між державними та приватними структурами тощо.

Цілком зрозуміло, що міжнародні організації виказують стурбованість з цього приводу та відзначають необхідність скоординованої міждержавної взаємодії при розслідуванні кіберзлочинів. Саме завдяки роботі таких міжнародних організацій, як Організація економічного співробітництва і розвитку (далі – ОЕСР), Інтерпол, Група Восьми (далі – G8), Рада Європи, ООН, розвивається міжнародна співпраця країн у сфері протидії кіберзлочинності, формується міжнародне законодавство. Проте для розробки і впровадження міжнародно-правових норм в національне законодавство вкрай необхідно сформу-

лювати єдиний підхід до розуміння, як єдиних завдань, вироблення загальних принципів, так і визначення пріоритетних напрямів вирішення наявних проблем.

Неузгоджений підхід у кримінальному законодавстві різних держав до формулювання конкретних складів злочинів не сприяє ефективній протидії комп'ютерним злочинам у глобальному масштабі. У зв'язку з цим міжнародно-правове регулювання повинне відігравати головну роль в гармонізації національного кримінального законодавства з міжнародно-правовими актами, розробленими і прийнятими відповідними організаціями.

Крім того, з метою реалізації ефективних заходів протидії кіберзлочинності підрозділами боротьби з кіберзлочинністю Національної поліції України важливо враховувати позитивний досвід правоохоронних органів зарубіжних країн. Так, наприклад, національні законодавства і правоохоронні органи різних країн у своїй діяльності вимушені брати до уваги особливості кордонів, мовні, політичні, релігійні особливості, що впливають на ефективність протидії злочинності в досліджуваній сфері.

Специфічність характеристик вимагає міждержавного підходу до протидії кіберзлочинам, ефективність якого недосяжна без міжнародної співпраці. Необхідно також звернути увагу на те, що досвід розвинених зарубіжних країн говорить про неухильне збільшення із року в рік кількості служб і відомств в сфері протидії кіберзлочинності, тому варто систематично вивчати і переймати їх досвід. Наприклад, у США створені такі відомства, як Electronic Crimes Task Forces ECTF, підрозділ Секретна служба США (United States Secret Service USSS). Ці підрозділи створюють взаємодію між службами, правоохоронними органами (федерального рівня, рівня штату, локальними), приватним сектором, академічним співтовариством і виявляють і запобігають кіберзлочинам.

У Великій Британії боротьбою з кіберзлочинністю займається відділ по боротьбі з кіберзлочинами, що входить до складу Агентства по боротьбі з організованою злочинністю. У ФРН основну діяльність щодо боротьби з кіберзлочинністю здійснює Федеральна кримінальна поліція. У Франції 1 липня 2008 р. шляхом об'єднання двох спецслужб Центрального директорату загальної розвідки (RG) і Директорату стеження за територіями (DST) створено Головне управління внутрішньої розвідки Direction centrale du Renseignement interieur, DCRI.

В Естонії в 2006 р. створено комп'ютерну групу реагування на надзвичайні ситуації (CERT-EE). У Республіці Білорусь Управління по розкриттю злочинів у сфері високих технологій Міністерства внутрішніх справ є самостійним оперативно-розшуковим підрозділом Міністерства, безпосередньо підпорядкованим першому заступникові Міністра внутрішніх справ – начальникові головного управління кримінальної міліції [1].

Власну стратегію щодо вирішення проблем протидії кіберзлочинності розроблено також Європейським поліцейським відомством (Європол). На даний час Європол надає членам ЄС слідчу і аналітичну підтримку через свою систему онлайн-розслідувань і базу даних злочинів. З січня 2013 року під егідою Європолу розпочав діяльність новий Європейський центр боротьби з кіберзлочинністю. Серед пріоритетів Центру – розслідування шахрайства через онлайн-мережі, зокрема у системі електронного банкінгу та інших видах фінансової діяльності, протидія сексуальній експлуатації дітей через Інтернет, а також розслідування інших злочинів, що посягають на безпеку важливої інфраструктури та інформаційних систем ЄС.

Перераховані вище обставини обумовлюють прийняття спеціального законодавства та розробки загальнодержавної комплексної стратегії протидії кіберзлочинності в Україні із урахуванням європейського досвіду, а також визначення основних напрямів діяльності державних органів та органів місцевого самоврядування, інститутів громадянського суспільства, юридичних і фізичних осіб щодо захисту основ конституційного устрою, прав і свобод людини та громадянина, забезпечення цілісності й національної безпеки держави, виявлення і ліквідації причин та умов, що сприяють проявам кіберзлочинності.

З урахуванням зазначених пропозицій та рекомендацій протидія кіберзлочинності в України буде відповідати міжнародним стандартам, що сприятиме покращенню правоохоронної діяльності у сфері інформаційної та економічної безпеки України в цілому.

Список використаних джерел:

1. Интерпол: Киберпреступления являются самой опасной криминальной угрозой. URL: http: //www.virusovnet.org/main/309. (дата звернення: 10.10.2017).

Одержано 30.10.2017

УДК 343.4 : 343.431 : 004.056.53

Сергій Віталійович КАВУН,
Prof., Dr.Sc.(Econ), Ph.D.(CS&E), начальник відділу інформаційних технологій Харківського навчально-наукового інституту Державного вищого навчального закладу «Університет банківської справи»

Наталія Олексіївна ВАКУЛЕНКО,
студентка Харківського навчально-наукового інституту Державного вищого навчального закладу «Університет банківської справи»

МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Безперечно, на сучасному етапі розвитку людського суспільства важливим стратегічним ресурсом, що потребує охорони, є інформація, яка містить надзвичайно широкий спектр зведень: від простих даних про громадян країни до стратегічних державних програм. Тому ці дані все частіше стають предметом злочинних зазіхань. Комплексне і широкомасштабне використання інформаційних технологій на основі персональних комп'ютерів, інформаційно-обчислювальних мереж і комп'ютеризованих комунікаційних систем забезпечило людству вихід на новий етап свого розвитку – етап інформаційного суспільства. Як наслідок – поява нового виду злочинності – комп'ютерної, або кіберзлочинності [7].

Зростання обсягів інформації, комп'ютерних мереж та кількості користувачів, спрощення їх доступу інформації, що циркулює мережами суттєво підвищує ймовірність розкрадання або руйнування цієї інформації.

В даний час значущість проблеми захисту інформаційних ресурсів, у тому числі особистих, визначається наступними факторами:

- розвитком світових і національних комп'ютерних мереж і нових технологій, які забезпечують доступ до інформаційних ресурсів;
- перекладом інформаційних ресурсів на електронні носії й концентрацією їх в інформаційних системах;
- підвищенням «ціни» створюваної та накопиченої інформації, яка є реальним ресурсом соціально-культурного та особистісного розвитку;

- розробкою і вдосконаленням інформаційних технологій, які можуть ефективно використовуватися кримінальними структурами.

Комп'ютерна злочинність стала справжнім бичем економіки розвинених держав. Так, наприклад, 90% фірм і організацій у Великобританії в різний час ставали об'єктами електронного піратства або перебували під його загрозою, у Нідерландах жертвами комп'ютерної злочинності стали 20% різного роду підприємств. У ФРН з використанням комп'ютерів щорічно викрадається інформація на суму 4 млрд євро, а у Франції - 1 млрд євро.

Про проблему торгівлі людьми, два основних моменти: її суспільна небезпечність і її поширеність у світі.

Основними проявами суспільної небезпеки торгівлі людьми, у свою чергу, ґрунтуючись на тому, що загальновідомо про торгівлю, і на те, що доведено в науці, слід визнати:

- перетворення людини в річ, нехтування його прав і свобод;

- первинну і вторинну криміногенність торгівлі людьми:

- первинна: сама торгівля людьми - злочинне діяння;

- вторинна: торгівля людьми - криміногенний фактор, який манить вчинення інших злочинів;

- порушення норм міжнародного та національного законодавства.

Про поширеність такого явища, як торгівля людьми, у світі можна судити на підставі експертних даних, і (або) на підставі статистичних даних про вчинені злочини. Експертні дані зводяться до наступних:

- кількість жертв торгівлі людьми обчислюється в межах від 700 тисяч до 2-4 мільйонів (за даними Уряду США);

- щорічно у світі продають 1,2 мільйона дітей (за даними ЮНІСЕФ);

- тільки в країнах колишнього СРСР щороку жертвами торгівлі людьми стають від 20 тисяч до 700 тисяч чоловік;

- щорічний дохід від торгівлі людьми у світі становить від 6-8 млрд доларів (за даними Інтерполу) до 19 млрд доларів (дані експертів).

Можна виділити основні органи, які займаються розробленням і впровадженням профільних норм міжнародного права у напрямі протидії торгівлі людьми. До них ми включаємо:

- Організацію Об'єднаних Націй;

- Європейський Союз;

- Раду Європи;
- Організацію з безпеки й співробітництва в Європі (ОБСЄ);
- міжнародні міжурядові та неурядові організації, такі як, наприклад, Міжнародна Ліга жінок за мир і свободу, Міжнародна Демократична Федерація жінок, Всесвітня організація за виживання (The Global Survival Network), Фонд проти торгівлі людьми (The Foundation Against Trafficking) та багато інших.

Вважаємо, що розробка та прийняття міжнародних конвенцій, декларацій, інших міжнародно-правових документів у сфері прав людини сприяє загальному визнанню вимог про рівноправність статей. Міжнародні акти, зобов'язуючи держави здійснювати проголошені в них права, виступають як додаткові міжнародно-правові гарантії захисту прав людини. При цьому підкреслимо, що, по-перше, безпосередня регламентація правового становища людини є компетенцією держави та залежить від її соціально-економічного розвитку; по-друге, дотримання міжнародних норм про захист прав, їх впровадження в життя значною мірою залежить від активності самих людей.

На сьогодні приблизно 180 країн мають законодавство, що дозволяє протидіяти проявам торгівлі людьми. Складність та багатогранність цього явища обумовили різні підходи до криміналізації діяння кримінальні кодекси різних країн трактують цей злочин по-різному, в одних країнах торгівля людьми виділена в окремий склад злочину, в інших не виділена в окремий склад та переслідується в рамках інших наявних законів або не переслідується зовсім.

Список використаних джерел:

1. Назаренко Г. В. Кримінальне законодавство: навч. посібник. М. : Нове видання, 2008. 214 с.
2. Модели киберпреступностей. URL: https://goo.gl/BxC5Xu (дата звернення: 23.10.2017).
3. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочиності. URL: https://goo.gl/c8heHE (дата звернення: 23.10.2017).
4. Міжнародні стандарти протидії торгівлі людьми / GOAL. 2014. URL: https://goo.gl/F6D9sp (дата звернення: 23.10.2017).
5. Tosin Osasona. Time to Reform Nigeria's Criminal Justice System, Journal of Law and Criminal Justice. December 2015, Vol. 3, No. 2, pp. 73-79.

6. Ramsaroop P. Cybercrime, Cyberwarfare, Terrorism, and Sabotage: Critical Issues in Data Protection for Health Services Information Pan American Health Organization. Washington, D.C.: PAHO, 2003. 85 p.
7. Струков В. М. До визначення напрямів протидії кіберзлочинності URL: http://bit.ly/2imbPQe (дата звернення: 23.10.2017).

Одержано 01.11.2017

УДК 343.98

Сергій Павлович ЛАПТА,
кандидат юридичних наук, доцент, доцент кафедри криміналістики та судової експертології факультету №1 Харківського національного університету внутрішніх справ

ФБР У БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

Проблема боротьби зі злочинами у кіберпросторі наразі визнається одною із найгостріших серед проблем боротьбі зі злочинністю. Викликано це рядом факторів, які у значній мірі ускладнюють протидію кіберзлочинності. Для того щоб розпочати «бізнес» злочинцям іноді потрібні лише незначні грошові кошти. Злочинці можуть «атакувати» одночасно значну кількість потенційних жертв, рахунок яких іноді йде на сотні тисяч. Відповідно, якщо злочинна діяльність направлена на отримання кримінальних прибутків, вони значно збільшуються порівняно з іншими, традиційними способами. Так, у ході масованої кібератаки із застосуванням вірусу-вимагача Petya, яка відбулася 27 червня 2017 року, тільки в Україні постраждало близько 12,5 тисяч комп'ютерів та вийшла з ладу система радіаційного моніторингу Чорнобильської АЕС. У світі жертвами стали такі гіганти, як британська рекламна компанія WPP; датський бізнес-конгломерат Maersk, який є найбільшим оператором корабельної контейнерної доставки у світі; німецька логістична компанія DHL; американська продуктова компанія Mendelez; група американських госпіталів Heritage Valley Health System. та багато інших [1]. Перед цим, 12 травня 2017 року від вірусу-вимагача WannaCry постраждало більше 300 тисяч комп'ютерів у 150 країнах світу, а злочинці отримали понад 100 тисяч доларів [2].

Є й інші фактори, що ускладнюють протидію кіберзлочинності порівняно із злочинністю традиційною:

- повністю виключений реальний контакт злочинців і жертв;

- у момент вчинення злочину злочинці можуть перебувати, фактично, у будь-якій країні світу;

- співучасники кіберзлочинів можуть не знати один одного особисто.

Усі ці моменті значно ускладнюють викриття кіберзлочинців та притягнення їх до кримінальної відповідальності.

Знаходячись на передньому краї боротьби із злочинами у мережі Інтернет, США визначилися із основними напрямами такої боротьби та з розподілом обов'язків і сфер відповідальності державних агенцій. Так, у 2016 році були прийняті Національний план з протидії кіберзлочинності [3] та Директива-41 Президентської політики (PPD-41) [4]. У них Федеральному бюро розслідувань (ФБР) визначена ключова роль у боротьбі з кіберзагрозами. ФБР підключається у випадках значних кіберінцидентів і забезпечує координацію дій як власних «польових» агентів, так і взаємодію з іншими державними агенціями. На ФБР також покладено обов'язок забезпечити необхідну правоохоронну та слідчу діяльність, до яких відноситься збір доказів та збір розвідувальної інформації щодо осіб, які можуть представляти загрозу кібербезпеці Сполучених Штатів. Крім того, у випадку масштабних надзвичайних подій у сфері кібербезпеки, представники ФБР включаються до складу Кібернетичної об'єднаної координаційної групи (Cyber Unified Coordination Group) до якої входять представники інших федеральних агенцій, місцевих органів управління, а за необхідності залучаються також представники недержавних організацій та міжнародної спільноти.

На теперішній час у структурі ФБР, діють наступні підрозділи, метою яких є протидія комп'ютерній злочинності [5]:

- Кібернетичне Управління (Cyber Division) при штабквартирі ФБР для здійснення максимальної координації сил, задіяних у боротьбі з кіберзлочинами;

- Кібернетичні підрозділи (Cyber Squads) при штабквартирі ФБР та при кожному із 56 «польових» офісів ФБР, укомплектовані агентами та аналітиками, завданням яких є протидія незаконному втручанню у роботу комп'ютерних мереж, викраденню інтелектуальної власності та персональних даних, дитячій порнографії та експлуатації дітей, кібершахрайствам;

- Команди кібернетичної дії (Cyber Action Teams), які працюють по всьому світу та оперативно реагують на вчинення глобальних кіберзлочинів. Крім того, їхнім завдання є збір роз-

відувальної інформації стосовно можливих кіберзагроз безпеці Сполучених Штатів;

- Підрозділи боротьби з комп'ютерними злочинами (Computer Crime Task Forces), які працюють на території США і здійснюють протидію комп'ютерній злочинності, використовуючи всі доступні федеральні та місцеві ресурси.

Реалізуючи програму по боротьбі з кіберзлочинністю, ФБР тісно співпрацює з Міністерством оборони та Міністерством національної безпеки, які часто вирішують схожі задачі. Для найбільш оперативного отримання інформації щодо вчинених комп'ютерних злочинів, у рамках ФБР створено Центр з прийому заяв стосовно вчинених інтернет-злочинів (Inernet Crime Complaint Center), де як потерпілі, так і треті особи, заповнивши спеціальну форму онлайн або просто зателефонувавши, можуть надати інформацію стосовно вчинених злочинів у мережі Інтернет.

Список використаних джерел:

1. Petya (Malware). URL: https://en.wikipedia.org/wiki/Petya_(malware) (дата звернення: 28.10.2017).
2. 64 країни і 12,5 тисяч заражених комп'ютерів: у Microsoft підтвердили провину M.E.Doc. URL: https://tsn.ua/nauka_it/64-krayini-i-12-5-zarazhenih-komp-yuteriv-u-microsoft-pidtverdili-provinu-m-e-doc-953003.html (дата звернення: 28.10.2017).
3. Cybersecurity National Action Plan. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan (дата звернення: 28.10.2017).
4. Presidential Policy Directive-41. URL: https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident (дата звернення: 28.10.2017).
5. Cyber Crime – FBI. URL: https://www.fbi.gov/investigate/cyber (дата звернення: 28.10.2017).

Одержано 30.10.2017

УДК 341.456 : 341.123

Катерина Миколаївна ОЛІЙНИК,
слухач магістратури факультету №3 Харківського національного університету внутрішніх справ

Андрій Васильович ВОЙЦІХОВСЬКИЙ,
кандидат юридичних наук, доцент, професор кафедри конституційного і міжнародного права факультету № 4 Харківського національного університету внутрішніх справ

КІБЕРБЕЗПЕКА ЯК НАПРЯМ ДІЯЛЬНОСТІ ООН

Одним з ключових тенденцій світового розвитку на початку XXI ст. є процес формування глобального інформаційного суспільства. Під впливом інформаційних потоків відбуваються глибокі зміни в міжнародних відносинах, пов'язані з виникненням інформаційних загроз міжнародного характеру, що вимагають активної співпраці держав у боротьбі з ними.

Становлення інформаційного суспільства не лише дає змогу будувати більш ефективне та успішне суспільство, але й надає нових імпульсів традиційним загрозам безпеки держави та створює принципово нові складнощі для системи національної безпеки. В таких умовах особливого значення набуває пошук нових можливостей забезпечення безпеки держави з огляду на формування нового поля протиборства – кіберпростору.

Формулювання міжнародної інформаційної безпеки, що знайшли відображення в «Вкладі Міжнародного союзу електрозв'язку в Декларацію принципів і План дій Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства» надалі лягли в основу відповідних положень підсумкових документів регіональних конференцій з підготовки до Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства - Загальноєвропейська конференція (м. Бухарест, 7-9 листопада 2002 р.) і Азіатська конференція (м. Токіо, 13-15 січня 2003 р.).

Бухарестська декларація 2002 р. передбачає розробку «глобальної культури кібербезпеки», що повинна забезпечуватися шляхом прийняття превентивних засобів та підтримуватися усією спільнотою за умови збереження свободи передання інформації. Країни погодилися з тим, що необхідно «упереджувати використання інформаційних ресурсів або технологій зі злочинними або терористичними цілями» та зміцнювати міжнародну співпрацю у цій сфері.

У Токійській декларації 2003 р. важливе місце щодо забезпечення інформаційної безпеки займає питання використанням інформаційних технологій і засобів. Визнаючи принцип справедливого, рівного і адекватного доступу до інформаційно-комунікаційних технологій сторони вважають необхідним приділити особливу увагу загрозі потенційного військового використання цих технологій.

Сторони погодилися з необхідністю розвивати регіональну і міжнародну співпрацю для зміцнення кібербезпеки. Було висловлено думку проте, що ефективне забезпечення кібербезпеки може бути досягнуте не лише технологічно, для цього знадобляться зусилля із правового регулювання питання і вироблення відповідної національної політики держав.

Прийнята 22 листопада 2002 р. ГА ООН резолюція (A/RES/57/53) «Досягнення у сфері інформатизації і телекомунікації в контексті міжнародної безпеки» від 22 жовтня 2002 р. вказує на неприпустимість використання інформаційно-телекомунікаційних технологій і засобів з метою негативного впливу на інфраструктуру держав. Резолюція підтверджує прохання до Генерального секретаря ООН, що міститься в пункті 4 резолюції (A/RES/56/19), відносно створення спеціальної групи урядових експертів держав-членів ООН.

Відповідно до зазначеної резолюції були створені дві Групи урядових експертів ООН по міжнародній інформаційній безпеці, які продовжили дослідження загроз у сфері інформаційної безпеки.

Важливі аспекти протидії кіберзлочинності були закріплені у резолюції (A/RES/64/211) ГА ООН від 21 грудня 2009 р. про «Створення глобальної культури кібербезпеки і оцінка національних зусиль по захисту найважливіших інформаційних інфраструктур». Найсуттєвішим з них можна назвати формулювання переліку елементів для захисту найважливіших інформаційних інфраструктур. Тобто були вказані ті захисні механізми, як міжнародного так і національного рівня, котрі є базовими елементами для побудови глобальної системи протидії спробам використання і використанню інформаційно-комунікаційних технологій у цілях не сумісними з основними принципами міжнародного права та безпекою держав, суспільства та особи [1].

Міжнародний характер загроз кібербезпеки визначає необхідність взаємодії як на регіональному, так і на глобальному рівні, з тим, щоб вжити погоджені заходи для зниження існу-

ючих загроз. Жодній державі не під силу добитися цього самостійно. Тому паралельно з розвитком спеціалізованих органів і інститутів ООН створюються міжурядові організації міжрегіонального і регіонального характеру, спрямовані на розширення співпраці держав в різних областях міжнародних відносин. Розробка міжнародно-правової бази в галузі забезпечення кібербезпеки ведеться повільно і непросто, оскільки світова спільнота зіткнулася із завданням кодифікації діяльності в новій, технологічно складній і украй чутливій для їх національної безпеки сфері. Робота над цими домовленостями проходить поетапно, кожен подальший документ спирається на попередній, паралельно приймаються загальні принципи діяльності держав у відповідних сферах.

Список використаних джерел:

1. Войціховський А.В. Забезпечення безпеки інформаційного простору як напрям правоохоронної діяльності ООН. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2015. № 2 (76). С.76-85.

Одержано 30.10.2017

UDC 343.544 - 053.2

Iryna Igorivna POZHYDAIEVA,
student of Faculty of International Economic Relations and Travel Business V. N. Karazin Kharkiv National University

PROTECTION FROM CHILD EXPLOITATION IN PROSTITUTION: INTERNATIONAL LEGAL ASPECT

Child prostitution (an exploitation of a child in prostitution) is a form of commercial sexual child exploitation which violates their basic rights for life, freedom and other kinds of rights. In international documents especially of the International organization ECPAT there are 5 basic forms of commercial sexual child exploitation: exploitation in prostitution, for pornography, in tourism, children trafficking with sexual purposes and early marriage.

Article 34 of Convention on the Rights of the Child, which was ratified by Ukraine in 1991 prohibits all kinds of sexual exploitation and sexual abuse in particular the inducement or coercion of a child to engage in any unlawful sexual activity, the exploitative use of children in prostitution or other unlawful sexual practices. Any forms of such actions will be considered as a crime against children who are also protected by the Convention on the Rights of the Child [1].

A term “child prostitution” is mentioned in Article 2 of Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography mentions that “child prostitution means the use of a child in sexual activities for remuneration or any other form of consideration”. Article 3 of this Protocol points out that such activities are covered by penal law and there are punishments for committing such actions [2].

The Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse determines in Article 19 that “child prostitution” shall mean the fact of using a child for sexual activities where money or any other form of remuneration is given as payment promise or consideration is made to the child or to a third person. This kind of earning money must be prohibited all over the world [3].

This Convention which is mentioned above prohibits child involvement into prostitution and gaining an income from it. In Ukrainian legislature there is no term “prostitution” even more “child prostitution”. But this notion is mentioned in international documents which were ratified by Ukraine that is why it is necessary to investigate this question. Article 303 of Penal Code of Ukraine prohibits the process of involvement into prostitution and prostitution activities using fraud, intimidation or vulnerable condition of the person applying violence or with a threatening of violence [4].

Prostitution is administrative wrongdoing for which children from 16 years old can be exposed to liability according to article 181-1 of the Code of Ukraine on Administrative Offences [5]. It contradicts international rules which foresee that children, who were victims of exploitation in prostitution, should be properly treated, but not be punished as offenders. The Protocol to Prevent, Suppress and Punish Trafficking in Persons, especially Women and Children notes first time that it is important for state to provide all necessary remedies for decreasing demand for child prostitution.

There are some countries in the world where child prostitution is mostly spread. Among them we can observe Sri Lanka, Thailand, Brazil, Bangladesh, the Philippines and some other countries. In many states prostitution is legalized and allows employment from 18 years old. Prostitution is legal and regulated in Germany, the Netherlands, Greece, Austria, Hungary and Latvia. These Member States recognize prostitutes as legal workers and

consider engaging in sexual activities as legitimate profession. In Lithuania, Romania and some other Member States prostitution is outlawed with the meaning that such job is illegal. In some other countries prostitution itself is not illegal but such activities as running brothels, pimping, and others are considered as criminal offences (Cyprus, Belgium, Bulgaria, Denmark, Czech Republic, France, Italy, Malta, Luxemburg, Finland, Estonia, Portugal, Spain, Slovakia, Slovenia, Poland) [6, p. 29]. For example, prostitution in Bangladesh was legalized in 2000 and national law stipulated that only individuals who reached 18 can work in assignation house. According to UNICEF data about 13% of children aged 5-14 years in Bangladesh are involved in child labor [7].

Moreover there are a lot of women (up to half) who start selling sex in young ages. Some surveys conducted in the Netherlands showed that 5% of prostitutes in the licensed sector had started their "career" before the age of 18. Investigating the escort sector we can observe that more than 10% were actually underage, and more than 50% started when they were younger than 20 years old [8, p. 78].

Rights and obligations of parents in the sphere of juvenile justice are showed in the Committee of Ministers of the Council of Europe Recommendation Act "European Rules for juvenile offenders subject to sanctions or measures" from 5 November 2008, which states in Article 14 that "any legal body which deals with issues of juveniles should take into account the rights and obligations of parents and tutor-at-law and involve them into legal procedures and appliance of sanctions and measures, excluding cases when it contradicts better interests of juvenile". Therefore parents should take the responsibility for their children and pay attention to their breeding [9, p. 3].

Vulnerable groups (children among them) have some advantages prescribed in Article 51 of Constitution of Ukraine, which undertakes protection of childhood [10].

Notwithstanding international standards the issue of child prostitution still exists. International bodies cannot interfere with national policy of some countries. We pay attention but to overcome this problem states must take necessary actions by themselves and to show a wish to stop the process of children involvement into sexual exploitation.

References:

1. Convention on the Rights of the Child Adopted and opened for signature, ratification and accession by General Assembly reso-

lution 44/25 of 20 November 1989 entry into force 2 September 1990, in accordance with article 49. URL: http://www.ohchr.org/EN/ProfessionalInterest/Pages/CRC.aspx (Access date: 28.10.2017).
2. The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography. Adopted and opened for signature, ratification and accession by General Assembly resolution A/RES/54/263 of 25 May 2000 entered into force on 18 January 2002. URL: http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx (Access date: 28.10.2017).
3. Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, Council of Europe Treaty Series - No. 201, URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680084822. (Access date: 28.10.2017).
4. Кримінальний кодекс України. Закон від 05.04.2001 № 2341-III // База даних «Законодавство України»/ ВР України. URL: http://zakon3.rada.gov.ua/laws/show/2341-14. (Access date: 28.10.2017).
5. Кодекс України про адміністративні правопорушення (статті 1 - 212-21). Закон від 07.12.1984 № 8073-X // «Законодавство України»/ ВР УРСР. URL: http://zakon2.rada.gov.ua/laws/show/80731-10. (Access date: 28.10.2017).
6. Sexual exploitation and prostitution and its impact on gender equality. Directorate-General for Internal Policies. Policy Department, Citizens Rights and Constitutional Affairs. European Parliament, Brussels, 2014, p. 90.
7. Asia Child Rights. Bangladesh's Child Sex Workers: No Place To Go. URL: http://acr.hrschool.org/mainfile.php/0103/20/. (Access date: 28.10.2017).
8. Daalder A. A. . Prostitution in the Netherlands since the lifting of the brothel ban. *WODC*. 2007. p. 103..
9. Крестовська Н. Міфи про ювенальну юстицію. *Віче*. 2010. № 15. URL: http://www.viche.info/journal/2126.(Access date: 28.10.2017).
10. Конституція України. Закон від 28.06.1996 № 254к/96-ВР // «Законодавство України» / ВР України. URL: http://zakon3.rada.gov.ua/laws/show/254к/96-вр. (Access date: 28.10.2017).

Одержано 01.11.2017

УДК 341.217

Павло Вікторович ФОМІН,
аспірант кафедри міжнародного і європейського права юридичного факультету Харківського національного університету імені В. Н. Каразіна

ДЕЯКІ АСПЕКТИ ПОДАЧІ ЗАЯВ ДО ТРИБУНАЛУ ЗІ СПОРІВ ООН ЧЕРЕЗ ПОРТАЛ EFILING

Міжнародно-правовими актами універсального і регіонального характеру з прав людини гарантується право кожної людини на справедливий і публічний розгляд справи компетентним, незалежним і безстороннім судом. Необхідність урегулювання суперечок, які виникають між співробітниками й адміністрацією міжнародних міждержавних організацій, включаючи спори, пов'язані з дисциплінарними заходами зумовила створення внутрішньої системи правосуддя з огляду на те, що вони користуються імунітетом від місцевої юрисдикції і до них не можна пред'явити позов у національному суді.

У 2007 році Генеральна Асамблея ООН у своїй резолюції A/RES/61/261 постановила заснувати нову, незалежну, прозору, децентралізовану систему відправлення правосуддя, яка узгоджується з відповідними нормами міжнародного права та принципами дотримання законності і належних процесуальних норм, із метою забезпечення дотримання прав співробітників і виконання ними своїх обов'язків та забезпечення підзвітності як керівників, так і співробітників (п. 4) [1].

Так, внутрішня система правосуддя ООН передбачає можливість урегулювання спору, який виник між співробітником та адміністрацією за допомогою неформальних способів (омбудсмен, посередницькі послуги) або шляхом звернення із відповідною заявою безпосередньо до Трибуналу зі спорів ООН.

Така заява може бути подана будь-яким співробітником ООН, у тому числі Секретаріату ООН або окремо керованих фондів і програм ООН; будь-яким колишнім співробітником ООН, у тому числі Секретаріату ООН або окремо керованих фондів і програм ООН; будь-якою особою, яка заявляє вимоги від імені недієздатного або померлого співробітника ООН, у тому числі Секретаріату ООН або окремо керованих фондів і програм ООН (ст. 3(1)) [2].

Особа може подати заяву шляхом направлення її в електронному вигляді (електронною поштою), в друкованому вигляді або безпосередньо до Секретаріату Трибуналу зі спорів ООН

через портал eFiling, який передає її до відповідного Секретаріату.

Варто зазначити, що портал eFiling є основним способом подання документів до Трибуналу зі спорів ООН, який забезпечує доступ до веб-системи обробки судової документації та дозволяє сторонам спору надавати свої документи в електронній формі, забезпечуючи їх направлення до відповідного Секретаріату. Він також дозволяє отримувати повідомлення і забезпечує легкий доступ до документів по справі (повідомлень, наданих документів, розпоряджень Трибуналу тощо).

Співробітник персоналу, який бажає подати заяву через портал eFiling, має, перш за все, отримати обліковий запис. Після отримання облікового запису особа може вільно користуватися порталом eFiling і надавати свої документи за допомогою відповідних бланків.

Так, для того, щоб подати заяву через портал eFiling особа повинна заповнити необхідний бланк заяви на комп'ютері, направити заявку про відкриття облікового запису для отримання доступу до порталу eFiling. Після прийняття та затвердження заявки особа отримує доступ до порталу і може направити свою заяву. Отримавши відповідний доступ, особа має ввести свої облікові дані, заповнити онлайновий бланк (включаючи розділи «Особисті відомості і трудовий статус», «Контактна інформація» та «Юридичний представник»), обрати тип заяви та завантажити заповнений і підписаний бланк зі свого комп'ютера.

Враховуючи положення Регламенту Трибуналу зі спорів ООН, відповідно до якого бланк заяви повинен бути підписаний (ст. 8(3)) [3], особа може подати підписану заяву у форматі PDF, або у форматі Word, додавши окремий PDF-документ із підписом.

Крім цього, заявникам рекомендується подавати всі документи, за можливості, у форматі «PDF», які можуть бути створені шляхом прямого перетворення файлів Word у PDF (бажаний метод) або, як альтернатива, шляхом сканування друкованих документів у форматі PDF. При цьому, при скануванні документів рекомендовано не використовувати режим сканування із високою роздільною здатністю для того, щоб уникнути надто великого розміру файлу (п. 7).

Усі файли, завантажені на портал eFiling, у своїй назві повинні містити інформацію про заявника (позивач, відповідач), а також відображати зміст назви документу (п. 8) [4].

Крім цього, згідно вимог Регламенту Трибуналу зі спорів ООН підписаний оригінал заповненого бланку заяви надається разом із додатками до неї. До таких документів належать, зокрема, копія оскаржуваного рішення, будь-яка підтверджуюча документацію (яка додається і нумерується), за необхідності, підписана довіреність юридичного представника.

Варто зауважити, що істотною умовою забезпечення конфіденційності поданих документів є положення Практичного керівництво щодо подачі заяв через eFiling портал, відповідно до якого всі заяви, направлені до Трибуналу зі спорів ООН, незалежно від способу їх подання, недоступні третім особам, крім тих випадків, коли доступ до них буде надано відповідно до наказу Трибуналу після подачі відповідного клопотання (п. 4) [4].

Список використаних джерел:

1. Резолюция Генеральной Ассамблеи ООН A/RES/61/261 URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N06/510/05/PDF/N0651005.pdf?OpenElement (дата звернення: 18.10.2017).
2. Statute of the United Nations Dispute Tribunal URL: http://www.un.org/en/oaj/files/undt/basic/2008-12-24-undt-statute.pdf (дата звернення: 18.10.2017).
3. Регламент Трибунала по спорам Организации Объединенных Наций A/RES/64/119. URL: http://www.un.org/ru/oaj/dispute/dispute_tribunal_rules.pdf (дата звернення: 18.10.2017).
4. United Nations Dispute Tribunal Guidelines on the filing of submissions through the eFiling portal URL: http://www.un.org/en/oaj/files/undt/basic/guidelines_on_efiling.pdf (дата звернення: 18.10.2017).

Одержано 01.11.2017

УДК 341.217

Ліна Олександрівна ФОМІНА,
викладач кафедри міжнародного і європейського права юридичного факультету Харківського національного університету імені В. Н. Каразіна

ДЕЯКІ АСПЕКТИ ДІЯЛЬНОСТІ РАДИ З УПРАВЛІННЯ ІНФОРМАЦІЄЮ МІЖНАРОДНОГО КРИМІНАЛЬНОГО СУДУ

Забезпечення інформаційної безпеки є одним із основоположних напрямків функціонування Міжнародного кримінального суду (далі – МКС), діяльність якого безпосередньо

пов'язана з процесом збору, обробки та зберігання великого масиву інформації щодо стану розгляду справи, особистих даних учасників кримінального процесу, отриманих доказів тощо.

Процедурно-процесуальними актами МКС передбачено існування електронної системи, що являє собою інформаційну систему, яка здійснює управління документами, матеріалами, розпорядженнями і рішеннями та забезпечує доступ до них (положення 10 РСС МКС) [1].

Так, Суд створює надійну, захищену та ефективну електронну систему, яка забезпечує підтримку повсякденного управління судовими та адміністративними справами Суду і провадження в Суді. Секретаріат несе відповідальність за функціонування системи, враховуючи при цьому конкретні вимоги, пов'язані з судовою діяльністю Суду, в тому числі необхідність забезпечити автентичність, точність, конфіденційність і збереження судових протоколів та матеріалів (положення 26 РС МКС) [2].

У п'ятирічній стратегії Міжнародного кримінального суду «Управління інформаційними технологіями та інформацією МКС (2017-2021)» зазначено, що «Суд значно виріс з часу його заснування, що в свою чергу вплинуло на існуючі вимоги в сфері інформаційно-комунікаційних технологій, а також обсяг отриманих даних. Зокрема, вимоги в таких сферах, як збір цифрових доказів, інформаційна безпека та управління інформацією задовольняються існуючими системами лише частково».

Варто зазначити, що за період свого існування МКС здійснив низку важливих інвестицій у сфері інформаційних технологій та управління інформацією з метою підтримки його судових, слідчих та адміністративних операцій, серед яких зокрема: Ringtail; SAP та TRIM/HP Records Manager; платформа ECOS.

Разом із тим, необхідність вирішення існуючих проблем у сфері зберігання, використання та розповсюдження інформації, яка перебуває у розпорядженні МКС призвела до створення нової структури – Ради з управління інформацією (далі – Рада) (пп.3-4) [3, с. 191].

Так, згідно з Адміністративною інструкцією МКС ICC/AI/2017/001 (далі – AI ICC/AI/2017/001) Рада з управління інформацією заснована в якості консультативної ради щодо політики, яка повинна бути прийнята Судом з метою забез-

печення комплексного підходу до процесу управління інформацією і оптимізації вкладу Суду в управління інформацією та інформаційні технології (положення 2).

Відповідно до AI ICC/AI/2017/001 до структури Ради входить директор Служби судової підтримки, який виступає одночасно її Головою; один представник від Президії; один представник від Палат Суду; один представник від Канцелярії Обвинувача, крім того на розсуд Канцелярії Обвинувача і за погодженням із Головою Ради може бути призначений один додатковий представник Відділу розслідувань, Відділу обвинувачення і Секції послуг; один представник із Канцелярії Секретаря; співробітник з інформаційної безпеки; Директор Відділу управлінського обслуговування.

У положеннях AI ICC/AI/2017/001 також визначено коло повноважень Ради, серед яких, зокрема: надання рекомендацій Координаційній раді МКС щодо стратегії управління інформацією та інформаційних технологій, визначення пріоритетності проектів і розподіл ресурсів, включаючи фінансування, в тому випадку, коли це зачіпає декілька органів Суду [4].

Так, на виконання своїх повноважень Рада, зокрема, може розглядати і виносити рекомендації щодо політики, стандартних оперативних процедур і керівних принципів, які стосуються управління інформацією і розробки систем, які створюють і підтримують Інформацію; запрошувати управлінські звіти з питань, які викликають занепокоєність у рамках діяльності Суду, включаючи, але не обмежуючись випадками у сфері інформаційної безпеки; розглядати питання, що стосуються управління інформацією і надавати пропозиції Координаційній раді для вирішення будь-яких пов'язаних із цим конфліктів; за необхідності, створювати додаткові Форуми з питань управління; надавати пропозиції Координаційній раді щодо внесення поправок до кола повноважень будь-якого з Форумів з питань управління тощо.

Варто вказати, що під Форумами з питань управління слід розуміти міжорганізаційні форуми за участі зацікавлених сторін, створені для діалогу з питань політики в сфері інформаційних технологій та управління інформацією.

В рамках діяльності МКС передбачено функціонування таких Форумів як: Судовий технологічний форум; Адміністративний технологічний форум; Форум з безпеки та управління інформацією.

Означені Форуми можуть надавати ініціативні пропозиції, які стосуються питань, що входять до їх мандату, відносно яких Рада уповноважена надавати відповідні рекомендації у встановлених процедурно-процесуальними актами МКС випадках.

Виходячи з означеного, доходимо висновку, що МКС приділяє значну увагу питанню інформаційних технологій та управління інформацією, забезпечення інформаційної безпеки у його діяльності, вдосконалюючи існуючу систему Суду та виробляючи нові напрямки діяльності в цій сфері.

Список використаних джерел:

1. Регламент Секретариата Суда ICCBD/030106Rev.1. URL: http://www.icc-cpi.int/NR/rdonlyres/A57F6A7F-4C20-4C11-A61F-759338A3B5D4/140147/ICCBD_030106Rev1_Russian.pdf (дата звернення: 18.10.2017).
2. Регламент Суда ICC-BD/01-01-04 URL: https://www.icc-cpi.int/NR/rdonlyres/B920AD62-DF49-4010-8907-E0D8CC61EBA4/277532/ICCBD010104_Russian.pdf (дата звернення: 18.10.2017).
3. Proposed Programme Budget for 2018 of the International Criminal Court ICC-ASP/16/10 URL: https://asp.icc-cpi.int/iccdocs/asp_docs/ASP16/ICC-ASP-16-10-ENG.pdf (дата звернення: 18.10.2017).
4. Administrative Instruction ICC/AI/2017/001 Establishment of the Information Management Governance Board, its composition and terms of reference. URL: https://www.icc-cpi.int/resource-library/Vademecum/ESTABLISHMENT%20OF%20THE%20INFORMATION%20MANAGEMENT%20GOVERNANCE%20BOARD%20ITS%20COMPOSITION%20AND%20TERMS%20OF%20REFERENCE.PDF (дата звернення: 18.10.2017).

Одержано 01.11.2017

Наукове видання

АКТУАЛЬНІ ПИТАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Збірник матеріалів
Всеукраїнської науково-практичної конференції,
(15 листопада 2017 року, м. Харків)

Українською, англійською та російською мовами

Відповідальні за випуск: *Н. В. Кондибіна, О. В. Манжай*
Редактор: *О. В. Манжай*
Корегування списків бібліографічних посилань: *О. В. Манжай*
Комп'ютерне верстання: *О. В. Манжай*

Формат 60х84 1/16. Ум. друк. арк. 11,24 Обл.-вид. арк. 12,4.
Тираж 200 пр.