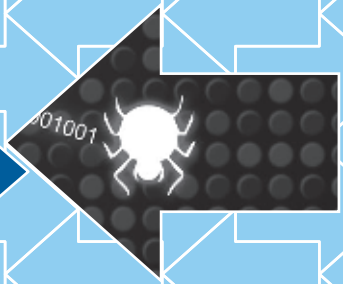
ПРОТИДІЯ



КІБЕРЗАГРОЗАМ ТА ТОРГІВЛІ ЛЮДЬМИ

Матеріали Міжнародної науково-практичної конференції
26.11.2019 р. м. Харків

ОБСЄ Організація з безпеки та співробітництва в Європі
Координатор проектів в Україні

Міністерство внутрішніх справ України

Харківський національний університет внутрішніх справ

U.S. Mission to the OSCE

МВС України
Харківський національний університет
внутрішніх справ
Координатор проектів ОБСЄ в Україні

ПРОТИДІЯ КІБЕРЗАГРОЗАМ ТА ТОРГІВЛІ ЛЮДЬМИ

Збірник матеріалів
Міжнародної науково-практичної конференції

(26 листопада 2019 року, м. Харків)

Харків
ХНУВС
2019

УДК [351.74:343.85](062.552)
П83

Друкується згідно з рішенням оргкомітету за дорученнями Харківського національного університету внутрішніх справ від 17.09.2019 № 125

П83 Протидія кіберзагрозам та торгівлі людьми (26 листоп. 2019 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. – Харків : ХНУВС, 2019. – 330 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)

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/).

Видано Координатором проектів ОБСЄ в Україні в рамках проекту «Посилення кримінального переслідування торгівлі людьми з використанням інформаційних технологій в Україні», за фінансової підтримки уряду Сполучених Штатів Америки.

ЗМІСТ

Розділ 1
Окремі питання правового
та організаційного забезпечення протидії кіберзлочинності
та торгівлі людьми

Розділ 2
Кримінально-правові, процесуальні та криміналістичні аспекти протидії кіберзлочинності та торгівлі людьми

Розділ 3
Використання інформаційних технологій і технічних засобів у протидії кіберзлочинності та торгівлі людьми

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 004.7.056.5

Дмитро Володимирович Швець,
кандидат педагогічних наук, доцент, ректор Харківського національного університету внутрішніх справ

Механізми забезпечення кібербезпеки в інформаційному просторі

Для забезпечення національних інтересів та їх захисту на міжнародному рівні виняткового значення набуває обґрунтування ефективних механізмів забезпечення кібербезпеки держави. В Україні ці механізми все ще знаходяться на етапі становлення. Деякі з них потребують удосконалення, а окремим елементам більшості з них не вистачає концептуального обґрунтування.

Актуальність зазначеної теми зумовлена необхідністю подолання суперечностей між стрімким зростанням важливості кібербезпекової проблематики та частковою готовністю України відповісти на новітні кібербезпекові виклики, а також нагальною потребою визначення ключових стратегічних проблем і шляхів їх вирішення для розбудови ефективних механізмів забезпечення кібербезпеки України.

Кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [1].

Одним із пріоритетних напрямків інформатизації українського суспільства є впровадження електронного управління. Механізми забезпечення кібербезпеки в інформаційному просторі є технологічною основою застосування електронного управління, вони є захистом доступу осіб, підприємств, установ та організацій до електронних послуг в інформаційному просторі.

Взаємодія між компонентами будь-якої системи, описується, насамперед, поняттям доступу суб'єктів до об'єктів. Суб'єктом може бути користувач або процес (задача, трансакція, запущена програма або сервіс), а об'єктом – логічний або фізичний ресурс системи (файл, набір

даних, програма, сервіс, база даних, канал передачі даних тощо). Базовою характеристикою доступу є те, що в результаті його створюється потік інформації від об'єкта до суб'єкта шляхом виконання таких операцій, як читання, запис, модифікація, пошук тощо.

Управління доступом є ключовим механізмом забезпечення кібербезпеки в інформаційному просторі. Механізми управління доступом можуть бути класифіковані: за рівнями реалізації механізмів безпеки та за етапами роботи і компонентами.

За рівнями реалізації виділяють три категорії механізмів кібербезпеки: адміністративно-правові, програмно-технічні та фізичного захисту.

Механізми кібербезпеки за етапами роботи і компонентами, які реалізують підсистему управління доступом, поділяють на механізми ідентифікації, автентифікації, авторизації та моніторингу.

На етапі ідентифікації визначаються та перевіряються ідентифікатори суб'єкта й об'єкта системи. При автентифікації перевіряється достовірність суб'єкта – чи дійсно він той, за кого себе видає. Якщо суб'єкт автентифікований і має відповідні права на об'єкт, він буде авторизований, тобто йому буде надано доступ до запрошеного ним об'єкта. Моніторинг передбачає протоколювання йаналіз подій безпеки.

Під час опису систем управління доступом, як правило, відзначають базові властивості системи інформаційної кібербезпеки: конфіденційність, цілісність, доступність, підзвітність. Підзвітність характеризує те, що всі події та дії суб'єкта в системі інформаційної безпеки ідентифікуються, реєструються й можуть бути перевірені. Властивість підзвітності в системі реалізується чотирма методами: ідентифікацією, автентифікацією, авторизацією і аудитом.

Серед нормативно-правових актів Європейського Союзу, які визначають основні засади законодавства у сфері електронної ідентифікації слід відзначити регламент ЄС № 910/2014 Європейського Парламенту та Ради Європи «Про електронну ідентифікацію та довірчі послуги для електронних трансакцій на внутрішньому ринку» [2]. Цей регламент спрямований на підвищення рівня безпеки електронних трансакцій на внутрішньому ринку шляхом надання загальної основи для безпечної та цілісної електронної взаємодії між підприємствами, громадянами і державними органами, тим самим підвищуючи ефективність державних і приватних онлайн-послуг, електронного бізнесу й електронної торгівлі в ЄС. Він робить вагомий внесок у побудову єдиного цифро-

вого ринку шляхом створення умов для взаємного крос-кордонного визнання ключових компонентів, таких як електронна ідентифікація, електронні документи, електронні підписи та електронні послуги, а також для сумісності послуг електронного управління на території ЄС.

Згідно з європейським регламентом засоби електронної ідентифікації в контексті схеми електронної ідентифікації позділяються на три рівні безпеки (гарантії) та відповідні засоби їх забезпечення: обмежений (низький), суттєвий, вищий (високий).

Кожен рівень гарантії повинен належити до засобів електронної ідентифікації в контексті схеми електронної ідентифікації, які забезпечують відповідний ступінь безпеки до ідентичності особи, про яку заявляється або стверджується, і характеризуються відповідними технічними специфікаціями, стандартами та процедурами, пов'язаними з ними, в тому числі з технічними засобами контролю, метою яких є зниження ризику зловживання або підміни ідентичності.

При цьому встановлено мінімальні технічні характеристики, стандарти та процедури стосовно низького, суттєвого та високого рівнів гарантії, які повинні бути застосовані для засобів електронної ідентифікації.

Аналіз загального стану впровадження інфраструктури електронної ідентифікації в державах – членах ЄС свідчить про неоднорідність прийнятих у різних країнах політик у цій сфері, використання різних технологій ідентифікації та автентифікації, які відповідають різним рівням довіри електронної ідентифікації.

Архітектура інфраструктури електронної ідентифікації має передбачати можливість використання декількох інструментів електронної ідентифікації. Це буде сприяти поширенню послуг на базі електронної ідентифікації серед громадян.

Упровадження електронної ідентифікації в Україні призвело до ситуації, коли в інформаційних системах різного призначення та масштабу часто використовуються засоби електронної ідентифікації користувачів без урахування таких основних принципів, як кібербезпека, захист персональних даних, достовірність ідентифікації, інтероперабельність і комфортність використання [3].

Таким чином, відсутність єдиної нормативної та технічної політики використання і захисту ідентифікаційних даних користувачів, загальних процедур і алгоритмів автентифікації та захисту інформації в системах, забезпечення їх інтероперабельності й ефективної взаємодії

інформаційних систем стає стримуючим чинником для ефективного забезпечення кібербезпеки в Україні.

Список бібліографічних посилань

1. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 30.10.2019).
2. Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014. URL: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG (дата звернення: 30.10.2019).
3. Національна стратегія електронної ідентифікації України. Біла книга з електронного урядування / під ред. О. Потія та Ю. Козлова. 145 с. URL: https://cdn.regulation.gov.ua/8d/f3/4c/32/regulation.gov.ua_File_196.pdf (дата звернення: 30.10.2019).

Одержано 01.11.2019

УДК 343.98

Галина Костянтинівна Авдєєва,
кандидат юридичних наук, старший науковий співробітник, провідний науковий співробітник Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України (м. Харків)

Проблеми застосування інноваційних продуктів у протидії кіберзагрозам

За допомогою інформаційно-комунікаційних технологій та програмно-апаратних засобів в усьому світі щороку вчиняються десятки тисяч злочинів. Генеральний секретар ООН Антониу Гуттереш зазначає, що щорічні збитки від кіберзлочинності у світі складають 1,5 трлн доларів. Не зважаючи на те, що у статистичних звітах Генеральної прокуратури рівень злочинності щороку знижується, у 2018 р. в Україні кіберзлочинів зафіксовано у 10 разів більше, ніж у 2017 р. Правопорушники використовують новітні науково-технічні засоби та інноваційні продукти не лише як предмет злочину, а й як засіб його підготовки та вчинення.

Останніми роками великі державні і приватні установи України і інших країн неодноразово потерпали від кібератак. Яскравим прикладом слугує розповсюдження вірусу Petya влітку 2017 року, через який було тимчасово заблоковано роботу аеропорту «Бориспіль», «Ощадбанку», «Укртелекому», «Укрпошти», «Укрзалізниці» та низки інших державних і приватних установ. Частково пошкоджена інформація в інформаційних системах Кабінету Міністрів, окремих міністерств і навіть кіберполіції. Це обумовлює необхідність використання адекватних засобів протидії кіберзлочинності – інноваційних продуктів у вигляді стандартного і спеціального програмного забезпечення, сучасних програмно-апаратних приладів і систем, а також методів їх застосування.

Вчені-криміналісти та експерти з кібербезпеки вважають, що в майбутньому кіберзагрози посиляться, а кількість злочинів та збитків від кібератак зростатиме тому, що правопорушники спочатку використовують певні інноваційні продукти для вчинення злочину, а лише після цього розробляються і застосовуються відповідні механізми щодо їх запобігання і розкриття. Тобто, кіберзлочинці завжди випереджають осіб, які їм протидіють.

Правова основа кібернетичної безпеки в Україні складається з відповідних норм Конституції України, Кримінального кодексу України, законів України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки» та ін., Доктрини інформаційної безпеки України, Конвенції Ради Європи про кіберзлочинність та інших міжнародних нормативно-правових актів, ратифікованих Верховною Радою України.

Реалізацію державної політики у сфері боротьби з кіберзлочинністю здійснює низка державних органів, а саме: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України. В кожному із зазначених державних органів створено відповідні підрозділи, співробітники яких постійно підвищують свою кваліфікацію. Зокрема, у 2016–2017 рр. співробітники Департаменту кіберполіції пройшли курси з підвищення кваліфікації на базі Харківського національного університету внутрішніх справ та взяли участь у тренінгах за участі експертів Великої Британії.

Протягом 2018 року працівники Департаменту кіберполіції України викрили більше 800 осіб, які були причетні до вчинення злочинів, що вчинялися з використанням інформаційних технологій. Найбільше виявлено правопорушників, які вчиняли злочини за допомогою вірусних програм, придбаних через анонімну «мережу» DarkNet. Однак, виходячи з показників роботи кіберполіції України у 2018 р., відсоток розкритих злочинів, що вчиняються з використанням інформаційних технологій, є не досить високим. Однією з причин такого становища є проблеми впровадження інноваційних продуктів у роботу органів правопорядку.

На шляху впровадження інновацій у практику боротьби з кіберзлочинністю існує низка перешкод, а саме: недостатність знань співробітників слідчих органів в даній галузі і відсутність можливості їх отримати, професійна деформація або неправильне відношення до всього нового, передового та ін. Гальмують впровадження інновацій у діяльність органів правопорядку також втрата професійного ядра співробітників слідчого апарату і оперативних підрозділів органів внутрішніх справ, недостатність наявних тактичних засобів здійснення слідчої діяльності, недостатнє бюджетне фінансування процесів розроблення і впрова-

дження інновацій; наявність складнощів у залученні кваліфікованих ІТ-спеціалістів до участі у слідчих діях; проблеми взаємодії слідчого з обізнаними особами; недостатність інформації про розслідувану подію; недостатність надійних джерел отримання інформації; наявність протидії розслідуванню з боку зацікавлених осіб та ін. Більше того, в усіх країнах світу існують проблеми визнання «цифрових» доказів судом через їх неналежну фіксацію.

Подолання існуючих проблем застосування інноваційних продуктів у протидії кіберзагрозам є можливим за умови системної державної підтримки, яка передбачатиме тісну співпрацю розробників і користувачів інноваційних продуктів та державне фінансування процесів розроблення і впровадження інновацій в практику боротьби з кіберзлочинністю.

Одержано 19.10.2019

УДК 343.1

Аліна Олександрівна Балаклієць,
курсантка навчально-наукового інституту № 1 Національної академії внутрішніх справ (м. Київ)

Олександр Валерійович Калиновський,
кандидат юридичних наук, старший науковий співробітник, заступник начальника відділу організації науково-дослідної роботи Національної академії внутрішніх справ (м. Київ)

Проблема торгівлі людьми в Україні

Проблема торгівлі людьми в Україні набула нового етапу у своєму розвитку та значно активізувалася за останні роки. Зокрема, протягом дев'яти місяців поліція зафіксувала 278 кримінальних правопорушень у сфері торгівлі людьми. Зокрема, на брифінгу в Укрінформі директором Департаменту комунікацій Міністерства внутрішніх справ Артемом Шевченком повідомлено, що за дев'ять місяців 2019 року виявлено загалом 278 кримінальних правопорушень, передбачених статтею 149 Кримінального кодексу України, – торгівля людьми. І левова частина, тобто 251 такий злочин – виявлено саме працівниками підрозділів боротьби зі злочинами, пов'язаними із торгівлею людьми, Національної поліції [1].

За його словами, у рамках супроводу кримінальних проваджень у 230 провадженнях цієї категорії були встановлені особи, які вчинили такі злочини, і їм повідомлено підозру.

В цілому досудове розслідування завершено у рамках 211 проваджень щодо факту торгівлі людьми, а це більше на 46,5 відсотків, ніж у 2018 році. І левова частина, тобто 204 таких злочини, розкриті безпосередньо працівниками підрозділів ДБЗПТЛ (Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми Нацполіції). Також за 9 місяців цього року встановлено 228 потерпілих – юридично – від торгівлі людьми, з них чоловіків – 124, жінок – 96, неповнолітніх – 6 і малолітніх – двоє [1].

Крім цього, впродовж 9 місяців 2019 року працівники підрозділів боротьби зі злочинами, пов'язаними з торгівлею людьми, викрили 4 організовані групи, що вчиняли кримінальні правопорушення у сфері торгівлі людьми, досудове розслідування у кримінальних проваджен-

нях за якими завершено. Виявлено, що на території Києва діяло 2 такі групи, і ще по 1 виявили у Одеській та Чернігівський областях. Якщо порівнювати з аналогічним періодом 2018 року, то тоді було виявлено 2 такі групи [1].

З метою вербування потенційних жертв створюються напівлегальні агенції по працевлаштуванню та фірми-одноденки, в засобах масової інформації поширюється брехлива рекламна інформація щодо працевлаштування за кордоном. Тим не менше, в більшості випадків злочинці вибирають такі методи вербування, які не привертають уваги компетентних органів, діючи методом індивідуального підбору. З цією метою вербувальники часто знайомляться з жертвами в громадських місцях, діють через спільних знайомих, родичів, сусідів. Власне, можуть виявитися такими вербувальниками і самі родичі, сусіди, знайомі.

Варто зазначити, що згідно з щорічним звітом Державного департаменту США про торгівлю людьми у світі, Україну з кінця 2017 року уже виключено з Контрольного списку: «Відтак Україна увійшла до – "другої" групи – як держава, влада якої докладає достатніх зусиль з викорінення торгівлі людьми» [2]. Про глобальність проблеми використання праці людей, торгівля ними, говорить і той факт, що нещодавно правоохоронці викрили міжнародний канал торгівлі людьми. Поліція виявила вісім завербованих жінок та спроби переправлення громадянок України до Китаю. Там вони мали б працювати в порно-бізнесі [2].

Враховуючи особливу поширеність торгівлі людьми у світі 30 липня кожного року тепер відзначають День протидії торгівлі людьми. Адже кожного року десятки тисяч людей у всьому світі стають предметом торгівлі, їх обманюють,примушують, продають, схиляють до праці та життя в рабських умовах. Незалежно від того, з якою метою здійснюється торгівля людьми, останні стають при цьому об'єктами фізичних та психологічних катувань, зґвалтувань, залякування [3].

17 грудня 2007 року Генеральна Асамблея ООН прийняла рішення про те, що, починаючи з 2008 року, 25 березня буде відзначатися як Міжнародний день пам'яті жертв рабства та скасування трансатлантичної работоргівлі. Своєю резолюцією 64/293 від 30 липня 2010 року Генеральна Асамблея ухвалила Глобальний план дій ООН по боротьбі з торгівлею людьми, в якому вона звернулася до всіх відповідних органів ООН із закликом координувати зусилля для ефективної боротьби з торгівлею людьми і для захисту прав людини та жертв такої торгівлі.

Висловлена і надія на те, що ефективне виконання цього плану дозволить внести істотний внесок у викорінення цієї форми сучасного рабства [4].

Перетворення Європейських співтовариств і Союзу в територію без внутрішніх кордонів (у рамках Загального ринку, а потім Шенгенського простору) стимулювало процес інтернаціоналізації злочинної діяльності, посилило його негативні наслідки. Такій впливовій структурі, як Рада Європи, загальної правоохоронної політики створити не вдалося. Будучи за своєю природою міжнародною міжурядовою організацією, вона приймає рішення або у формі резолюцій і рекомендацій, не обов'язкових для виконання, або розробляє проекти конвенцій між державами-учасниками, які, знову ж таки, ці країни не зобов'язані підписувати і ратифікувати. Такий стан речей і зумовив необхідність боротьби зі злочинністю в рамках ЄС.

Відповідно до ст. 3 Протоколу про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї, що доповнює Конвенцію ООН проти транснаціональної організованої злочинності від 15 листопада 2000 року, «торгівля людьми» означає такі дії, що здійснюються з метою експлуатації, вербування, перевезення, передачі, приховування або одержання людей шляхом загрози силою або її застосування або інших форм примусу, викрадення, шахрайства, обману, зловживання владою або уразливістю становища, або шляхом підкупу у вигляді платежів або вигод для одержання згоди особи, яка контролює іншу особу. Згода жертви торгівлі людьми на заплановану експлуатацію не береться до уваги, якщо було використано будь-який із вищезазначених заходів впливу [5, с. 36–37].

З метою ефективного регулювання міграційними процесами, країнами Європейського Союзу було розроблено єдину політику, фінансові інструменти та механізми, що спрямовані на удосконалення державного управління міграційними процесами на національному та наднаціональному рівнях. Ця амбітна мета була реалізована в форматі реалізації зовнішньої політики ЄС, що має назву «Європейська політика сусідства». Особливу увагу цим питанням приділяє Рада Європи, членом якої Україна є з 1995 року, що покладає на неї зобов'язання привести своє законодавство у відповідність до стандартів Ради Європи в галузі прав людини і, зокрема, з питань запобігання торгівлі людьми. Політика України щодо інтеграції в Європейському Союзі також обумовлює актуальність гармонізації національного законодавства щодо захисту

прав людини із законодавством Європейського Союзу, в тому числі у галузі запобігання торгівлі людьми. Для України нагальною є потреба створення ефективних механізмів державного управління міграційними процесами, які б сприяли запровадженню дієвих заходів з протидії нелегальній міграції та торгівлі людьми. Важливою складовою процесу є використання європейського досвіду державного управління з протидії незаконній міграції та торгівлі людьми зокрема [6, с. 133].

Україна в наш час не змогла встояти перед транснаціональними злочинцями – торгівцями людьми. Величезні прибутки в цьому виді злочинної діяльності вдало поєднуються з відносно невеликим ризиком для злочинців. Саме тому торгівля людьми розцвіла на теренах України буйним цвітом. Адже наша країна являється одночасно і країною – постачальником живого товару, і країною – транзитером для переміщення жертв в інші місця, і країною, де власне існує торгівля власними громадянами в межах України. Тому, і це зовсім не несподіванка, часто-густо виявляється, що продані люди являються громадянами нашої держави.

Підводячи підсумки, можна сказати, що проблема торгівлі людьми стосується нас усіх, адже ось лише деякі наслідки цього ганебного явища для нашої країни – криміналізація суспільства, загострення економічної ситуації в результаті відтоку робочої сили, збільшення кількості дітей – фактичних сиріт при живих батьках, поширення хвороб, понівечені долі тощо. Звичайно, для вирішення такої глобальної проблеми, як торгівля людьми необхідні спільні зусилля міжнародної громадськості. Також необхідно підвищувати життєвий рівень наших громадян, аби вони не їхали за шматком хліба в іншу країну.

Але не менш важливі і наші конкретні зусилля. Тільки спільними зусиллями ми зможемо зупинити потік наших співгромадян за кордон.

А організації суспільного спрямування мають проводити профілактичну роботу з молоддю із групи ризику, поширювати інформацію про протидію торгівлі людьми, зробити все, щоб наші громадяни не були довірливими жертвами, адже вони потребують нашої всебічної допомоги.

Список бібліографічних посилань

1. Торгівля людьми: в Україні з початку року виявили майже 300 злочинів // Укрінформ : сайт. 18.10.2019. URL: https://www.ukrinform.ua/rubric-society/2801788-torgivla-ludmi-v-ukraini-z-pocatku-roku-viavili-majze-300-zlociniv.html (дата звернення: 28.10.2019).

2. Жахлива статистика: за півроку в Україні нарахували понад 100 випадків секс-експлуатації // 5 канал : сайт. 30.07.2018. URL: https://www.5.ua/suspilstvo/zhakhlyva-statystyka-za-pivroku-v-ukraini-186-vypadkiv-torhivli-liudmy-z-iakykh-108-seksekspluatatsiia-174624.html (дата звернення: 28.10.2019).
3. Торгівля людьми – ганебне явище XXI століття // Мережа центрів соціальних служб для сім'ї, дітей та молоді м. Києва : сайт. 19.07.2019. URL: http://ssm.kiev.ua/2019/07/19/торгівля-людьми-ганебне-явище-xxi-стол/ (дата звернення: 28.10.2019).
4. Торговля людьми / Департамент общественной информации ООН. URL: http://www.un.org/ru/rights/trafficking/ (дата звернення: 28.10.2019).
5. Вієрс М., Хавеман Р. Огляд законодавства про боротьбу з торгівлею людьми в Україні. 2001. С. 36–37.
6. Буреш І. В. Європейський досвід державного управління з протидії торгівлі людьми. *Економіка та держава*. 2013. № 5. С. 131–133.

Одержано 29.10.2019

УДК 004.946.5.056

Вікторія Русланівна Балик,
студентка 2 курсу юридичного факультету
Тернопільського національного економічного університету

Кіберзлочинність: правові аспекти та механізми забезпечення протидії

Інформаційний злочин – це навмисні дії, спрямовані на руйнування та розкрадання інформації в мережі, інформаційних джерелах, тощо. Згідно Кримінального кодексу України статті 361–363 кіберзлочинами є злочини, що входять до розділу 16 «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [2, с. 170–175]. Злочини, вчинені шляхом незаконних операцій з використанням електронно-обчислювальної техніки мають свої закономірності виникнення матеріальних та ідеальних слідів-відображень, що властиві тому чи іншому способу впливу на комп'ютерну інформацію.

Специфічними для цієї групи злочинів є віртуальні сліди – тобто будь-які зміни стану автоматизованої інформаційної системи, що залишаються на машинних носіях, відображаючи зміни в програмах, базах даних і текстових файлах упродовж часу вчинення злочину, як при безпосередньому так й віддаленому доступі [1, с. 52–53].

Учинення комп'ютерного злочину у більшості випадків має на меті будь-який вплив на машинний носій в ЕОМ – файл і, відповідно, файл даних або прикладного програмованого забезпечення з точки зору криміналістики стає носієм інформаційних слідів, що класифікуються за різними ознаками. До них відносять структурні сліди файлів – зміна тексту, локальні сліди, які з'являються на робочих місцях користувача як результат роботи клієнтської частини операційної системи, мережні сліди, тобі ті, які виникають як результат роботи операційної системи мережі чи прикладного програмного забезпечення мережі та утворюються на вузлах мережі або пристроях та інші.

Нажаль, кіберзлочинність з кожним роком стає все більшою проблемою. За офіційними даними Національної поліції України у 2016 році зафіксовано 3594 кіберзлочинів, а у 2017 їх кількість зросла вдвічі – до

6974. Близько 40% правопорушень з використанням ІТ залишаються не розкритими [3].

Сьогодні всесвітня павутина – це простір для вчинення неправомірних дій організованими злочинними угрупованнями або злочинцями-одинаками. Злочини в мережі відбуваються найрізноманітніші: вимагання з погрозою знищення або блокування баз даних, інформація про теракти, компромат, розкрадання інтелектуальної власності або майна. Комп'ютер все частіше стає знаряддям для вчинення і більш традиційних злочинів. Шахраї в інтернеті можуть використовувати віртуальну мережу для розтрат, розкрадань та привласнення грошових коштів, підробки грошових купюр, документів і кредитних карт, посягання на авторські права і багато чого іншого.

В Україні на законодавчому рівні приймаються відповідні закони та нормативні акти, які регулюють відносини, пов'язані із злочинами у інформаційних системах, мережах. Станом на 2019 рік до правової основи кібернетичної безпеки України входять такі нормативно-правові акти: Конституція України, Кримінальний кодекс України, закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки» інші закони, доктрина інформаційної безпеки України, Конвенція Ради Європи про кіберзлочинність та інші міжнародні договори, згода на обов'язковість яких надана Верховною Радою України. Це пов'язано з тим, що у сучасному світі послуги, виробництво все більше використовує інформаційні технології. Ми залежимо від безперервності та коректності функціонування комп'ютерних систем об'єктів критичної інфраструктури, і атаки з боку та засобами кіберпростору на такі системи спричиняють реальні загрози для безпеки людей і суспільства.

Для захисту своїх особистих прав, інтересів та даних варто дотримуватися правил безпечного використання мережі Інтернет. Насамперед варто встановити комплексну систему захисту, користуватися ліцензійним програмним забезпеченням, здійснювати покупки в офіційних Інтернет-магазинах, з обережністю ставитись до завантажуваних файлів [4].

Злочинці можуть намагатися отримати доступ до вашої інформації, а саме пароль електронної пошти, банківські реквізити чи номер соціального страхування. Для цього вони можуть установлювати зловмисне програмне забезпечення на ваш комп'ютер, пробувати зламати ваш

обліковий запис або оманливим шляхом змушувати вас надати цю інформацію. Після цього злочинці можуть обкрадати вас, видавати себе за вас або навіть продавати ваші дані на торгах.

З огляду на вищезазначене, можу сказати, що кіберзлочинність набирає обертів у сучасному суспільстві, тому створюються відповідні заходи для захисту інтересів громадян. Кібербезпека – це безпека життя, майна людини, так як ми тісно пов'язані з інформаційними технологіями, які заполонили увесь спектр життя суспільства в цілому. Сьогодні на законодавчому рівні створюються всі можливі заходи щодо врегулювання питання кіберзлочинів.

Список бібліографічних посилань

1. Виявлення та розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій : посібник // Б. В. Романюк, М. І. Камлик, В. Д. Гавловський та ін. Київ : Нац. акад. внутр. справ України, 2000. 64 с.
2. Кримінальний кодекс України: зі змінами та доповненнями станом на 25.09.2019 р. : офіц. текст. Київ : Паливода А. В., 2019. 212 с.
3. Уряд погодив проект національної Стратегії забезпечення кібернетичної безпеки // Newsme : сайт. 19.07.2014. URL: http://newsme.com.ua/ua/tech/technologies/2561163/ (дата звернення: 21.10.2019).
4. Як захистити себе в мережі // Українська Наукова Інтернет-Спільнота : сайт. 21.12.2013. URL: https://nauka-online.org/content/yak-zakhystyty-sebe-interneti (дата звернення: 21.10.2019).

Одержано 01.11.2019

УДК 343.43

Олександр Маркович Бандурка,
доктор юридичних наук, професор, академік Національної академії правових наук України, заслужений юрист України,
професор кафедри теорії та історії держави і права
Харківського національного університету внутрішніх справ

Окремі напрями взаємодії Харківського національного університету внутрішніх справ з територіальними органами Національної поліції щодо протидії технологічним наркозлочинам

Збільшення рівня обізнаності правопорушників у комп'ютерних технологіях спричинило появу нових способів учинення тяжких та особливо тяжких злочинів. Правоохоронні органи не завжди можуть вчасно й ефективно реагувати на пов'язані з цим виклики через наявність певних об'єктивних і суб'єктивних причин.

Одним із проблемних питань, пов'язаних з описаною ситуацією, є неможливість швидкого реагування поліції на зростаючу кількість наркомагазинів в інтернеті. Через брак технічних знань, а часом не встигаючи одночасно розслідувати (супроводжувати) велику кількість проваджень, слідчі й оперативні працівники стикнулися з валом відповідних правопорушень, кількість яких лише зростає.

У таких умовах за ініціативи Харківського національного університету внутрішніх справ було порушено питання щодо залучення науково-педагогічного складу та курсантів факультету № 4 (протидії кіберзлочинності та торгівлі людьми) до протидії наркозлочинам, які вчиняються з використанням можливостей кіберсфери. Серед іншого працівники та курсанти факультету брали участь у документуванні роботи інтернет-наркомагазинів на території Харківської та Сумської областей (ч. 3 ст. 307 – незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів; ч. 4 ст. 28 – вчинення злочину групою осіб, групою осіб за попередньою змовою, організованою групою або злочинною організацією; ч. 1 ст. 255 – створення злочинної орга-

нізації – Кримінального кодексу України). За результатами набутого досвіду було підготовлено науково-методичні рекомендації «Особливості документування наркозлочинів, які вчиняються з використанням можливостей кіберсфери», які успішно використовуються оперативними працівниками Управління протидії наркозлочинності ГУНП в Сумській області. Крім того, фахівцями факультету було підготовлено кілька розгорнутих довідок про низку агрегаторів наркомагазинів. Надані до територіальних органів Національної поліції файли довідки з даними сайтів, користувачів і таблицями аналізу можуть бути використані для подальшого проведення кримінального аналізу та документування правопорушень.

У рамках підтримки однієї з громадських ініціатив з протидії розповсюдженню наркотиків фахівцями факультету було також розроблено Telegram-бот «СтопНаркотик» @StopDrugsBot, призначений для допомоги у блокуванні інтернет-ресурсів з продажу наркотичних засобів з використанням месенджеру Telegram.

Враховуючи набутий досвід, а також високу завантаженість працівників територіальних органів Національної поліції, для покращення рівня протидії наркозлочинності, набуття практичного досвіду майбутніми поліцейськими, в університеті на стадії реалізації перебуває пілотний проект із залучення окремих курсантів у позанавчальний час в якості спеціалістів до роботи слідчо-оперативних груп, що здійснюють досудове слідство щодо наркозлочинів, які вчиняються з використанням можливостей кіберсфери. Для цього розроблено окремий алгоритм їх роботи, який уже апробовано у практичних умовах.

Одержано 25.10.2019

УДК 341.231.14

Анастасія Геннадіївна Батог,
студентка 4 курсу кафедри міжнародного і європейського права юридичного факультету Харківського національного університету імені В. Н. Каразіна

Альона Леонідівна Шевченко,
викладач кафедри міжнародного і європейського права юридичного факультету Харківського національного університету імені В. Н. Каразіна

Право на інтернет як фундаментальне право людини

1 липня 2016 року Генеральна Асамблея ООН ухвалила Резолюцію Ради з прав людини про заохочення, захист і реалізацію права людини в Інтернеті (A/HRC/RES/32/13), якою публічно засудила країни, які навмисно обмежують доступ своїх громадян до глобальної мережі Інтернет. В основу Резолюції покладені попередні заяви щодо цифрових прав, що відображають незмінну позицію Організації: «люди повинні бути однаково захищені як офлайн, так і онлайн» [1], зокрема ті, в яких особливий акцент зроблено на свободу слова. Нагадаємо, це право опосередковано згадано в таких міжнародних документах з прав людини, як Загальна декларація прав людини 1948 р. (ст. 19) [2] та Конвенція про захист прав людини і основоположних свобод 1950 р. (ст. 10) [3].

Слід зазначити, що фінальний варіант Резолюції натрапив на деякий опір з боку країн з авторитарним режимом, в числі яких Росія, Китай і Саудівська Аравія, а також низки демократичних держав на кшталт ПАР та Індії. Згадані країни зажадали виключити з Резолюції уривок, де йдеться про «беззастережне засудження будь-яких заходів щодо умисного обмеження або блокування доступу до розміщеної в мережі інформації» [1].

Хоча подібні резолюції носять виключно рекомендаційний характер і не мають обов'язкової юридичної сили, вони мають надзвичайно важливий політичний вплив і часто є ефективним засобом тиску на уряди держав-членів ООН.

Дане рішення ООН є особливо актуальним в світлі ситуації, за умов якої почастішали випадки, коли різні держави обмежують доступ до Інтернету для своїх громадян. Тільки впродовж липня 2016 року подібних випадків було кілька: блокування соціальних мереж в Туреччині після теракту в аеропорту Стамбула, відключення мобільного інтернету в Бахрейні та Індії через місцеві протести, а також блокування соціальних мереж в Алжирі на час шкільних іспитів. За даними некомерційної організації Access Now, що відстоює цифрові права користувачів, у 2015 році було як мінімум 15 випадків блокування доступу до Інтернету по всьому світу, тоді як в 2016 році було зафіксовано вже 20 подібних порушень.

Відзначимо, що Резолюція A/HRC/RES/32/13 не є першим документом подібного змісту. Подібні резолюції були прийняті Комісією з прав людини і Радою з прав людини про право на свободу думки і її вільне вираження, зокрема, резолюція Ради 20/8 від 5 липня 2012 р. і 26/13 від 26 червня 2014 р. про заохочення, захист і реалізацію прав людини в інтернеті, а також резолюція 12/16 від 2 жовтня 2009 р. про свободу думки і її вільне вираження, 28/16 від 24 березня 2015 р. про право на недоторканість приватного життя в епоху цифрових технологій; 31/7 від 23 березня 2016 р. про права дитини: використання інформаційно-комунікаційних технологій і сексуальна експлуатація дітей; а також резолюції ГА ООН, зокрема, 68/167 від 18 грудня 2013 р. і 69/166 від 18 грудня 2014 р. про право на недоторканість приватного життя в епоху цифрових технологій, 70/184 від 22 грудня 2015 р. про використання інформаційно-комунікаційних технологій з метою розвитку і 70/125 [1], тощо.

Слід сказати, що критики концепції, запропонованої ООН, ставлять логічне запитання: а чи дійсно право на Інтернет – це фундаментальне право? Попри всі намагання міжнародної спільноти створити однаковий для всіх правопорядок, важко не погодитися з тим, що у світі наразі все ще зберігається певна соціальна нерівність між громадянами різних держав і в кожному конкретному суспільстві в цілому. Існує погляд, що право на Інтернет у середовищі, яке склалося, – це все ще привілей окремих груп населення, а не фундаментальне право кожного.

Проте, з юридичної точки зору вживання в Резолюції саме таких термінів є об'єктивно вмотивованим, адже в загальному вигляді основу правового статусу особи становлять не тільки права і обов'язки, а ще й гарантії їх дотримання і реалізації, а тому можемо сказати, що

проголошуючи право на Інтернет фундаментальним правом людини, ООН пропонує державам-учасницям не просто визнати дане положення у своїх національних правопорядках, а й очевидно закріпити у законодавстві гарантії його реалізації. Тобто, ми бачимо, що дотримання права на Інтернет є скоріше новим міжнародним стандартом у галузі прав людини, імплементація якого має на меті розширити коло носіїв цього права до «кожного».

Таким чином, можемо зробити висновок, що визнання на міжнародному універсальному рівні права на Інтернет, як фундаментального права людини, є загалом позитивним шляхом не тільки у сфері забезпечення свободи вираження думки, права на інформацію та інших прав людини, а й у подоланні проблем загальносвітового масштабу, як-то майнова нерівність, безробіття, неможливість доступу до освіти тощо.

Список бібліографічних посилань

1. The promotion, protection and enjoyment of human rights on the Internet : Resolution adopted by the Human Rights Council on 1 July 2016 32/13. URL: https://undocs.org/en/A/HRC/RES/32/13 (дата звернення: 30.10.2019).
2. Загальна декларація прав людини : прийн. і проголош. резолюцією 217 А (III) Ген. Асамблеї ООН від 10.12.1948 // База даних (БД) «Законодавство України) / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/995_015 (дата звернення: 30.10.2019).
3. Конвенція про захист прав людини і основоположних свобод : від 04.11.1950 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/995_004 (дата звернення: 30.10.2019).

Одержано 01.11.2019

УДК 004.056

Сергій Миколайович Бортник,
доктор юридичних наук, перший проректор Харківського національного університету внутрішніх справ

Соціальна інженерія як метод вчинення злочинів

Із кожним днем по всьому світу розвиток інформаційних технологій набирає все більших обертів, вони застосовуються майже в усіх сферах людської діяльності. Злочинці теж не стоять на місці, зловживають даними можливостями й вигадують і застосовують кожного разу більш витончені способи та методи досягнення своїх цілей. Одним із основних сучасних інструментів, який є в арсеналі шахраїв і швидко розвивається, є соціальна інженерія.

Соціальна інженерія – це метод керування діями індивідууму без використання технічних засобів, що ґрунтується на використанні слабкостей людського фактора. Найчастіше соціальну інженерію розглядають як незаконний метод отримання інформації, тому сьогодні її активно використовують в інтернеті для отримання закритої інформації або інформації, яка являє велику цінність.

Соціальна інженерія є небезпечним фактором у контексті безпеки роботи підприємства, установи чи організації в цілому, тому що системи захисту створюють для зловмисника бар'єр, який досить складно подолати без спеціальних знань і навичок. У цьому випадку неважливо, якого саме працівника вдалося ввести в оману зловмиснику, тому що результатом є доступ до всіх внутрішніх ресурсів з обминанням бар'єру захисту. Атаки за допомогою методів соціальної інженерії нерідко орієнтуються на працівників, у яких є найбільші права доступу до конфіденційної інформації. Однією з важливих причин поширення соціальної інженерії як методу атаки є те, що це досить дешевий вид нападу. При цьому зловмисник може не бути фахівцем у сфері інформаційних технологій.

Найпопулярнішим серед численних сучасних інструментів соціальної інженерії є фішинг, метою якого може бути заволодіння обманним шляхом інформацією приватного характеру. Попри те, що про нього

широко відомо, успіх фішингу продовжує зростати через недостатню освіченість, низький рівень так званої кіберкультури людей.

Фішинг застосовується за певною схемою. Зловмисники можуть маскуватися під установи, яким довіряє людина. Наприклад, прикидаючись представниками оператора мобільного зв'язку або працівниками банку, вони можуть надсилати електронні листи з додатком або посиланням, за яким людина має ввести свої особисті дані. Потенційній жертві соціальної інженерії також можуть додатково зателефонувати з проханням відкрити певний додаток або перейти за надісланим посиланням. Вважається, що таке «живе» спілкування додає ситуації чималої правдоподібності та зазвичай змушує людей відкривати вкладення. Слід зазначити, що на такий «гачок» потрапляють не лише звичайні громадяни, а й навіть досвідчені експерти з кібербезпеки різних підприємств, установ та організацій.

Зважаючи на актуальність цієї проблеми, є необхідність у дослідженні й аналізі найбільш поширених алгоритмів злочинних дій у мережі Інтернет і виокремленні проблем, що виникають під час профілактики та боротьби з кіберзлочинністю, а також у наданні рекомендацій щодо протидії використанню різноманітних технік соціальної інженерії для здійснення шахрайських дій у мережі Інтернет.

Слід зазначити, що основними недоліками у сфері запобігання негативним проявам соціальної інженерії є відсутність системної роботи щодо її виявлення та подолання, низький рівень проінформованості населення щодо можливих загроз соціальної інженерії (варто відзначити позитивну роботу деяких банків у цій сфері), а також висока латентність таких злочинів, що унеможливлює виявлення та притягнення до відповідальності всіх винних осіб.

Одержано 01.11.2019

УДК 343

Поліна Романівна Бортнік,
студентка 4 курсу юридичного факультету
Харківського національного університету імені В. Н. Каразіна

Ігор Сергійович Воєводін,
викладач кафедри міжнародного і європейського права
юридичного факультету Харківського національного
університету імені В. Н. Каразіна

Правова природа та сутність кіберзлочинності

Невідворотність глобалізаційних процесів призвела до появи принципово нового сприятливого середовища для вчинення кіберзлочинів. Даний вид суспільно-небезпечного діяння характеризується креативним підходом, інноваційними методами досягнення злочинної мети та високою латентністю.

Терміни «кіберзлочин» та «комп'ютерний злочин» дуже часто стоять поруч у науковій літературі, проте за своєю суттю не є синонімічними. Зокрема «кіберзлочин» є більш широким, в той час, як середовищем вчинення комп'ютерних злочинів виступає інформаційний простір, мережа Інтернет.

Конвенція Ради Європи «Про кіберзлочинність» не містить легальної дефініції кіберзлочинності [1]. Проте, даний термін визначений в українському законодавстві. У ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» кіберзлочинність трактується як сукупність кіберзлочинів [2, ст. 1]. У свою чергу, кіберзлочин ототожнюється із комп'ютерним злочином та трактується як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України. Кіберпростором є середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене у результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних ко-

мунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних.

Серед найпоширеніших кіберзлочинів виділяють:

- використання програм, що несуть загрозу;
- DDOS атаки (злочинець надсилає велику кількість запитів, що в результаті виводить з ладу об'єкт функціонування);
- комбінація соціальної інженерії і шкідливого коду (фішинг) – передбачає спонукання жертви до певних дій. Наприклад відвідання сайту, натискання на вміст електронного листа, що в подальшому призводить до зараження системи;
- незаконна діяльність: домагання, поширення незаконного контенту. У цьому випадку зловмисники приховують свої сліди за допомогою анонімних профайлів, зашифрованих повідомлень та інших подібних технологій;
- незаконна діяльність з обчислювальними машинами та фінансовими апаратами [3].

У механізмі детермінації кіберзлочинності можна умовно виділити такі групи чинників: соціальні, політичні, економічні, технологічні, психологічні, а також чинники пов'язані з діяльністю правоохоронних органів та віктимною поведінкою потерпілих.

Небезпека кіберзлочинності полягає ще й у її територіальній розповсюдженості. Даний злочин є транснаціональним, що значно ускладнює розслідування та відстеження місцезнаходження суб'єктів злочину.

Серед основних нормативних джерел, що регулюють вищезазначені правовідносини виділяють:

- Конвенцію Ради Європи про кіберзлочинність від 23.11.2001 р.
- Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003 р.
- Кримінальний кодекс України від 05.04.2001 р.
- Закон України «Про розповсюдження примірників аудіовізуальних творів, фонограм, відеограм, комп'ютерних програм, баз даних» від 23.03.2000 № 1587-III
- Закон України «Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи» від 21.07.2006 № 23-V.

Аналізуючи сучасний стан справ, можна помітити низький рівень кібербезпеки в Україні. Це пояснюється недостатнім розумінням самої природи та системи інформаційних технологій, що в свою чергу унеможливлює створення каркасу правових норм, які б на належному рівні врегулювали дані правовідносини.

Дотепер у національному і навіть міжнародному законодавстві бракує єдиного підходу до визначення підстав віднесення протиправних діянь до категорії кіберзлочинів. Отже, першим кроком до створення безпечного кіберпростору є гармонізація національного законодавства із міжнародними нормативно-правовими актами. Важливим елементом є міжнародна співпраця та залучення професіоналів у царині ІТ. Також варто зосередитися на належному функціонуванні єдиних баз (реєстрів) кіберзлочинців та веденні статистики.

Список бібліографічних посилань

1. Конвенція про кіберзлочинність : від 23.11.2001 // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 30.10.2019).
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 30.10.2019).
3. Киберпреступления: понятие, виды и методы защиты // IT-Skills : сайт. 27.03.2018. URL: https://sys-team-admin.ru/stati/bezopasnost/170-kiberprestupnost-ponyatie-vidy-i-metody-zashchity.html (дата звернення: 30.10.2019).

Одержано 01.11.2019

УДК 343.1:65.012.8

Михайло Юрійович Бурдін,
доктор юридичних наук, професор, проректор
Харківського національного університету внутрішніх справ

Кримінальний аналіз у роботі оперативних підрозділів Національної поліції України

Інтенсифікація процесу інтеграції України до Європейського Союзу спонукала вітчизняні правоохоронні органи до імплементації європейських практик протидії злочинності та поліпшення взаємодії між європейськими правоохоронними органами щодо обміну інформацією оперативного характеру. Серед іншого у вітчизняних поліцейських підрозділах відбувається поетапне впровадження проактивної стратегії протидії злочинності, яка орієнтована передусім на попередження злочинів.

Зміщення пріоритетів з реагування на вже вчинені злочини в бік їх попередження в європейських країнах зумовило зміну підходів у роботі поліцейських підрозділів. Однією з ключових новацій стало впровадження моделі стримування злочинності, заснованої на розвідувальних даних (intelligence-led policing) [1]. Вказана модель передбачає широке застосування негласних методів роботи поліції, до яких після Другої світової війни в поліцейських підрозділах Західної Європи ставилися вкрай обережно, а самі вони були переважно прерогативою спеціальних служб. Після розпаду СРСР в Європі поступово на законодавчому рівні унормували застосування негласних методів роботи поліції та почали більш активно використовувати їх для попередження злочинів. До зібраних у процесі кримінальної розвідки даних застосовуються прості та складні математичні методи оцінки й обробки. У результаті одержується нова інформація, яка представляється у вигляді аналітичного висновку. Залежно від характеру вміщуваної інформації такі висновки використовуються на оперативному, тактичному або стратегічному рівнях. Описаний процес оцінки й обробки інформації сьогодні асоціюють із поняттям «кримінальний аналіз», а його структуру та порядок

проведення на тривіальному рівні можна зрозуміти через ознайомлення з методологією Anacapa [2].

Слід відзначити, що для українських поліцейських підрозділів здійснення кримінального аналізу в цілому не є якимось новим явищем, оскільки ще з радянських часів його застосовували під час оперативного обслуговування окремих об'єктів і ліній роботи. Водночас у цьому напрямку відбулися певні організаційні та методологічні зрушення. Зокрема, було створено профільне управління, яке спеціалізується на проведенні кримінального аналізу, затверджено шаблони аналітичних довідок, унесено зміни до низки наказів МВС України щодо запровадження системи оцінки інформації 4х4 тощо.

Суттєвого успіху в проведенні кримінального аналізу в українській поліції вдалося досягти завдяки запровадженню новітніх технологій. Використання в оперативній роботі програм розпізнавання облич, обробки й аналізу великих масивів даних дало змогу суттєво підвищити якість розшукової роботи та висунутих версій, скоротити тривалість оперативного супроводження кримінальних проваджень і встановлення зв'язків фігурантів, забезпечити візуалізацію та хронологічну розстановку великих об'ємів даних.

Діяльність щодо кримінального аналізу в оперативних підрозділах не позбавлена і проблемних моментів. Передусім це відсутність належного апаратного та програмного забезпечення, вкрай обмежений доступ до інформаційних ресурсів державних органів, недостатня кількість фахових працівників у сфері аналізу. Існують і певні проблеми суб'єктивного характеру. Так, через недостатній професійний рівень у сфері здійснення аналізу недосвідчені аналітики нерідко припускаються таких помилок:

- тенденційності, яка полягає у спрямуванні зусиль на підтвердження лише однієї версії;

- хибних уявлень про наявність зв'язків між досліджуваними суб'єктами й об'єктами;

- підготовки висновків на основі неповних даних або різних висновків на основі одних і тих саме даних;

- інтерпретації подій, спираючись на власні фантазії;

- ігнорування незручних фактів і методик оцінки даних;

- корегування висновків під впливом керівників або необґрунтованої думки інших аналітиків.

Підсумовуючи, зазначимо, що практика проведення кримінального аналізу в оперативних підрозділах Національної поліції засвідчила необхідність у навчанні базових знань і навичок такої діяльності всього оперативного складу. Працівники, які на практиці проводять кримінальний аналіз на системному рівні, відповідно мають і кращі показники оперативно-службової діяльності.

Список бібліографічних посилань

1. Манжай О. В., Жицький Є. О. Кримінальна розвідка та її співвідношення з оперативним обслуговуванням. *Jurnalul Juridic Naţional: Teorie şi Practică*. 2015. № 3 (13). С. 100–105.
2. Манжай О. В. Аналіз методології кримінальної розвідки в зарубіжних країнах. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*. 2016. № 3 (75). С. 256–265.

Одержано 25.10.2019

УДК 343.5

Анна Олександрівна Ведернікова,
ад'юнкт Луганського державного університету внутрішніх справ імені Е. О. Дідоренка

Необхідність кримінально-правового регулювання кібербулінгу

Закон України «Про охорону дитинства» визначає охорону дитинства в Україні як стратегічний загальнонаціональний пріоритет, що має важливе значення для забезпечення національної безпеки України, ефективності внутрішньої політики держави. Із метою забезпечення реалізації прав дитини на життя, здоров'я, освіту та враховуючі світові суспільні течії, 18 грудня 2018 року було прийнято Закон України «Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню)». Вищевказаним законом сформульоване визначення булінгу та внесені зміни до Кодексу України про адміністративні правопорушення, в якому передбачено адміністративну відповідальність за цькування у закладах освіти.

Булінг (цькування) – це діяння учасників освітнього процесу, які поля-гають у психологічному, фізичному, економічному, сексуальному насильстві, у тому числі із застосуванням засобів електронних комунікацій, що вчиняються стосовно малолітньої чи неповнолітньої особи або такою особою стосовно інших учасників освітнього процесу, внаслідок чого могла бути чи бу-ла заподіяна шкода психічному або фізичному здоров'ю потерпілого [1]. Саме булінг, який здійснюється із застосуванням засобів електронних комунікацій, називається кібербулінг. Як бачимо законодавець не закріплює дане поняття, а тільки уточнює у який саме спосіб може здійснюватися булінг. Так само, і у науковій літератури досі немає єдиного правового визначення кібербулінгу, як суспільно небезпечного протиправного діяння.

За даними опитування Дитячого фонду ООН (ЮНІСЕФ) та Спеціальної представниці Генерального секретаря ООН з питань насильства щодо дітей, яке було проведене у 2019 році, третина молодих людей у 30 країнах світу стають жертвами онлайн-булінгу, а кожна п'ята молода людина змушена бу-ла пропускати заняття в школі через кібербулінг та

насильство. В Україні 29% опитаних підлітків були жертвами онлайн-булінгу, а 16% були змушені пропускати через це шкільні заняття [2].

Кібербулінг хоча і походить від звичайного булінгу, але має ряд своїх особливостей, які значно підвищують його суспільну небезпечність у порівнянні з останнім. Інтернет – це масовий ресурс і чутки, фейки, невдалі чи від-редаговані фото швидко розповсюджуються й складно вилучаються з мережі. Вони можуть бути розмножені, а також зберігатись у цифровому вигляді. Поняття системності трансформується через масовість аудиторії користувачів. Від онлайн-булінгу неможливо приховатися. Наявності підключення до мережі робить цей вид цькування цілодобовим, незалежно від місцезнаходження жертви. Знеособлення булера та неможливість належної відповіді призводить до постійного відчуття загрози [3, 47–49].

Існують такі різновиди кібербулінгу: використання особистої інформації; анонімні погрози; телефонні дзвінки з мовчанням; переслідування (як елемент фізичного переслідування, шляхом розсилки повідомлень на електронну пошту чи телефон, збирання інформації про жертву, відстеження її переписки); тролінг (розміщення провокаційних повідомлень в мережі); хепі-слепінг (happy slapping) (насильство заради розваги, у тому числі знімання насильства на камеру для подальшого розповсюдження в мережі); сексуальні посягання [4].

В Україні ці питання чітко не визначені законодавцем, хоча зарубіжний досвід свідчить, що саме кримінально-правовому регулюванню кібербулінгу та такому його підвиду, як кіберпереслідування, приділяється велика увага світової спільноти.

У 2018 році американські науковці Sameer Hinduja й Justin W. Patchin проаналізували кримінально-правове законодавство США щодо протидії кібербулінгу та дійшли висновку, що: 48 штатів мають закони, які включають положення про кібербулінг або інтернет-домагання; 44 штати передбачають кримінальні санкції за електронне цькування; 49 штатів застосовують шкільну антибулінгову політику, а 45 штатів передбачають шкільні санкції за вказані правопорушення, у 17 з них відповідальність настає за дії вчинені поза межами навчального закладу [5]. У всіх штатах є різні кримінальні закони щодо протидії булінгу, і більшість з них містять чіткі посилання на електронні форми. Наприклад, у Каліфорнійському кодексі про освіту розкривається визначення булінгу, а також чітко прописані усі можливі його прояви із використан-

ням засобів зв'язку. Окрім поняття «кібербулінг» законодавець вводить поняття «кіберсексуального булінгу». Особливістю цього закону є те, що передання або розміщення в Інтернеті неналежної інформації не вважається розповсюдженою поведінкою, тобто не дає системності [6].

Встановлення чіткого понятійного апарату, дозволяють налагодити ефективну систему протидії проявам булінгу із застосуванням засобів електронних комунікацій. Пропонуємо визначення, яке на наш погляд розкриває найважливіші його аспекти. Кібербулінг – це насильницькі дії учасників освітнього процесу із застосуванням електронних форм комунікацій, включаючи мобільний і стільниковий телефони, інші пристрої бездротового зв'язку, комп'ютер, що вчиняються стосовно неповнолітньої особи або такою осо-бою, і могли спричинити або спричинили наступні наслідки: втручання у навчальний процес, шкільну дисципліну або суттєве їх недодержання, порушення прав учасників освітнього процесу, завдання їм моральної, психічної, фізичної, матеріальної шкоди.

Часто булінг фактично переростає в катування з наявністю всіх ознак складу цього злочину, за винятком суб'єкта. Діти-булери до 16-ти років, які вчинили дії, що утворюють склад катування, не несуть кримінальної відповідальності за ст. 127 КК України, оскільки в ч. 2 ст. 22 КК України цей зло-чин не передбачено в переліку тих, кримінальна відповідальність за які настає з 14-ти років. Якщо ж вони здійснюють свої неправомірні дії через мережу Інтернет (кібербулінг), то за погрози іншим дітям в Інтернеті відповідальність несе власник того комп'ютера, з якого було поширено неправдиву інформацію або залякування. З огляду на наявну в Україні практику, найчастіше дії кібербулерів кваліфікують як хуліганство (ст. 296 КК України) [7, 281].

Необхідність кримінально-правового регулювання кібербулінгу обумовлена масштабністю даних проявів. А відсутність законодавчого закріплення цього поняття та його видів, заважає належній реалізації наявних правових норм.

Список бібліографічних посилань

1. Про внесення змін до деяких законодавчих актів України щодо протидії булінгу (цькуванню) : Закон України від 18.12.2018 № 2657-VIII. *Відомості Верховної Ради України*. 2019. № 5. Ст. 33.
2. Опитування ЮНІСЕФ: понад третина молодих людей у 30 країнах світу потерпають від онлайн-булінгу // Unicef Ukraine : сайт. 04.09.2019. URL:

https://www.unicef.org/ukraine/uk/прес-релізи/опитування-юніcеф-понад-третина-молодих-людей-у-30-країнах-світу-потерпають-від-онлайн (дата звернення: 18.10.2019).
3. Стоп шкільний терор. Особливості цькувань у дитячому віці. Профілактика та протистояння булінгу : дослідження. 2017. 84 с. // Український інститут дослідження екстремізму : сайт. 20.01.2018. URL: http://uire.org.ua/wp-content/uploads/2017/11/Doslidzhennya-buling.pdf (дата звернення: 18.10.2019).
4. Кібербулінг: загроза XXI століття // На Урок : сайт. 26.12.2017. URL: https://naurok.com.ua/post/kiberbuling-zagroza-hhi-stolittya (дата звернення: 18.10.2019).
5. Hinduja S., Patchin J. W. State Bullying Laws. Updated November 2018. URL: https://cyberbullying.org/Bullying-and-Cyberbullying-Laws.pdf (дата звернення: 18.10.2019).
6. California Code, Education Code – EDC § 48900 URL: https://codes.findlaw.com/ca/education-code/edc-sect-48900.html (дата звернення: 18.10.2019).
7. Миронюк Т. В., Запорожець А. К. Кібербулінг в Україні – соціально небезпечне явище чи злочин: визначення та протидія. *Юридичний часопис Національної академії внутрішніх справ*. 2018. № 2. С. 275–284. URL: http://nbuv.gov.ua/j-pdf/aymvs_2018_2_25.pdf (дата звернення: 18.10.2019).

Одержано 01.11.2019

УДК 341.3

Ігор Сергійович Воєводін,
викладач кафедри міжнародного і європейського права юридичного факультету Харківського національного університету імені В. Н. Каразіна

Кібервійна як сучасний метод ведення збройних конфліктів

Розділення дійсності на реальність і віртуальність, пов'язану з появою всесвітньої мережі Інтернет, у найближчі кілька років буде подолано і остаточно сформується єдина дійсність. Фактично це означає, що інформаційні технології будуть присутні повсюдно і будуть постійно використовуватись у всіх сферах побуту, соціальному, політичному, економічному житті, формуючи так званий «кіберпростір». В той же час, це передбачає нові ризики і нові види вразливості. Зокрема, мова йде про кібервійну – цілеспрямований деструктивний вплив інформаційних потоків у вигляді програмних кодів на матеріальні об'єкти та їх системи заради їх знищення, порушення функціонування або перехоплення керування ними [1].

Міжнародний Комітет Червоного Хреста під терміном «кібервійна» розуміє операції, за допомогою потоку даних, спрямовані проти комп'ютера або комп'ютерних систем, коли такі використовуються у якості засобу і методу війни в ситуації збройного конфлікту [2, с. 69].

Кібервійна викликає потенційну стурбованість з огляду на вразливість кібермереж і наслідки гуманітарного характеру, до яких можуть призвести кібератаки. Шкода, яка завдана фізичним особам, організаціям або об'єктам інфраструктури в результаті інцидентів у кіберпросторі, зокрема цілеспрямованих атак, може бути не менш істотною, аніж наслідки традиційних збройних конфліктів і зіткнень [3, с. 101].

Стосовно питання застосовності міжнародного гуманітарного права в кіберпросторі, слід зазначити, що переважно більшість його норм формувалася досить давно, коли людство навіть не уявляло можливість переведення війн у нову «кіберплощину» і автори текстів міжнародних конвенцій не могли описати правила поведінки, які б поширювали свою дію на ще не існуючий простір, новітній театр ведення війни.

Кіберконфлікти за своєю сутністю є унікальним явищем. По-перше, вони не пов'язані із застосуванням звичайної, кінетичної зброї, у зв'язку з чим достатньо складно визначити місце проведення бойових дій. Кібератаки можуть мати місце в різних місцях планети, знаходитися під юрисдикцією різних держав, а тому визначити театр ведення війни і обмежити цю територію на практиці виявляється вкрай складно. Іншою особливістю є складність у визначенні складу учасників, адже від цього залежить не тільки кваліфікація конфлікту, але й обсяг захисту, що надається кожній особі, визначення законних цілей для нападу і можливість притягнення до відповідальності [3, с. 101–102].

В 2013 р. Об'єднаним центром передового досвіду по кібероборoні НАТО було прийнято документ, відомий як «Таллінське керівництво щодо застосування юридичних норм міжнародного права до військових дій у кіберпросторі». Він став першим документом такого роду і закладає основи юридичного забезпечення застосування засобів ведення інформаційно-технічного протиборства у комп'ютерних мережах. Основний висновок полягає в тому, що згідно з існуючими поглядами, основоположні принципи міжнародного права застосовні до дій у кіберпросторі. Той факт, що комп'ютерні атаки в ході збройних конфліктів не мають безпосередньої динамічної, фізичної або насильницької форми не виводить їх за межі дії міжнародного гуманітарного права [4, с. 18]. Тобто кіберпростір нічим не відрізняється від інших сфер протиборства і не вимагає особливих підходів до його юридичного забезпечення.

У своїй доповіді за 2015 р. Група урядових експертів по досягненням в галузі інформатизації і телекомунікацій в контексті міжнародної безпеки ООН зазначила, що в процесі використання інформаційно-комунікаційних технологій держави зобов'язані керуватися принципами міжнародного гуманітарного права – гуманності, необхідності, пропорційності і вибірковості [5].

Таким чином такий феномен як кібервійна виводить міжнародно-правове регулювання збройних конфліктів на новий рівень складності, який може поставити перед міжнародним гуманітарним правом низку принципово нових питань. Доки немає спеціалізованого юридично обов'язкового міжнародного документу, який би регулював правила ведення війни у кіберпросторі, мають застосовуватися принципи та норми міжнародного гуманітарного права щодо пропорційності та

незастосування невибіркової зброї, проведення розмежування між військовими цілями і цивільними особами і недопущення віроломства.

Список бібліографічних посилань

1. Овчинский В., Ларина Е. Кибервойны XXI века. О чем умолчал Эдвард Сноуден. М. : Книжный мир, 2014. 352 с.
2. Международное гуманитарное право и вызовы современных вооруженных конфликтов : доклад / подгот. Междунар. Комитетом Красного Креста. XXXII Междунар. конф. Красного Креста и Красного Полумесяца. Женева, Швейцария, 8–10 дек. 2015 г. 108 с.
3. Применение международного права в киберпространстве. *Индекс безопасности*. 2015. № 3 (114), т. 21. С. 101–118.
4. Гриняев С. Таллиннское руководство по применению юридических норм международного права к военным действиям в киберпространстве в оценках западных экспертов. *Обзор НЦПТИ*. 2015. № 3. С. 18–22.
5. Бойко С. М. Группа правительственных экспертов ООН по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности: взгляд из прошлого в будущее. *Международная жизнь*. 2016. № 8. С. 53–71.

Одержано 01.11.2019

УДК 004.946.5.056

Юлія Вікторівна Гурзель,
студентка 2 курсу юридичного факультету
Тернопільського національного економічного університету

Кіберзлочинність: основні причини та методи боротьби

Розповсюдження комп'ютерних технологій та техніки, повсюдне існування телекомунікаційних мереж як полегшило, так і ускладнило сучасний інформаційний світ. Йдеться про створення безпечних умов використання віртуального простору, адже з кожним днем збільшується злочинність у всесвітній мережі. Більш того, розмах комп'ютеризації та рівень можливостей, які при цьому одержують зловмисники, й тенденція збільшення кількості злочинів у комп'ютерних інформаційних технологій становлять загрозу національній безпеці України. Поширення комп'ютерних вірусів, шахрайство, крадіжки коштів із банківських рахунків, викрадення персональної та комерційної інформації – це ще не весь перелік кіберзлочинів, оскільки з кожним днем їх кількість та різноманіття тільки збільшується.

Слід зазначити, що з приводу поняття кіберзлочинів в науці кримінального права досі триває дискусія, адже на національному рівні це поняття не має нормативного регулювання, проте цим терміном оперує Конвенція про кіберзлочинність (2001 р.) [1].

Боротьба з кіберзлочинністю неможлива без розуміння правового регулювання інформаційних мереж. Щоб це зробити, потрібно з'ясувати основні причини цього злочину. Ними зокрема є:

1. Головна причина кіберзлочинності – велика прибутковість; внаслідок окремих кіберзлочинів можна отримати великі гроші. Дослідження показує, що кіберзлочинність посідає третє місце після торгівлі наркотиками та зброєю за рівнем збагачення.

2. Соціальні чинники – зміни в суспільному житті, пов'язані із комп'ютеризацією, а також із формуванням інформаційного простору.

3. Технологічні причини – це ті, які проявляються в технічному просторі вчинення кіберзлочинів. Високопрофесійні хакери можуть обходити будь-який захист і замаскувати всі сліди вторгнення. Негатив-

ним чинником є також поширення вірусного ринку в Інтернеті, що дає можливість вчинити злочин навіть тим, хто не володіє комп'ютерними знаннями.

4. Політичні причини, що проявляються в недостатній компетентності уряду щодо можливих слідів кіберзлочинності. Досить мало уваги приділяється правовому регулюванню комп'ютерної системи, яка в порівнянні з іншими деградує у своєму технічному розвитку.

Сьогодні є безліч злочинів, які не знайшли своє місце в законодавстві, тому слід удосконалювати кібербезпеку, залучати до цього спеціалістів, також потрібно не забувати про міжнародне співтовариство, що сприятиме посиленню безпеки.

Кіберзлочинність є один із найпоширеніших видів суспільно небезпечних діянь. Зокрема соціальна небезпека інтернет-піратства постійно зростає. Порушення авторських прав – дія, спрямована на незаконне використання об'єктів інтелектуальної власності, що належать іншим особам. За даними дослідження Асоціації виробників програмного забезпечення (BSA), на 2011 р. рівень піратства в Україні становив майже 85% [2].

Згідно із чинним законодавством, порушення авторського права і суміжних прав чітко визначений як кримінальний злочин, передбачений ст. 176 Кримінального кодексу України, згідно з якою максимальний штраф становить від двохсот до тисячі неоподатковуваних мінімумів доходів громадян або такий злочин карається виправними роботами на строк до двох років або позбавлення волі на той самий строк [3].

Що ж потрібно робити для захисту у мережі?

1. Встановіть надійний пароль, не коротший за 12 символів, не зберігайте його у браузері. Використовуйте різні паролі для кількох облікових серверів.

2. Виходьте зі своїх профілів, якщо ви користувались публічним комп'ютером.

3. Не завантажуйте файли із ненадійних сайтів.

4. Прогляньте і налаштуйте приватність своїх акаунтів у соціальних мережах.

5. Використовуйте двофакторну автентифікацію.

6. Не ходіть по підозрілих посилань

7. Довіряйте антиспам-фільтрам електронної пошти.

Як правило, вони фільтрують практично всі листи, обманом заманює вас на той чи інший хакерський сайт.

8. Встановіть комплексну систему захисту. Сьогодні актуальні так звані «комплексні системи захисту», які включають в себе антивірус, файрволл, антиспам-фільтр і ще пару-трійку модулів для повного захисту вашого комп'ютера.

9. Робіть покупки тільки в перевірених онлайн-магазинах.

10. Користуйтеся ліцензійним програмним забезпеченням [4].

Зважаючи на вищесказане, можна дійти висновку, що кіберзлочинність набула популярності саме у XXI ст., коли зросла модернізація технологій та суспільства. Звичайно, вживаються заходи щодо боротьби із цим злочином, але їх недостатньо. Тому варто приділяти більше уваги цій проблемі, розробляти нові методи боротьби, що дадуть набагато більше позитивних результатів, а також покращити систему захисту у соціальних мережах.

Список бібліографічних посилань

1. Конвенція про кіберзлочинність : від 23.11.2001 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 10.09.2018).
2. Голуб А. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби // Ресурсний центр гурт : сайт. 03.10.2016. URL: https://www.gurt.org.ua/articles/34602/ (дата звернення: 30.10.2019).
3. Кримінальний кодекс України: чинне законодавство зі змінами та допов. Станом на 1 верес. 2019 року : офіц. текст. Київ : Паливода А.В., 2019. 264 с.
4. Українська Антипіратська Асоціація : офіц. сайт. URL http://apo.kiev.ua/index.php (дата звернення: 30.10.2019).

Одержано 01.11.2019

УДК 341.4:004

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

Кібератаки як елемент гібридної війни

Гібридна війна може розглядатися як більш досконалий або ефективний спосіб ведення війни, оскільки вона прагне досягти політичних цілей без широкого використання збройних сил та насильства. Особливістю гібридної війни є свідоме розмиття меж між війною і миром, вона не оголошується, її ініціювання зазвичай проходить непомітно. Використання цілого ряду інструментів гібридної війни, таких як кібератаки, заходи економічного впливу, інформаційні операції та обмежені фізичні атаки, які породжують невизначеність у широких верств населення, можуть бути достатніми для досягнення політичних цілей.

Одним із ефективних елементів гібридної війни є кібератаки. Вони направлені, насамперед, на дестабілізацію комп'ютерних систем держави. Міждержавні відносини і політичне протистояння інколи знаходять своє продовження в мережі Інтернет у вигляді окремих проявів втручання в комп'ютерні системи. Розглянемо лише декілька видів кібератак, що є елементами гібридної війни:

- вандалізм – атака, яка завдає удару по авторитету держави як у світі, так і серед населення, простими словами, завдає репутаційних втрат. До таких кібернетичних атак можна віднести пошкодження вебсайтів державних органів і установ, заміну змісту образливими чи пропагандистськими малюнками тощо;

- пропаганда – розсилка спаму, що містить інформацію пропагандистського характеру, фейкові новини для просування вигідної точки зору та дезорієнтації населення;

- збір інформації (кібершпигунство) – злом приватних сторінок або серверів баз даних для збору цінної інформації та її заміни на інформацію, корисну іншій стороні;

- відмова сервісу – атаки з великої кількості комп'ютерів, основна мета яких є порушення функціонування сайтів або комп'ютерних систем;

- втручання в роботу обладнання – атаки на комп'ютери або сервери, які, наприклад, забезпечують роботу комунікаційних цивільних або військових систем, що призведе до відключення або виникнення помилок при обміні даними;

- атаки на об'єкти критичної інфраструктури – атаки на комп'ютери та системи, що забезпечують життєдіяльність населених пунктів і держави взагалі, а саме: системи водопостачання, електроенергії, транспорту тощо [1].

З розвитком інформаційно-комунікаційних технологій рівень і чисельність кібератак постійно зростає. Деякі держави почали приділяти значну увагу захисту від кібератак – розробляти необхідні засоби для організації системної оборони і захисту об'єктів критичної інфраструктури, а також формувати спеціальні підрозділи, основним завданням яких є забезпечення національної кібербезпеки.

Крім того, держави почали витрачати більше ресурсів на створення своїх кіберможливостей, і роль використання кібердомену (віртуальної сфери) неспинно зростає саме у військовій сфері. Такий стан речей свідчить про початок гонки цифрових озброєнь, де правила участі міжнародною спільнотою ще не кодифіковані.

Розвинені країни докладають значних зусиль для вироблення власної кібернетичної зброї, яка замінить за ефективністю класичну зброю (кулі, бомби, танки, літаки тощо). Такий сценарій розвитку військової стратегії вже стає реальністю. Так, наприклад, Міністерство оборони США відкрито заявляє, що вони створюють комп'ютерний код, здатний вбивати. Згідно з опублікованим посібником Міністерства оборони США про військові дії, операції із використанням кіберзброї можуть викликати такі загрози як знищення або пошкодження ядерної установки; відкриття дамби над населеним пунктом, що спричинить руйнування; відключення служби управління повітряним рухом, що спричинить аварії літаків тощо [2, с. 522].

У сучасних умовах розвитку інформаційного суспільства ефективна протидія кібератакам як проявам гібридної війни потребує не лише спільних зусиль розвинутих країн світу, але й розробку і здійснення максимально ефективних міжнародних інструментів. Тому всі економічні і політичні ресурси з протидії загрозам кібербезпеки повинні розглядатися на найвищому світовому рівні за участю основних кібердержав.

Забезпечення ефективної протидії кібератакам диктує важливість розробки, здійснення й удосконалення ефективних національних і міжнародних заходів:

- розробка державами ефективних моделей державної політики та національної концепції з кібербезпеки, що відповідають вимогам національної безпеки держав в контексті глобальних викликів та інших тенденцій сучасності;

- розвиток міжнародно-правових механізмів і загальної міжнародної політики по розробці і здійсненню ефективних інструментів з протидії кібератакам;

- налагодження і розвиток тісного співробітництва з НАТО, ОБСЄ, ЄС у галузі протидії різним проявам гібридної війти, у тому числі кібератака тощо.

Список бібліографічних посилань

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. Кібербезпека як важлива складова всієї системи захисту держави // Міністерство оборони України : офіц. веб сайт. 07.05.2018. URL: http://www.mil.gov.ua/ukbs/kiberbezpeka-yak-vazhliva-skladova-vsiei-sistemi-zahistu-derzhavi.html (дата звернення: 26.10.2019).
3. Limnell J. The Exploitation of Cyber Domain as Part of Warfare: Russo-Ukrainian War. *International Journal of Cyber-Security and Digital Forensics (IJCSDF).* 2015. Vol. 4, No. 4. P. 521–532. DOI: https://doi.org/10.17781/P001973.

Одержано 28.10.2019

УДК 343.901.8(343.352)

В'ячеслав В'ячеславович Гладкий,
аспірант Навчально-наукового інституту
права імені князя Володимира Великого

Корупційна толерантність до торгівлі людьми

Лауреат Нобелівської премії миру та 7-й Генеральний секретар ООН К. Аннан справедливо стверджував, що корупція – це «підступна чума, що чинить широкий спектр агресивних впливів на суспільство». Серед іншого, цей феномен підриває демократію і верховенство права, веде до порушень прав людини, спотворює ринкові відносини, підриває якість життя і «дозволяє процвітати організованій злочинності, тероризму та іншим загрозам безпеки людини» [1, с. iii]. Цілком закономірно припустити, що корупція обумовлює також і торгівлю людьми або ж, як мінімум, є фактором, що полегшує вчинення цього злочину, зважаючи на сутнісну природу корупції [2, с. 2018–2019]. Зокрема, один з провідних сучасних дослідників феномена рабства проф. К. Бейлз стверджує, що в усьому світі рабство зростає там, де корупція підриває верховенство права і робить людей вразливими перед торговцями людьми [3, с. 15]. Водночас, американські вчені проф. Ш. Чжан та С. Пінеда звертають увагу на те, що хоча дослідники проблематики торгівлі людьми час від часу вказували на корупціогенність правоохоронних органів в якості такого собі фактору, що полегшує торгівлю людьми, в той же час, мало хто зосереджує свою дослідницьку увагу на тому, що саме корупція є фундаментальною причиною цього злочину [4, с. 45, 53].

Поза сумнівом, зв'язок корупції з торгівлею людьми є абсолютно закономірним, хоча, торгівля людьми може мати місце також і в тих державах, в котрих рівень панування корупції знаходиться на мінімальному рівні або ж цей феномен взагалі не здатний досягти панування в суспільстві (і державі) через низький поріг толерантності суспільства до корупційної практики. Тому, ми можемо припустити, що *корупція посилює успішність здійснення торгівлі людьми, а, відповідно – сприяє зростанню ринку рабів*. Це припущення про *«корупційну толерантність до торгівлі людьми»* можна пояснити, щонайменше, такими міркуваннями: (1) торгівля людьми криміналізована (криміналізація

будь-якого діяння за умови, коли правоохоронна система знаходиться поза ефективним контролем, обумовлює вибірковість кримінального переслідування й вибіркове судочинство, що, зрозуміло, засновані на корупційному фундаменті); (2) торгівля людьми є найважливішою економічною діяльністю, що кримінально переслідується (після незаконної торгівлі зброєю і наркотиками [4, с. 41]), а також надає злочинцям значний дохід і, відповідно, становить собою інтерес для тих суб'єктів, що покликані запобігати та протидіяти відповідному суспільно небезпечному діянню, проте, не спроможні протистояти т. зв. »корупційній спокусі» [5, с. 86–88].

Разом із тим, висока рентабельність корупційної змови публічного службовця з работорговцем, особливість работоргівлі (латентний характер злочину; цей злочин вчиняється професійними злочинцями, що мають відповідний авторитет, який чиновник може перевірити в злочинному світі) є серйозним стимулом для чиновника, що толерантно ставиться до корупції.

Крім того, важливо взяти до відома, що зі збільшенням чисельності населення планети, а особливо в державах, які неможливо зараз назвати правовими, знизилася і номінальна «ціна» за людину. Процеси, котрі спонукають зниження ціни пропозиції за людину, здійснюються разом із процесами збільшення рівня вразливості людей перед зловмисниками. За нашим спостереженням, цей рівень вразливості забезпечується саме особами, котрі володіють публічною владою та/або публічним впливом (зокрема, громадські активісти, що маскуються, приміром, за антикорупційною діяльністю чи боротьбою за соціальну рівність), а, таким чином, мають можливість сприяти безкарності работорговців, приховувати їх діяльність. Відповідно, корумпована особа є високо толерантною до торгівлі людьми, а тому може сприятиме зниженню безпеки людини (це спричиняє додаткове зниження «ціни» людини) в тій мірі, в якій рівень безпеки людини буде економічно вигідним для ринку рабів (тобто, коли витрати на поневолення людини, сукупно з витратами на здійснення відповідної організованої злочинної діяльності, становитимуть загальну суму, що не впливатиме на «конкурентоздатність» людини; у цьому контексті можна в повній мірі ґрунтуватись на раніше концептуалізованій нами формулі ціни корупційної послуги [6]). У той же час, наявність в державі людей, поневолення яких видається економічно виправданим, спонукає до торгівлі людей (або ж до зростання вже існуючого ринку рабів) зловмисників, які готові будуть співпрацювати з чиновниками

для отримання рівня протекції, необхідного для успішного здійснення торгівлі людьми. Крім цього, не слід також ігнорувати і той факт, що організаторами ринку рабів або ж їх суб'єктами можуть бути й самі публічні службовці чи їхні близькі родичі.

Список бібліографічних посилань

1. Annan K. A. Foreword. United Nations Convention against Corruption. New York : UN Press, 2004. P. iii–iv.
2. Hladky V. V. The Structure of the System of Corruption Crime Subjects according to the Legislation of Ukraine. *Path of Science.* 2019. Vol. 5 (4). P. 2008–2021. DOI: https://doi.org/10.22178/pos.45-4.
3. Bales K. Understanding Global Slavery: A Reader. Berkeley : University of California Press, 2005. 212 p. DOI: https://doi.org/10.1525/californ ia/9780520245068.001.0001.
4. Zhang S. X., Pineda S. L. Corruption as a Causal Factor in Human Trafficking // Organized Crime: Culture, Markets and Policies / ed.: D. Siegel. New York, NY : Springer, 2008. P. 41–55. DOI: https://doi.org/10.1007/978-0-387-74733-0_4.
5. Гладкий В. В. Зв'язок торгівлі людьми з корупцією // Вища освіта – студентська наука – сучасне суспільство: напрями розвитку : матеріали III Міжнар. студент. наук.-практ. конф. (м. Київ, 19 квіт. 2019 р.) / ПВНЗ «Міжнародний науково-технічний університет імені академіка Юрія Бугая», каф. ЮНЕСКО «Інформаційно-комунікаційні технології в освіті». Київ : МНТУ, 2019. С. 85–89.
6. Hladky V. V. Criminometric Analysis of Corruption Permissiveness and Conditions of Pricing in Corrupt Services. *Journal of the National Academy of Legal Sciences of Ukraine.* 2019. Vol. 26 (2), P. 22–34. DOI: https://doi. org/10.31359/1993-0909-2019-26-2-22.

Одержано 28.09.2019

УДК 004.056

Владислав Сергійович Герасимюк,
курсант 4 курсу факультету № 4
Харківського національного університету внутрішніх справ

Юрій Миколайович Онищенко,
кандидат наук з державного управління, доцент,
доцент кафедри інформаційних технологій та кібербезпеки
факультету № 4 Харківського національного університету
внутрішніх справ

Проблеми забезпечення кібербезпеки як складової публічної безпеки

Останнім часом в умовах стрімкого розвитку інформаційних технологій і виникнення численних гібридних загроз проблема забезпечення публічної безпеки стає все більш складною. Згідно п. 4 ст. 3 закону України «Про національну безпеку України» державна політика у сферах національної безпеки і оборони охоплює низку різних напрямів і спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, в тому числі й кібербезпеки України. Відповідно до ст. 1 закону України «Про основні засади забезпечення кібербезпеки України» кібербезпекою визнається захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі. Таким чином відповідно до чинного законодавства кібербезпека визнається важливою складовою публічної безпеки і органи Національної поліції України є частиною національної системи кібербезпеки України (п. 3 Стратегії кібербезпеки України).

Інформаційні технології трансформують світ, розширюють особисту свободу і можливості людей, допомагають створювати нові ідеї та інновації. Проте разом із перевагами сучасного цифрового світу та розвитком інформаційних технологій також зросла і кількість загроз публічній безпеці, супроводжуваних зростанням кількості та потужності

кібератак, вмотивованих інтересами окремих держав, груп та індивідів. Актуальною проблемою сьогодення є низький рівень комп'ютерної грамотності та кіберкультури користувачів мережі.

Проаналізувавши дані, отримані в результаті інформаційного запиту, направленого до Генеральної Прокуратури України, про статистику вчинення кіберзлочинів в Україні станом на 2018 рік, можна констатувати, що сучасний стан системи публічної безпеки не забезпечує у повному обсязі нейтралізацію існуючих кіберзагроз. Так, у 2018 році в Україні зареєстровано 2470 кримінальних правопорушень у сфері кіберзлочинності, із них закриті – 169, направлені до суду (з урахуванням правопорушень минулих років) – 1515. Аналізуючи статистику кіберзлочинів в України можна прийти до висновку, що найбільшу кількість зареєстрованих кіберзлочинів зафіксовано у наступних областях: Миколаївська – 378; Одеська – 351; Львівська – 272 та у місті Києві – 283 злочини. Найменшу кількість кіберзлочинів зареєстровано в Івано-Франківській – 20; Тернопільській – 25; Волинській – 29 та Сумській – 30 злочинів.

Аналізуючи кримінологічні характеристики осіб, що вчинили кіберзлочини у 2018 році, можна прийти до наступних висновків: більшість осіб, що вчинили злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) у віці 29–39 років. З 254 облікованих, осіб, що вчинили зазначені злочини у 2018 році, 145 осіб мали повну вищу або базову вищу освіту, 66 осіб – вищу загальну середню або базову загальну середню освіту, 40 осіб – професійно технічну освіту, 3 особи – початкову базову або взагалі не мали освіти.

Щороку кількість виявлених кіберзлочинів збільшується в середньому на 2,5 тисяч. У 2017 році підрозділи Кіберполіції супроводжували близько 7 тис. кримінальних проваджень, з них 4,5 тис – винятково кіберзлочини. За одинадцять місяців 2017 року було направлено до суду обвинувальні акти щодо 726 осіб. Відповідно до отриманої статистики Генеральної Прокуратури України у 2018 кількість кримінальних проваджень, направлених до суду з обвинувальним актом зросла вдвічі і складає 1515 кримінальних справ, що свідчить про поліпшення роботи правоохоронних органів у напрямку протидії кіберзлочинам.

Способи вчинення кіберзлочинів постійно удосконалюється, що у свою чергу ускладнює виявлення та протидію зазначеним правопорушенням. Одними з першочергових заходів на шляху побудови системи кібербезпеки є вдосконалення державного управління у даній сфері та

нормативно-правової бази для забезпечення такої діяльності. Крім того важливим є здійснення посиленої професійної підготовки, проведення курсів підвищення кваліфікації, тренінгів, з питань кібербезпеки і не лише для працівників Кіберполіції України, а й для усіх співробітників правоохоронних органів. Так, наприклад, підготовка суддів, слідчих та прокурорів для роботи з доказами, що стосуються злочинів, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів є одним із важливих заходів, передбачених Стратегією кібербезпеки України.

Крім того для підвищення поінформованості громадян про безпеку в кіберпросторі важливим є проведення превентивних заходів: лекцій у навчальних закладах, на підприємствах, організаціях; розміщення інформації у місцях найбільшої активності людей щодо безпечного користування всесвітньою мережею Інтернет. Реалізація комплексу зазначених заходів є необхідною умовою забезпечення публічної безпеки в нашій державі.

Одержано 28.10.2019

УДК 004.056.53

Юрій Валерійович Гнусов,
кандидат технічних наук, доцент, завідувач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Сергій Володимирович Калякін,
викладач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Кримінальний аналіз у роботі підрозділів Національної поліції України

Проблема впровадження сучасних методів роботи у діяльність правоохоронних органів України є надактуальною. Результативність діяльності у боротьбі зі злочинністю безпосередньо залежить від якісного, своєчасного і достатнього інформаційно-аналітичного забезпечення цієї діяльності. Сучасний рівень злочинності, вимагає від правоохоронних органів здійснення своєчасного, оперативного та достовірного аналізу діяльності організованих груп та злочинних організацій.

У країнах Європейського Союзу, США та інших розвинених країнах світу, розуміючи потребу в здійснення кримінального аналізу, у боротьбі зі злочинністю використовують модель Intelligence-Led Policing (ILP – поліцейська діяльність, керована аналітикою), яка полягає в аналізі відомостей, здобутих шляхом специфічної поліцейської діяльності у сфері збирання інформації, а отримана оперативно-аналітична інформація є підставою для проведення операцій/розслідувань, а не навпаки [2].

Кримінальний аналіз можна визначити як діяльність аналітиків – працівників правоохоронних органів, що полягає у перевірці, оцінці та інтерпретації інформації про протиправні, кримінально карані діяння окремих осіб та груп, яка отримана в ході проведення оперативно-розшукової діяльності або під час досудового розслідування, а також у встановленні суттєвих зв'язків між вищевказаною інформацією з метою їх подальшого використання для визначення тактичних та стратегічних напрямків протидії та запобіганню злочинності [2].

В аналітичній роботі правоохоронних органів і служб використовується: оперативний аналіз; тактичний аналіз; стратегічний аналіз; аналіз даних з відкритих джерел (OSINT); аналіз даних з багатьох джерел (Multi-Source Analysis).

На сьогодні у підрозділах кримінального аналізу найбільш часто використовують оперативний кримінальний аналіз, який призначений для забезпечення оперативно-розшукових підрозділів необхідною інформацією в рамках роботи щодо оперативно-розшукових справ.

Оперативний кримінальний аналіз може здійснюватися у трьох формах:

1) аналіз, що супроводжує оперативно-розшукову діяльність (наявна інформація, що стосується справи, упорядковується, нова інформація відповідно співвідноситься та оцінюється, у поточному порядку формулюються гіпотези, які підтримуються доказами чи висновками або за їх допомогою спростовуються);

2) аналіз, який ведеться для підтримки оперативно-розшукової діяльності (аналітик бере на себе аналітичні завдання, представляє результати аналізу, займається пошуком інформації з власних баз тощо);

3) аналіз, що ініціює оперативно-розшукову діяльність.

Для проведення аналізу застосовуються сучасні аналітичні інструменти, відповідне програмне забезпечення, а також наявні інформаційні ресурси. Найбільш поширеним інструментом, що сьогодні використовується у повсякденній роботі органів Національної поліції, є Microsoft Office (Word та Excel), та лише в деяких департаментах застосовується аналітичне програмне забезпечення, зокрема IBM i2 Analyst's Notebook, Maltego, E-Gis maps, ArcGIS, тощо.

Пріоритетним напрямом діяльності інформаційно-аналітичних підрозділів Національної поліції України є вжиття комплексу заходів, спрямованих на успішну реалізацію та впровадження нових методів кримінального аналізу, що дасть можливість активно використовувати сучасні аналітичні технології для створення передумов ефективного виконання оперативними і слідчими підрозділами своїх завдань, підвищить ефективність документування та розкриття злочинів, що вчиняються за складними схемами, потребують обробки великих масивів даних.

Список бібліографічних посилань

1. Мовчан А. В. Актуальні проблеми впровадження в органах Національної поліції України моделі поліцейської діяльності, керованої аналітикою. *Соціально-правові студії*. 2018. Вип. 1. С. 17–22.
2. Кіреєва О. Використання альтернативних аналітичних інструментів у кримінальному аналізі. *Збірник наукових праць Національної академії Державної прикордонної служби України*. 2016. № 4 (70). С. 64–76.
3. Половніков В. В. Характеристика кримінального аналізу з урахуванням практики його використання в оперативно-розшуковій діяльності Державної прикордонної служби України. *Питання боротьби зі злочинністю*. 2017. Вип. 34. С. 28–40.

Одержано 01.11.2019

УДК 342:343.346.8

Ольга Михайлівна Головко,
кандидат юридичних наук, старший викладач кафедри публічного права Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Кіберзлочини та парадигма Human Rights

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163, кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей:

1) порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів;

2) порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем;

3) використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту.

Перше, що завжди привертає увагу в контексті посягань у кіберпросторі – це питання конфіденційності та збереження приватності. Варто зазначити, що цей аспект корелює зі ст. 12 Загальної декларації прав людини (далі – Декларація), яка виокремлює свободу від втручання в особисте і сімейне життя, від посягання на недоторканність житла, таємницю кореспонденції. Наразі, питання збереження приватності стоїть досить гостро та стосується не тільки технологічної складової забезпечення такої безпеки, однак заключає в собі й елементи особистої гігієни у кіберпросторі. Серед ключових принципів кібербезпеки визначають конфіденційність, цілісність та доступність інформаційної

системи. Якщо один з цих принципів порушується, вірогідність стати жертвою кіберзлочинця підвищується.

Так, в епоху цифрових трансформацій фраза «розумний будинок» перестає бути футурологічною ідеєю. Це цілковита реальність, яка стала можливою завдяки реалізації технологій Інтернету речей (IoT). Втім, досить гостро постала загроза посягання на свободу від втручання в особисте і сімейне життя, від посягання на недоторканність житла, адже інформаційна система, яка керує будинком фактично може стати знаряддям злочину для зловмисників.

У випадку зі ст. 9 Декларації, яка передбачає свободу від безпідставного арешту і вигнання можлива ситуація, в якій через дії злочинців особа, яка не вчиняла нічого протизаконного може бути піддана арешту. Йдеться про ситуації, коли через гаджет сторонньої особи без фізичного доступу до нього було вчинено злочинні дії, наприклад, зламано банківський рахунок. В такому випадку, фактично супутня жертва кіберзлочинця може бути піддана кримінальному переслідуванню. В цьому ж контексті можна розглядати порушення свободи вираження поглядів і переконань. Йдеться про випадки зламу особистої сторінки в соціальних мережах та поширення про певну особу недостовірної інформації, яка принижує її честь та гідність, завдає шкоди діловій репутації. Особа, яка стає жертвою такої кібератаки може бути звинувачена в дифамації.

Зазначені приклади та їх кореляція з деякими основоположними правами людини особливо загострюють увагу на тому, що такі атаки в більшості випадків є результатом недотримання особистої гігієни в кіберпросторі. Найчастіше, особа стає жертвою фітингу або фармінгу, коли особа несвідомо передає зловмиснику свої дані, потрапляючи «на гачок» кіберзлочинця. Тож, перше, на що треба робити акцент в питаннях превенції кіберзлочинів – впровадити освітні процедури, що допоможуть пересічному громадянину виокремити кібератаку чи кіберпастку та діяти таким чином, щоб максимально убезпечити себе від протиправних дій сторонніх осіб.

Одержано 30.10.2019

УДК 343.436

Юлія Володимирівна Градова,
кандидат юридичних наук, доцент кафедри
конституційного і муніципального права
Харківського національного університету імені В. Н. Каразіна

Кібербулінг як загроза психологічному здоров'ю підлітків

Науково-технічний прогрес полегшив життя багатьох людей, проте разом з тим він приніс нові загрози суспільству. Однією з таких загроз є кібербулінг, який є видом насильства, що здійснюється із застосуванням засобів електронних комунікацій. За останніми даними ЮНІСЕФ 44,7% підлітків в Україні проводять в соціальних мережах чотири і більше годин в навчальні дні, у вихідні ця цифра зростає до 54,9%. Це говорить про те, що вони є потенційними жертвами/агресорами/свідками кібербулінгу. Кібербулінг – це насильство, яке не має меж, і будь-яка людина може стати його жертвою.

Термін «кібербулінг», введений канадським вченим Білом Белсі, означає використання інформаційних та комунікаційних технологій для підтримки навмисної, повторної та ворожої поведінки особи чи групи осіб, яка має на меті заподіяти шкоду іншим особам [1, с. 15]. Характерними рисами кібербулінгу є те, що це а) навмисна агресивна поведінка, яка б) здійснюється неодноразово; в) відбувається між злочинцем та жертвою, які нерівні за владою, і г) відбувається за допомогою електронних технологій [2].

Булери в кіберпросторі є більш агресивними, ніж в офлайні, оскільки для них відсутній зворотній зв'язок між своїми діями та негативними наслідками цих дій для жертви, що зменшує ймовірність емпатичної реакції до жертви. Проблема кібербулінгу характеризується й тим, що така агресія може статися в будь-який час і в будь-якому місці. На відміну від шкільного булінгу, коли жертва найбільше потерпає від нападів під час перерви або по дорозі в школу, жертва кібербулінгу доступна майже цілодобово. Ще однією відмітною ознакою кібер-жорстокого поводження є те, що кібербулери почуваються в безпеці тероризуючи своїх жертв. Вони вважають себе «непереможними» завдяки анонімності, запропонованій електронними засобами. Елементи сприйнятої

анонімності в режимі он-лайн та безпека перебування за екраном комп'ютера допомагають звільнитись від тиску з боку суспільства, совісті, моралі та етики.

Кібербулінг негативно впливає на психологічне здоров'я підлітків, викликаючи депресію, зниження самооцінки та суїцидальні думки. Так, 50% підлітків, госпіталізованих у відділення гострої стаціонарної дитячої та підліткової психіатрії в Майамі зазнавали кібер-знущань [3, с. 104]. Результати досліджень говорять про кореляцію кібербулінгу з депресією, тривожністю, соматизацією, ворожістю, кібер-жорстокістю та віктимізацією.

Слід зазначити, що негативні наслідки кібербулінгу можуть виникнути у дорослому віці, при чому як у жертви, так і у агресора, оскільки обидві сторони піддаються психічним відхиленням. Емоційний інтелект відіграє буферну роль у такій ситуації.

Кібербулінг – небажаний побічний продукт об'єднання агресії підлітків та електронних комунікацій, і його зростання викликає занепокоєння. Директор дослідницького центру кібербулінгу у США Джастін У. Патчін зазначає, що відсоток жертв кібербулінгу в США виріс з 16,5% у 2016 році до 17,4% у 2019 році. В Україні майже кожен п'ятий підліток (21,5%) визнав себе жертвою кібербулінгу [4, с. 43].

Статистика свідчить, що кібержорстокість продовжує набирати обертів, незважаючи на протидію держави та запровадження різних програм проти знущань. Хоча адміністративна відповідальність за булінг, в тому числі в кіберпросторі, в Україні була введена менше року тому, говорити про позитивну динаміку поки рано. На жаль, це не той метод боротьби, який дає очікуваний результат. Успіх боротьби з кібербулінгом лежить в іншій площині. Основні заходи повинні вживати батьки та адміністрація школи.

Довірчі стосунки з батьками є важливим елементом в профілактиці кібербулінгу. Дитина має знати, що у разі такої ситуації її не будуть сварити, і її телефон чи комп'ютер не відберуть. Сьогодні для молоді втрата комунікаційних технологій схожа з ізоляцією, тому підлітки часто вважають за краще залишатись об'єктом кібербулінгу, ніж втратити свої гаджети.

Батьки повинні знати про потенціал кібербулінгу та моніторити комунікаційну діяльність дітей. Багато дорослих вважають, що вста-

новлюючи фільтри на комп'ютерах, вони захищають своїх дітей від небажаних контактів та сайтів. Проте цього замало.

Роль шкільної адміністрації також важлива і полягає у проведенні освітніх заходів, які формують негативне ставлення до кібербулінгу. До цих заходів повинні бути залучені працівники міліції, психологи, батьки та вчителі. Шкільна політика має бути спрямована на впровадження програм проти знущань у освітню систему.

Але головну роль у протидії кібербулінгу відводиться самій жертві, її поведінці та заходам, що вона здійснює: захист особистої інформації; уникнення електронних повідомлень від незнайомців; блокування повідомлень за допомогою програмного забезпечення; уникнення відповідей на знущальну поведінку; збір доказів образливих повідомлень та фотографій тощо.

Сьогоднішнє цифрове середовище – це новий ризик (від кібербулінга та продажу наркотичних речовин до дитячої порнографії). Відповіддю на ці ризики має стати цифрова грамотність. Тому основним профілактичним напрямом є формування загальної медіакультури у сфері використання інформаційно-комунікаційних технологій.

Список бібліографічних посилань

1. Belsey B. Cyberbullying: A real and growing threat. *ATA Magazine.* Fall 2007. Vol. 88, No. 1. P. 14–21. URL: https://www.teachers.ab.ca/News%20Room/ata%20magazine/Volume%2088/Number%201/Articles/Pages/Cyberbullying.aspx (дата звернення: 29.10.2019).
2. Kowalski R. M., Giumetti G. W., Schroeder A. N., Lattanner M. R. Bulling in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin.* 2014. Vol. 140, Iss. 4. P. 1073–1137. DOI: https://doi.org/10.1037/a0035618.
3. Hinduja S., Patchin J. W. Offline Consequences of Online Victimization: School Violence and Delinquency. *Journal of School Violence.* 2007. Vol. 6, Iss. 3. P. 89–112. DOI: https://doi.org/10.1300/J202v06n03_06.
4. Соціальна обумовленість та показники здоров'я підлітків та молоді: за результатами соціологічного дослідження в межах міжнародного проекту «Здоров'я та поведінкові орієнтації учнівської молоді» : монографія / О. М. Балакірєва, Т. В. Бондар та ін. ; наук. ред. О. М. Балакірєва ; ЮНІСЕФ ; ГО «Укр. ін-т соц. дослідж. ім. О. Яременка». Київ : Фоліант, 2019. 127 с.

Одержано 29.10.2019

УДК [343.9:343.431]477

Яким Олексійович Григорчак,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

Щодо ролі засобів масової інформації у протидії торгівлі людьми

На сьогоднішній день практично нормою життя стали асоціальні явища, пов'язані з матеріальними накопиченнями будь-якими способами. На цьому тлі принцип «все на продаж» став, нажаль, життєвим кредо багатьох, якщо не більшості. Вражаючим і шокуючим при цьому є той факт, що людина перейшла в розряд товару, який продають та купують. Незважаючи на те, що торгівля людьми є однією з найжорстокіших форм порушення основних прав і свобод людини, гарантованих Конституцією держави, реально вона є прибутковим злочинним бізнесом з надвисокими прибутками, стійкими міжнародними злочинними зв'язками та великою кількістю осіб, залучених до цієї діяльності.

Протидія торгівлі людьми є проблемою, що характеризується своєю багатоплановістю і широким спектром заходів запобігання, які слід застосовувати в різних сферах життя суспільства. У цій діяльності приймає участь широке коло суб'єктів (ряд державних структур, громадські, міжнародні організації).

Важливу роль у розв'язанні багатьох соціальних завдань, пов'язаних із протидією торгівлі людьми, відіграють засоби масової інформації (далі – ЗМІ). На сьогоднішній день, нажаль, ЗМІ досить часто позитивно висвітлюють, ніби рекламують, шляхи швидкого заробітку за кордоном, що є вкрай небезпечним і містить в собі реальну загрозу вироблення в суспільстві стереотипу позитивного ставлення до означеної проблематики. До основних завдань ЗМІ щодо протидії торгівлі людьми слід віднести:

- доведення до широких верств населення правдивої інформації про реальні факти торгівлі людьми, та злочини, що її супроводжують, шкідливі, а іноді незворотні наслідки цього явища;

- сприяння впровадженню в соціальну практику державних проектів, цільових програм з протидії торгівлі людьми з висвітленням їх реальних результатів у ЗМІ;
- активізація профілактичної діяльності серед населення щодо інформування громадськості про реальні загрози, що спричиняє торгівля людьми;
- всебічне дослідження феномену жертви торгівлі людьми з висвітленням основних причин віктимізації;
- поширення інформації про організації, які допомагають жертвам торгівлі людьми, їх основні методи роботи;
- висвітлення телефонів довіри та гарячих ліній для жертв торгівлі людьми;
- систематичне інформування населення щодо найбільш резонансних злочинів, пов'язаних із торгівлею людьми, типові способи їх вчинення та необхідні і допустимі заходи самозахисту від такого роду посягань;
- систематичне оприлюднення матеріалів прес-конференцій, брифінгів, звітів щодо протидії торгівлі людьми.

ЗМІ при висвітленні проблем злочинності володіють значним профілактичним потенціалом і здатні викликати у населення нетерпимість до цього антисоціального явища, активізувати участь громадян у боротьбі з суспільно небезпечними посяганнями, допомогти в забезпеченні особистої безпеки. Вони можуть надати неоціненну послугу населенню в доведенні до свідомості громадян різних юридичних термінів, вирішенні практичних юридичних питань, в тому числі пов'язаних з торгівлею людьми.

Таким чином, можна з впевненістю констатувати, що ЗМІ становлять значний масовий ефективний та інтенсивний потенціал протидії злочинності в цілому, та торгівлі людьми, зокрема. Саме їх активність в політичному та соціальному житті країни повинна привертати увагу всього суспільства до появи та розповсюдження торгівлі людьми. Зважаючи на те, що це злочинне явище соціально обумовлене, то протидіяти йому окрім спеціалізованих суб'єктів має саме соціум в особі громадських організацій на основі росту національної свідомості та в тісній взаємодії державних та недержавних організацій, використанні зарубіжного досвіду та потужних можливостей ЗМІ. Це є запорукою зміцнення гарантій прав і свобод людини та успішної протидії означеному злочинному явищу.

Одержано 30.10.2019

УДК 343.4

Микола Володимирович Єрошкін,
старший викладач кафедри тактико-спеціальної підготовки факультету № 1 Донецького юридичного інституту МВС України

Заборона насильницьких зникнень в Україні

Будь-яке насильницьке зникнення порушує цілу низку прав і свобод людини, багато з яких є загальновизнаними і невід'ємними як в міжнародному праві, так і на національному рівні. У той же час безкарність була і залишається однією з ключових проблем у функціонуванні правової системи України – так само, як дотримання прозорості, незалежності та інших критеріїв ефективного розслідування випадків порушень фундаментальних прав людини, зокрема насильницького зникнення.

Термін «насильницьке зникнення» був вперше застосований неурядовими організаціями Латинської Америки в 1960-ті роки та є дослівним перекладом іспанського словосполучення «disaparacion forzada», який розкриває концепцію насильницького зникнення, як жорстоке порушення прав людини та злочин, вчинений прямо чи опосередковано та за підтримки органів державної влади з метою усунення політичних опонентів. Це явище отримало широке розповсюдження в кінці 60-х та на початку 70-х років в багатьох країнах Латинської Америки у вигляді державної політики систематичних репресій проти неугодних осіб [1, с. 12].

Абсолютна заборона насильницьких зникнень міститься в ст. 1 Міжнародної конвенції про захист усіх осіб від насильницьких зникнень від 20 грудня 2006 року [2]. У цій же статті уточнюється, що жодні виключні обставини, якими б вони не були, чи то стан війни або загроза війни, внутрішня політична нестабільність чи інший надзвичайний стан, не можуть слугувати виправданням насильницького зникнення. Конвенція 2006 року на сьогодні є першим і єдиним міжнародно-правовим актом універсального характеру, який присвячений проблемі насильницьких зникнень.

Завдання посилення протидії таким кримінальним правопорушенням стоїть як на міжнародно-правовому рівні, так і на рівні національного законодавства; поряд з міжнародно-правовими є необхідними і внутрішньодержавні механізми боротьби із зазначеними протиправними діями.

Насильницькі зникнення – достатньо поширені злочинні діяння, характерні для періоду проведення локальних (адресних) спеціальних операцій по встановленню місцезнаходження та затриманню учасників незаконних збройних формувань. Складність розслідування таких злочинів обумовлена труднощами у встановленні осіб, задіяних в спеціальних заходах, серед яких, як правило, представники самих різних силових структур, а також самих спецоперацій, відомості про проведення яких нерідко засекречуються [3, с. 44].

Насильницькі зникнення, як і деякі інші порушення прав людини, вважаються злочином за міжнародним правом, а держави-учасники відповідних договорів, крім передбачених ними заходів для запобігання насильницьких зникнень, зобов'язані віднести такі діяння до кримінальних злочинів також в національному законодавстві.

Диспозиції ст. 1461 КК України цілком відповідають змісту Конвенції 2006 р. Так, ч. 1 ст. 1461 КК України визначає насильницьке зникнення як арешт, затримання, викрадення або позбавлення волі людини в будь-якій іншій формі, вчинене представником держави, в тому числі іноземної, з подальшою відмовою визнати факт такого арешту, затримання, викрадення або позбавлення волі людини в будь-якій іншій формі або приховуванням даних про долю такої людини чи місце перебування [4].

Отже, насильницьке зникнення на сьогодні є одним із найжорсткіших порушень прав людини, яке представляє доволі складне та сукупне порушення основних прав і свобод людини. Зазначене кримінальне правопорушення, за вчинення якого передбачена кримінальна відповідальність й законодавством України, може відбуватися як в мирний час, так і в період збройних конфліктів.

Список бібліографічних посилань

1. Цвікі В. Ю. Міжнародно-правовий захист осіб від насильницьких зникнень : дис. … канд. юрид. наук : 12.00.11. Одеса, 2017. 240 с.
2. Міжнародна конвенція про захист усіх осіб від насильницьких зникнень : від 20.12.2006 // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/995_l54 (дата звернення: 29.10.2019).
3. Гузеева О. С. Проблемы квалификации насильственных исчезновений. *Уголовное право*. 2014. № 5. С. 44–47.
4. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 29.10.2019)

Одержано 01.11.2019

УДК 343.85:343.431

Віта Олександрівна Іващенко,
кандидат юридичних наук, доцент,
професор кафедри кримінології та кримінально-виконавчого права
Національної академії внутрішніх справ (м. Київ)

Окремі аспекти нормативно-правового забезпечення протидії торгівлі людьми

Однією з гострих проблем для України залишається боротьба з торгівлею людьми. Вперше Законом України від 24 березня 1998 року було криміналізовано зазначене діяння. Зростання масштабів і небезпеки цього злочину обумовило необхідність прийняття спеціальної нормативно-правової бази щодо протидії торгівлі людьми. Посприяли цьому підписання та ратифікація Україною Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності, прийнятої резолюцією 55/25 Генеральної Асамблеї від 15 листопада 2000 р., та Протоколу про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї, що доповнив зазначену Конвенцію [1].

Зокрема, цілями Протоколу стали попередження торгівлі людьми і боротьба з нею, приділяючи особливу увагу жінкам і дітям; захист та допомога жертвам такої торгівлі при повній повазі їхніх прав людини; заохочення співробітництва між державами у цій сфері. Відповідно до п. а ст. 3 вказаного Протоколу «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.

З метою приведення законодавства України у відповідність до міжнародних стандартів у сфері протидії торгівлі людьми прийнято Закон України від 20 вересня 2011 року «Про протидію торгівлі людьми» [2], який визначив організаційно-правові засади протидії торгівлі людьми, гарантуючи гендерну рівність, основні напрями державної політики та засади міжнародного співробітництва у цій сфері, повноваження органів виконавчої влади, порядок встановлення статусу осіб, які по-

страждали від торгівлі людьми, та порядок надання допомоги таким особам. Торгівля людьми закріплена в законодавчому акті як здійснення незаконної угоди, об'єктом якої є людина, а так само вербування, переміщення, переховування, передача або одержання людини, вчинені з метою експлуатації, у тому числі сексуальної, з використанням обману, шахрайства, шантажу, уразливого стану людини або із застосуванням чи погрозою застосування насильства, з використанням службового становища або матеріальної чи іншої залежності від іншої особи, що відповідно до Кримінального кодексу України визнаються злочином.

На виконання Закону України «Про протидію торгівлі людьми» згодом були прийняті відповідні підзаконні нормативно-правові акти. Серед них: постанови Кабінету Міністрів України «Про затвердження Положення про створення та функціонування Єдиного державного реєстру злочинів торгівлі людьми» від 18 квітня 2012 року № 303, «Про затвердження Порядку встановлення статусу особи, яка постраждала від торгівлі людьми» від 23 травня 2012 року № 417, «Про затвердження Порядку виплати одноразової матеріальної допомоги особам, які постраждали від торгівлі людьми» від 25 липня 2012 року № 660, «Про затвердження Порядку взаємодії суб'єктів, які здійснюють заходи у сфері протидії торгівлі людьми» від 22 серпня 2012 року № 783, «Про затвердження Державної соціальної програми протидії торгівлі людьми на період до 2020 року» від 24 лютого 2016 року № 111, відповідні накази Міністерства соціальної політики України та ін.

Так, Державна соціальна програма протидії торгівлі людьми на період до 2020 року [3] передбачила, зокрема, удосконалення нормативно-правової бази у сфері протидії торгівлі людьми, запровадження стандартів надання соціальних послуг особам, які постраждали від неї, інформування громадськості про нові тенденції цього злочину.

У цьому напряму 06 вересня 2018 року прийнято Закон України «Про внесення змін до статті 149 Кримінального кодексу України щодо приведення у відповідність з міжнародними стандартами». Так, ч. 1 ст. 149 КК передбачила відповідальність за торгівлю людиною, а так само вербування, переміщення, переховування, передачу або одержання людини, вчинені з метою експлуатації, з використанням примусу, викрадення, обману, шантажу, матеріальної чи іншої залежності потерпілого, його уразливого стану або підкупу третьої особи, яка контролює потерпілого, для отримання згоди на його експлуатацію [4]. Разом з тим, як зазна-

чалося вище, Закон України «Про протидію торгівлі людьми» містить визначення торгівлі людьми, зокрема, як здійснення незаконної угоди, об'єктом якої є людина. Тому з метою однакового розуміння торгівлі людьми відповідні зміни потрібно внести в розглянутий базовий законодавчий акт.

Підсумовуючи викладене, можна зробити висновок, що в Україні створена спеціальна правова база з протидії торгівлі людьми, яка і в подальшому має вдосконалюватися.

Список бібліографічних посилань

1. Протокол 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 : прийн. резолюцією 55/25 Ген. Асамблеї ООН від 15.11.2000 // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/995_791 (дата звернення: 24.10.2019).
2. Про протидію торгівлі людьми : Закон України від 20.09.2011 № 3739-VI // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/3739-17 (дата звернення: 24.10.2019).
3. Про затвердження Державної соціальної програми протидії торгівлі людьми на період до 2020 року : Постанова Кабінету Міністрів України від 24.02.2016 № 111 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/111-2016-п (дата звернення: 24.10.2019).
4. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 24.10.2019).

Одержано 28.10.2019

УДК 004.946.5.056

Роман Андрійович Івасечко,
студент 2 курсу юридичного факультету
Тернопільського національного економічного університету

Кіберзлочинність як один із найбільш прогресивних видів злочинів сучасності

Свого часу Білл Гейтс зазначав, що в майбутньому на ринку будуть присутні тільки два види компаній: ті, хто в Інтернеті і ті, хто вийшов з бізнесу.

Можна сказати, що це майбутнє вже настало, адже бізнес масово починає «переходити» у Всесвітню павутину, і поряд із цим виникає і масово розвивається кіберзлочинність, однією з причин якої є величезний обіг коштів у даній сфері суспільних відносин.

З огляду на те, що проблема кіберзлочинності на сучасному етапі розвитку України набуває популярності та становить загрозу інформаційному суспільству, вона вже отримала відображення у нормативно – правових актах національного та міжнародного рівнів. Зокрема, 15 березня 2016 року Президент України видав Указ «Про введення в дію рішення Ради національної безпеки та оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». У складі Ради національної безпеки створено робочий орган – Національний координаційний центр кібербезпеки.

Г. М. Чернишов стверджує, що кіберзлочинність у сучасних умовах інформаційного суспільства та глобальної комп'ютеризації є однією з найбільших загроз світовій безпеці. Кіберзлочинність – явище, яке виражається у системі злочинів, вчинених у кіберпросторі з використанням та/або проти комп'ютерних даних, мереж або систем, а також інших телекомунікаційних мереж, включаючи Інтернет та технології мобільного зв'язку. Кіберзлочинність – злочини, в яких кіберпростір є середовищем, предметом (метою) посягання та/або способом вчинення [1].

Станом на сьогодні кіберзлочинність є одним з найбільш активно прогресуючих видів злочинності. Великими темпами розвиваються нові види кіберзлочинів, а також суттєво збільшується їх кількісне

значення та територія поширення. Для прикладу, Н. Міщук зазначає, що за даними фахівців США, розмір збитків від кіберзлочинності кожного року зростає в середньому на 35% порівняно з попереднім. Однією з причин такого стрімкого розвитку є саме кількість коштів, яку можна отримати при вчиненні кіберзлочину. Середня кількість збитків від кіберзлочину у світі становить приблизно 560 тисяч доларів, тоді як при звичному пограбуванні банку – приблизно 20 тисяч доларів [2, с. 174].

Як вже було сказано, кібернетична злочинність посягає на банківські рахунки як компаній чи організацій, так і пересічних громадян. Зі зростанням обсягів безготівкових розрахунків зростає і кількість потерпілих від кібершахраїв. Чинниками, які сприяють зростанню кіберзлочинів є розвиток та удосконалення ІТ-технологій, значна географія для скоєння злочинів, недостатня теоретична та практична підготовка працівників органів внутрішніх структур та недосконаліть вітчизняного законодавства [3].

Суспільну небезпечність кіберзлочинів та актуальність цієї проблеми ілюструє таке явище, як кібератака. Кібератака – спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій та спрямовані на досягнення таких цілей: порушення конфіденційності, доступності електронних інформаційних ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту [4].

Кібератаки, в силу своєї специфіки, дуже часто спрямовані на автоматизовані та інформаційні системи, що мають державне значення. прикладом цього можуть слугувати відомі кібератаки на енергетичні компанії України 23 грудня 2015 року, коли зловмисникам вдалось успішно атакувати комп'ютерні системи управління трьох енергопостачальних компаній України, або кібератака 17–18 грудня 2016 року, коли була виведена з ладу підстанція «північна» енергокомпанії «Укренерго», що мало наслідком залишення без струму споживачів певних районів Києва.

Серед основних помилок користувачів виокремлюються такі як: використання одного і того ж паролю у кількох облікових записах, надсилання паролів чи даних банківських карток незахищеними каналами зв'язку, невикористання Proxy-сервісів або VPN-сервісів у момент

підключення до спільних безкоштовних точок WiFi-доступу до мережі Інтернет, в ході якої особисті дані користувача можуть вилучені сторонніми особами тощо.

На думку Г. М. Чернишова, враховуючи стрімкий розвиток комп'ютерних та Інтернет-технологій, залежність всіх сфер суспільства від їх функціонування, є доцільним внесення змін до КК України та доповненням певними статтями [5].

З огляду на це, можемо підсумувати, що кіберзлочинність є одним із найбільш прогресивних видів злочинності на сучасному етапі розвитку суспільства, що породжено значним поширенням використання мережі Інтернет у різних сферах суспільного життя та низькою захищеністю персональних даних користувачів Всесвітньої павутини.

Список бібліографічних посилань

1. Чернишов Г. М. Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження. *Прикарпатський юридичний вісник*. 2018. Вип. 3 (24). С. 158–162.
2. Міщук Н. Кіберзлочинність як загроза інформаційному суспільству. *Вісник Львівського університету*. 2014. № 51. С. 173–179.
3. Некрасов В. Легкие деньги: Украина превращается в Мекку для киберпреступников // Экономическая правда : сайт. 28.03.2016. URL: https://www.epravda.com.ua/rus/publications/2016/03/28/587004/ (дата звернення: 29.10.2019).
4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради*. 2017. № 45. Ст. 403.
5. Чернишов Г. М Кібершахрайство: визначення та кримінологічні показники. *Порівняльно-аналітичне право*. 2018. № 5. С. 318–321.

Одержано 01.11.2019

УДК 343.9

Аліна Владиславівна Калініна,
кандидат юридичних наук, науковий співробітник відділу кримінологічних досліджень Науково-дослідного інституту вивчення проблем злочинності імені академіка В. В. Сташиса Національної академії правових наук України (м. Харків)

Криптовалюта – «цифровий актив» злочинності?[1]

Цифрові технології в наш час можна назвати сферою, що розвивається найактивніше. Здобутки спеціалістів у цій галузі вражають майже не щодня. Діджиталізація суспільства відбувається значними темпами, охопивши всі аспекти життєдіяльності людини – від побутових питань до розвитку бізнесу на високому рівні.

Одним із напрямів діджиталізації суспільних відносин є створення та розвиток цифрових (віртуальних) активів – вираження валюти у певному середовищі або ситуації, за якої валюту можна визначити або як засіб обміну, або як власність, що має цінність у визначеному середовищі [1, с. 48].

Міжурядова організація, що займається розробленням світових стандартів у сфері протидії відмиванню злочинних доходів та фінансуванню тероризму – група розроблення фінансових заходів боротьби з відмиванням грошей (FATF – Financial Action Task Force) акцентує увагу на такому можливому зв'язку між віртуальними та реальними валютами, як конвертація перших. У зв'язку з цим серед віртуальних валют виділяються: 1) ті, що конвертуються – віртуальні валюти, що мають еквівалентну вартість у реальній валюті, що можуть бути знову обміняні на фіатні валюти[2]; 2) ті, що не конвертуються – віртуальні валюти, що є специфічними для визначеного віртуального домена чи світу, та, відповідно до правил, якими регулюється його використання, не можуть обмінюватися на фіатну валюту [2, с. 4–5].

1 Тези підготовлено на виконання теми фундаментального наукового дослідження НДІ ВПЗ «Стратегія зменшення можливостей вчинення злочинів: теорія та практика».

2 Фіатні гроші (англ. fiat currency), також фідуціарні гроші – тип грошей або валюти, цінність яких походить не від власної вартості або гарантії обміну на золото або іншу валюту, а від державного наказу (fiat) використання їх як засобу платежу [3].

Таким чином, не зважаючи на те, що віртуальна валюта фактично не є матеріальним вираженням будь-яких цінностей, її природа та мета створення, все ж таки, дозволяє закріплювати такі цінності безпосередньо за нею. Тобто, враховуючи можливість конвертації криптовалюти в реальні гроші, це дозволяє використовувати її не лише для правомірних дій, а й зі злочинною метою.

Останніми роками популярність криптовалют в Україні сприяла розвитку окремого напряму ділової діяльності – криптобізнесу. У 2017 р. в державі з'явилися навіть спеціальні термінали для придбання біткоінів – одного із найпопулярніших видів криптовалют – за готівкові кошти (у містах Київ, Харків, Миколаїв та ін.) [4].

Значний попит на криптовалюту спровокував обґрунтований інтерес до її використання у злочинній діяльності. При детальному аналізі процесів формування і використання криптовалюти в Україні можна виявити, що існує низка факторів, що сприяють вчиненню кримінально-караних діянь у цій сфері, зокрема: *1)* відсутність нормативних актів, що регулюють суспільні відносини, пов'язані із криптовалютою в Україні. Наразі таке часткове державне регулювання знаходиться на рівні проектів нормативних актів. Таким чином, особа вільна у виборі будь-яких операцій з криптовалютою одночасно із тим, що правоохоронці не мають можливості захистити її інтереси; *2)* надзвичайна складність контролю процесів, пов'язаних із формуванням та використанням криптовалют. До того ж, за словами експертів, наразі державні органи не мають змоги контролювати операції з криптовалютою, так як існуючими ресурсами це не видається можливим (найпростіше порівняння – контроль за обігом готівкового долару США в Україні, що фактично неможливо здійснити) [5]. Тобто, криптовалюта може безперешкодно використовуватися злочинцями для операцій під час вчинення кримінально-караних діянь (наприклад, придбання наркотичних речовин, вогнепальної зброї, вчинення злочинів на замовлення, легалізації доходів, отриманих злочинним шляхом і т. п.). Однак навіть при встановленні державного контролю за криптобізнесом, існує висока вірогідність легкої тінізації цього сектору [5], оскільки використання комп'ютерних технологій можна здійснювати й поза межами держави; *3)* криптовалюта за своїм характером є спекулятивним цифровим активом. Ціноутворення на неї формується переважно залежно від попиту у суспільстві, що нерідко залежить від суб'єктивних факторів, зокрема, психологічного та емоційного сприйняття громадянами певної інформації. Це породжує шахрайські ризики,

наслідком яких є втрата власниками (майнерами) такої валюти своїх коштів; *4)* відповідальність за володіння, збереження і переміщення криптовалюти лежить на суб'єкті операцій, що з нею пов'язані. Наразі держава не надає жодних гарантій для осіб, що здійснюють операції з криптовалютою, що також створює додаткові віктимологічні ризики для майнерів.

Ще одним питанням, пов'язаним із віртуальною валютою, є її розгляд як відповідної складової кіберзлочинності. У літературі під кіберзлочинністю розуміється сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних (О. В. Новіков, 2014) [6, с. 293]. Судова практика свідчить, що термін «криптовалюта» активно вживається правоохоронцями при розгляді питань кримінальної відповідальності осіб за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (наприклад, що передбачені статтями 361, 361^1, 361^2 КК України).

Отже, охорона суспільних відносин, пов'язаних із обігом криптовалют в Україні, можлива лише тоді, коли держава створює якісні умови для їх ефективного захисту, зокрема, законодавчі, організаційно-управлінські, економічні та ін.

Список бібліографічних посилань

1. Кудь А. А. Методика диагностики токена блокчейна на соответствие цифровому активу : метод. пособие. Харьков : НИИ ХОГОКЗ, 2019. 56 с.
2. Financial Action Task Force. Virtual currencies – key definitions and potential AML/CFT risks. Paris : RATF/OECD, 2014. 15 p. URL: http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf (дата звернення: 29.10.2019).
3. Фіатні гроші / Вікіпедія : віл. енцикл. URL: https://uk.wikipedia.org/wiki/Фіатні_гроші (дата звернення: 29.10.2019).
4. В Киеве установили первые в Украине терминалы для продажи криптовалюты // ТСН : сайт. 05.09.2017. URL: https://tsn.ua/ru/groshi/v-kieve-ustanovili-pervye-v-ukraine-terminaly-dlya-prodazhi-kriptovalyuty-924538.html (дата звернення: 29.10.2019).

5. Некрасов В. Нужен ли Украине закон о криптовалютах и будет ли он работать // Экономическая правда : сайт. URL: https://www.epravda.com.ua/rus/publications/2018/10/8/641337/ (дата звернення: 29.10.2019).
6. Кримінологія : підручник / за ред. В. В. Голіни, Б. М. Головкіна. Харків : Право, 2014. 440 с.
7. Єдиний державний реєстр судових рішень : портал. URL: http://reyestr.court.gov.ua (дата звернення: 29.10.2019).

Одержано 01.11.2019

UDC 342.841(477)

Maryana Kachynska,
Ph.D., associate professor of police activity and public administration department of Kharkiv National University of Internal Affairs

Developing a labor perspective to human trafficking in the political-economic context of ukraine

Ukraine is well known as a developing, post-Soviet country. People in Ukraine face numerous problems due to poor economic development. Nevertheless, Ukraine is not the only post-Soviet country with such development problems – some countries managed to improve these problems quicker, such as Poland, Lithuania and Latvia, who are now members of the European Union (EU). Some, like Ukraine, have gone through this process slower, and are still not EU members. In Ukraine, this development process has been made harder due to the 2014 conflict in Crimea. This not only took up significant resources and budget from the government, but had indirect influences. For example, most of Ukraine's hard industries are located in the conflict zones, which means that money received from natural resources are going to Russian separatists, rather than the Ukrainian government. This has slowed down the process of Ukraine's economic development significantly. These challenges are combined with political uncertainty in Ukraine, internal corruption, and whether the country should be on a path to join the EU.

These circumstances have forced Ukrainians to search for a better life. In combination, existing Ukrainian labor laws are relatively weak and lack enforcement when compared to its European neighbors, which have encouraged many Ukrainians to seek better work abroad, and have encouraged large waves of emigration. Many Ukrainians tolerate poor labor conditions but seek to work abroad in order to at least earn more money. As such, they remain vulnerable to exploitation, and in more severe instances, labor trafficking. However, there has been relatively little research attention given to examining the specific dynamics of Ukrainian political-economy and labor practices in relation to labor exploitation. Therefore, this research aims to examine Ukrainian labor law in the context of its political-economic climate, and so develop strategies to reduce vulnerability to labor exploitation. The key question to be addressed is 'how do the dynamics of political-economic conditions in Ukraine result in human trafficking for labor exploitation?'.

There is a body of literature that critiques existing approaches to human trafficking, especially those focusing just on legal interventions (Kotiswaran 2019; Shamir 2012) [1; 2]. Not only are such approaches reactionary to specific cases, and tend to be discussed in the context of developed countries, but they overlook the social, economic, and political circumstances within which exploitation and trafficking develops. For example, trafficking does not necessarily originate from the poorest countries or poorest regions, but those currently experiencing economic transition such as South-Eastern Europe or China. On this basis, P. Kotiswaran (2019) argues for a 'development' approach to trafficking that incorporates the nuances of developing countries, including state, market, civil society, and legal system configurations into analyses of labor market exploitation [2]. Part of this approach involves recognizing that informal markets are unlikely to simply disappear, and could be utilized in a positive way to support workers. This development approach seems to overlap with the broader labor perspective to human trafficking, which emphasizes the structural causes and solutions to labor exploitation, rather than considering just the actions of individual criminals. Ukraine is an important example of how these issues can be studied as part of developing a labor-centered perspective to human trafficking.

Ukraine was historically part of the Soviet Union, which had a significant influence on its economy until its dissolution in 1991. Since Ukraine gained independence in 1991, the process of development was comparatively slower to other post-Soviet countries, but there was still growth. The first damage on this process was the global economic/financial crisis in 2008, which made the value of Ukrainian currency lower. For example, before the 2008 crisis, the value of USD $1 equaled 4.5 UAH (Ukrainian hryvnia); thereafter, the rate was USD $1 to 8 UAH; and the second damage occurred after the 2014 Crimea occupation, where the currency has further weakened from USD $1 to 27 UAH. This is one indication of the damage to the Ukrainian economy, combined with a decline in population of 52 million in 1995 to 38 million in 2018, largely due to emigration, as well as low birth rates in the 1990s, which is now resulting in an ageing population.

Nearly 22 million people emigrating from Ukraine is due to large scale emigration which occurred from 1991 until today. Earlier patterns of migration were encouraged due to uncertainty in the economy during the post-Soviet era 1990s, and more recent patterns due to the global financial crisis and ongoing Crimea conflict. Most migrants who leave Ukraine want to find a 'better life' (including work) in order to support their families at home. Most people who decide to leave home are already vulnerable due to few work

opportunities, job insecurity, and associated precariousness in Ukraine. Therefore, if workers are approached by recruitment agencies with the promise of better work abroad and assistance with applying for work visas, then this appears as a beneficial option for them. However, this makes such migrants vulnerable to labor trafficking, and reduces the likelihood of those who remain in Ukraine to address labor exploitation.

One of the reasons that Ukraine has become a donor of victims for labor exploitation is a lack of social protection for citizens, including a low level of labor protection tools. For example, workers have a lack of legislative tools in order to protect themselves against excessive working hours and workloads, as well as a high level of corrupt enforcement/officials. A key explanation for not identifying severe forms of exploitation is that Ukraine has a number of gaps in legislation and ineffective mechanisms of labor rights protection processes. This situation in the present legal system in Ukraine was caused by the lasting effects of post-Soviet countries.

In the USSR, the government and its public officials retained the dominant role in political-economic matters. The needs of the "motherland" were the priority, and the tool to fulfil them was public authority, which typically forced factories to be more productive. A planning system was created: for instance, a factory was instructed to produce a number of goods – this number was decided by central headquarters and not based on the capabilities of the factory. Therefore, there was almost no attention given to workers, their safety measures in the workplace, overworking on shifts, and other dangers occurring in the workplace. Also, in the central headquarters, the role of labor rights was given little attention, since the main priority was on meeting production targets.

These issues are significant in their own right, but link with the broader issues of labor exploitation and human trafficking. This is because many workers are used to such violations in Ukraine, so accept it as normal behavior and may do so in other countries or sectors. For example, if they are used to working for long hours in dangerous areas with poor health and safety in Ukraine, they may accept that they can do the same type of work but for higher salaries in other countries.

Reference list

1. Shamir H. A. Labor Paradigm for Human Trafficking. *UCLA Law Review*. 2012. No. 76. P. 77–136.
2. Kotiswaran P. Trafficking: A Development Approach. *Faculty of Law University College London Law Research Paper*. 2019. No. 4. P. 1–36.

Одержано 29.10.2019

УДК 37.013.78:[343.541:004]:159.922.6

Вікторія Олександрівна Ковтун,
курсантка 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

Протидія кібербулінгу як сучасній формі агресії

Різновидом булінгу є кібербулінг, який вчиняється із застосуванням засобів електронних комунікацій. Кібербулінг – це та форма агресії, на яку дуже легко натрапити у мережі Інтернет. Це явище не залежить від місця знаходження агресора та жертви, може мати різні прояви.

Під кібербулінгом слід розуміти новітню форму агресії, що передбачає жорстокі дії з метою дошкулити, нашкодити, принизити людину з використанням інформаційно-комунікаційних засобів: мобільних телефонів, електронної пошти, соціальних мереж тощо.

Різновидами кібербулінгу є:

- анонімні погрози – анонім надсилає листи погрозливого змісту довільного або цілеспрямованого характеру, особлива ознака – наявність ненормативної лексики та груба мова;

- телефонні дзвінки з мовчанням. Не тільки погрози лякають. Мовчання чи жахання в слухавку бентежать дитину, вона не знає як і, головне, від чого потрібно захищатись;

- переслідування – це може бути елемент фізичного переслідування, залякування досягається шляхом розсилки повідомлень на електронну пошту чи телефон;

- тролінг – розміщення провокаційних повідомлень в мережі для привернення уваги та збудження активності, що може спричинити конфлікт (флеймінг).

- хепі-слепінг (happy slapping) – насильство заради розваги, актуальне здебільшого для фізичного цькування, проте в Інтернеті також актуально, коли мова йде про моральне насильство. Яскрава особливість – звичка знімати насильство на камеру для подальшого розповсюдження в мережі [1, 2].

Кібербулінг має декілька проявів, жоден з яких не можна ігнорувати:

- відправка текстових повідомлень погрозливого та образливого змісту;

- розповсюдження (спам) відео та фото порнографічного характеру;

- троллінг (надсилання погрозливих, грубих повідомлень у соціальних мережах, чатах чи онлайн-іграх);

- демонстративне видалення дітей зі спільнот у соцмережах, з онлайн-ігор;

- створення груп ненависті до конкретної дитини;

- пропозиція проголосувати за чи проти когось в образливому опитуванні;

- провокування підлітків до самогубства чи понівечення себе (групи смерті типу «Синій кит»);

- створення підробних сторінок у соцмережах, викрадення даних для формування онлайн-клону;

- надсилання фотографій із відвертим зображенням (як правило, дорослі надсилають дітям);

- пропозиції до дітей надсилати їх особисті фотографії відвертого характеру та заклик до сексуальних розмов чи переписок за допомогою месенджерів [3].

Щоб не стати жертвою кібербулінгу потрібно дотримуватись певних правил. При реєстрації на різних сайтах слід не вказувати особисту інформацію (номер телефону, фото тощо), створювати надійні паролі, використовувати вебкамеру тільки при спілкуванні з друзями або близькими, одиничні випадки агресії в Інтернеті варто ігнорувати, тоді найчастіше кібербулінг завершується на початковій стадії. Ще одним способом уникнути булінгу є блокування агресорів, більшість сайтів це дозволяють [4].

Отже, кібербулінг – це вид кібернасильства, що створює загрозу здоров'ю та життю людини, і з ним потрібно боротись. Спостерігачам не варто стояти осторонь. Потрібно виступити проти агресора і підтримати жертву, в деяких випадках повідомити дорослих, а також звернутися до правоохоронних органів.

Список бібліографічних посилань

1. Міхеєва О. Ю., Корнієнко М. М. Кібербулінг як соціально-педагогічна проблема. *Молодий вчений.* 2018. № 11 (63). С. 247–251. URL: http://

molodyvcheny.in.ua/files/journal/2018/11/60.pdf (дата звернення: 24.09.2019).
2. Агресія у вигляді кібербулінгу: що провокує це явище і як виявити агресора // ЗОЛОЧІВ.НЕТ : сайт. 10.10.2018 URL: https://zolochiv.net/agresiya-u-viglyadi-kiberbulingu-shho-provokuye-tse-yavishhe-i-yak-viyaviti-agresora/ (дата звернення: 24.09.2019).
3. Поради щодо кібербулінгу // Чернігівська загальноосвітня школа I–III ступенів № 3 : сайт. URL: http://cheschool3.pp.ua/ua/poradi_schodo_kiberbulingu (дата звернення: 24.09.2019).
4. Гой В. Що таке кібербулінг та як з ним боротись? // Природничі та гуманітарні науки. Актуальні питання : матеріали міжнар. студентської наук.-техн. конф. (м. Тернопіль, 26–27 квіт. 2018 р.) / Тернопіл. нац. техн. ун-т ім. В. Пулюя. Тернопіль, 2018. С. 170–171. URL: http://elartu.tntu.edu.ua/bitstream/lib/25145/2/MSNK_2018v2_Hoi_V-What_is_cyberbullying_and_how_170-171.pdf (дата звернення: 24.09.2019).

Одержано 29.09.2019

УДК 004.946.5.056

Тарас Васильович Коженівський,
студент 2 курсу юридичного факультету
Тернопільського національного економічного університету

Кіберзлочинність як загроза сучасній безпеці

Активний розвиток ІТ (інформаційних технологій), комп'ютеризація та створення світового комп'ютерного простору формують нові терміни і норми – ІС (інформаційне суспільство), кіберпростір, що мають необмежений потенціал і вносять глобальний вклад у економічний та соціальний розвиток.

Проте утворення ІС призводить до формування багатьох кіберзагроз (потенційні явища та чинники, які створюють небезпеку у кіберпросторі), а основним завдання ІС є забезпечення кібербезпеки [4].

На сьогодні загрози, які надходять з кіберпростору, відбуваються дедалі активніше та зазіхають навіть на національну безпеку. Організовані «набіги»на приватні та державні організації подекуди наносять критичну шкоду по економіці не тільки певної організації, а й не дають можливості подальшого розвитку держав. Джерелом усіх загроз є як іноземні військово-роздувальні служби, терористичні групи, так і ОЗУ (організовані злочинні угрупування), хакери, метою яких є протиправний заробіток [2].

До зовнішніх загроз відносяться: шкідливе ПЗ (програмне забезпечення); DDoS-атаки; фішинг-атаки; проникнення у локальну мережу; втрата ґаджету з важливою інформацією. Внутрішньою загрозою може бути вразливе ПЗ та людський фактор, який ніхто не відміняв [5].

Збільшення обсягу клієнтських даних, що весь час знаходиться в обробці та зростаюча вартість, а відповідно і роль інтелектуальної власності приводить до створення нових методів розкрадання приватної інформації. Зловмисників цікавлять дані щодо внутрішньої системи приватної організації чи державної установи: інформація про працівників, бухгалтерія, особиста інтелектуальна власність тощо.

Проблематика кібербезпеки характеризується тим, що ІС рідко або взагалі не використовує антивірусне ПЗ, не вживає заходів для захи-

сту приватної інформації, що включає в себе дані банківських карток, паролів до тих же банківських застосунків. Особливо важливими є персональні коди доступу, оскільки більшість використовують одну і ту ж комбінацію символів і чисел до всього що потребує авторизацію.

Заголовки статей засобів масової інформації (ЗМІ) містять в собі велику кількість повідомлень про електронне шахрайство, витік баз даних, хакерські атаки комерційних та державних структур, крадіжки інтелектуальної власності тощо.

Наприклад у 2014 році Інтерпол та Європол завдяки співпраці з компанією «Лабораторія Касперського» викрили групу Carbanak, яка протягом багатьох років успішно знімала кошти через онлайн-банкінг чи банкомати. Діяльність групи була досить проста, завдяки вірусу, що надсилався через електронну пошту на комп'ютери рядових співробітників, копіювалися дані про структуру та роботу банку. Згодом це допомагало створювати шляхи крадіжки грошей.

Також в практиці WIPO Arbitration and Mediation Center зустрічалися домені справи з організаціями, що просили змінити домен відповідачів у зв'язку з тим, що вони використають його для фішингу користувачів та працівників, наприклад виставлення підроблених рахунків клієнтам.

Щодо українських ЗМІ, то протягом останніх років новини про кібернетичні атаки на енергетичні компанії України, розсилку вірусного ПЗ через електронну пошту з підписом від податкової та майнінг криптовалюти шляхом розміщення шкідливого коду на сайтах державних установ стрімко зростають.

У червні 2017 року відбулась наймасштабніша кібернетична атака, що зупинила роботу декількох тисяч українських компаній та держорганів [1]. Пріоритетною жертвою вірусу «Petya A» виявилася Україна. Лише протягом одного дня комп'ютерний шкідник «Ransom: Win32/Petya» здійснив атаку на державний та приватний сектор економіки країни, до них належать банки, державна залізниця, аеропорти, телекомпанії, гіганти супермаркети, державні фіскальні служби, органи місцевого самоврядування тощо. Вірус-вимагач заморожує дані і вимагав внесення викупу 300 доларів у криптовалюті за відновлення доступу [6].

Вперше проект Закону України про кібернетичну безпеку був зареєстрований депутатами в червні 2015 року. На початку 2016 року у зв'язку з затвердженням президентом «Стратегії кібербезпеки України» нормативний акт втратив актуальність і був відкликаний. Згодом було

зареєстровано вже новий суттєво доопрацьований акт. 5 жовтня 2017 року закон «Про основні засади забезпечення кібербезпеки України» був остаточно прийнятий парламентом. Він спрямований на створення загальної державної політики кібербезпеки, а також розподіл функцій між різними держорганами.

Також цим законом передбачено створення Національної системи кібернетичної безпеки, що об'єднає низку міністерств та відомств, до якої входить державна служба спеціального зв'язку та захисту інформації, Національна поліція, Служба безпеки України (СБУ), Міністерство оборони та Генеральний штаб, Нацбанк, а також розвідувальні органи. Нормативно-правовий акт чітко визначає, яке відомство за що відповідає у сфері кіберзахисту [3].

Отже, забезпечення державної та міжнародної безпеки в інформаційній сфері та світовому кіберпросторі вимагає не тільки зусиль окремих країн світу, а й розробку і здійснення максимально ефективних міжнародних інструментів для контролю кіберзлочинності. Тому всі без виключення економічні та політичні ресурси з протидії загрозам міжнародної інформаційної кібербезпеки мають розглядатися на найвищому світовому рівні за участю основних кібердержав. Забезпечення кібербезпеки в контексті глобальних загроз, поряд з спільними зусиллями міжнародного співтовариства, диктує важливість розробки і здійснення превентивних дієвих заходів проти кібератак і кіберзлочинів в державному та світовому кіберпросторі.

Список бібліографічних посилань

1. Від кібератаки вірусом Petya.A постраждали до 10 % комп'ютерів в Україні – Шимків // НВ : сайт. 07.07.2017. URL: https://nv.ua/ukr/ukraine/events/vid-kiberataki-virusom-petya-a-postrazhdali-do-10-komp-juteriv-v-ukrajini-shimkiv-1442363.html (дата звернення: 25.10.2019).
2. Войціховський А. В. Кібербезпека як напрям євроатлантичної інтеграції України // Право і безпека у контексті європейської та євроатлантичної інтеграції : зб. ст. та тез наук. доп. за матеріалами дискус. панелі II Харків. міжнар. юрид. форуму (м. Харків, 28 верес. 2018 р.) / Нац. юрид. ун-т імені Ярослава Мудрого, НАПН України, Фонд Конрада Аденауера. Харків : Право, 2018. С. 42–48. URL: http://univd.edu.ua/science-issue/issue/3036 (дата звернення: 25.10.2019).
3. Піскорська Г. А., Яковенко Н. Л. Сучасні виклики і загрози в кіберпросторі: формування механізму міжнародної інформаційної безпеки. *Міжнародні*

відносини. Серія: Політичні науки. 2018. № 18–19. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/download/3389/3066 (дата звернення: 25.10.2019).
4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 25.10.2019).
5. Раєцький А. Кібербезпека бізнесу це не лише технічні заходи // Legal Group : сайт. URL: https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/ (дата звернення: 25.10.2019).
6. Україна стала першою ціллю принципово нового виду кіберзброї // Укрінформ : сайт. 05.07.2017. URL: https://www.ukrinform.ua/rubric-technology/2259655-ukraina-stala-persou-cillu-principovo-novogo-vidu-kiberzbroi.html (дата звернення: 25.10.2019).

Одержано 01.11.2019

УДК 341:[343.9:004]

Карина Сергіївна Коломоєць,
студентка 4 курсу юридичного факультету
Харківського національного університету імені В. Н. Каразіна

Євген Борисович Тітов,
кандидат юридичних наук, доцент,
доцент кафедри міжнародного і європейського права
юридичного факультету Харківського національного
університету імені В. Н. Каразіна

Незаконне розповсюдження наркотичних речовин через мережу інтернет як загроза правопорядку

Проблема незаконного обігу наркотичних речовин є предметом міжнародного співробітництва держав вже не одне десятиліття. Наркобізнес можна вважати міжнародним або транснаціональним явищем, зважаючи на негативні наслідки такої діяльності, які загрожують безпеці далеко не однієї країни. Однак, ще складніша ситуація постає у зв'язку з використанням особами, які скоюють цей злочини, новітніх інформаційних технологій та телекомунікаційних мереж, зокрема й мережі Інтернет.

Виготовлення, збереження та реалізація наркотичних речовин визнається міжнародним співтовариством протиправним діянням, тому на універсальному рівні була прийнята низка міжнародних договорів, що стосуються даного питання: Єдина конвенція про наркотичні речовини (1961), Конвенція про психотропні речовини (1971), Конвенція ООН про боротьбу проти незаконного обігу наркотичних і психотропних речовин (1988).

Окрім того, можна виокремити основні міжнародні органи, що здійснюють контроль над наркотичними і психотропними речовинами: Комісія з наркотичних речовин, Управління ООН з наркотиків і злочинності, Міжнародний комітет ООН з контролю за наркотиками (далі – МККН).

МККН, зосереджуючи увагу на сучасних інформаційних технологіях, визначає три основні способи незаконного використання інновацій: 1) розповсюдження за допомогою ЗМІ матеріалів, підбурюючих до вживання наркотиків; 2) поширення за допомогою мережі Інтернет інструкцій,

щодо вживання та виготовлення наркотиків; 3) використання мережі Інтернет як ринку товарів та засобу збуту наркотичних речовин.

Беззаперечно, використання інформаційних технологій та мережі Інтернет полегшує життя у багатьох сферах, однак саме завдяки Мережі поширюється новітній спосіб обігу і розповсюдження наркотичних речовин – віртуальний наркобізнес. Злочинці у своїй протиправній діяльності мають на меті у такий спосіб приховати свою злочинну діяльність від правоохоронних органів, уникнути безпосереднього обміну наркотиків на гроші та, як наслідок, можливості бути затриманими «на гарячому». Тому вони вдаються до використання зашифрованих Інтернет-ресурсів, псевдонімів, кодових слів та координують свої дії та здійснюють обмін інформацією за допомогою мобільних додатків.

Звичайно, для залучення потенційних покупців наркотичних речовин, збувачі можуть вдаватися до сучасних методів реклами: розсилка тематичних повідомлень, інтернет-форуми та чати, соціальні мережі тощо. Однак, особливої популярності набуло явище розміщення на різних об'єктах міської інфраструктури надписів із пропозиціями продажу наркотиків. Переважно це різноманітні надписи на стінах будинків, під'їздах, гаражах, зупинках громадського транспорту, підземних переходах тощо, сутність та зміст яких є зрозумілим особам, які мають намір придбати заборонені речовини. При подальшому контакті осіб для продажу наркотичних речовин, кіберзлочинці можуть використовувати TOR-браузери – система проксі-серверів, що дозволяє встановлювати анонімне мережне з'єднання, захищене від прослідковування. Також злочинці вдаються до використання VPN підключення – тобто технології, яка забезпечує створення в мережі Інтернет зашифрованої додаткової «чорної» сітки для передачі даних.

Останнім часом для повної конспірації та анонімності он-лайн збувачі почали використовувати «ЧАТ-боти», або іншими словами віртуальні автоматичні співрозмовники через мобільні інтернет-месенджери, що розповсюджують рекламу наркотиків через повідомлення та мають змогу підтримувати переписку, приймати замовлення та відповідати на запитання.

Після встановлення контакту та узгодження питань про вид, обсяг наркотику, його ціну, спосіб передачі, особи, що мають намір придбати наркотики, мають здійснити передоплату. Зазвичай, оплата здійснюється електронними платіжними засобами.

Після оплати покупець отримує від збувальника інформацію про місце, час та спосіб отримання наркотиків. Найчастіше злочинці реалізовують передачу наркотичних речовин шляхом здійснення так званих «закладок», тобто схованки у безлюдних або прихованих від людської уваги місцях: поштовий ящик, батарея опалення, електричний або пожежний щиток у під'їзді багатоповерхового житлового будинку, клумба з квітами поблизу житлових будинків тощо. При цьому наркотик маскується або упаковується таким чином, щоб не привертати уваги сторонніх і уникнути можливості вилучення сторонніми особами, а вся координація дій і обмін інформацією між співучасниками, а також із замовником, здійснюється за допомогою телекомунікаційних мереж і мобільних додатків, таких як «Telegram», «Viber», «WhatsApp», «Jabber», «Skype» та ін.

Отже, проаналізований механізм незаконного збуту наркотичних речовин через мережу Інтернет дає підстави стверджувати, що цей спосіб здійснення злочинної діяльності є занадто вигідним для кіберзлочинців, через що ця проблема є актуальною і вимагає якнайшвидшого вирішення на законодавчому рівні та створення ефективних методик виявлення і припинення таких злочинних кібероперацій.

Одержано 01.11.2019

УДК 340.12

Світлана Миколаївна Кравчук,
присяжна суддя Шевченківського районного суду м. Львова,
здобувач наукового ступеня кандидата юридичних наук кафедри історії держави, права та політико-правових учень
Львівського національного університету імені Івана Франка,
старший викладач кафедри суспільно-гуманітарних наук Української академії друкарства (м. Львів)

Теоретико-правові дослідження торгівлі людьми як підґрунтя для її подолання

Торгівля людьми – глобальна проблема, хоча більшість вважає, що цей аспект його не торкається та права людини перебувають під ретельним захистом держав, а така нелюдська форма дій просто вигадка та пережиток минулого. Проте, це не так. Експерти ООН констатують факт більш значної привабливості торгівлі людьми в порівнянні навіть з торгівлею наркотиками та зброєю, та ще за умов менш значних ризиків. Отож, боротьба з цими діями, як способами поневолення людини, обмеження її життєвих (фізичних), економічних та ін. прав потребує об'єднання міжнародних зусиль у сучасному світі. Означеній проблемі не відомі державні межі, поділ держав за економічним рівнем розвитку, тощо. Ця проблема стосується як народів втягнених у війну, так і тих, які живуть у мирі. Загалом це низькі у моральному сенсі дії, що ґрунтуються на введенні в оману. Такі дії тісно переплітають з трудовою експлуатацією і давно стали викликом сучасному суспільству. Доречно наголосити, що у Європі це найпопулярніший підпільний бізнес і це навіть тісно пов'язано з успішним економічним розвитком країн-учасниць Європейського Союзу. Оскільки, останні стають привабливими для людей які бажають покращити свій життєвий рівень. Економічно незабезпечені, невдоволені матеріальним станом люди прагнуть у них потрапити у будь-який спосіб. Не секрет, що за сучасних економічних умов це стало вадою багатьох українців, які «шукають» деінде матеріального та особистого (шлюби) «щастя».

В теоретико-правовому сенсі явищу торгівлі людьми властиві такі елементи: дії (вербування, перевезення, вербування, передання приховування чи отримання людей); засоби (погрози, насилля, ін. форми

примусу, шахрайство, обман, зловживання владою чи вразливість становища, підкуп у вигляді платежів чи вигід (зисків) для отримання згоди особи); цілі – як певні прагнення досягти тих чи інших результатів, внаслідок вчинення відповідних дій.

Роль держави – пункт призначення чи шлях (транзит, переміщення). Багато країн є і вихідним пунктом, і кінцевим (поєднують у собі декілька цілей).

Важливим є дослідження Тюрканової Є. В. [1, с. 12], яка в т. ч. провела класифікацію торгівлі людьми. Так, за критерієм сфери експлуатації в науці виведено наступні види: 1. Торгівля людьми (частіше жінками та дітьми) з метою сексуальної експлуатації: для організації «цивільної» проституції; для організації проституції у місцях військових дій і розташуванні військ; для організації секс-туризму; для виробництва порнографії. 2. Торгівля людьми з метою експлуатації їх праці в т. ч.: в «поточному виробництві»; в неформальній і тіневій економіці; на підпільному виробництві та при виробництві контрафактної продукції; в домашньому господарстві; дитяча праця. 3. Торгівля людьми (особливо діти та інваліди) з метою жебрацтва, в т. ч.: використання дітей; використання інвалідів; «оренда немовлят» для жебрацтва. 4. Корисливі фіктивні шлюби («наречена по листуванню») в т. ч.: для використання в домашньому господарстві; примусового сурогатного материнства; для обслуговування хворих, дітей та пристарілих родичів. Доповню цю сферу ще одним виділеним авторським підвидом: примусове донорство (вилучення яйцеклітин для репродукції) та сурогатне материнство. Оскільки він тісно пов'язаний саме з вищенаведеною сферою та не потребує виокремлення в особливу групу відносин (випливає з «шлюбних»). Такі корисливі шлюби найчастіше виникають через легковірне листуванням через соціальні мережі. Створюється можливість відбору «людського матеріалу» – зовнішні риси, колір очей, волосся, ріст, тощо. 5. Торгівля для трансплантації органів та тканих. 6. Торгівля дітьми задля усиновлення/удочеріння. 7. Торгівля з метою використання в збройних конфліктах. 8. Використання солдат і в'язнів для примусових робіт. Вважаю за доцільне додатково продовжити наведену класифікацію: 9. Використання в'язнів у збройних конфліктах. 10. Використання людей (особливо дітей) задля «прищеплення» чи ін. типів тоталітарної фанатичної свідомості (деструктивне прислужництво, тощо).

Досліджена та допрацьована класифікація не є перфектною, оскільки явище характеризується особливим динамізмом, «пристосуванням» до реалій сучасної життєвої дійсності (інформаційне суспільство), та слугує легким шляхом до певних вигод (зисків) окремих осіб, груп, організацій.

Наведемо виведені причини цього нелюдиномірного явища: політичні (курс держав повинен мати гуманістичний напрям); економічні (держави повинні працювати над подоланням бідності); адміністративно-організаційні (є потреба посилення адміністративного контролю); правові (відсутність правового регулювання або ж його недосконалість); морально-етичні (низький рівень етики та моралі).

Однією з основних підстав подолання торгівлі людьми є осмислене та безспірне визнання цього явища як негативного державами світу та встановлення відповідного внутрішньодержавного правового регулювання. Об'єктивне (писане) право повинне ґрунтуватись на наукових дослідженнях, передусім – теоретико-правових. Закони повинні прийматися з врахуванням багатьох аспектів законодавства інших держав. Це зробить їх ефективнішими та зміцнить захист прав людини. Торгівля людьми має транснаціональний характер, тому єдність щодо наслідків для людини та специфіка неправомірних дій мають бути враховані в законодавстві кожної з держав. Закони повинні працювати й є способи «заставити» їх це зробити – створити таке правове поле та життєві умови для людини, за яких торгівля людьми стане малоприбутковою, ризикованою і марною з кожного погляду справою.

Список бібліографічних посилань

1. Тюрканова Е. В. Торговля людьми в Российской Федерации: обзор и анализ текущей ситуации по проблеме. М. : Изд-во ЮНИСЕФ, 2006. 154 с.

Одержано 30.10.2019

УДК 340.12

Ілля Сергійович Коротков,
студент Харківського національного університету внутрішніх справ

Протидія торгівлі людьми в інформаційній сфері

Торгівля людьми – це сучасна форма рабства. Вона розглядає людей як товар, який можна продати чи купувати. Торгівля людьми згідно ст. 4 Конвенції Ради Європи «Про заходи щодо протидії торгівлі людьми» від 16 травня 2005 р. означає найм, перевезення, передачу, приховування, або одержання осіб шляхом погрози або застосування сили…

У дослідженні, зробленому під егідою Ради Європи, використання інформаційних технологій для вербування жертв не є новою формою торгівлі людьми, а є лише новим інструментом.

Правопорушники створюють активні вебсайти пошуку моделей та фотомоделей або шлюбні агенції, які виступають платформою для вербування потенційних жертв торгівлі людьми.

Слід розрізняти між вебсайтами, які пропонують можливість купити наречену(рабиню), та агенціями знайомств, які функціонують як вебсайти, де розміщується незаконний контент.

Сьогодні злочинні групи під виглядом законослухняних компаній підписують контракти, переважно для роботи у Західній Європі, гарантуючи виплату заробітної плати після виконання певної роботи, наприклад, демонтажу будівлі. У таких випадках злочинці шукають групу людей для дешевої робочої сили, знижуючи їм заробітну плату та не забезпечуючи їх мінімальними умовами праці, проживання, соціального захисту. У таких випадках частіше всього вербують чоловіків.

В Інтернеті також можна зустріти немало сайтів ескорт-агентств. Це компанії, які надають ескорт-партнерів клієнтам, переважно для сексуальних послуг. Ескорт-агентства часто вербують людей для роботи ескорт-партнерами, публікуючи оголошення в Інтернеті, журналі або газетах.

Діяльність сайтів з пошуку моделей, сайтів ескорт-агентств та сайтів з пропозицією працевлаштування свідчать про наявність ознак складу злочинів, передбачених ст. 149 «Торгівля людьми або інша незаконна

угода щодо людини», 303 «Сутенерство або втягнення особи в заняття проституцією» КК України.

Ідентифікацію та збір інформації потрібно починати зі встановлення даних реєстратора доменного імені та хостингу. Інформацію можна зібрати за допомогою сервісів whois (https: centralops.net). Встановити ір-адресу за певний період користування. З ір-адреси можливо встановити Інтернет провайдера, далі потрібно надіслати офіційних запит, після отримання інформації, при укладанні договору людина вказує свої особисті данні, які потім провайдер повинен передати правоохоронцям після відповідного запиту.

Також можна відстежити за номером телефону, якщо на сайті він є, для цього треба звернутися для мобільного оператора, для встановлення району, де знаходиться абонент, чи які інші сім карти він використовував на своєму пристрої, за допомогою IMEI коду (особистого коду кожного мобільного телефону, навіть, якщо пристрій не підтримує вихід до мережі Інтернет.

Таким чином, торгівля людьми залишається проблемою людства навіть у нас час, для протидії цьому пропонуємо такі заходи:

- посилити відповідальність за такі види злочинів;

- зменшити кількість часу на оформлення документів, відсутність яких не дозволяю правоохоронцям своєчасно заарештувати, чи викрити злочин;

- блокувати сайти, які мають хоч якийсь стосунок до ескорт-послуг чи інших сайтів, які порушують законодавство.

Одержано 31.10.2019

УДК 159.92

Павло Валентинович Макаренко,
кандидат психологічних наук, доцент,
заступник декана факультету № 4 з навчально-методичної роботи Харківського національного університету внутрішніх справ

Вікторія В'ячеславівна Доценко,
кандидат психологічних наук, доцент,
доцент кафедри педагогіки та психології факультету № 3
Харківського національного університету внутрішніх справ

Психологічні аспекти протидії гендерному насильству

Впродовж останніх років вивчення проблеми протидії гендерному насильству стало одним із пріоритетних напрямків діяльності правозахисників, психологів, медичних та педагогічних працівників. Гендерне насильство – це порушення прав людини і форма дискримінації щодо однієї зі статей включаючи всі види насильства на основі гендерних ознак, які призводять до фізичної, сексуальної, психологічної або економічної шкоди [3].

При здійсненні профілактичних заходів щодо гендерного насильства, фахівцям, які працюють у сфері запобігання та протидії насильству за ознакою статті, а також працівникам правоохоронних органів, необхідно розуміти психічні механізми, що забезпечують перебування жертви в ситуації насильства і формують у неї специфічний травматичний ефект.

Існує декілька підходів до пояснення прив'язаності жертви до кривдника.

Перший підхід базується на теорії навчання. Низка вчених використала концепцію навчання безпорадності, яку розробив М. Селігман, для пояснення стосунків між агресором і жертвою. Безпорадність – це психічний стан, який виникає у випадках, коли події непідконтрольні суб'єкту [2]. Іншими словами, ми не можемо зробити нічого, щоб запобігти цій події і вона буде повторюватися знову і знову, що б ми не робили. Безпорадність, як психічний стан має наступну структуру: 1) розлад мотиваційної сфери (пасивність), 2) розлад інтелектуальної сфери

(зниження здатності до вирішення проблем), 3) емоційна травма (зростаюче почуття безсилля, некомпетентності, фрустрації і депресії) [2].

Л. Уолкер застосувала теорію навчання безпорадності в своїх дослідженнях проблеми перебування жінок в ситуації гендерного насильства. Вона зазначила, що періодична агресія знижує мотивацію жінки до реагування. Поступово жінка стає пасивною. Паралельно з цим, її когнітивна здатність до сприйняття успіхів і досягнень знижується. Жінка перестає вірити в можливість позитивного результату своїх власних дій [1]. Для пояснення психології взаємовідносин жертви і агресора Л. Уолкер запропонувала 3-х фазний «цикл насильства», який служить засобом створення травматичного емоційного зв'язку між жертвою і агресором [4]:

1) фаза акумуляції або наростання напруги – жінка перебуває в стані екстремальної психічної гіпернастороженості, намагаючись уникнути епізоду агресії. Її стан можна порівняти зі станом людей, які намагаються вижити в ситуації утримання в заручниках або внаслідок природних катаклізмів;

2) фаза агресії або розряд напруги – жінка перебуває в стані дисоціації, що супроводжується невірою в те, що епізод агресії дійсно має місце (що його не вдалося уникнути незважаючи на всі старання і обережність). Дисоціація призводить до розвитку пасивності, депресії, тривоги, самообвинувачення і почуття безпорадності;

3) фаза каяття – відтворення агресором якоїсь фікції закоханості. Агресор поводить себе прямо протилежно епізоду насильства, відбувається підкріплення ідеального образу партнера і створення ілюзії, що своєю досить хорошою і правильною поведінкою жінка зможе зробити постійною ситуацію «медового місяця».

Другий підхід розкриває особливості відносин жертви і агресора засновані на нерівному розподілі влади, що породжує травматичний зв'язок між ними. В таких відносинах один партнер (агресор) домінує, має владу і поперемінно переслідує, б'є, загрожує і залякує того, хто не має доступу до позицій влади (жертва). Такі відносини формують у жертви сильну емоційну залежність від агресора. Наприклад, відносини між жінкою – жертвою гендерного насильства та її агресором, між викрадачем і заручником, між членом секти і її лідером, між полоненим і наглядачем. Такі відносини мають дві спільні риси: дисбаланс влади і переривчастий характер насильства (чергування ситуацій насильства і

його відсутності). У міру того, як дисбаланс влади збільшується, людина, що знаходиться в стані підпорядкування, буде проявляти суб'єктивне відчуття залежності від «могутнього» агресора. В останнього, в свою чергу, буде формуватися ідея власної величі і всемогутності. Слід зауважити, що чергування фізичного насильства з актами примирення і винагороди підсилює ефект травматичного зв'язку. Так, в ситуації гендерного насильства фаза каяття асоціюється з припиненням агресії і отримує стійке підкріплення як позитивна ситуація, якої необхідно досягти, і яка, в процесі нескінченного повторення циклів насильства, стає все більш бажаною і підкріплює травматичний зв'язок.

Третій підхід досліджує ідентифікацію з агресором як захисний механізм поведінки жертви. Для гендерного насильства був розроблений термін «побутовий Стокгольмський синдром». Цим терміном вчені описують психічний розлад дезадаптативного типу, коли жертви гендерного насильства активно встають на захист свого агресора. Виникає як спроба жертви захистити власну психічну цілісність і відновити фізіологічний і поведінковий гомеостаз. У спробі уникнути і / або зменшити ефект насильства жертва ідентифікує себе з агресором і виправдовує перед собою та іншими його дії [4]. Однак, дослідники підкреслюють [1, 4, 5], що в разі гендерного насильства мова йде не стільки про адаптацію до особистості агресора, скільки про втрату жертвою власної ідентичності. Тобто, має місце не адаптивний механізм, а реальний процес руйнування особистості жертви. «Під примусом заручник поступово втрачає свою попередню систему переконань; він зрештою починає співпереживати поневолювачу і бачити світ його очима. У сімейному насильстві, навпаки, жертву ув'язнюють поступово, залицяючись» [1, с. 146].

Четвертий підхід пояснює процес «ментального контролю» або психологічного чи примусового переконання, що використовує агресор у стосунках з жертвою. Він поєднує різні стратегії, спрямовані на підпорядкування і дезідентифікацію жертви. Агресор може використовувати наступні стратегії: домінування чоловіка за допомогою поведінки, яка помилково інтерпретується жертвою як поведінка «справжнього чоловіка»; відокремлення жертви від зовнішніх зв'язків (батьків, друзів, роботи); поступове навіювання жертві почуття страху; індукція почуття провини («ти мене змусила», «якби ти не була такою дурною (товстої, некрасивою)» тощо); патологічні ревнощі; індукція почуття нікчемності і беззахисності («крім мене ти нікому не потрібна», «мені від сусідів соромно»).

Слід зауважити, що способи, які дають одній людині поневолити іншу досить подібні між собою. Так, в ситуації гендерного насильства агресор використовує метод «промивання мізків» описаний А. Бідерманном як поєднання методів примусу в системі тортур: одиночне ув'язнення, монополізація сприйняття, індукція стану ментального і фізичного виснаження (вимотування), загрози, докази всемогутності, приниження, чергування епізодів «прихильності» [1, 4].

П'ятий підхід базується на особливостях дитинства жертви. В батьківській сім'ї формується уявлення про те, що насильство є нормою сімейного життя. У жінок-жертв ще в дитинстві були сформовані стигми «жінка в сім'ї – не людина», «ні на що не здатна» тощо [5]. Глибокі психологічні травми з дитинства формують «нав'язливі повторення», як спробу суб'єкта опанувати дитячу травму (З. Фройд) та прагнення дорослого до комбінації протилежних емоцій, які він переживав ще дитиною (Р. Фейрбейрн). Р. Фейрбейрна пропонує переконливе пояснення стійкої прихильності до поганого об'єкту. Його дослідження показали, як не парадоксально, але приниження тільки підвищують потребу дитини в батьках, а в більш дорослому віці – в партнері, який виступає в ролі батька. У дорослому віці люди, які недоотримали уваги в дитинстві, схильні впадати в крайню залежність від інших особистостей, тим самим стабілізуючи свою самосвідомість або ж отримуючи відчуття внутрішнього спокою [4].

На підставі вище сказаного констатуємо: жертви гендерного насильства досить різні особистості: за віком, за життєвим досвідом, за психологічними особливостями (цінностями, настановленнями, рисами характеру, мотивацією, потребами) тощо. Жертва далеко не завжди звертається по допомогу, їй важко самостійно покласти край своїм стражданням і почати активно боротися за автономне життя. Для протидії окресленій проблемі необхідний комплексний підхід скоординованої співпраці між правоохоронними органами, правозахисними організаціями, представниками соціальних та педагогічних спільнот, працівниками медичних і психологічних служб.

Список бібліографічних посилань

1. Герман Дж. Психологічна травма та шлях до видужання: наслідки насильства – від знущань у сім'ї до політичного терору; переклад з анг. О. Лизак, О. Наконечна, О. Шлапак. Львів : Вид-во Старого Лева, 2019. 424 с.

2. Гордеева Т. О. Психология мотивации достижения. М. : Смысл; Академия, 2006. 336 с.

3. Лист МВС України від 21.10.2019 року № 22/5/2-5985 про методичні рекомендації з профілактики гендерно-обумовленого насильства учасників антитерористичної операції та операції Об'єднаних сил.

4. Селани Д. П. Иллюзия люби : Почему женщина возвращается к своему обидчику / пер с англ. И. Л. Писаренко. М. : Класс, 2013. 264 с.

5. Соціально-педагогічні основи захисту прав людини, протидії торгівлі людьми та експлуатації дітей : навч.-метод. посіб. / за заг. ред. К. Б. Левченко, Л. Г. Ковальчук. 2-ге вид., допов. і перероб. Київ : Агенство Україна, 2016. 368 с.

Одержано 05.11.2019

УДК 004.946.5.056

Вікторія Русланівна Лисак,
студентка 2 курсу юридичного факультету
Тернопільського національного економічного університету

Кіберзлочинність: як захистити себе в мережі

За останні кілька років комп'ютерні технології глибоко проникли в повсякденне життя людини. Заперечувати їх важливість практично неможливо, адже кожен день людина використовує різні комп'ютерні блага, вони стали невід'ємною частиною її звичного способу життя.

Проте, разом з розвитком інформаційних технологій зростає і кількість злочинів у цій сфері. Кіберзлочини, або іншими словами комп'ютерні злочини, – це суспільно небезпечні винні діяння, вчинені у кіберпросторі за допомогою комп'ютера та Інтернету. Кіберзлочинці зазвичай полюють на персональні дані, банківські рахунки, конфіденційну та комерційну інформацію, паролі тощо. Потерпілими від цих атак можуть бути як фізичні, так і юридичні особи, а також держава [1].

Для ефективної боротьби з кіберзлочинністю та регулювання відносин у цій сфері держава на законодавчому рівні впроваджує різноманітні нормативно-правові акти. До таких актів, зокрема, належать Конституція України, Кримінальний кодекс України, закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки» та інші закони [4].

Крім того, важливу роль у протидії кіберзлочинності відіграє Конвенція про кіберзлочинність, яка належить до українського законодавства, адже належним чином ратифікована ВРУ. Відповідно до цієї Конвенції, кіберзлочини поділяються на чотири види, а саме: правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ; нелегальне перехоплення; втручання у дані; втручання у систему; зловживання пристроями), правопорушення, пов'язані з комп'ютерами (шахрайство), правопорушення, пов'язані зі змістом (дитяча порнографія), а також правопорушення, пов'язані з порушенням авторських та суміжних прав [3].

Кількість кіберзлочинів в Україні щороку зростає. Найпоширенішим видом злочинів є шахрайство. Зокрема, впродовж 2019 року було зареєстровано 45836 злочинів у сфері шахрайства, 21153 проваджень з яких було закрито. Найчастіше шахраї створюють сайти і продають неіснуючий товар, дуже багато злочинів, які стосуються виманювання інформації з карток та онлайн-кредитування [5].

Друге місце посідають кіберзлочини у сфері незаконного втручання в роботу комп'ютерів – у 2019 році зареєстровано 1079 правопорушень, серед яких 74 було закрито. Розповсюдження порнографії займає третє місце серед найбільш популярних кіберзлочинів. Згідно з даними Генеральної прокуратори України, у 2019 році було зареєстровано 774 проваджень і лише 47 вирішено [5].

Варто зазначити, що повністю захистити себе від кібератак неможливо. Проте виконання хоча б мінімальних правил техніки безпеки поводження в мережі значно підвищить шанси, що вас не зламають. До основних правил належать: уважно читайте сайти, де залишаєте персональні дані; створюйте складні паролі, не варто використовувати один і той самий пароль і для банківської картки, і для входу в соціальні мережі; не використовуйте громадський Wi-Fi для важливих цілей, не здійснюйте платіжних операцій, адже через них хакери можуть перехопити ваші дані, тому краще користуватись мобільним Інтернетом.

Не давайте нікому персональні дані, паролі і коди-підтвердження з СМС для операцій з картками; перевіряйте інформацію за офіційним номером банку; не скачуйте в Інтернеті сумнівні файли; користуйтесь ліцензійним програмним забезпеченням; не переходьте на підозрілі посилання та за спливаючими вікнами; періодично здійснюйте резервне копіювання важливої інформації; тримайте свої гаджети в полі зору, коли знаходитеся у місцях, де до них може бути доступ сторонніх осіб [2].

До того ж, варто встановити двофакторну автентифікацію для email та акаунтів у соцмережах. Для входу в акаунт, окрім паролю, налаштуйте відправлення СМС на ваш мобільний із одноразовим кодом або ж встановіть додаток – генератор кодів. Мало хто знає про те, що сумнівний номер телефону чи картки можна перевірити на сайті кіберполіції, а також звернутися до спеціалістів із запитом [5].

Можна зробити висновок, що сучасний світ живе в епоху інформаційних технологій. Можливості мережі є не лише джерелом інформації, знань та спілкування, але й джерелом підвищеної небезпеки. Саме тому

потрібно бути готовим до того, що в будь-який момент у кого-небудь може виникнути бажання отримати доступ до ваших персональних даних, банківських рахунків чи паролів. Саме тому дотримання певних правил зменшить ризик цих кібератак. Це унеможливить доступ зловмисників до ваших аккаунтів та вбереже вас від потрапляння в пастки кіберзлочинців [2].

Список бібліографічних посилань

1. За п'ять років кіберзлочинність в Україні виросла вдвічі / Економічна правда : сайт. 21.10.2019. URL: https://www.epravda.com.ua/news/2019/10/21/652782/ (дата звернення: 21.10.2019).
2. Нікулеско Д. Кібербезпека: вразливі моменти // Юридична газета online : сайт. URL: http://yur-gazeta.com/publications/practice/inshe/kiberbezpeka-vrazlivi-momenti.html (дата звернення: 21.10.2019).
3. Конвенція про кіберзлочинність : від 07.09.2005 // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 21.10.2019).
4. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 21.10.2019).
5. Що варто знати про кіберзлочинців в Україні? // Радіо Свобода : сайт. URL: https://www.radiosvoboda.org/a/details/29031166.html (дата звернення: 21.10.2019).

Одержано 01.11.2019

УДК 343.97:[343.341:316.774](477)

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

Татьяна Алексеевна Фролова,
курсант 3 курса факультета № 4
Харьковского национального университета внутренних дел

Манипуляция информацией как метод информационного терроризма и информационной войны

На рубеже XX и XXI вв. развитие современных технологий и активное развитие коммуникационных технологий значительно облегчило производство и распространение социально значимой информации и привело к формированию глобального информационного пространства, которое заложило основу формирования общества совершенно нового типа – информационного общества [1].

Статистические данные показывают [2], насколько велико значение Интернета как средства массовой коммуникации в Украине, а также в мировом сообществе. К сожалению, современные технологии применяются не только во благо человека, но и во вред, например, при проведении информационного терроризма, ведении информационных войн и совершении информационных преступлений.

Термин «информационный терроризм» является более общим, чем «кибертерроризм»; охватывает вопросы использования разнообразных методов и средств информационного воздействия на различные стороны человеческого общества (физическую, информационную, когнитивную, социальную). Под информационным терроризмом следует понимать один из видов террористической деятельности, ориентированный на использование различных форм и методов временного или безвозвратного вывода из строя информационной инфраструктуры государства или ее элементов, а также целенаправленное использование этой инфраструктуры для создания условий, влекущих за собой катастрофические

последствия для различных сторон жизнедеятельности общества и государства. При этом можно выделить следующие основные его виды:

1) информационно-психологический терроризм – контроль над СМИ с целью распространения дезинформации, слухов, демонстрации мощи террористических организаций; воздействие на операторов, разработчиков, представителей информационных и телекоммуникационных систем путем насилия или угрозы насилия, подкупа, введения наркотических и психотропных средств, использование методов нейролингвистического программирования, гипноза, средств создании иллюзий, мультимедийных средств для ввода информации в подсознание и т. д.;

2) информационно-технический терроризм – нанесение ущерба отдельным физическим элементам информационной среды государства; создание помех, использование специальных программ, стимулирующих разрушение систем управления, или, наоборот, внешнее террористическое управление техническими объектами (в т. ч. самолетами), биологические и химические средства разрушения элементной базы и т. д.; уничтожение или активное подавление линий связи, неправильное адресование, искусственная перегрузка узлов коммутации и т. д. [3].

Рассмотрим более подробно информационно-психологический терроризм, его влияние на общество в целом.

Информационно-психологический терроризм – это новый вид террористической деятельности, ориентированный на использование различных форм и методов негативного воздействия на информационно-психологическую среду с использованием СМИ и информационно-телекоммуникационных систем для создания негативных условий, влекущих за собой дестабилизацию социально-политической обстановки [4].

В настоящее время информационный терроризм набирает все большие обороты, и его последствия просто ужасающи. Роль СМИ настолько велика в современном обществе, что СМИ часто называют «четвертой властью» (наряду с законодательной, исполнительной и судебной) [5–7].

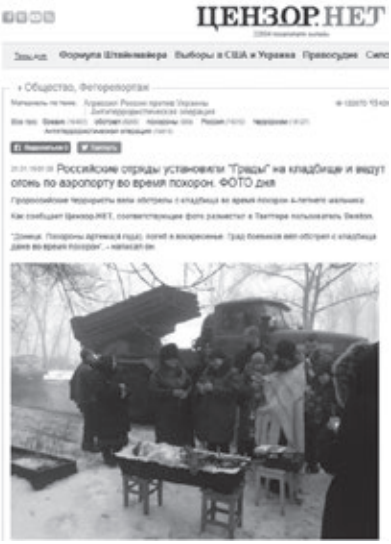
Что же представляет собой СМИ и являются ли они в действительности этой четвертой властью? Радио, телевидение, интернет и другие технические средства массовой информации распространяют информацию на большие расстояния, для рассредоточенной в пространстве огромной аудитории слушателей, зрителей и читателей в реальном режиме времени.

СМИ выступают в роли общественного эксперта, формируют отношение, представления, мнения, взгляды, стремления. Отношение общества к тому или иному вопросу формируется на основании полученной информации.

Но существуют наиболее опасные для государства и международного сообщества действия, затрагивающие информационную безопасность, совершаемые одним государством в отношении другого государства, которые объединяются в понятие «информационная война».

Ярким примером последствий информационной войны является конфликт на Востоке Украины. Нет такой семьи в нашей стране, которой бы не коснулась эта трагедия. Весомую роль в данном конфликте сыграли СМИ, которые излагали информацию в том формате, в котором требовалось, и формировали у населения те взгляды на происходящие в государстве процессы, которые были выгодны этой стороне конфликта.

Для примера продемонстрируем, как освещались в разных СМИ одни и те же факты, вследствие чего у людей формировались разные отношения к данной ситуации.


ЦЕНЗОР.НЕТ

Формула Штайнмайера Выборы в США и Украина Правосудие

Общество, Фоторепортаж

Российские отряды установили "Грады" на кладбище и ведут огонь по аэропорту во время похорон. ФОТО дня

Рисунок 1 – Публикация на сайте ЦЕНЗОР.НЕТ [8]

Рисунок 2 – Публикация на сайте SNR24 [9]

Итак, в указанных статьях (рис. 1 и 2) описывается один и тот же факт – большое горе – смерть ребенка. Только вот суть статей в разных СМИ абсолютно противоречит друг другу. Разные СМИ преподносит материал в выгодном для себя свете, дабы сформировать в сознании людей ту точку зрения, которая им выгодна. И отношение людей к этому событию будет зависеть от того какой сюжет они посмотрят, и какие выводы сделают.

Вот еще один сюжет, который можно рассмотреть.

ROISSYA24.NET: ВСЕ НОВОСТИ ИЗ ОДНОГО МЕСТА

Рисунок 3 – Публикация на сайте STOPFAKE.ORG 5 [10]

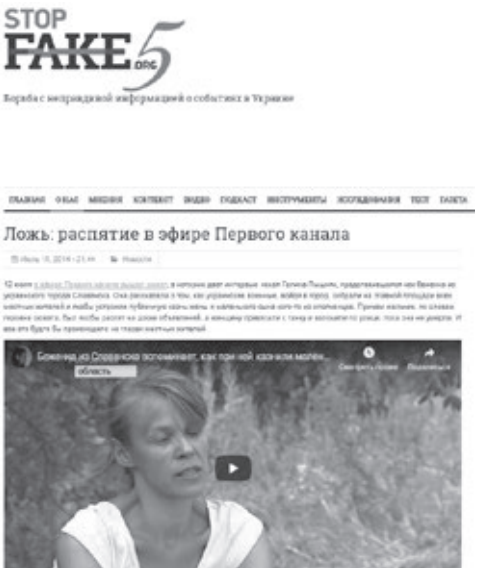


Рисунок 4 – Публикация на сайте STOPFAKE.ORG 5 [11]

Информационная война против Украины была ещё видна очень ярко в самом начале военного конфликта. Когда СМИ одной из сторон пытались нарисовать образ украинской власти, как некоего карательного органа, преследующего украинский народ. Так на сайте «roissya24.net» в 2014 году появилась информация про мальчика, который был распят в городе Славянск (рис. 3). Впоследствии информация была опровергнута. Поскольку она не нашла своего подтверждения и среди жителей Славянска, этому нет ни фото, ни видео доказательств, ни свидетелей. Однако, большинство людей формируют свое мнение о том или ином событии именно из источника, который первым обнародовал информацию или доступ только к которому они имеют. Изменить мнение людей даже опровергая информацию, довольно тяжело.

Приведенные примеры это всего лишь «капля в море» информационного хаоса, с помощью которого ежедневно пытаются влиять на сознание больших групп населения. Исходя из вышеизложенного, можно сделать вывод, что противодействие информационной войне и информационному терроризму – это одно из направлений обеспечения информационной безопасности как составляющей части национальной безопасности государства. Механизмы противодействия указанным

угрозам должны быть высокотехнологическими и иметь системный характер.

Какие шаги необходимо предпринять для противодействия этим двум указанным выше угрозам:

1. Усовершенствование нормативно-правовой базы Украины в части информационной безопасности. Несмотря на то, что в Украине приняты ряд нормативно-правовых актов, направленных на обеспечение информационной безопасности, таких как указ Президента Украины от 25.02.2017 № 47/2017 «О Доктрине информационной безопасности», Закон Украины «О национальной безопасности Украины» от 21.06.2018, четкий механизм противодействия информационному терроризму и информационной войне так и не был выработан.

2. Создать систему органов кибербезопасности, которые бы контролировали Интернет-пространство нашего государства, мониторили, выявляли, блокировали и принимали бы меры к нейтрализации лиц, распространяющих информацию, которая вредит национальной безопасности.

3. С целью эффективного противодействия в дальнейшем информационной войне, не восприятия неправдивой информации, целесообразно ввести в системе образования в школах уроки по информационной безопасности и анализу полученной информации.

Сейчас органами власти делаются шаги к решению данных проблем. Так в Луганской и Донецкой областях установлены телевышки, которые позволяют вещать украинские радио- и телеканалы на временно оккупированную часть Донбасса и это является одним из первых шагом к реинтеграции оккупированных территорий обратно в Украину!

Список библиографических ссылок

1. Методы, виды террористической деятельности и тенденции развития современного терроризма // Портал органов государственной власти Ярославской области : сайт. URL: https://www.yarregion.ru/Pages/terrorizm_vid.aspx (дата обращения: 27.09.2019).
2. Сергеева Ю. Вся статистика интернета на 2019 год – в мире и в России // WebCanape : сайт. 11.02.2019. URL: https://www.web-canape.ru/business/vsya-statistika-interneta-na-2019-god-v-mire-i-v-rossii/ (дата обращения: 29.09.2019)
3. Киберпространство и информационный терроризм // Наука и образование против террора : сайт. 11.05.2017. URL: http://scienceport.ru/

news/kiberprostranstvo-i-informatsionnyy-terrorizm/ (дата обращения: 29.09.2019).
4. Проблема терроризма в сети интернет и пути её решения // Молодежь и чистый Интернет : сайт. 07.09.2011. URL: http://www.honestnet.ru/terrorizm/problema-terrorizma-v-seti-internet-i-puti-eyo-resheniya.html (дата обращения: 02.10.2019).
5. Негодаев И. А. Информатизация культуры : монография. Ростов н/Д. : Книга, 2003. 320 с.
6. Сафарян А. В. СМИ как «четвертая власть» и институт социализации. *Власть.* 2008. № 5. С. 62–65.
7. Коновченко С. В. Общество – средства массовой информации – власть. Ростов н/Д. : СКАГС, 2001. 230 с.
8. Российские отряды установили «Грады» на кладбище и ведут огонь по аэропорту во время похорон // ЦЕНЗОР.НЕТ : сайт. 21.01.2015. URL: https://censor.net.ua/photo_news/320800/rossiyiskie_otryady_ustanovili_grady_na_kladbische_i_vedut_ogon_po_aeroportu_vo_vremya_pohoron_foto (дата обращения: 05.10.2019).
9. Состоялись похороны ребёнка, убитого украинскими карателями // SNR24 : сайт. 20.01.2015. URL: http://snr24.com/ekstrennye-novosti/5469-sostoyalis-pohorony-rebenka-ubitogo-ukrainskimi-karatelyami.html (дата обращения: 05.10.2019).
10. Мальчик в Славянске действительно был распят // ROISSYA24.NET : сайт. 24.10.2014. URL: https://roissya24.net/proud-it/boy-slavyansk-really-crucified/#comments (дата обращения: 05.10.2019).
11. Ложь: распятие в эфире Первого канала // StopFake : сайт. 15.07.2015. URL: https://www.stopfake.org/ru/lozh-raspyatie-v-efire-pervogo-kanala/ (дата обращения: 05.10.2019).

Получено 31.10.2019

УДК 341.1.8

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

Право на інтернет як базове право людини

Інтернет – найвеличніший інформаційний механізм створений людиною. Сьогодні він є дієвим інструментальним засобом, що дозволяє людям реалізовувати своє право на свободу думки та слова, вільне їх вираження. Водночас, мережа дарує нам можливість доступу до надбань усієї світової культури і загалом практично до будь-якої інформації. Інтернет поєднав усіх бажаючих, сформувавши єдину комунікаційну систему, а відтак став значним стрибком людства в інтерактивне середовище.

Враховуючи масштаб впливу Інтернет-мережі на життя кожної людини, логічно, що проблема правового врегулювання відносин між користувачами Інтернету та провайдерами є актуальною. Тому зараз кожна країна вживає усіх можливих заходів задля врегулювання цього питання у національному законодавстві: чи то шляхом обмеження доступу до Інтернету, чи навпаки нормативного закріплення права на доступ до світової мережі, як базового права людини.

Зважаючи на це, у резолюції Ради ООН з прав людини «Про сприяння, захист та здійснення прав людини в Інтернеті» від 5 липня 2012 року право на доступ до Інтернету визнається одним з невід'ємних прав людини [1]. Даний документ визнає глобальний характер Інтернету як світової мережі та пропагує спрощення державами доступу до неї. Зауважимо, що під правом доступу до мережі Інтернет у даному акті розуміється максимально вільне поширення інформації у мережі, що обмежується лише випадками, коли воно може призвести до порушення прав інших осіб (наприклад, кібернапад).

Інтернет дає можливість людям шукати, отримувати та передавати інформацію, миттєво обмінюватися ідеями незалежно від національних кордонів. Тобто, світова мережа суттєво розширює можливість людей користуватися своїм правом на інформацію, яке «сприяє» іншим еко-

номічним, культурним та соціальним правам, зокрема, право на освіту, право брати участь у культурному житті, а також громадянським та політичним правам – право на свободу мирних зборів та асоціацій. Отже, діючи як певний каталізатор для людей, що реалізують своє право на інформацію та право на свободу думки і слова, на вільне вираження своїх поглядів і переконань, Інтернет автоматично сприяє реалізації ряду інших прав людини.

Водночас, повна гарантія свободи доступу до інформації та свобода вираження поглядів у мережі Інтернет – це норма функціонування інформаційного простору, а будь-яке обмеження повинно розглядатися виключно як виняток.

Величезний потенціал Інтернет-простору корініться в його унікальних характеристиках, таких як, швидкість, всесвітнє охоплення та відносна анонімність. Водночас, ці відмінні риси Інтернету дозволяють людям поширювати інформацію у «реальному часі» та оперативно мобілізувати суспільне обговорення навколо конкретної теми, що, з одного боку дозволяє об'єднати громадськість у процесі вирішення найважливіших суспільних питань, а з іншого – подібна згуртованість породжує страх державних владних структур. Усе це призвело до збільшення обмежень в Інтернеті шляхом використання більш досконалих технологій для моніторингу та блокування контенту. Але подібні обмеження стосуються не тільки права на Інтернет, але й фундаментального права на свободу самовираження.

Ще Джон Стюарт Мілль казав, що коли ми щось називаємо правом людини, ми маємо на увазі, що людина може пред'явити суспільству справедливу вимогу захистити його в цьому праві [2]. Тому, законними видами інформації, яку слід обмежувати є дитяча порнографія (задля захисту дітей), наклеп (задля захисту прав та репутації інших людей від протиправних дій), пряме підбурення до скоєння геноциду (задля захисту прав інших), а також пропаганду національної, расової чи релігійної ненависті, що є відвертим розпалюванням дискримінації, ворожості чи насильства (задля захисту прав інших людей, зокрема, права на життя).

Зауважимо також, що далеко не всі країни виявили бажання підтримувати реалізацію права на доступ до Інтернету. Вони, у свою чергу, обмежують, контролюють, маніпулюють та піддають цензурі весь Інтернет-контент на своїй території без наявності будь-якої обґрунтованої юридичної підстави, або на основі законів, які суперечать розумінню

фундаментальних прав людини. Яскравим прикладом є Китайська Народна Республіка, державна влада якої тоталітарно контролює Інтернет-простір, шляхом фільтрації контенту за допомогою «Великого китайського фаєрвола» на основі «чорного списку» та ключових слів, а це прямо свідчить про наявність обмеження права на свободу слова у цій країні.

Натомість в Україні доступ до мережі Інтернет не є таким, який гарантується державою на рівні з іншими правами людини. Отже, вірогідними лишаються такі ситуації, коли доступ до Інтернету може бути обмежений. Водночас віднесення доступу до Інтернету до прав людини автоматично унеможливить такі обмеження.

З даного приводу зауважимо, що у Верховній Раді України уже зареєстровано законопроект «Про забезпечення права фізичної особи на доступ до Інтернету». Як зазначає ініціатор законопроекту – народний депутат О. Фельдман у пояснювальній записці до законопроекту – «Сьогодні Інтернет став ключовим засобом, завдяки якому люди можуть здійснювати своє право на свободу думок та їх вільне вираження, гарантоване Загальною декларацією прав людини та Міжнародним пактом про громадянські та політичні права. Рада з прав людини ООН підтвердила, що ті ж права, які людина має в оффлайновому середовищі, повинні також захищатися і в онлайновому середовищі, зокрема право на свободу вираження думок, незалежно від кордонів і для будь-яких вибраних людиною засобів масової інформації» [3].

Підсумовуючи можемо відзначити, що обмеження доступу до всесвітньої мережі Інтернет сьогодні переходить «із категорії недоцільного у категорію неприпустимого», оскільки запровадження такого механізму дозволить знехтувати правом на свободу слова, доступу до інформації тощо.

Україна, як повноправний член ООН, стоїть на позиції поступової імплементації даного права, оскільки права людини повинні захищатися однаковою мірою, як офлайн, так і онлайн, але при цьому саме на владу повинно бути покладене завдання встановлення оптимального балансу між інтересами користувачів та держави та захисту вразливих верст користувачів від небезпечного контенту.

Список бібліографічних посилань

1. Про сприяння, захист та здійснення прав людини в Інтернеті : резолюція Ради ООН з прав людини від 5 лип. 2012 р. URL: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session20/Pages/ResDecStat.aspx (дата звернення: 22.10.2019).
2. Міль Дж. Ст. Про свободу : есе / пер. з англ. Київ : Основи, 2001. 724 с.
3. Пояснювальна записка до проекту Закону України «Про внесення доповнень до Цивільного кодексу України (щодо гарантування права фізичної особи на доступ до Інтернету)». URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc34?id=&pf3511=55127&pf35401=342358 (дата звернення: 22.10.2019).

Одержано 01.11.2019

УДК 351.745.7

Анатолій Васильович Мовчан,
доктор юридичних наук, професор,
професор кафедри оперативно-розшукової діяльності
Львівського державного університету внутрішніх справ

Окремі аспекти протидії кіберзлочинності підрозділами кіберполіції Національної поліції України

Термін «кіберзлочинність» (cybercrime) часто вживається поряд з терміном комп'ютерна злочинність» (computer crime), причому нерідко ці поняття використовуються як синоніми. Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» кіберзлочин (комп'ютерний злочин) – це суспільно небезпечне винне діяння у кіберпросторі та / або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та / або яке визнано злочином міжнародними договорами України [1].

Згідно з даними офіційної статистики в Україні за 9 місяців 2019 р. зареєстровано 1796 кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж або мереж електрозв'язку, у тому числі:

- несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж або мереж електрозв'язку (ст. 361 КК України) – 1014;

- несанкціоновані дії з інформацією, яка обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362 КК України) – 576;

- створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 КК України) – 165;

- несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах

(комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України) – 33 [2].

Одним із суб'єктів протидії кіберзлочинності в Україні є підрозділи кіберполіції. Зокрема, основним завданням Департаменту кіберполіції Національної поліції України є участь у формуванні та забезпеченні реалізації державної політики щодо запобігання та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Наприклад, у вересні 2019 р. поліцейські Департаменту кіберполіції викрили хакера, який за час своєї злочинної діяльності отримав несанкціонований доступ до тисяч серверів постраждалих з більш ніж 100 країн світу. Отримані інструменти він використовував як для продажу даних, так і для отримання доступу до банківських аккаунтів і платіжних систем. Для залучення клієнтів 29-річний житель Харкова розміщував на спеціалізованих сайтах і форумах оголошення про продаж доступів до віддалених серверів. Для оплати таких послуг використовувалися електронні платіжні системи [3].

Також кіберполіцейські викрили злочинну групу з п'яти осіб, які протягом останніх двох років створювали і продавали в мережі шкідливі технічні засоби, призначені для несанкціонованого втручання в роботу систем постачання та обліку спожитої електроенергії. Надалі ці апаратні комплекси налаштовувалися і використовувалися для блокування роботи процесора електролічильника, у результаті чого енергопостачальні підприємства несли мільйонні збитки. Для збуту цих пристроїв організатор злочинної групи створив окремий інтернет-сайт. Залежно від виду електролічильника вартість кожного такого технічного засобу коливалася від 3 до 15 тисяч гривень. Таким чином зловмисники заробили понад мільйон гривень [4].

11 вересня 2019 р. в ході проведення в Києві форуму «Cellebrite User Forum Kyiv 2019» фахівці компанії Cellebrite і Лабораторії комп'ютерної криміналістики ЕПОС розповіли учасникам конференції про свої напрацювання протягом останнього року і поділилися кращими практиками останніх досягнень цифрової криміналістики. У сучасних умовах боротися з комп'ютерною злочинністю державі самостійно важко, адже технології розвиваються щохвилини, а злочинці постійно вдосконалюють свої схеми, щоб максимально приховати сліди. Нині

злочинці вже перестають користуватися аналоговими каналами зв'язку і класичними місцями для зберігання інформації. Все частіше вони використовують хмарні сервіси зберігання інформації і абузостійкі хостинги, які не контролюються з боку держави.

Тому для кіберполіції важливо використовувати сучасні високотехнологічні інструменти для отримання доказової бази. Завдяки співпраці з приватними організаціями кіберполіцейським вдається отримувати дані, які в подальшому використовуються в якості цифрових доказів. Крім того, за допомогою якісної аналітики Національна поліція отримує не тільки докази протиправної діяльності, а й виявляє нові злочини [5].

Список бібліографічних посилань

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.
2. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування // Генеральна прокуратура України : офіц. сайт. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113897&libid=100820&c=edit&_c=fo (дата звернення: 21.10.2019).
3. Кіберполіція викрила злочинну групу у створенні приладів для блокування роботи лічильників // Кіберполіція України : офіц. сайт. 04.10.2019. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-zlochynnu-grupu-u-stvorenni-pryladiv-dlya-blokuvannya-roboty-lichylnykiv-1345/ (дата звернення: 21.10.2019).
4. Кіберполіція викрила хакера у зламі більше двох тисяч комп'ютерів українців // Кіберполіція України : офіц. сайт. 04.10.2019. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-xakera-u-zlami-bilshe-dvox-tysyach-kompyuteriv-ukrayincziv-4967/ (дата звернення: 21.10.2019).
5. Сергій Демедюк: Для протидії сучасній злочинності правоохоронці потребують якісних інструментів реверсної інженерії // Кіберполіція України : офіц. сайт. 11.09.2019. URL: https://www.cyberpolice.gov.ua/news/sergij-demedyuk-dlya-protydiyi-suchasnij-zlochynnosti-pravooxoronczi-potrebuyut-yakisnyx-instrumentiv-reversnoyi-inzheneriyi-1575/ (дата звернення: 21.10.2019).

Одержано 22.10.2019

УДК 004.047

Юрій Миколайович Онищенко,
кандидат наук з державного управління, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Оксана Іванівна Шарабан,
головний судовий експерт сектору дактилоскопічних досліджень відділу криміналістичних видів досліджень Харківського науково-дослідного експертно-криміналістичного центру МВС України

Сучасні інструменти аналітичної роботи для підрозділів Національної поліції України

В умовах розповсюдження групової злочинності, що має пірамідальну ієрархічну структуру, вузькоспеціалізовані підрозділи, високий рівень оснащеності та конспірації, для проведення ефективного аналізу оперативної інформації та розвідувальних даних перспективним є використання багатофункціональних програмних засобів в діяльності Національної поліції України при розслідуванні злочинів. Розглянемо основні можливості пакетів IBM I2, що можуть бути застосовані для організації аналітичні роботи в оперативних та інформаційно-аналітичних підрозділах поліції.

I2 – це потужна аналітична база даних, яка дозволяє об'єднати інформацію з різних джерел на одній схемі. Інтеграційні рішення системи I2 уможливлюють об'єднання даних, забезпечують сумісність з реляційними системами управління базами даних (СУБД Oracle, Microsoft SQL server, Microsoft Access), а також та статистичними інструментами для аналізу.

IBM i2 Analyst's Notebook – візуальне аналітичне середовище, яке дозволяє максимально ефективно використовувати величезні обсяги інформації, накопичені державними службами та підприємствами. Завдяки інтуїтивно зрозумілому інтерфейсу з урахуванням контексту дозволяє аналітикам швидко зіставляти, аналізувати і наочно представляти дані з різних джерел, скорочуючи час на пошук важливої інформації в складних даних. IBM i2 Analyst's Notebook надає актуальні і дієві

аналітичні засоби, що допомагають виявляти, передбачати, запобігати і припиняти злочинну, терористичну і шахрайську діяльність.

IBM i2 iBase – це інтуїтивно зрозумілий аналітичний додаток баз даних, який дозволяє спільно працювати колективам аналітиків, збирати, контролювати і аналізувати дані з декількох джерел. Цей продукт дозволяє вирішити повсякденну проблему аналітиків, яка полягає у виявленні і розкритті особливостей взаємозв'язків, шаблонів і тенденцій в сучасних умовах, що характеризуються стрімким зростанням обсягів складних структурованих і неструктурованих даних.

IBM i2 iBridge – це розширене рішення для зв'язку та аналітичного пошуку, яке з'єднує користувачів IBM i2 Analyst's Notebook безпосередньо з базами даних підприємств, установ, організацій. Ефективні інструменти пошуку та виконання запитів повертають результати у вигляді готових до аналізу даних з візуалізацією зв'язків між записами для прискорення створення аналітичних даних.

I2 відображає взаємозв'язки між людьми, банківськими рахунками, організаціями, номерами телефонів, майном фірм та іншими речами. Подібний аналіз спрощує роботу з великими обсягами даних, автоматично створюючи діаграми зв'язків об'єктів. Діаграми, які дозволяють простежити послідовність і взаємозв'язок певних подій протягом конкретного проміжку часу, також дозволяють виявити і проаналізувати стійкі, повторювані в часі послідовності подій (телефонні розмови, банківські трансакції тощо).

За наявності необхідної кількості даних про злочинне угруповання та злочини, до яких воно має пряме чи опосередковане відношення, фахівці-аналітики, обробляючи дані оперативних зведень та інформацію з відкритих джерел за допомогою спеціалізованих програм (класу IBM I2), обробляючи та аналізуючи великі масиви даних, зможуть надавати ефективну допомогу для розкриття злочинів, що вчиняються за складними схемами.

Одержано 29.10.2019

УДК 343.1

Ірина Анатоліївна Осятинська,
вчитель інформатики Харківської спеціалізованої школи з поглибленим вивченням окремих предметів № 133 «Ліцей мистецтв»

Напрями роботи з потерпілими від злочинів, пов'язаних з торгівлею людьми

Під час розслідування злочинів, пов'язаних з торгівлею людьми, вітчизняні правоохоронні органи головну увагу зосереджують на особі злочинця та носіях доказової інформації. У той же час нерідко потерпіла особа залишається на одинці зі своїми проблемами та її роль зводиться лише до надання відповідних показів на досудовому слідстві та суді.

На теперішній час в Україні намагаються вирішити вказану проблему, зокрема шляхом надання офіційного статусу особи, яка постраждала від торгівлі людьми. Серед іншого було прийнято Закон України «Про протидії торгівлі людьми» від 20.09.2011, Постанови Кабінету Міністрів України від 23 травня 2012 р. № 417 та від 25 липня 2012 р. № 660, якими затверджено порядок встановлення статусу особи, яка постраждала від торгівлі людьми, та порядок виплати одноразової матеріальної допомоги особам, які постраждали від торгівлі людьми.

Статус особи, яка постраждала від торгівлі людьми, може бути наданий не лише особам, які проходять в якості потерпілих у кримінальному провадженні, і це певним чином додатково соціально убезпечує цю вразливу категорію громадян. У той же час статус постраждалої особи поширюється тільки на жертв торгівлі людьми, а не на жертв злочинів, пов'язаних з торгівлею людьми, що певним чином звужує захист громадян. Це пояснюється тим, що безпосередньо злочин торгівлі людьми (стаття 147 Кримінального кодексу України) вкрай важко довести, тому кваліфікація відповідних дій може бути здійсненна за іншими статтями Кримінального кодексу. Таким чином, особа, яка фактично постраждала від торгівлі людьми, може не одержати статусу постраждалої. Це стосується наприклад, дітей, яких залучили до створення дитячої порнографії, тощо.

На нашу думку, для покращення роботи з потерпілими від злочинів, пов'язаних з торгівлею людьми, під час розслідування слід використовувати підхід, орієнтований на приділення першочергової уваги проблемам потерпілої особи, зокрема, в частині надання їм тимчасового притулку у разі такої необхідності, медичної та правової допомоги, психологічної підтримки. У разі, якщо потерпіла особа не є громадянином України можливо слід розглянути питання про надання їй посвідки на проживання в обмін на дієве співробітництво зі слідством. Описанні питання мають вирішуватися державними органами у спрощеному порядку на підставі даних, одержаних від слідчих підрозділів. На етапі досудового розслідування також слід передбачити можливість надання такими потерпілими анонімних свідчень із приховуванням їх вигляду, зміною голосу та дотриманням інших вимог безпеки та конфіденційності свідків.

Одержано 29.10.2019

УДК 343.43

Каріна Володимирівна Печора,
курсантка 4 курсу навчально-наукового інституту № 1
Національної академії внутрішніх справ (м. Київ)

Нормативно-правові засади діяльності Національної поліції України у сфері протидії торгівлі людьми

Актуальність теми дослідження полягає в тому, що торгівля людьми, особливо жінками і дітьми – реальність нашого часу. Незважаючи на те, що рабство як таке скасовано понад 200 років тому, сучасність відродила до життя подібний з ним інститут. У всьому світі щорічно від 700000 до 4000000 чоловіків, жінок і дітей купуються, продаються, перевозяться і утримуються проти їх волі в умовах, подібних до рабства. Торгівля людьми, за оцінками експертів, вважається третьою за прибутковістю сферою діяльності організованої злочинності, особливо в частині її транснаціональної складової, поряд з торгівлею зброєю і наркотиками

Кримінальна відповідальність за торгівлю людьми передбачена ст. 149 Кримінального кодексу України, де кримінально караними визнаються як безпосередньо торгівля людьми, так і вербування, переміщення, переховування, передача або одержання людини, вчинені з метою експлуатації, з використанням примусу, викрадення, обману, шантажу, матеріальної чи іншої залежності потерпілого, його уразливого стану або підкупу третьої особи, яка контролює потерпілого, для отримання згоди на його експлуатацію [1].

Торгівля людьми є однією з найглобальніших проблем всього світу, і тому дуже важливими є діяльність представників влади, у формі складання та затвердження нормативних актів, які спрямовані на протидію даному явищу. Міжнародними нормативно-правовими документами, що регулюють реалізацію політики з питань протидії торгівлі людьми є Конвенція ООН про боротьбу з торгівлею людьми і з експлуатацією проституції третіми особами від 02.12.1949, Конвенція ООН про права дитини від 20.11.1989, Конвенція Ради Європи про заходи щодо протидії торгівлі людьми від 16.05.2005, Конвенція Ради Європи про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом,

та про фінансування тероризму від 16.05.2005, Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства від 25.10.2007, Протокол про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї, що доповнює Конвенцію ООН проти транснаціональної організованої злочинності від 15.11.2000, Рамкова Конвенція ООН проти організованої злочинності від 21.07.1997 та Факультативний протокол до Конвенції ООН про права дитини щодо торгівлі дітьми, дитячої проституції і дитячої порнографії від 01.01.2000.

В Україні нормативно-правовою базою у сфері протидії торгівлі людьми є Закон України «Про протидію торгівлі людьми» від 20.09.2011, Постанова Кабінету Міністрів України «Про Національного координатора у сфері протидії торгівлі людьми» від 18.01.2012 року № 29, Постанова Кабінету Міністрів України «Про затвердження Порядку встановлення статусу особи, яка постраждала від торгівлі людьми» від 23.05.2012 № 417.

Важливим аспектом боротьби з торгівлею людьми в Україні є допомога з боку ОБСЄ. План дій ОБСЄ з боротьби з торгівлею людьми є основою для діяльності ОБСЄ в наданні підтримки зусиллям держав-учасниць ОБСЄ по боротьбі з торгівлею людьми. Відносно дій на національному рівні в ньому містяться наступні три пункти з основними рекомендаціями:

- попередження, включаючи підвищення обізнаності та усунення корінних причин;

- переслідування, включаючи розслідування і співробітництво з міжнародними правоохоронними органами;

- захист прав жертв, включаючи надання допомоги та надання компенсації.

Міжнародна торгівля людьми залишається гострою соціальною проблемою багатьох країн світу. Україна є країною походження, транзиту і призначення в торгівлі чоловіками, жінками і дітьми. Зростає також проблема внутрішньої торгівлі людьми. Торгівля людьми є дуже прибутковим нелегальним бізнесом. Тому вербувальники придумують все нові і нові способи експлуатації людини і власного збагачення, наживи. У зв'язку зі складною економічною і соціальною ситуацією в Україні, українці все частіше шукають заробітку за кордоном (в Польщі, Росії, Чехії, Італії). Не дивлячись на незнання мови, законодавства, звичаїв і

правил офіційного працевлаштування в країні призначення, громадяни України з легкістю погоджуються на спокусливі пропозиції злочинців і несвідомо стають жертвами торгівлі людьми, «живим товаром». Гострою проблемою і важкої злочинною діяльністю торговців людьми, за останні роки, стало втягування громадян України до перевезення і розповсюдження наркотичних речовин на території іноземних держав: Російської Федерації, Таїланду»,– каже Ірина Бойко [2]. За даними Національної поліції України у 2018 році зареєстровано 346 фактів торгівлі людьми, з них 11 стосуються торгівлі дітьми. А за даними Міжнародної організації з міграції в Україні, з 2000 року 574 дитини постраждали від торгівлі людьми та отримали допомогу. Це свідчить, що статистична інформація відображає лише деякі випадки торгівлі дітьми і не дає можливості оцінити проблему торгівлі дітьми в Україні в цілому [2].

Проте Національна поліція старається активно протидіяти торгівлі людьми. Так, 12 травня 2019 року, за процесуального керівництва Ужгородської місцевої прокуратури працівники Відділу боротьби зі злочинами, пов'язаними з торгівлею людьми, ГУНП в Закарпатській області, спільно зі спецпідрозділом «КОРД» та прикордонниками на переході КПП «Малі Селменці» затримали громадян України та двох громадян Словаччини. Українці за допомогою іноземців намагалися переправити в країни Євросоюзу для сексуальної експлуатації двох громадянок, мешканок Закарпатської області. На даний час проводяться слідчі. У діях затриманих вбачаються ознаки кримінального правопорушення за ч. 2 ст. 149 Кримінального кодексу України [3].

Список бібліографічних посилань

1. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341 III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 149.
2. 30 липня – Всесвітній день боротьби з торгівлею людьми // ZIK : сайт. URL: https://www.google.com/amp/s/zik.ua/ru/amp/news/2019/07/30/30_yyulya__vsemyrniy_den_borbi_s_torgovley_lyudmy_1615907 (дата звернення: 10.10.2019).
3. Закарпатські поліцейські попередили спробу торгівлі людьми. URL: https://zak.depo.ua/ukr/zak/zakarpatski-politseyski-poperedili-sprobu-torgivli-lyudmi-20190513960932 (дата звернення: 10.10.2019).

Одержано 11.10.2019

УДК 340:12:004.77

Наталія Олегівна Расторгуєва,
курсантка 3 курсу факультету № 1
Харківського національного університету внутрішніх справ

Юлія Олександрівна Загуменна,
кандидат юридичних наук, доцент, професор
кафедри теорії та історії держави і права факультету № 1
Харківського національного університету внутрішніх справ

Діджиталізація сучасного суспільства

Одним з найбільш складних, комплексних та малодосліджених феноменів XXI століття з яким ми стикаємося сьогодні, є діджиталізація сучасного суспільства або активне використання цифрових технологій в повсякденності. Багато видатних вчених очікували, що майбутнє буде насичено цифровими технологіями і людина не буде мислити себе без них [1, с. 7].

Поняття «діджиталізація» (англ. «Didgitalization», дослівно перекладається як «digital» – «цифра» + суфікс «-ization», що має на увазі процес) можна підібрати синонім «оцифровування», переклад аналогових даних в цифровий вигляд. Оцифрування стало можливим завдяки розробці і повсюдного поширення цифрових технологій і подальшого їх повсюдного використання для обробки, зберігання і трансляції інформації [2].

Але неможливо обмежуватися тільки таким визначенням, адже явище «діджиталізації» стосується не тільки цифрових пристроїв, але людей, активно залучених у взаємодію з цифровими технологіями. Причому це дійсно взаємодія, тобто контакт, спрямований на взаємне перетворення його учасників. Це перетворення дозволяє цифровим технологіям і людям, залученим в їх експлуатацію безпосередньо впливати один на одного і взаємопроникати один в одного.

Діджиталізація – це, перш за все, явище, що несе процесуальний характер. Ми можемо говорити про діджиталізацію суспільства як про послідовну трансформацію соціокультурного коду, об'єднаних загальним вектором розвитку. Сьогодні експоненціальне зростання цифрових технологій тягне за собою і зростання кількості та якості інтеграційних змін в системі комунікації суспільства. Поява таких технічних засобів, як

Інтернет і мобільні пристрої, що дозволяють суспільству знаходитися в постійній комунікації один з одним. Це і стало першою сходинкою діджиталізації і відповідно, провісником глобальних модифікацій соціальних інститутів та вектором розвитку суспільства в цілому.

25 квітня 2018 року Європейська Комісія опублікувала два проекти директив, спрямованих на діджиталізацію правового регулювання:

1) процесів, пов'язаних з існуванням компаній (реєстрація, розкриття інформації, припинення компанії)

2) будь-яких транскордонних трансформацій компаній (злиття, поглинання, перетворення, відкриття/закриття відокремлених підрозділів) [3].

Успішне запровадження діджиталізації вимагає дотримання певних вимог, а саме:

1. Зміцнення довіри громадян до потреби інформаційно трансформувати суспільство;

2. Надійний захист конфіденційності персональної інформації;

3. Недоторканність особистого життя та прав користувачів інформаційно-комунікативних технологій.

Діджиталізація (цифрові технології) приходить на зміну старим засобам електронної комунікації – телефону, факсу, телеграфу. Нові цифрові технології дозволяють створювати і поширювати величезні обсяги інформації майже необмеженому колу осіб – швидко, якісно, без будь-яких істотних витрат.

У травні 2015 року Європейська комісія оприлюднила Стратегію цифрового єдиного ринку. Мета стратегії – створити відкритий взаємопов'язаний цифровий єдиний простір (ринок) та збільшити позитивний вплив цифрової трансформації на суспільство та бізнес[4].

Розглянувши явище діджиталізації суспільства можна сказати, що епоха цифрових технологій невпинно входить в життя громадян XXI століття. По-перше, це чіткий тренд неухильного і безперешкодного розвитку технологій та розширення сфери застосування технологічних новинок. По-друге, відсутність географічно обумовлених бар'єрів для поширення цифрових технологій і знань, зростаюча доступність інформації для всіх представників суспільства.

Підсумовуючи, хотілося б зазначити, що діджиталізація суспільства сприймається багатьма інтуїтивно, як само собою зрозуміле явище.

Головним чином тому, що люди звикли до цифрових пристроїв і здійснення будь-якої діяльності в рамках сучасного суспільства імпліцитно передбачає звернення до цих пристроїв.

Список бібліографічних посилань

1. Кастельс М. Информационная эпоха. Экономика, общество и культура / пер. с англ. ; под науч. ред. О. И. Шкаратана ; Гос. ун-т. Высш. шк. экономики. М., 2000. 606 с.
2. Лиотар Ж. Ф. Состояние индустрии / пер. с франц. Н. А. Шматко. М. : Ин-т эксперимент. соц. ; СПб. : Алетейя, 2007. 160 с.
3. Кібенко О. Р. Діджиталізація як нова ера розвитку корпоративного права // Судебно-юридическая газета : сайт. 16.07.2019. URL: https://sud.ua/ru/news/blog/145948-didzhitalizatsiya-yak-nova-era-rozvitku-korporativnogo-prava (дата звернення: 10.10.2019).
4. A Digital Single Market Strategy for Europe. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN (дата звернення: 10.10.2019).

Одержано 16.10.2019

УДК 338.64

Андрій Володимирович Серватовський,
слухач магістратури факультету № 1
Харківського національного університету внутрішніх справ

Юрій Миколайович Онищенко,
кандидат наук з державного управління, доцент, доцент кафедри
інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ

Легалізація (відмивання) доходів, одержаних злочинним шляхом, за допомогою криптовалют

За останні роки криптовалюта викликала до себе інтерес не тільки людей, а цілих держав, які почали активно її впроваджувати в свій повсякденний обіг. Криптовалюти є особливим видом електронних (або цифрових) грошей, які мають власну децентралізовану платіжну систему та функціонують зазвичай на основі блокчейн-технології (blockchain). Суть блокчейну полягає у тому, що інформація, закодована в ньому, зберігається на різних, незалежних один від одного комп'ютерах, тобто для неї відсутній єдиний сервер.

Під час переказу криптовалюти між відправником та одержувачем створюється однорангова мережа, яка може не мати посередників (без згоди самих користувачів). Саме тому криптовалюти і стали стрімко розвиватися, оскільки дана концепція абсолютно нова для ринку: криптовалютні операції неможливо ні контролювати, ні відслідковувати – вони здійснюються виключно між двома користувачами. Слід сказати, що ми формуємо попит на ринку, під впливом чого змінюється ціна на цікавий для нас товар. Під впливом ажіотажу курс провідної криптовалюти стрімко зростає, після чого деякі галузі економіки збільшують своє часткове співвідношення на фінансовому ринку. Ніхто не може відчути, контролювати, повністю оволодіти і зупинити її розвиток.

Дані новітні технології, які стрімко зростають, не змогли обійти увагою й особи, які займаються незаконною діяльністю, оперуючи при цьому великими сумами грошей (наркобізнес, торгівля зброєю, тероризм тощо). Звісно в подальшому виникає питання, щодо легалізації

(відмивання) даних коштів. Швидкі і анонімні трансакції, які пропонують криптовалюти, не могли не зацікавити зловмисників. Тільки за минулий і поточний рік через криптовалюти «відмили» понад 1,2 млрд доларів. Даним процесом зацікавились та вивчали декілька великих Американських компаній, які спеціалізуються на кібербезпеці й встановили основні етапи даної процедури, хоча й теоретично сам процес доволі простий.

Першим етапом є нашарування. У традиційній фінансовій сфері він включає покупку дорогих активів за «брудні» гроші. Наприклад, нерухомості. Далі цей актив перепродається кілька разів, що ускладнює визначення початкового покупця. У світі криптовалют цей етап включає придбання криптовалюти. На наступному етапі за допомогою різних бірж і спеціальних сервісів-міксерів, початкові монети роздрібнюють і конвертуються в інші криптовалюти. Гроші можуть пройти сотні адрес, що ускладнює відстеження початкового власника. Сервісів-міксерів дуже багато. Вони у вільному доступі і ніхто не заважає їм працювати. Принцип роботи подібних сервісів простий. Вони беруть криптовалюту у різних клієнтів, перемішують її, у кінцевому результаті виходить «мікс», який не дозволяє відстежити власника грошей.

Ще один популярний спосіб легалізувати «брудні» гроші – провести фейковий ICO. Мало того, що шахраї зможуть зібрати додаткові гроші від довірливих вкладників, це дозволить «відбілити» кошти, отримані незаконним шляхом. Для цього достатньо проінвестувати нелегальними грошима свій же проект.

Способів легалізації грошей дуже багато, але процес боротьби з подібним видом злочину є досить складним, оскільки вимагає значної кількості спеціалістів у цій галузі, а також багато сил та засобів правоохоронних органів. Подібні валютні трансакції відбуваються по всьому світу, отже, є реальна необхідність у тісній міжнародній співпраці для ефективної боротьби з подібним видом злочину.

Одержано 29.10.2019

УДК 342.9

Валерій Васильович Сокуренко,
доктор юридичних наук, професор, заслужений юрист України,
начальник ГУНП в Харківській області

Комплексний підхід до вирішення питання кібербезпеки України

Питання про те, чи існує взагалі якась система кібербезпеки в Україні, є базовим для вирішення завдань кібербезпеки в державі в цілому. За всі роки незалежності до цього питання, що є критично важливим, не було системного підходу. Створювалися нормативна база та система захисту, але ключових документів, на основі яких можна було б вибудовувати систему кібербезпеки, не існувало. Навіть у Законі України «Про основи національної безпеки України», який діяв з 2003 по 2018 роки, були лише окреслені загрози в інформаційній сфері. У січні 2016 року РНБО нарешті ухвалила Стратегію кібербезпеки України. Це дало поштовх для вирішення інших завдань, оскільки Стратегія визначила ланцюг напрямів, за якими потрібно далі вибудовувати національну систему кібербезпеки.

Що ж являє собою національна система кібербезпеки? Перш за все, це суб'єкти, визначені Стратегією, зокрема Міністерство оборони, Державна служба спеціального зв'язку та захисту інформації, Служба безпеки, Міністерство внутрішніх справ, Національна поліція України, тобто органи, які забезпечують кібербезпеку в державі. Координатором цієї системи, згідно зі Стратегією, є РНБО. Для функціонування в постійному режимі було створено Національний координаційний центр кібербезпеки, який очолює секретар РНБО. У Центрі постійно проводяться засідання й ухвалюються рішення, які стають основою для рішень РНБО та діяльності всіх органів влади.

У держави є інформаційні ресурси та критична інфраструктура. Для державних інформаційних ресурсів легше вибудовувати систему кібербезпеки на основі чинної законодавчої бази, однак багато об'єктів критичної інфраструктури перебувають у приватній власності, тому захистити обчислювальні ресурси таких об'єктів є великою проблемою. З метою її вирішення сьогодні створюється перелік таких об'єктів для їх подальшого обліку та забезпечення на них кібербезпеки.

Побудову ефективно функціонуючої системи кіберзахисту бажано розділити принаймні на кілька частин. Є державні інформаційні ресурси, якими займаються окремі спеціальні державні організації, – це перший полюс. Другим є приватні системи окремих осіб, дані яких є об'єктом атак окремих зловмисників. Цілеспрямованих атак на такі об'єкти ніхто здійснювати не буде. Посередині залишився ще великий пласт комерційних підприємств із різною формою власності.

Позитивним є той факт, що РНБО почала приділяти серйозну увагу безпеці об'єктів критичної інфраструктури, тобто проблема почала вирішуватися. Водночас сегмент комерційних підприємств становить основу економіки України, але до сьогодні проблемою забезпечення їх кібербезпеки ніхто в державі не займався. Тому вбачається доцільним створити певне співтовариство представників приватного сектора, яке займатиметься створенням штабів, підготовкою відповідного персоналу компаній, виявленням загроз тощо. За ініціативи бізнесу повинні бути створені центри обміну інформацією, які співпрацюватимуть один з одним та з усіма державними органами щодо створення метрики загроз, методології захисту інформації аж до інструкцій з алгоритмом дій у разі виявлення кіберінциденту. Для тих компаній, які не мають ІТ-відділів або відповідних фахівців, потрібно створити «гарячий резерв», фахівці якого могли б бути тимчасово найняті для відновлення ІТ-систем.

Для забезпечення ефективного кіберзахисту необхідно провести аналіз характеристик сучасної кіберзброї, яку можна порівняти із засобами масового ураження, однак стосовно комп'ютерів та інформаційних систем. Кіберзброя може одночасно вивести з ладу велику кількість об'єктів критичної інфраструктури як на рівні однієї держави, так і на рівні об'єднання кількох держав. Кіберпростір – це середовище взаємодії різноманітних нестандартизованих уразливих інформаційних систем, в яких використовуються чутливі до злому дані та комунікаційні можливості. Кіберзброя націлюється як на окремі сегменти економіки та локальні компанії, так і на окремих громадян. Кібератаки дуже ретельно готуються. У 2011 році дослідники кіберзагроз, вихідці зі спецслужб США, розробили методологію «kill chain», яка спочатку використовувалася у військовій концепції, що стосується структури атаки. Вона містить низку послідовних дій або ланцюжок фаз, а порушення будь-якої з них може перервати весь процес. Більшість кібератак включають декілька цих фаз. Сучасні атаки готуються таким чином, щоб вони не могли бути

виявлені й ідентифіковані, а їх дія була максимально тривалою для досягнення поставлених цілей.

Уразливим місцем при подібних кібератаках є відсутність окремих департаментів кібербезпеки. Зазвичай цим опікуються ІТ-відділи, але в них, як правило, немає кризових регламентів, вони не знають, як діяти в таких ситуаціях. А там, де є навички швидкого реагування, часто немає повноважень.

Що потрібно? Перше, це система CERT. При цьому необхідні спеціалізовані CERT. Наприклад, у США є загальний CERT, який займається загальними питаннями кібербезпеки, є ICS (Industrial Control System) CERT, який займається об'єктами критичної інфраструктури, і є NERC – некомерційна організація, що займається питаннями безпеки в енергетиці. Необхідно налагодити обмін інформацією. Компанії зациклені здебільшого на відбитті атак і ліквідації їх наслідків. В Європі та США є організації, які випускають документи щодо запобігання атак, які містять готові «рецепти».

У світі функціонує приблизно 300 таких центрів. В Україні також є команда CERT-UA, яка працює під егідою Держспецзв'язку. Після атаки на фінансовий сектор у січні 2016 року було поставлено завдання щодо формування і затвердження протоколу спільних дій під час кіберінцидентів. Йдеться про вдосконалення нормативної бази, наділення повноваженнями суб'єктів забезпечення кібербезпеки, щоб вони могли швидко реагувати і взаємодіяти для протидії атакам.

Важливу роль у забезпеченні кібербезпеки України відіграють підрозділи МВС, які керуються у своїй діяльності положеннями Концепції Програми інформатизації системи Міністерства внутрішніх справ України на 2018–2020 роки. Основними завданнями, що стоять перед органами Національної поліції України, є захист інформації, що обробляється в інформаційно-телекомунікаційних системах, та контрольована на всіх етапах обробка службової інформації в ЄІС МВС.

Отже, для вирішення зазначених проблем в Україні буде впроваджено дієву систему захисту інформації на всіх етапах функціонування ІТ-інфраструктури, контрольовану технологію обробки службової інформації, захист інформаційних ресурсів під час інтеграції з автоматизованими системами інших державних органів та установ, що дозволить істотно покращити кіберзахист інформаційного простору держави.

Одержано 06.11.2019

УДК 004.946.5.056

Анастасія Миколаївна Стець,
студентка 2 курсу юридичного факультету
Тернопільського національного економічного університету

Онлайн-шахрайство та його небезпека

Кіберзлочинність – це саме та сфера злочинів, яка набирає обертів все швидше і швидше. Технології розвиваються, наука йде вперед, людство не стоїть на місці. Але з огляду на сьогодення, такий стрімкий розвиток має свої ж недоліки. Небезпека в Інтернеті- це не новизна навіть для наймолодших українців. Як вберегтися від рук злочинців та як не попастися на гачок? Саме про це ми поговоримо.

Отже, кіберзлочинністю (інформаційним злочином) є навмисні дії, спрямовані на розкрадання або руйнування інформації в інформаційних системах і мережах, які виходять з корисливих або хуліганських спонукань [1]. Важливим є відмітити, те, що Кримінальний кодекс України (далі- ККУ) визначає покарання за інформаційні злочини, а саме розділ 16 [3]. Найпоширенішими видами таких злочинів є : кардинг, фішинг, вішинг, піратство, кард-шарінг, мальваре, рефайлінг та онлайн-шахрайство [4].

Онлайн- шахрайство давним-давно відоме всім, і багато співгромадян попадалося на гачок до аферистів. Здавалося б, як можна сидячи вдома перед монітором потрапити в руки злочинців. Я скажу вам більше – Ви можете потрапити на їх гачок, не підозрюючи нічого – онлайн-шахраї діють дуже обачно, але чітко і точно. Найпоширенішою аферою в онлайн-шахрайстві є дії, пов'язані з інтернет-магазинами та сайтами оголошень. Отже, розглянемо найпоширеніші схеми, за якими Вас можуть обдурити:

1. Кожна жінка мріє виглядати привабливо, але не всі мають змогу купувати одяг в брендових магазинах, тому на допомогу приходять інтернет-магазини з дешевим товаром. Але де є можливість зекономити – є ризик бути ошуканим. Тому, вибираючи інтернет-магазин, потрібно бути впевненим, що це добросовісні продавці. А щоб захистити себе використовуйте послугу післяплати.

2. Не менш поширеною є проблема шахрайства на платформі OLX. Я впевнена на 100 %, що всі українці, хоча б раз у житті були ошукані продавцями цього сайту. Спочатку недобросовісний продавець викликає неабияку довіру, тим самим беручи на гачок покупця. Покупець в свою чергу стає зацікавленим, бо ціна приваблює, та ще й продавець ввічливий. Покупець перекидає гроші на банківську карточку, і в результаті – ні товару, ні грошей. Але існує вихід з ситуації. Розробники OLX створили так звану функцію «OLX доставка», яка полягає в наступному: продавець зможе отримати свої кошти тільки тоді, коли покупець отримає товар. На мою думку, хороша та безпечна функція.

3. Все більше набирає оборотів кіберзлочинність на сайті знайомств. До прикладу всім нам відомий Tinder, який створився з метою пошуку другої половинки, але шахраї мають на меті вимивання коштів чи даних банківської карточки. Для такого виду шахрайства в Інтернеті зловмисники вдаються до різних методів та хитрощів. Наприклад: емоційне маніпулювання, кіберзлочинець просить відправити інтимне фото або відео, а потім шляхом шантажу, вимагає гроші.

4. Не менш популярним є створення сторінок в Instagram псевдо волонтерами, які ніби то організовують збір коштів на лікування хворої дитини. Таких випадків сотні, і насправді, люди «сідають на гачок» злочинця, і відправляють на банківську карту волонтера шалені суми. Поки що така проблема немає вирішення, хоча можна поскаржитись на сторінку користувача, і його буде заблоковано. Тим самим цей злочин можна буде припинити.

5. Ще одна з популярних схем- допомога другові. Реалізовується через різні соцмережі, месенджери та електронні пошти. Суть «допомоги» полягає в наступному- так званий друг пише Вам, що він потрапив в неприємну ситуацію, і йому потрібна термінова допомога та просить грошової допомоги у Вас. Цим самим зловмисник хоче ввести Вас у стресову ситуацію, і щоб Ви не обдумуючи допомоги йому. Також в Україні існує старий метод, який «віджив своє». Зловмисники телефонують серед ночі, переважно до людей похилого віку, і розповідають, що їхнього сина/дочку збила машина, і необхідно терміново переслати гроші, щоб загладити питання з поліцією.

Отже, у висновок хочу сказати, що злочинність в Інтернеті є дуже небезпечною. В 2017 році було зафіксовано 1795 справ, в 2018 – 1023, за останні півроку – 1005. На даний момент в судовому реєстрі є 1500

справ [2]. Як вберегтися від кіберзлочинів запитаєте Ви? Банальні поради: не надавати нікому персональні дані, паролі і коди-підтвердження з СМС для операцій з картками, не довіряти повідомленням про виграші в лотереях, перевіряти інформацію за офіційним номером банку, не скачувати в інтернеті сумнівні файли, користуватись ліцензійним програмним забезпеченням тощо. Тому, будьте обережні, бережіть свої гроші та гаманці від обману.

Список бібліографічних посилань

1. Інформаційні злочини // Вікіпедія : віл. енцикл. URL: https://uk.wikipedia.org/wiki/Інформаційні_злочини (дата звернення: 21.10.2019).
2. Кількість кіберзлочинів в Україні зросла вдвічі за останні п'ять років – Opendatabot // Mind : сайт. 21.10.2019. URL: https://mind.ua/news/20203511-kilkist-kiberzlochiniv-v-ukrayini-zrosla-vdvichi-za-ostanni-p-yat-rokiv-opendatabot (дата звернення: 21.10.2019).
3. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. *Офіційний вісник України*. 2001. № 21. Ст. 264.
4. Голуб А. Кіберзлочинність у всіх своїх проявах: види, наслідки та способи боротьби // Ресурсний центр гурт : сайт. 03.10.2016. URL: https://www.gurt.org.ua/articles/34602/ (дата звернення: 21.10.2019).

Одержано 01.11.2019

УДК 343.9:004.738.5(075.8)

Володимир Михайлович Струков,
кандидат технічних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Дмитро Юрійович Узлов,
кандидат технічних наук, начальник управління інформаційно-аналітичної підтримки ГУНП в Харківській області

Аділь Рза Огли Пірієв,
генеральний директор компанії «Vega-Plus» (Азербайджан, Баку)

Сучасні високотехнологічні тренди у кримінальному світі

Процес стрімкого переходу більшої частини відносин матеріального світу в віртуальну сферу супроводжується бурхливим розвитком як легальної складової ІТ-сфери так і нелегальної. Причому спостерігається певна паралельність (дзеркальність) цих процесів. Відмітимо дві характерні особливості. Перша полягає в тому, що стрімко зростає число доступних через Мережу «некваліфікованих користувачів», в першу чергу, внаслідок всеосяжного поширення смартфонів. По-друге, стрімко розвивається і розгалужується високотехнологічна і високопрофесійна частина ІТ-сфери. Причому рівень і темпи розвитку нелегальної частини цього напрямку не відстає від легальної. Є дані, що вже в даний час всередині корпоративних мереж лідерів американського хайтека і біотехнологій діють багатоцільові і багатофункціональні хакерські програмні модулі, побудовані на основі самовдосконалючихся програм.

Правоохоронці по всьому світу всерйоз готуються до появи підпільних синдикатів, що спеціалізуються на замовних високотехнологічних вбивствах і терактах, замаскованих під технічні інциденти різного роду. Беручи до уваги обсяг ринку замовних вбивств в Сполучених Штатах, що становить близько 2 млрд дол. на рік, а також зростаючу активність терористичних угруповань, очікується поява таких мережних синдикатів протягом найближчих двох років.

У 2014 р. в Мексиці в одному з віддалених районів столиці країни завдяки успішним діям агентурної розвідки був розкритий завод по збірці дронів різних конструкцій, що належить одному з наркосиндикатів. Цей завод виробляв транспортні дрони і готувався налагодити виробництво бойових дронів прикриття. Ці дрони повинні супроводжувати транспортні дрони і виводити з ладу поліцейські автомобілі, оснащені радарами повітряного спостереження[1].

За інформацією російських спецслужб в штабі ІГІЛ створено підрозділ високотехнологічних терактів. Бойовики роблять ставку на малі керовані літальні системи: дрони з саморобними бомбами, які планується використовувати для терактів в країнах Європи.

Зараз ринок високотехнологічних інструментів насичений сучасними ефективними рішеннями, причому вартість компонентів, що включають елементи складних інтелектуальних і конструктивних рішень, стрімко здешевлюється, що робить їх доступними не тільки великим потужним структурам, а й невеликим групам і навіть окремим фізичним особам. Так, наприклад, на сайті китайської кампанії ali baba вічко для дверей, яке укомплектоване наукоємною технологією 3D-розпізнавання обличчя, коштує лише 120 дол. США.

В результаті стрімкого розвитку біотехнологій та генної інженерії останні роки склалася парадоксальна ситуація: «за оцінками експертів, лабораторія з виробництва біологічної зброї в сучасних умовах разом з усім обладнанням може коштувати в межах від декількох десятків до декількох сотень тисяч доларів США, а в якості біологічної зброї можуть бути використані і ті патогени, які конвенціонально не заборонені для застосування в дослідницьких цілях, отримання діагностичний систем, вакцин та інших медичних препаратів. Найбільш значущими загрозами біотероризму є різке збільшення числа фахівців з біотехнологій, доступність інформації за рецептурами біологічних та бактеріологічних препаратів, а також можливість легендування окремих актів біотероризму під прояви природних епідемій і інфекцій.

В кінці 2005 р. генетик Р. Брент з Каліфорнійського інституту молекулярних наук (Molecular Sciences Institute – MSI) провів експеримент, який доводить, що сьогодні технології в генній інженерії досягли вже такого рівня, коли один тлумачний лаборант з невеликим обсягом «правильних» ресурсів може виготовити біологічну зброю зі згубною міццю, яка не поступається атомній бомбі.

Американський вчений Р. Карлсон, фізик і біолог, який працював деякий час з Брентом в MSI, прогнозує, що приблизно протягом наступного десятиліття створення біологічної зброї з нуля стане настільки ж легким і дешевим, як побудова сайту.»[1].

Яскравою ілюстрацією такого становища є наступний випадок[1].

«У червні 2006 року співробітники британської газети The Guardian з'ясували, що створити біологічну зброю сьогодні може буквально будь-який зацікавлений в цьому житель Сполученого Королівства. Увагу журналістів привернув сайт компанії VN Bio Ltd, яка здійснювала постачання обладнання та витратні матеріали для біологічних лабораторій. В одному з каталогів біосировини були знайдені вельми дивні «товари» – на продаж виставили фрагменти ДНК смертельно небезпечних для людини вірусів віспи та іспанського грипу. Для оформлення замовлення на ДНК віспи знадобилося лише надати адресу, номер мобільного телефону та адресу електронної почти – вже через три години до редакції The Guardian подзвонив кур'єр і повідомив, що замовлення доставлено. Ніяких перевірок того, кому відправляється потенційно небезпечний вантаж, проведено не було – отримувачем міг би виявитися як законослухняний вчений, так і можливий терорист».

«Справжнім кошмаром для розвідувальних і правоохоронних структур усіх країн світу є бойові роботи, оснащені біологічною і хімічною зброєю. Щоб створити бойового робота, який використовує біологічну зброю, досить використати розроблені в даний час дрони сільськогосподарського призначення, заповнивши відповідні їх ємності не добривами, а бактеріями, вірусами або хімічними сполуками. Вартість сільськогосподарського дрона з дальністю польоту до 150 км і ємністю завантаження до 50 л становить лише 6 тис. дол. США, а ємністю до 200 л – менше 9 тис. дол. Купівля такого дрона доступна не тільки терористичній мережі, а й окремій групі фанатиків і екстремістів. «

Якщо брати до уваги наступні очевидні факти: 1) деякі терористичні організації (ТО) та організовані злочинні групи (ОЗГ) мають бюджет, більший ніж в деяких країнах; і 2) керівники ТО та ОЗГ є люди, як правило, не обділені розумом, і дуже прагматичні, а також деякі події останніх років, то можна дійти до простого логічного висновку – якщо правоохоронні структури будь-якої держави будуть «пасти задніх» у технологічних рішеннях, то безпека громадян, бізнесу і держави в цілому в цих країнах буде знаходитися під великою загрозою.

Так, наприклад, навіть керівники ФБР вважають, зокрема, що Америка сьогодні не готова до відсічі хакерським угрупованням, що націлені на інтелектуальну власність, що належить корпораціям, федеральному уряду і університетам [1].

Список бібліографічних посилань

1. Овчинский В. С. Криминология цифрового мира : учеб. М. : Норма ; Инфра-М, 2018. 352 с.
2. Gartner: Топ-10 стратегических трендов развития технологий в 2019 году // Київський міжнародний економічний форум : сайт. 26.10.2018. URL: https://ain.ua/2018/10/26/gartner-top-10-trendov-razvitiya-texnologij/ (дата звернення: 27.10.2019).

Одержано 29.10.2019

УДК 34:004-049(477)

Маріям Рзаївна Чалабієва,
аспірант Харківського національного університету внутрішніх справ

Дезінформація в електронних засобах масової інформації

Пропаганда, дезінформація, кібератаки – нові загрози інформаційно-цифрового простору України. Країна наразі знаходиться у епіцентрі російсько-української інформаційної війни, тому як ніколи потребує рішучих кроків державної влади на шляху до побудови міцної системи кіберзахисту.

Дезінформація у електронних засобах масової інформації є одним з найбільш дієвих прийомів впливу на широкі верстви населення у політичній, економічній, соціальній та інших сферах діяльності людини. Подібний рівень дієвості провокує високу популярність дезінформації у процесі діяльності державних/політичних суб'єктів, спецслужб; також вона поширена у злочинному середовищі.

Водночас, крадіжка даних, злом індивідуальних чи робочих аккаунтів є допоміжними засобами у процесі дезінформації у мас-медіа. Оприлюднене особисте листування чи інші викрадені дані можуть бути використані для шантажу чи посилення громадського напруження.

Зі свого боку, засоби масової інформації повинні власноруч виявляти дезінформацію у інформаційному потоці, блокувати пропагандистський російський контент, нести відповідальність за викладений матеріал на своїх медіа-платформах. Мас-медіа слід видаляти фейкові та автоматизовані акаунти (боти) задля попередження поширення свідомо неправдивої інформації, яка створена з метою введення в оману населення.

Крім того, соціальні мережі, як особливий вид електронних засобів масової інформації, мусять сформувати алгоритм виявлення реклами, що популяризує викривлену та неправдиву інформацію, яка спотворена умисно з метою провокування негативних суспільних настроїв.

Задля забезпечення цілковитої модерації контенту, засоби масової інформації можуть залучати до процесу пересічних громадян, а не покладатися виключно на електронні алгоритми. Так, штучний інтелект

(machine learning) допомагає виявити терористичний контент, але його можливості мають межі (наприклад, коли екстремістські ідеї у потоці інформації є очевидними виключно для людини). Ми пропонуємо сформувати спеціальні редакційні підрозділи, які будуть створені виключно задля фільтрації анонімного контенту, поширюваного на електронних медіа-платформах. Водночас, рекомендуємо приватним електронним засобам масової інформації особисто досліджувати причину привабливості вірусної інформації та пропонувати на противагу правдивий контент.

В умовах інформаційного суспільства дезінформація у мас-медіа, як спосіб впливу на суспільство, є специфічним проявом кібератаки, що направлена на людей задля формування у них хибного уявлення про події чи явища, провокування до прийняття певних рішень, які вигідні об'єкту впливу. Пріоритетним каналом поширення дезінформації все частіше виступають саме електронні засоби масової інформації.

Все це вимагає удосконалення нормативно-правового регулювання інформаційної діяльності в Україні з метою забезпечення безпеки кібернетичного простору.

Ми розуміємо, що Україна наразі знаходиться в складному становищі та продовжує бути жертвою дезінформаційних атак у електронних засобах масової інформації.

Природно, що країна буде ще не раз зіштовхуватися з різноманітними формами просування фальшивої інформації з боку Російської Федерації, оскільки глобалізаційні процеси невпинно тягнуть за собою розвиток новітніх технологій, а отже й появу нових електронних медіа-майданчиків.

Враховуючи, що Україна не єдина країна, яка потерпає від дезінформаціних атак у мас-медіа, слід надалі переймати міжнародний досвід боротьби з подібними формами кіберзагроз, популяризувати співпрацю громадськості з державною владою.

Одержано 01.11.2019

УДК [343.575:004.77](477)

Тетяна Анатоліївна Шевчук,
курсантка 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

Розповсюдження наркотичних засобів, психотропних речовин або їх аналогів через мережу інтернет

На сьогоднішній день проблема розповсюдження наркотичних засобів через мережу інтернет набула досить високої актуальності. Дана проблема має не лише регіональний характер, а й міжнародний. Сьогодні країни всього світу гостро відчувають проблему незаконного обігу наркотичних речовин та ведуть активну боротьбу з нею. За останній час світовий ринок наркотичних речовин дуже сильно змінився, сьогодні основною ареною для розповсюдження наркотиків є Інтернет – «безконтактний» засіб збуту, в якому наркоторговці можуть співпрацювати роками і при цьому не втрачати свою анонімність.

Зважаючи на те, що в Інтернеті більшість користувачів є молодими людьми то і розповсюдження наркотиків більше відбувається серед молоді. Сьогодні завдяки інтернету, не маючи жодних зв'язків зі злочинним світом можна швидко і без зайвих проблем роздобути наркотичні речовини, при цьому залишаючись анонімом. Так само без проблем маючи базові вміння використання Інтернету можна і власноруч розвивати свій наркобізнес в мережі. При цьому таких «бізнесменів», які знають як зберегти анонімність в кіберпросторі практично не можливо знайти.

Департаментом кіберполіції проводиться великий обсяг роботи для боротьби з Інтернет-ресурсами, за допомогою яких відбувається розповсюдження наркотичних речовин. Тільки за сім місяців цього року поліцейські викрили 255 фактів збуту наркотиків, більшість з них – за допомогою месенджерів Телеграм, Вайбер, Вотсапп тощо.

В Україні найпоширеніший наркотик, як і у всій Європі, це канабіс. Аудиторія – молодь. Далі за популярністю йдуть опіати – опій, макова солома, їх синтетичні аналоги, такі як метадон. Потім йдуть стимулятори амфетамінового ряду – амфетамін, метамфетамін, МДМА (екстазі). І тільки потім – нові психоактивні речовини. Збут наркотиків через

Інтернет розвивається набагато швидше, ніж розробляються ефективні механізми збору електронних доказів та документування такої протиправної діяльності. Інтернет розмив всі межі, члени однієї злочинної групи часто перебувають у різних країнах і могли ніколи не бачитися в житті. Наприклад, є Інтернет-ресурс, на якому українські користувачі купують наркотики. Людина, яка адмініструє цей ресурс, може знаходитися в будь-якій точці світу, інформує українського покупця, де взяти наркотик при цьому ніколи у житті безпосередньо може не стикатися з наркотиками.

Інша частина цієї злочинної групи постійно стикається з наркотиками, але ніколи не контактує з їх покупцями. Вони організовують їх постачання в Україну (часто через міжнародні поштові відправлення або іншими безконтактними засобами), розфасовку на дози і безконтактний збут. Члени групи, які розкладають наркотики по місту у «схованки», практично ніколи не мають прямого контакту з організаторами поставок наркотиків. Всі інструкції отримують через Інтернет, у тому числі і місце зберігання чергової партії наркотиків. У підсумку це – найбільш вразлива частина групи, так званий «витратний матеріал» для їх лідера. Тому практично завжди з ними вибудовують роботу таким чином, щоб у разі затримання вони не володіли інформацією, що представляє оперативний інтерес для поліції.

Всі ми стикаємося з написами на стінах будинків і парканів з рекламними графіті Інтернет-ресурсів зі збуту наркотиків. Як ці написи з'являються? В основному їх наносять молоді люди, користувачі цих Інтернет-ресурсів для отримання знижки на наркотики або за грошову винагороду. Треба розуміти, що нові психоактивні речовини молоддю помилково сприймаються як безпечна альтернатива традиційним наркотикам. Тому що їх збувають під виглядом легальних наркотиків, які «менш» небезпечні, навіть ніж звичайні сигарети або алкоголь. Розвиток месенджерів з можливістю шифрування даних користувачів призвів до того, що за останні декілька років роздрібний продаж наркотиків майже повністю перейшов у цифровий формат.

Кожне нове оновлення таких месенджерів ускладнює роботу правоохоронних органів за рахунок використання новітніх методів шифрування інформації та підвищення рівня анонімності учасників спілкування. Найбільш популярним месенджером серед роздрібних наркоторговців є Telegram. Для розв'язання цієї проблеми було проведено накопичен-

ня та класифікацію інформації щодо використання наркоторговцями можливостей мережі Інтернет та месенджерів, що використовуються з метою пошуку нових клієнтів та розповсюдження наркотичних засобів, а також створено відповідну аналітичну підсистему.

Реалізація цього завдання дозволить правоохоронним органам більш ефективно протидіяти правопорушенням та виконувати інші завдання, які виникають під час оперативно-службової діяльності, зокрема концентрувати увагу патрульної поліції на місцях можливого розташування так званих «кладів» – прихованих місць збереження та передачі «клієнтам» наркотичних засобів.

Нещодавно, для того щоб знизити рівень наркоторговлі в Telegram Групою фахівців та курсантів факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ під керівництвом декана факультету підполковника поліції В'ячеслава Маркова у рамках проекту «MRIYA» створено чат-бот «СтопНаркотик», призначений для блокування Інтернет-ресурсів з продажу наркотичних засобів з використанням месенджеру Telegram. З його допомогою всі користувачі месенджеру зможуть блокувати Інтернет-магазини, які продають наркотичні засоби, шляхом надсилання звернення-скарги до адміністрації Telegram з відомостями про акаунт, з якого здійснюється наркоспам.

З метою протидії збуту наркотичних засобів за допомогою мережі Інтернет та мобільних додатків зв'язку необхідний комплекс заходів щодо оптимізації законодавства з урахуванням сучасних способів здійснення організованої злочинної діяльності у цій сфері. Необхідно вдосконалювати законодавство і посилювати контроль за його дотриманням в сфері телекомунікаційних мереж і мобільних додатків.

В першу чергу, в Україні необхідно змінити процедури зі створення Інтернет-ресурсів, а саме виключити таку можливість без реєстрації достовірних персональних даних, що дозволило б правоохоронним органам ідентифікувати особи злочинців. В цілому, це дозволить виключити можливість створення анонімних сайтів, з'єднань, чатів тощо, які можуть використовуватися з метою незаконного обігу наркотиків.

Доцільно розвивати підрозділи кіберполіції із залученням фахівців найвищого рівня, для виявлення та припинення діяльності з незаконного обігу наркотиків у мережі Інтернет, аналізу поточного стану нарко-кіберзлочинності, ідентифікації осіб, причетних до незаконного обігу наркотиків з використанням мережі Інтернет, шляхом відстежен-

ня підозрілих грошових потоків і криптовалюти, а також поштових і електронних відправлень, виявлення міжнародного наркотрафіка. Крім цього, доречна імплементація міжнародного досвіду боротьби з підриву економічних основ наркозлочинності, а саме здійснення кібератак на Інтернет-ресурси, які здійснюють незаконний обіг наркотиків, арешт електронних рахунків злочинців, блокування їх серверів тощо.

Тож, варто сказати що проблема розповсюдження наркотичних речовин за допомогою Інтернету сьогодні є досить болючою у всьому світі. Для її вирішення в першу чергу потрібно переглянути законодавчу базу, та винаходити нові шляхи та методи виявлення злочинних організацій які займаються такою діяльністю. Ця проблема має міжнародний характер, тож варто розвивати зв'язки з іншими державами для її подолання.

Одержано 31.10.2019

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

УДК 343.9

Владислава Станіславівна Батиргареєва,
доктор юридичних наук, старший науковий співробітник, директорка Науково-дослідного інституту вивчення проблем злочинності ім. академіка В. В. Сташиса Національної академії правових наук України (м. Харків)

Сучасний віктимологічний портрет потерпілої особи від торгівлі людьми[3]

потерпілому від злочину присвячено безліч наукових публікацій. Це питання є дискусійним та актуальним для дослідження у будь-які часи. Адже суспільство за своєю суттю є динамічним, а отже, й зміни у всіх його сферах цілком закономірні. Це стосується і середньостатистичного учасника суспільних відносин, у тому числі й тих, що виникають під час вчинення злочинів, передбачених ст. 149 КК України.

Із метою визнання особи потерпілою від торгівлі людьми у літературі пропонується звертати увагу на такі критерії об'єктивного характеру: 1) застосування до особи або її близьких фізичного чи психічного насильства задля примушення її займатися певним видом діяльності або діяльністю в обсягах, які вона вважає для себе неприйнятними; 2) тримання особи в умовах, що заподіюють страждання; 3) пред'явлення до людини боргів, із якими вона повинна розплатитися, перш, ніж сама зможе розпоряджатися своїми власними прибутками, стане вільно вирішувати, чи зможе вона припинити роботу, або перш, ніж злочинець поверне їй документи; 4) тримання людини під контролем, наглядом, обмеження у вільному пересуванні або в можливостях спілкування з іншими людьми [1, с. 6]; 5) відібрання особистого майна й документів; 6) відібрання зароблених людиною грошей [2, с. 71].

Але перелічені критерії можна застосувати до тих, хто вже потрапив у «злочинні тенета». Але як же особа «заковтує гачок» злочинців?

Наукове дослідження НДІ ВПЗ показало, що значна частина як міських, так і сільських мешканців не можуть визначитися з ризиками стати жертвами торговців людьми, що свідчить про все ще недостатню поінформованість громадян щодо аналізованої проблеми та злочин-

3 Тези підготовлено на виконання теми фундаментального наукового дослідження НДІ ВПЗ «Стратегія зменшення можливостей вчинення злочинів: теорія та практика».

них схем потрапляння людини до рабства. Причому сільські жителі виглядають більш самовпевненими в тому, що з ними такі ситуації не трапляться, якщо вони вирішили б шукати роботу за кордоном: свої шанси уникнути неприємностей ними оцінюються у два з половиною рази вище за мешканців міст. У такому разі важливо з'ясувати, від кого може виходити небезпека потрапляння у рабство. Дослідженням установлено, що вербування потерпілих здійснювалося найчастіше з боку знайомих, друзів, родичів та ін. (61,1%), оскільки саме їм потерпілі довіряють більше за все.

Жителі міст та сіл України різняться за вподобаннями у виборі видів робіт, на які вони погодилися б. Так, жителі міст жіночої статі надають перевагу роботі, пов'язаній зі сферою послуг (туристичний та шоу-бізнес, догляд за дітьми або хворими), в той час як мешканки селищ згодні працювати на сільгоспроботах і домогосподарками. Чоловіки незалежно від регіону походження надають перевагу сільському господарству, будівництву і роботі, пов'язаній з транспортними послугами. Дещо іншу ситуацію нам демонструють матеріали кримінальних проваджень. Так, найчастіше потерпілі запрошувалися на роботу танцівницями у нічних клубах, кабаре тощо (41,4%); 24,2% пропонувалося надавати інтимні послуги; 13,8% – працювати офіціантками; у сільському господарстві – 9,9%; доглядати за дитиною або хворими – 3,4%; виконувати хатню роботу – також 3,4%; інше – 3,9%. Проте абсолютна більшість потерпілих (98,2%) так чи інакше зазнали сексуальної експлуатації, хоча у теперішній час трапляються й випадки визнання потерпілими чоловіків віком 25–35 років, зайнятих переважно на будівельних і сільгоспроботах. Що стосується аналізу попередньої трудової діяльності потерпілих, то в Україні офіційно працювали до моменту виїзду за кордон лише 19,2 % міських і 14,2 % сільських жителів. Переважна більшість потерпілих (63,3 %) виїхали з України за власним бажанням, маючи достовірну інформацію про дійсний характер роботи, що вони мають виконувати, у тому числі й про послуги сексуального характеру. В решті випадків виїжджаючі не мали достовірної інформації. Однак фактів примусового вивезення не констатовано, хоча раніше (15–20 років тому) такі факти траплялися [див.: 3, с. 4].

Серед жінок групу ризику від торгівлі людьми, як й 15–20 років тому, становлять особи віком 16–35 років. Жертви мають невисокий освітній рівень (77,9%), сім'я та діти є лише у 25,0%. Віктимна поведінка частини потерпілих виявляється у їх легковажності (52,2%), недооцінці ризиків,

пов'язаних із роботою за кордоном (40,1%), аморальному способі життя (33,1%), користолюбстві та бажанні заробити великі гроші (26,8%).

Потребує додаткового дослідження нова негативна тенденція, що виникла кілька років тому в Україні, – з країни походження постраждалих від торгівлі людьми вона перетворюватиметься на країну призначення живого товару, адже все частіше громадяни інших держав стають постраждалими від різних форм експлуатації саме в Україні: сексуальної, включно з примусовою проституцією та порнографією, трудової – у сільському господарстві, будівництві, секторі обслуговування, від примусового жебрацтва та вилучення органів [29, с. 6]. Проте лише лічені одиниці іноземців у теперішній час визнаються потерпілими від торгівлі людьми. Замість цього, такі особи, як правило, піддаються видворенню за межі нашої країни.

Таким чином, отримані результати, по-перше, дозволяють ознайомити широкий загал із основними рисами потерпілої особи від торгівлі людьми з українських міст та селищ, а, по-друге, можуть бути покладені у підґрунтя покращення інформаційно-аналітичного забезпечення роботи державних та правоохоронних органів з метою зменшення випадків торгівлі людьми як з України в цілому, так й із сільської місцевості, зокрема.

Список бібліографічних посилань

1. Довідник з проблеми запобігання торгівлі жінками для консультантів телефонів довіри. Київ : Ла Страда-Україна, 1999. 42 с.
2. Протидія організованій злочинності у сфері торгівлі людьми / за заг. ред. В. І. Борисова та Н. О. Гуторової. Харків : Одіссей, 2005. 288 с.
3. Батиргареєва В. С. Аналітична довідка за результатами узагальнення кримінальних справ за ст. 149 КК України 2001 року (ст. 124^1 КК України 1960 року), розглянутих судами України за 1998–2004 рр. // Архів Інституту вивчення проблем злочинності АПрН України. 2005.

Одержано 20.10.2019

УДК 351.76:343.98:343.431

Назар Романович Бабій,
курсант 2 курсу навчально-наукового інституту № 1
Національної академії внутрішніх справ (м. Київ)

Марія Василівна Бурак,
кандидат юридичних наук, старший науковий співробітник
наукової лабораторії з проблем протидії злочинності
Національної академії внутрішніх справ (м. Київ)

Отримання інформації про факти торгівлі людьми

Торгівля людьми дедалі більше стає підконтрольною транснаціональним злочинним угрупованням, оскільки є видом злочинної діяльності, що приносить високий прибуток від експлуатації постраждалих і має низький рівень розкриття й висунення звинувачення проти злочинців.

Моніторинг кримінальних правопорушень, пов'язаних з торгівлею людьми свідчить, що вербування, перевезення та експлуатацію постраждалих здійснюють різні особи, які на час виявлення факту кримінального правопорушення можуть перебувати на території різних держав – походження, транзиту чи призначення. Постраждалі, як правило, з недовірою ставляться до правоохоронців і, побоюючись розголосу обставин експлуатації та покарання з боку злочинців, відмовляються звертатися до правоохоронних органів і свідчити в суді. За таких обставин дуже складно зібрати достатні докази незаконної діяльності торгівців людьми, що можуть бути ефективно використані проти них у судовому процесі [1].

Тому, під час проведення заходів по боротьбі з незаконною міграцією та фіксації правопорушень у цій сфері підрозділам Національної поліції України необхідно звертати увагу на обставини переміщення іноземців в Україну та наявність мети вчинення кримінального правопорушення – подальшої експлуатації.

На разі, є багато джерел отримання інформації про факти торгівлі людьми в Україні. Одним із надійних шляхів отримання відомостей про факти торгівлі людьми є інформація від осіб, які конфіденційно співробітничають з оперативними підрозділами. Її ефективність полягає

у тому, що вона надходить безпосередньо від тих джерел, які мають доступ до злочинного середовища, а тому можуть найповніше надати відомості, що становлять оперативний інтерес [1, с. 34].

Крім того, не варто забувати, що досить ефективним способом отримання інформації про факти торгівлі людьми є звернення громадян. Вони можуть надходити як безпосередньо від осіб, які потерпіли від злочинних дій торгівців людьми, так і від громадян, яким тим чи іншим чином стало відомо про обставини вчиненого кримінального правопорушення. Водночас практика свідчить, що з огляду на специфіку торгівлі людьми потерпілі від таких діянь та інші особи, яким відомо про його обставини, досить рідко звертаються до органів поліції.

Так, залежно від виду експлуатації слід виявити об'єкти, що можуть бути місцями вчинення факту торгівлі людьми та прикриття злочинної діяльності. Необхідно відпрацьовувати об'єкти, в яких можуть здійснювати експлуатацію іноземців (наприклад, борделі чи приватні квартири, що використовують як борделі, нічні клуби, порностудії, ринки, невеличкі фабрики, сільськогосподарські угіддя, об'єкти будівництва тощо). Одним із можливих шляхів отримання інформації про факти торгівлі людьми є систематичне відпрацювання осіб з так званої «групи ризику», тобто тих, які опинялися в полі зору оперативних підрозділів за причетність до кримінальних правопорушень, пов'язаних з торгівлею людьми, наприклад, сутенерів або працівників секс-індустрії, працівників ринків, де працевлаштовані іноземці, тощо.

Як правило, при відпрацюванні об'єктів, які можуть бути місцями вчинення торгівлі людьми, необхідно пам'ятати, що будь-яка виявлена на них особа може бути постраждалим від торгівлі людьми незалежно від її віку, статті та країни походження. Тому, при виявленні таких осіб необхідно звертати особливу увагу на їх психічний та фізичний стан. Водночас, якщо особи перебувають у незадовільному фізичному та психічному стані, наприклад, виявляють ознаки фізичного та психічного виснаження через недостатність харчування чи сну, недостатність особистої гігієни, надмірне хвилювання та страх, є вірогідність того, що вони можуть бути постраждалими від торгівлі людьми [1, с. 37].

Виявлених осіб необхідно опитувати з метою підтвердження чи спростування підозри, що вони постраждали від торгівлі людьми. Таке опитування має на меті з'ясування обставин злочину торгівлі людьми на його чотирьох етапах: встановлення контролю над особою

(вербування, викрадення або незаконне позбавлення волі особи); переміщення особи; передача (одержання) особи; експлуатація особи. Ці етапи віддзеркалюють типову послідовність вчинення дій з торгівлі людьми. Водночас можливою є ситуація наявності лише однієї з трьох перших дій, вчинених з метою експлуатації особи (наприклад, вербування людини з метою експлуатації, вчинене особою, яка сама здійснює експлуатацію людини).

Переконані, що належне опитування та отримання цінної інформації від потерпілого, дасть змогу правильно спланувати і провести оперативні заходи та слідчі дії щодо отримання переконливої доказової бази й пред'явлення обвинувачення.

Список використаних джерел:

1. Васильєва М. О., Касько В. В., Орлеан А. М., Пустова О. В. Україна як країна призначення для торгівлі людьми. Київ : Фенікс, 2012. 120 с. URL: http://iom.org.ua/sites/default/files/krayina_pryzn4_layout_1.pdf (дата звернення: 05.10.2019).

Одержано 07.10.2019

УДК 343.1:65.012.8

Вадим Миколайович Давидюк,
кандидат юридичних наук, докторант
Харківського національного університету внутрішніх справ

Сучасні тенденції в роботі з конфідентами

Історично склалося, що в територіальних підрозділах правоохоронних органів осіб, які негласно сприяють правоохоронним органам, нерідко називають спеціальними силами. Як засвідчує практика конфіденти займають роль локомотива спеціальних сил оперативно-розшукової діяльності. Моральні та юридичні аспекти конфіденційного співробітництва є взаємообумовленими. З одного боку юридичні норми закріплюють моральні установки, які існують на даний час в суспільстві щодо відповідного явища, а з іншого боку виробляють нові напрямки суспільної поведінки, які впливають на моральні принципи.

На теперішній час в Україні та провідних країнах світу пріоритетним завданням використання конфідентів є попередження злочинів. З наукової точки зору для організації роботи з конфідентами використовується теорія агентурного методу, яка є частиною теорії сприяння осіб оперативним підрозділам, що у свою чергу є частиною загальної теорії оперативно-розшукової діяльності.

В сучасних умовах агентурна робота в світі зазнає докорінних змін. Однією з причин такої ситуації є науковий прогрес, а також зміна суспільно-політичних реалій. Так, у поліції на теренах колишнього СРСР роль спеціальних сил оперативно-розшукової діяльності помітно знизилася порівняно з XX – початком XXI століттям. Правоохоронні органи вже не мають в своєму розпорядженні великих можливостей для отримання агентурної інформації на приватних підприємствах, а адміністрація цих підприємств і їх служби безпеки не зацікавлені «виносити сміття з хати». Тому найдоступнішим методом отримання оперативної інформації сьогодні є збір і узагальнення відкритих інформаційних джерел [1, с. 71]. Таким джерелом здебільшого виступає кіберпростір [2, с. 649] у локальному та глобальному значеннях цього терміну.

Водночас, незважаючи на повсюдний розвиток технічної складової у протидії злочинності роль конфідентів у вирішенні цього завдання лишається традиційно високою в провідних країнах світу. Суспільні відносини, які є необхідним елементом кримінальної діяльності, передбачають спілкування між індивідуумами. Існування людського фактору у свою чергу забезпечує потік інформації, який здатні прийняти конфіденти, та передати його правоохоронним органам. Таку взаємодію можна спостерігати і з відкритих джерел. Серед іншого, на прикладі США можна простежити тенденцію до збільшення використання відомостей, наданих інформаторами, в якості підстав для проведення заходів, що потребують судового санкціонування [3, с. 4].

Синергія технологій та традиційних методів агентурної роботи призвели до того, що кіберсфера в оперативно-розшуковій діяльності почала розглядатися як середовище впливу. Кіберпростір дає можливість правоохоронним органам застосовувати нові технологічні методи і способи протидії злочинності, в тому числі адаптувати використання сил оперативно-розшукової діяльності до умов кіберсфери [4, с. 40].

Список бібліографічних посилань

1. Информационные технологии в деятельности подразделений экономической безопасности и противодействия коррупции: монография / А. А. Крылов, В. Н. Анищенко, Э. А. Васильев и др. М. : ФГКУ «ВНИИ МВД России», 2015. 304 с.
2. Манжай О. В. Проблеми нормативно-правового забезпечення боротьби з кіберзлочинністю в Україні. *Форум права*. 2013. № 1. С. 646–650. URL: http://nbuv.gov.ua/j-pdf/FP_index.htm_2013_1_109.pdf (дата звернення: 15.10.2019).
3. Dodge M. Juvenile police informants: friendship, persuasion, and pretense. *The Justice Professional.* 2001. № 1 (14). P. 3–18. DOI: https://doi.org/10.1080/1478601X.2001.9959607.
4. Давидюк В. М. Інтернет як соціальне середовище роботи з конфідентами // Актуальні питання протидії кіберзлочинності та торгівлі людьми : зб. матеріалів Всеукр. наук.-практ. конф. (м. Харків, 23 листоп. 2018 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків, 2018. С. 39–40.

Одержано 21.10.2019

УДК 343.3

Олександр Олександрович Загуменний,
старший інспектор відділу протидії кіберзлочинам в Харківській області Слобожанського управління кіберполіції Департаменту кіберполіції Національної поліції України

Співвідношення понять «кіберзлочинність» і «комп'ютерні злочини»

З розвитком інформаційних комп'ютерних технологій з'являються нові види злочинів, об'єктом злочинного посягання яких є інформаційна безпека, нормальне функціонування електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж, комп'ютерної інформації, права на неї, а також мереж електрозв'язку. Попри велику кількість злочинних посягань у сфері інформаційних технологій, загрози, що постійно виникають у цій сфері, на сьогодні в Україні відсутнє єдине розуміння поняття кіберзлочинності і, відповідно, немає офіційного уніфікованого нормативно правового його закріплення. Поряд із поняттям кіберзлочинності у повсякденному та, подекуди, науковому обігу активно використовуються такі поняття, як «комп'ютерна злочинність», «ІТ злочинність», «злочинність у сфері інформаційних відносин», «віртуальна злочинність».

Будь-які терміни із частиною «кібер-» на сьогодні ще не отримали сформованого визначення ні на науковому, ні на нормативно-правовому рівнях та залишаються предметом наукової дискусії. Поняття кіберзлочинності є найширшим в сфері інформаційних злочинів проти систем, мереж і комп'ютерних даних та охоплює найбільшу кількість злочинних посягань у віртуальному середовищі. Також використання поняття саме «кіберзлочинність» передбачає міжнародне законодавство [1, с. 173].

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» кіберзлочин (комп'ютерний злочин) суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [2]. У Конвенції «Про кіберзлочинність» від 23 листопада

2001 року містяться вказівки на: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; 2) правопорушення, пов'язані з комп'ютерами, 3) правопорушення, пов'язані з порушенням авторських та суміжних прав [3].

Таким чином, кіберзлочинність та міжнародному рівні розуміється як сукупність зазначених злочинів. Законодавча невизначеність поняття кіберзлочинності викликала не однозначну думку із цього питання серед науковців, які по різному тлумачать ці поняття, деякі їх чітко розмежовують, інші – ототожнюють, у зв'язку з чим, гостро постає питання щодо законодавчого визначення поняття кіберзлочинності, що сприятиме чіткому теоретичному, науковому розумінню ґенези розглядуваного суспільного феномену і виробленню на цій основі ефективних і оптимальних практичних заходів протидії.

Проаналізувавши роботи вітчизняних науковців можна резюмувати, що в Україні кіберзлочинність пов'язується передусім із віртуальним простором. На думку Д. П. Біленчука, кіберзлочинністю є злочинність у змодельованому за допомогою комп'ютера інформаційному просторі, в якому перебувають відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому виді, й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі [4, с. 32]. Таке поняття є найбільш адаптованим та наближеним до української кримінально-правової доктрини, оформленої Кримінальним кодексом України [5], але воно не повністю розкриває всю сутність поняття «злочинність».

О. М. Литвак, зазначає, що злочинністю є відносно масове явище кожного суспільства, що складається з сукупності окреслених кримінальним законом вчинків, скоєних на тій чи іншій території протягом певного часу [6, с. 9]. Таким чином, Д. П.Біленчук не врахував ознаки масовості кіберзлочинності, територіальності та хронологічності. Це означає, що сукупність кіберзлочинів повинні мати масовий характер, здійснюватись на території України протягом встановленого відрізку часу для того, щоб бути окресленими загальною категорією кіберзлочинності. Питання територіальності у кіберзлочинах є спірним поняттям, адже вони здійснюються у віртуальному просторі. Проте, якщо об'єкт

кібератаки знаходиться в Україні, або ж кіберзлочинець здійснює свою деструктивну діяльність на території України, такі діяння у сукупності варто відносити до категорії вітчизняної кіберзлочинності.

О. Ю. Іванченко розуміє кіберзлочинність подібним чином, як сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем, шляхом використання комп'ютерних мереж чи інших засобів віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [7, с. 173].

Автори підручника «Криміналістика» надають визначення поняттю «комп'ютерні злочини, а саме: «Комп'ютері злочини – криміналістичне поняття, яке об'єднує різноманітні кримінально карані діяння. У вузькому значенні слова до комп'ютерних можна віднести злочини, вказані у Розділі XVI Кримінального кодексу України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». У широкому значенні слова до комп'ютерних належать і злочини, в яких використання комп'ютерних засобів – спеціалізована частина протиправних дій. Що важливо, то акцентується ашуга на тому, що ключову роль у механізмі названої категорії злочинів відіграють комп'ютерні технології. Саме їх специфічні властивості використовуються злочинцями для досягнення протиправної мети [8, с. 261].

Спільною рисою, і відповідно недоліком, концепцій тлумачення явища кіберзлочинності є нехтування авторами ознак злочинності у цілому, акцентуючи увагу на специфіці кіберзлочинів та кіберпростору, як осередку їх вчинення. Термін «кіберзлочинність» часто вживається поряд з терміном «комп`ютерна злочинність», причому нерідко ці поняття використовуються як синоніми. Дійсно, ці терміни дуже близькі, але все-таки не синонімічні. Поняття «кіберзлочинність» (в англомовному варіанті – cybercrime) ширше, ніж «комп`ютерна злочинність» (computer crime), і більш точно відображає природу такого явища, як злочинність в інформаційному просторі. Таким чином, «cybercrime» це злочинність, пов`язана як з використанням комп`ютерів, так і з використанням інформаційних технологій і глобальних мереж. У той же час термін «computer crime» в основному відноситься до злочинів, направлених проти комп`ютерів або комп`ютерних даних [9]. Кіберзлочинність – найбільш об'ємне та містке поняття для означення злочинів,

що вчиняються з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Список бібліографічних посилань

1. Іванченко О. М. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції*. 2016. № 3. С. 172–177.
2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 29.10.2019).
3. Конвенція про кіберзлочинність : від 23.11.2001. *Офіційний вісник України*. 2007. № 65. Ст. 2535.
4. Біленчук Д. П. Кібрешахраї – хто вони? *Міліція України*. 1999. № 78. С. 32–34.
5. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131.
6. Литвак О. М. Злочинність, її причини та профілактика. Київ : Україна, 1997. 168 с.
7. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції.* 2016. Вип. 3. С. 172–177.
8. Криміналістика : підручник : у 2 т. / за заг. ред. А. Ф. Волобуєва, Р. Л. Степанюка, В. О. Малярової ; МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. Т. 2. 312 с.
9. Діордіца І. В. Поняття та зміст кіберзлочинності // Глобальна організація союзницького лідерства : сайт. URL: http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti (дата звернення: 29.10.2019).

Одержано 01.11.2019

УДК 65.012.8+004

Сергій Олександрович Золотарьов,
головний судовий експерт Харківського науково-дослідного експертно-криміналістичного центру МВС України

Дослідження розумних годинників

Розумний годинник (англ. Smartwatch) – комп'ютеризований наручний пристрій, який окрім вимірювання часу виконує додаткові функції: прийом сповіщень та дзвінків зі стільникового (мобільного) телефону (у разі наявності розніму для SIM-карт), відстеження маршрутів, збір інформації з вбудованих та зовнішніх датчиків, наприклад, акселерометра, відтворення мультимедіа контенту тощо.

За цільовим призначенням розумні годинники умовно можна розділити на годинники для загальних потреб та спортивні годинники. Пристрої для загальних потреб можуть виконувати функції камери, GPS навігатора, мультимедійного плеєра, мати доступ до мережі Інтернет, тощо. Спортивні годинники, окрім названих функцій, мають додаткові, призначені для поглибленого контролю та аналізу фізичної активності користувача, як приклад можна привести моніторинг серцевого ритму, підрахунок пройденої дистанції у кроках, кілометрах та інше.

Якщо на початку можливості розумних годинників були тісно пов'язані зі стільниковими (мобільними) телефонами, то вже на даному проміжку часу удосконалення існуючих функцій розумних годинників та впровадження нових все більше роблять ці пристрої повноцінними та незалежними від інших пристроїв. Вже зараз дослідження розумних годинників виділяють у окрему категорію у цифровій криміналістиці, а стрімко зростаючий інтерес до цих пристроїв з боку правоохоронних органів є виправданим, адже серед вмісту пам'яті розумних годинників можуть зберігатися унікальні дані користувача.

Більшість випущених після 2013 року розумних годинників керуються операційними системами Wear OS (раніше – Android Wear), Tizen, watchOS, а також збільшується кількість розумних годинників, які керуються повноцінною операційною системою Android.

Керовані операційними системами Wear OS, Tizen OS та watchOS розумні годинники тісно поєднані зі стільниковим (мобільним) телефо-

ном власника, та без постійної взаємодії один із одним (синхронізації) розумний годинник має обмежений функціонал на відміну від розумних годинників, які керуються операційною системою Android. Здебільшого розумні годинники на базі операційної системи Android позиціонуються як самостійний пристрій, який схожий у порівнянні зі стільниковим (мобільним) телефоном, адже також мають рознім для SIM-карт, який може бути використаний для прийняття/здійснення дзвінків, бездротові інтерфейси Bluetooth та Wi-Fi для доступу до мережі Інтернет, а також достатні об'єми внутрішньої пам'яті для зберігання та створення файлів (у деяких випадках з можливістю розширення картами пам'яті формату microSD) тому є найбільш цікавими для дослідження.

В залежності від особливостей встановленої операційної системи, розумні годинники можуть містити унікальні дані мережної активності користувача, файли користувача або їх фрагменти, інформацію про додатки та їх налаштування, та іншу інформацію, яка може бути досліджена за окремних умов, які у цьому випадку є важливими, а саме: наявності спеціального програмно-апаратного забезпечення, поглибленого знання алгоритмів захисту, схемотехніки та інше, адже у порівнянні з дослідженням мобільних телефонів, розумний годинник відносно новий об'єкт дослідження в Україні, тому потребує часу для поглибленого вивчення та можливостей для взаємодії/обміну досвідом з колегами з інших країн для швидкого розвитку.

Одержано 09.10.2019

УДК 796.323.2(477)

Дар'я Володимирівна Казначеєва,
кандидат юридичних наук, доцент, доцент кафедри кримінального права і кримінології факультету № 1 Харківського національного університету внутрішніх справ

Основні види злочинів, що вчиняються із застосуванням криптовалюти

На сьогодні цифрові технології стали невід'ємною частиною життя сучасної людини, розвиток технологій відбувається настільки стрімко, що право не завжди встигає оперативно реагувати на появу нових предметів, інвестиційних інструментів, технологічних рішень. Подібна ситуація склалася і з криптовалютами, коли криптовалюти об'єктивно існують, але їх правове визначення та регулювання відсутні.

Криптовалюти – децентралізовані конвертовані цифрові валюти, засновані на математичних принципах, які генеруються і управляються автоматично за допомогою програмного забезпечення. Паралельно з впровадженням криптовалюти широке поширення отримала і технологія блокчейн. Термін «криптовалюта» нарівні з поняттями електронної валюти виник в 2009 році, разом з появою революційної криптовалюти «біткоін». Виникнення біткоіну сприяло появі і інших криптовалют. З 2013 року до криптовалюти виникає широкий суспільний інтерес, а їх вартість починає зростати, виникають абсолютно нові незалежні валюти, які характеризуються індивідуальними риси й особливостями. На даний час відомо про більш ніж1880 криптовалют, і цей список щодня зростає [1].

Українське законодавство жодним чином не регулює питання обігу, зберігання, володіння, використання та проведення операцій за допомогою криптовалют, наслідком чого є незахищеність власників криптовалют та їхніх майнових прав.

В даний час популярність цифрових активів як об'єкта комплексних наукових досліджень обумовлена сукупністю економічних і технічних якостей технології розподілених реєстрів: безповоротність проведених операцій (транзакцій), відмова від централізованого зберігання даних на серверах і, як наслідок, набагато менша вразливість даних, можливість укладення і ведення смарт-контрактів безпосередньо між сторонами за відсутності посередників, можливість цілодобового функціонування системи, низька

ціна транзакцій тощо. Але ці та інші переваги нової технології не можуть бути в повному обсязі оцінені через відсутність правового статусу як у самого блокчейна, так і у його продуктів. Вимушений правовий вакуум призводить до збільшення числа ризиків їх використання. Так Національний банк України відстежує розвиток та використання нових платіжних послуг, беручи до уваги принцип співмірності, і вважає, що нові учасники повинні мати шанс виходу на ринок, проте на першому місці повинна бути забезпечена безпека платежів. Разом із центральними банками країн ЄС. Національний банк України застерігає банки, платіжні організації, учасників платіжних систем та власників віртуальних валют щодо наявних ризиків і потенційних загроз їх використання. Також Національний банк України попереджає, що не несе відповідальності за можливі ризики і втрати, пов'язані з використанням віртуальних валют у розрахункових операціях [2].

Вперше на ризики використання продуктів технології блокчейн звернув увагу Європол. У своєму звіті за 2015 року він проаналізував тренди обороту криптовалюти і зробив висновок, що найбільшу популярність нові фінансові інструменти набувають в кримінальній сфері (корупційні злочини, торгівля наркотиками, психоактивними речовинами і порнографією). Найчастіше криптовалюта використовується в нелегальному Інтернеті (даркнеті) при покупці вилучених з обороту предметів та речовин. У 2018–2019 роках зросла кількість протиправних діянь, при вчиненні яких використовуються криптовалюти, але, як і раніше, використання цифрових грошей як засобу розрахунків на тіньових інтернет-ринках знаходиться на першому місці [3, с. 149–150].

Можна виділити три основні сектори кріптозлочинності:

- незаконний збут психоактивних речовин (наркотичних засобів, психотропних речовин тощо), інших заборонених товарів, контенту або послуг;
- відмивання доходів, отриманих злочинним шляхом з використанням нової цифрової валюти;
- незаконне заволодіння самою криптовалютою.

На сьогодні, використовуючи криптовалюти, можна придбати широкий спектр нелегальних товарів і послуг. Віртуальні гроші використовуються в порноіндустрії, у сфері незаконного обігу персональних даних, в торгівлі підробленими документами, нелегальними ліками, і навіть криптовалютою оплачують замовні вбивства. Але при цьому найпоширенішим сегментом незаконного застосування криптовалюти залишається незаконний обіг наркотичних засобів і психотропних

речовин (80% загального обсягу ринку нелегальних товарів).

Першим вдалим досвідом виявлення нелегальної торгівлі з використанням криптовалюти була справа Silk Road. На цьому нелегальному інтернет-ринку збувалось більше 10 тис. різновидів нелегальних товарів, а загальний річний обіг перевищував 17 млн. дол. Масштаби наркоторгівлі в Інтернеті із використанням криптовалюти продовжують зростати великими темпами [4].

З іншого боку, новим і популярним способом легалізації кримінальних доходів є їх відмивання через сайти азартних ігор. Саме через ці сервіси відмивається близько трьох чвертей всіх брудних віртуальних грошей. Згідно з даними Trend Micro, злочинці все частіше стали використовувати ігрову валюту як спосіб зберігання вартості криптовалюти. Для цього купується валюта найбільш популярних віртуальних ігор. Вона продається за криптовалюту, а потім на спеціальних сервісах конвертації обмінюється у фіатну валюту [5].

Таким чином варто підкреслити, що на сьогодні простежується негативна тенденція зростання кількості та видів злочинів, що вчиняються з використанням криптовалюти, або направлені на незаконне заволодіння самою крипто валютою. Сучасна кріптозлочинність демонструє негативну якісну і кількісну трансформацію на фоні очевидної потреби у законодавчому закріпленні та визначені правового статусу криптовалют, інших цифрових продуктів блокчейну в Україні, а також розроблення єдиних стандартів попередження такого роду злочинів.

Список бібліографічних посилань

1. Електронний ресурс URL: https://ua.investing.com/crypto/currencies (дата звернення: 14.10.2019).
2. Спільна заява фінансових регуляторів щодо статусу криптовалют в Україні // Національний банк України : офіц. сайт. 30.11.2017. URL: https://bank.gov.ua/control/uk/publish/article?art_id=59735329 (дата звернення: 14.10.2019).
3. Сидоренко Э. Л. Криминологические риски оборота криптовалюты. *Экономика. Налоги. Право.* 2017. Т. 10, № 6. С. 147–155.
4. Гладкова Є. О. Стратегія й тактика протидії наркозлочинності. Харків, 2019. 415 с.
5. Ларина Е. Криптовалюта: свет и тени. *Наш современник*. 2018. № 8. С. 214–224.

Одержано 30.10.2019

УДК 343.98

Ілля Олександрович Коваленко,
аспірант кафедри криміналістики, судової медицини та психіатрії Дніпропетровського державного університету внутрішніх справ

Микола Миколайович Єфімов,
кандидат юридичних наук, доцент, доцент кафедри криміналістики, судової медицини та психіатрії Дніпропетровського державного університету внутрішніх справ

До питання протидії шахрайству у сфері використання банківських електронних платежів

З настанням XXI століття, яке сміливо можна назвати «комп'ютерним», особливістю якого став розвиток інформаційних технологій (ІТ), з'явилися нові форми злочинності. Ці форми пов'язані зі сферою високих технологій, коли самі комп'ютери, апаратне забезпечення і шкідливі програми виступають в якості засобу злочину. Такі кримінальні правопорушення в сучасній термінології називаються кіберзлочинами.

Темпи зростання кіберзлочинності почали набирати свої оберти, коли ІТ почали впроваджуватись практично в усі сфери діяльності людини та суспільства у всіх країнах світу, коли активно почали використовувати всесвітню мережу Інтернет. Такі злочини дійшли також і до банківського сектору, в якому головною проблемою стало вчинення шахрайства в сфері використання банківських електронних платежів. Кожного дня в Україні та всьому світі вчиняються десятки тисяч таких кримінальних правопорушень, і їх кількість, на превеликий жаль, тільки зростає.

Ми погоджуємося з науковцями, які зазначають, що протидія злочинності – це безперервний процес, у межах якого одночасно й паралельно здійснюються загальносоціальні та спеціальні заходи, що спрямовані на виявлення й розкриття злочинів [6, с. 288]. В той же час, інші автори, визначають її як особливий комплексний, багаторівневий об`єкт соціального управління, який складає різноманітна за формами діяльність відповідних суб`єктів (державних, недержавних органів, установ, громадських формувань та окремих громадян), які взаємодіють у вигляді системи різнорідних заходів, спрямованих на пошук шляхів, засобів та

інших можливостей ефективного впливу на злочинність з метою зниження інтенсивності процесів детермінізації злочинності на усіх рівнях, нейтралізації дії її причин та умов для обмеження кількості злочинних проявів до соціально толерантного рівня [1, с. 176]. Як бачимо, протидія злочинності у цілому широке поняття, яке вимагає конкретного підходу в залежності від досліджуваного кримінального правопорушення.

Відповідно до звіту «Norton Reports 2017» збиток таких злочинів у всьому світі склав 172 млрд. доларів США, а кількість потерпілих від шахрайських операцій становить 978 мільйонів користувачів. В 2018 році сума збитків в 4 рази та складає майже 800 млрд. доларів США [3].

Велике значення для протидії кіберзлочинам, до яких належать шахрайство в сфері банківських електронних платежів, має прийняття державою відповідних нормативно-правових актів, таких як: Указ президента України «Про рішення Ради національної безпеки і оборони України» від 27 січня 2016 року «Про Стратегію кібербезпеки України» [7], Закон України «Про основні засади забезпечення кібербезпеки України» [4], та заснування відповідного правоохоронного органу Департаменту кіберполіції Національної поліції України [2].

Щодо міжнародного співробітництва, то в 2017 році Україна ратифікувала міжнародну угоду з Європейським поліцейським офісом про оперативне та стратегічне співробітництво [6]. Метою даної угоди було встановлення відносин між Україною та Європолом щодо запобігання і боротьби з організованою злочинністю, в тому числі кіберзлочинністю, зокрема шляхом обміну інформацією між підписантами.

Підводячи висновки, зазначаємо, що кіберзлочини, як один з видів шахрайства в сфері банківських електронних платежів, є глобальною проблемою всього світу XXI століття. Протидія таким злочинам є доволі складною, це обумовлено відсутністю єдиної судової та слідчої практики по даним категоріям кримінальних проваджень, а також нестачею висококваліфікованих фахівців в системі слідства, як в області ІТ, а також слідчих, які спеціалізуються в розслідуванні таких злочинів.

Список бібліографічних посилань

1. Кримінологія. Загальна частина : навч. посіб. / А. Б. Блага, І. Г. Богатирьов, Л. М. Давиденко та ін. ; за заг. ред. О. М. Бандурки. Харків : Харків. нац. ун-т внутр. справ, 2011. 240 с.
2. Кіберполіція України : офіц. сайт. URL: https://cyberpolice.gov.ua/ (дата звернення: 28.10.2019).

3. Norton by Symantec : офіц. сайт. URL: https://us.norton.com/cyber-security-insights-2017 (дата звернення: 28.10.2019).
4. Про основні засади забезпечення кібербезпеки України : Закон України від 08.07.2018 № 2469-VIII URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 28.10.2019)
5. Севрук В. Протидія Національної поліції України злочинам, що вчиняються організованими групами та злочинними організаціями, які сформовані на етнічній основі. *Підприємство, господарство і право.* 2017. № 2. С. 288–293.
6. Угода між Україною та Європейським поліцейським офісом про оперативне та стратегічне співробітництво : від 14.12.2016 // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/984_001-16 (дата звернення: 28.10.2019).
7. Про рішення Ради національної безпеки і оболрони України від 17 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 28.10.2019).

Одержано 30.10.2019

УДК 343.542.1-053.2

Ірина Олександрівна Лесь,
кандидат юридичних наук, доцент кафедри міжнародного права та порівняльного правознавства, заступник декана факультету міжнародних відносин Національного авіаційного університету (м. Київ)

Характерні ознаки жертви дитячої порнографії

На сьогодні за оцінками зарубіжних експертів, дитяча порнографія за прибутком посідає у світі третє місце після торгівлі наркотиками та зброєю. За статистикою Генеральної прокуратури України на грудень 2017 року зареєстровано 282 випадки розбещення неповнолітніх, 50 випадків статевих зносин із особою, яка не досягла статевої зрілості тощо [1]. Звичайно, зазначені цифри не відображають реальних масштабів окресленої проблеми і свідчать лише про той факт, що ця категорія злочинів характеризується високим рівнем латентності. Тому вважаємо актуальним розглянути деякі кримінологічні особливості жертви дитячої порнографії.

У тлумачному словнику української мови під дефініцією «жертва» потрібно розуміти «того, хто загинув від нещасного випадку, від руки ворога та ін.» [2, с. 688]. Водночас у юридичній літературі це поняття розуміється дещо по-іншому. Поняття «потерпілий» і «жертва» ототожнюють, проте є деякі суттєві відмінності.

Як зазначають автори навчального посібника «Кримінологічна віктимологія», особу потерпілого можна розглядати лише в тому випадку, якщо людині внаслідок суб'єктивного бажання злочинця або суб'єктивної обстановки було завдано фізичного, морального або матеріального збитку від протиправної дії, незалежно від того, визнана вона у встановленому законом порядку потерпілою чи ні, і чи оцінює вона себе такою суб'єктивно [3, с. 37].

Відповідно до ст. 55 КПК України потерпілим може бути фізична особа, якій кримінальним правопорушенням завдано моральної, фізичної або майнової шкоди, а також юридична особа, якій кримінальним правопорушенням завдано майнової шкоди [4]. Жертва, у свою чергу,

може і не бути учасником процесу, тому може й не визнаватися такою процесуально. Таким чином, можна зробити висновок, що поняття жертви в кримінології є ширшим за змістом, ніж потерпілого у кримінальному процесі.

Результати проведеного опитування працівників правоохоронних органів свідчать про те, що у 58,8 % випадків злочини, пов'язані із дитячою порнографією, вчиняються частіше до дітей жіночої статі, а 41,2 % – що діти однаково стають жертвами осіб жіночої статі, так і чоловічої статі. Це підтверджується і зарубіжними дослідженнями, які свідчать про те, що жертвами даного виду злочинів найчастіше є особи жіночої статі – 88,0 %. Особи чоловічої статі у загальній масі потерпілих становить 12,0 %. За іншими даними, наприклад, гарячої лінії «Дружній Рунет» у 53,0 % проаналізованих зображень з дитячою порнографією фігурують хлопчики [5, с. 15].

За віковою характеристикою переважають особи віком від 10 до 14 років (46,1 %) та від 7 до 10 років (26,5 %). Особи, віком від 14 до 16 років становлять 24,0 % та від 16 до 18 років – 3,4 %. Дослідження свідчать, що найбільш віктимними здебільшого є діти від 7 до 16 років, вони становлять 72,6 % загальної кількості дітей.

За результатами дослідження, спрямованого на визначення причин за яких діти найчастіше стають жертвами дитячої порнографії, встановлено, що 27,1% – діти, які мають певні фізіологічні особливості та не усвідомлюють всієї небезпеки маніпуляцій з ними; 42,4 % – діти є більш довірливими та не рішучими а ніж дорослі; 28,8 % – діти не обізнані у тих чи інших сферах (зокрема, сексуальній). Поряд із тим, серед рис характеру, якими найчастіше володіє жертва сексуального насилля: довірливість – 44,9 %, аморальність – 27,5 %, легковажність – 20,3 %, агресивність – 3 %.

Рівень освіти таких дітей характеризується наступними показниками: 41,4 % становлять учні загальноосвітніх шкіл, учні професійно-технічних училищ – 12 %, навчаються у технікумі чи інституті – 15,5 % жертв, працюють – 11,5 %, ніде не навчаються і не працюють – 19,6 %.

На час вчинення проти них злочину проживали з обома батьками – 73 % дітей, проживали з однією матір'ю або батьком – 18,3 %, були сиротами 8,7 % дітей.

Найбільш вразливу групу становлять особи, знайомство з якими відбулося на вулиці – 54,5 %, що свідчить про поширеність бездогляд-

ності та безпритульності. 28,8 % жертв знайшли свого злочинця через мережу Інтернет. У 12,2 % випадків злочини вчинялися стосовно дітей дружини від іншого шлюбу, і відповідно 15 % до дітей друзів та інших знайомих. У 3 % випадків даний вид злочину вчинявся відносно власних дітей. Так, за даними Мін'юсту США за 2018 рік, найчастіше насильником виступає близька для дитини людина: 38 % – батьки, 36 % – інші родичі чи друзі сім'ї [5, с. 9].

Отже, загалом можемо констатувати, що віктимність неповнолітніх жертв сексуального насильства, до якого ми умовно відносимо й дитячу порнографію, проявляється у нездатності своєчасно та правильно оцінити передкримінальну ситуацію, спрогнозувати її розвиток чи напрацювати та реалізувати ефективні стратегії поведінки у ході взаємодії зі злочинцем і визначається взаємозв'язком вікового, особистісного, дізонтогенетичного та психопатологічного факторів [6, с. 525].

Список бібліографічних посилань

1. Пояснювальна записка до Проекту Закону України «Про внесення змін до деяких законодавчих актів України (щодо захисту дітей від сексуального насильства)» // ЛігаЗакон : сайт. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/GH69M00A.html (дата звернення: 18.10.2019)
2. Новий тлумачний словник української мови : у 3 т. / уклад. В. В. Яременко, О. М. Сліпушко. Київ : Аконіт, 2015. Т. 2. 920 с.
3. Кримінологічна віктимологія : навч. посіб. / Є. М. Моісеєв, О. М. Джужа, В. В. Василевич та ін. ; за заг. ред. О. М. Джужі. Київ : Атіка, 2006. 344 с.
4. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012. № 4651-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 18.10.2019).
5. Беспалов Е. И. Детская порнография: индустрия насилия. М. : Фонд «Дружественный Рунет», 2010. 134 с.
6. Детская психиатрия : учеб. / под. ред. Э. Г. Эйдемиллера. СПб. : Питер, 2005. 1120 с.

Одержано 01.11.2019

УДК 656.7:656.8

Володимир Сергійович Макаров,
старший судовий експерт Харківського науково-дослідного експертно-криміналістичного центру МВС України

Новітні технології в комп'ютерно-технічній експертизі: дослідження дронів

Дрони, також відомі як безпілотні літальні апарати, стають все більш популярними серед населення через свою доступність та постійне здешевлення вартості. Ця популярність не тільки сприяє швидкому зростанню глобальної комерційної діяльності, але також неминуче зростає кількість злочинів з використанням безпілотних літальних апаратів. Легкість транспортування за рахунок малої ваги та розміру, можливість польоту на порівняно великі відстані та їхнє дистанційне управління робить дронів ідеальним засобом для транспортування контрабанди, наприклад, скидання зброї, телефонів, наркотиків у в'язницях або доставки наркотиків в обхід кордонів. Камера, встановлена на дроні, може записувати відео- та фото- дані у пам'ять пристрою або вести їх потокову передачу. Звідси виникає проблема конфіденційності даних для організацій та громадськості. Також існує загроза безпеці стратегічних об'єктів, таких як аеропорти, військові частини, електростанції та інші об'єкти, через можливість високоточної розвідки зловмисників.

З цієї причини необхідність проведення судової комп'ютерно-технічної експертизи з дослідження дронів, вилучених з місць злочину та пристроїв, що використовуються разом з цими безпілотниками, має важливе значення у виявленні доказів.

Якщо розглядати продвинуті моделі дронів, які не відносяться до «іграшкових», у них завжди є накопичувач даних в пам'ять якого записується інформація з камери та датчиків присутніх на борту пристрою. Важливо зазначити, що окрім фотографій та відеозаписів зроблених за допомогою відео-камери змонтованої на корпусі літального апарату, в пам'ять записуються не менш важливі дані у вигляді журналів польоту. Журнали можуть зберігати в собі історію місцезнаходження на основі

координат «GPS» або «Глонас», координати старту, інформацію про висоту польоту та напрямку, швидкість польоту та дані розпізнавань обличчя.

Зараз є десятки виробників безпілотників і сотні різних моделей, однак досі немає єдиного стандарту про спосіб зберігання цифрових даних. Дані можуть зберігатися в декількох різних форматах, а координати GPS можуть кодуватися декількома способами. Через велику різноманітність форматів даних та потенційно велику кількість наявних доказів, ручне вилучення та вивчення цих доказів може бути дуже трудомістким. Тому у експертів виникає необхідність в швидкому та безпроблемному дослідженні цих пристроїв. Найкрупніші розробники програмного забезпечення для аналізу цифрових даних у сфері судової комп'ютерно-технічної експертизи Cellebrite (www.cellebrite.com), MSAB (www.msab.com) та Oxygen Forensics (www.oxygen-forensic.com) швидко відреагували на цю необхідність та включили до своїх програмних продуктів можливість вилучення образів пам'яті з дронів та їх подальшу обробку. В тому числі можливе вилучення інформації з мобільних додатків за допомогою яких велось керування БПЛА.

Незалежно від того, як задіяний у скоєнні злочину дрон буде вилучений правоохоронними органами, вилучення з нього цифрових доказів буде повністю пов'язано з комп'ютерно-технічною експертизою.

Вже зараз можна сказати, що розвиток безпілотних літальних апаратів тільки починається. Нові технології реалізуються у кожній складовій пристрою. Механічна та програмна частина, спосіб зберігання даних та їх вміст – все це з кожним роком удосконалюється, а постійне зниження ціни сприяє швидкому розповсюдженню пристроїв. Вже скоро ми зможемо спостерігати регулярне надходження дронів на криміналістичне дослідження.

Тож вилучення та вивчення даних з безпілотних літальних апаратів – це окремий напрямок та ще один крок в мобільній криміналістиці.

Список бібліографічних посилань

1. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування // Генеральна прокуратура України : офіц. сайт. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=112661&libid=100820&c=edit&_c=fo (дата звернення: 13.10.2019).
2. Hannan A. M. A., Allen B. T. E. Tasmina I. Drone Forensic Analysis Using Open Source Tools. *Journal of Digital Forensics, Security and Law*. 2018. Vol. 13б

No. 1. URL: https://doi.org/10.15394/jdfsl.2018.1513 (дата звернення: 04.10.2019).
3. Bento M. Unmanned aerial vehicles: An overview. *Inside GNSS.* 2008. URL: http://www.insidegnss.com/auto/janfeb08-wp.pdf (дата звернення: 05.10.2019).
4. Белоконь С. А., Золотухин Ю. Н., Котов К. Ю. Управление квадрокоптером AR.Drone при движении по заданной траектории // Проблемы управления и моделирования в сложных системах : труды XIV Междунар. конф. Самара : Самар. науч. центр РАН, 2012. С. 506–514.
5. Тимочко О. І., Голубничий Д. Ю., Третяк В. Ф., Рубан І. В. Класифікація безпілотних літальних апаратів. *Системи озброєння і військова техніка*. 2007. № 1. С. 61–66.

Одержано 16.10.2019

УДК 65.012.8+004

Олександр Володимирович Манжай,
кандидат юридичних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Способи та інструменти обробки даних великого об'єму в роботі правоохоронних органів

Під час розслідування сучасних злочинів правоохоронним органам нерідко доводиться стикатися з необхідністю обробки великих об'ємів даних, що безпосередньо пов'язано із впровадженням інформаційних технологій в усі сфери людського життя. Ця ситуація є характерною для більшості країн сучасного світу.

Велика кількість проваджень, які розслідуються або перебувають під процесуальним керівництвом в однієї особи, тільки ускладнюють проблему в арифметичній прогресії. Немаловажним аспектом цієї проблеми є те, що кадровий склад правоохоронних органів не завжди в повній мірі володіє знаннями і навичками для обробки та аналізу великих об'ємів даних. Тому при обробці та аналізі великих даних силами пересічних слідчих та оперативних працівників треба виходити з необхідності використання якомога простіших програмних рішень.

Одним з різновидів даних, з якими доводиться мати справу правоохоронцям є відповіді установ, підприємств, організацій. Найчастіше, коли мова йде про великі об'єми даних, правоохоронні органи мають справу з банківськими транзакціями, файлами протоколів провайдерів та операторів телекомунікацій, відповідями фінансових установ. Їх аналіз є достатньо нетривіальним завданням, але потрібним, оскільки описані документи можуть містити відомості про справжні IP-адреси фігурантів, їх номери телефонів, інформацію про рахунки для сплати комунальних послуг тощо.

Перша проблема, з якою стикаються правоохоронці, пов'язана з тим, що часто інформацію одержують на підставі запиту правоохоронного органу. Запит не є процесуальним документом, що зумовлює необхідність паралельного проведення слідчої (розшукової) дії «тимчасовий доступ до

речей і документів». Якщо цього не зробити, то строк зберігання відомостей може спливти. Тому, серед іншого, важливо постійно підтримувати контакт з виконавцем запиту. Другим проблемним моментом є те, що не завжди легко знайти контактні дані адресата запитуваних відомостей – відповідного підприємства, установи, організації. Крім того, існують певні вимоги, які слід висувати до змісту та форми наданих відомостей.

Так, під час складання запитової частини відповідного документу важливо скласти формулювання таким чином, аби одержати якомога повну інформацію та убезпечити себе від необхідності додаткового надсилання запитів. Наприклад, під час запитування відомостей по Інтернет-гаманцях слід одразу вказати на необхідності надання повних номерів банківських платіжних карток, які використовувались для поповнення / виведення коштів з гаманців. Також слід одразу запитати дані щодо гаманців, на які виводились кошти та про інші гаманці, з яких виводились кошти на такі ж банківські платіжні картки, що і з указаних в запиті гаманців.

Що стосується форми наданих відомостей, то оптимальним є їх одержання у форматі, придатному для аналізу в табличному процесорі. Проте нерідко трапляються випадки, коли відомості надаються у pdf форматі, та навіть у вигляді зображень. Якщо відомості від організації, підприємства, установи надійшли в pdf форматі, то найбільш якісне переведення до форми таблиці можна здійснити за допомогою функції експорту в програмі Adobe Acrobat Reader Pro. Очевидно, це пов'язано з тим, що компанія Adobe Systems є розробником стандарту pdf.

Під час опрацювання даних, наданих підприємствами, установами, організаціями слід звернути увагу на:

- засоби фільтрації табличних процесорів (простий та водночас потужний інструмент, доступний для розуміння пересічному правоохоронцю);

- засоби візуалізації текстової інформації (корисно використовувати для графічного представлення текстових даних та відображення відповідних зв'язків);

- методи логічного опрацювання;

- засоби автоматизації перевірки та вилучення даних.

В останньому пункті мова йде про програми, спеціально розроблені для вирішення нескладних завдань, спрямованих на автоматизацію

обробки даних:

- перевірка великої кількості IP-адрес на предмет їх належності до українського сегменту кіберпростору;

- вилучення номерів карток з файлів, наданих банками;

- побудова хмари ключових слів з файлу великих даних;

- проведення ретроспективного аналізу за авторством.

Так, наприклад, завантаження усього змісту даних з сайту оголошень протиправного характеру дає матеріал для подальшого аналізу. Цілком ймовірною ситуацією є те, що спочатку особа була пересічним користувачем на форумі, задавала питання, повідомляла якусь інформацію про себе, а згодом її діяльність стала більш злочинно-орієнтованою. Надалі це могло сприяти виникненню злочинного угруповання та, навіть, злочинної організації. Здійснюючи ретроспективний аналіз відповідних повідомлень, інколи можна встановити справжні особисті дані особи фігуранта.

Таким чином, елементарні знання та навички у сфері інформаційних технологій значно збільшують можливості розслідування.

Одержано 24.10.2019

УДК 343.102(477)

Павло Миколайович Мітрухов,
кандидат юридичних наук, викладач кафедри оперативно-розшукової діяльності та розкриття злочинів факультету № 2 Харківського національного університету внутрішніх справ

Шляхи вирішення окремих проблем роботи слідчо-оперативної групи

У кожному випадку отримання інформації про наявність ознак кримінального правопорушення на місце події невідкладно направляється слідчо-оперативна група (далі – СОГ). На місці події члени СОГ та інші працівники поліції діють відповідно до вимог Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України (далі – НПУ) в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні, затвердженої наказом МВС України від 07 липня 2017 р. № 575 (далі – Інструкція) [1].

Аналіз сучасної практики свідчить про наявність окремих проблем у роботі СОГ, що потребують негайного вирішення.

Серед сучасних науковців окремі проблеми СОГ та шляхи їх вирішення частково досліджено в роботах М. В. Калатура [2], А. В. Мировської [3], Л. Л. Патик [3] та ін. Однак їх роботи мають деякі прогалини, заповненню яких будуть присвячені ці тези.

Відповідно до діючих нормативно-правових актів наряди поліції забезпечуються планшетними пристроями з програмним забезпеченням, за допомогою якого здійснюється інформаційна взаємодія з інформаційними ресурсами системи «Інформаційний портал Національної поліції України» [4; 5].

Варто також зауважити, що слідчий невідкладно, але не пізніше 24 годин після подання заяви, повідомлення про вчинене кримінальне правопорушення або після самостійного виявлення ним із будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення, зобов'язаний внести відповідні відомості до Єдиного реєстру досудових розслідувань (далі – ЄРДР) та розпочати розслідування [1].

Однак, забезпечення планшетними пристроями СОГ стало проблемою сьогодення. Відсутність у СОГ планшетних пристроїв (із можливостями використання ЄРДР, інших баз даних, необхідного програмного забезпечення, високошвидкісного інтернету тощо) ускладнює слідчим можливість невідкладно вносити відповідні відомості до ЄРДР, виготовляти документи в електронній формі та розпочинати розслідування на місці події, а інколи, коли усі слідчі, які входять до складу СОГ (основної та додаткової), знаходяться на виїздах, унеможливлює здійснення вищевказаних дій. Із цього етапу вся робота СОГ з належної фіксації слідів кримінального правопорушення призупиняється. Тобто на місці події слідчі без розпочатого кримінального провадження, а оперативні працівники без письмових доручень не можуть проводити допити осіб, а лише опитування. Це призводить до затягування процесу розслідування злочинів і потреби повторно здійснювати виїзд на місце події для проведення допитів та інших слідчих дій тощо. Також зазначене призводить до можливої зміни вперше наданих свідчень особою і втрати доказів, так як пояснення не є джерелом доказів на відміну від протоколу допиту. Окрім цього, у протоколі допиту передбачено відповідальність особи. У разі допиту свідка він попереджається про кримінальну відповідальність за відмову давати свідчення і за давання завідомо неправдивих свідчень, а потерпілий – за давання завідомо неправдивих свідчень [6].

Отже, роботу НПУ, а зокрема СОГ, ще не повністю приведено у відповідність до діючого законодавства, і така проблема як відсутність планшетних пристроїв із вищевказаними можливостями в СОГ залишається нерозв'язаною. На наш погляд, це можна зробити шляхом забезпечення СОГ, а в подальшому і кожного працівника НПУ, планшетними пристроями з вищевикладеними можливостями.

Відповідно до пункту 5 розділу ІІ Інструкції, до складу СОГ включаються слідчий (старший СОГ), працівник оперативного підрозділу, інспектор-криміналіст (технік-криміналіст), а також (у разі потреби) кінолог зі службовим собакою [1].

На практиці майже всі вищевказані працівники органу, підрозділу поліції здійснюють фотофіксацію слідів кримінального правопорушення на мобільний телефон.

Однак відповідно до положень Кримінального процесуального кодексу (далі – КПК) України цей перелік осіб обмежено. У ч. 7 ст. 237 КПК

України вказано, що при огляді слідчий, прокурор або за їх дорученням залучений спеціаліст має право проводити вимірювання, фотографування, звуко- чи відеозапис, складати плани і схеми, виготовляти графічні зображення оглянутого місця чи окремих речей, виготовляти відбитки та зліпки, оглядати і вилучати речі і документи, які мають значення для кримінального провадження [6].

Цікавим є те, що положення Інструкції не мають чіткого відображення змісту ч. 7 ст. 237 КПК України [1; 6]. Відповідно до підпункту 2 пункту 10 розділу ІІ Інструкції на місці події вимірювання, фотографування, та ін. вищевказані дії проводить інспектор-криміналіст (технік-криміналіст). І лише зі змісту підпункту 1 пункту 8 розділу ІІ Інструкції ми бачимо, що слідчий на місці події зокрема фіксує відомості щодо обставин учинення кримінального правопорушення тощо [1]. Але втім, фіксувати можна й за допомогою науково-технічних засобів і спеціального обладнання, саме тому пропонуємо не вносити зміни до цього пункту, обмежуючи права слідчих.

Окремо слід зауважити, що фіксація повинна здійснюватися не на власний мобільний телефон, а на технічний засіб (зазвичай це фотоапарат, що перебуває на балансі в певному органі НПУ), із зазначенням про це у протоколі огляду місця події (далі – ОМП), до якого долучаються фототаблиця (ілюстративна таблиця до протоколу ОМП) та носії комп'ютерної інформації.

Отже, якщо в ході ознайомлення з матеріалами, зокрема з протоколом ОМП, додатками до протоколу ОМП, стороною кримінального провадження буде виявлено порушення застосування технічних засобів фіксації (наприклад, встановлено, що фотознімки здійснено на інший технічний прилад (прилад, що не перебуває на балансі в певному органі НПУ) і про що не зазначено у протоколі ОМП; відсутні носії інформації чи інші додатки, що повинні були бути долученими до протоколу тощо), а під час судового розгляду подано клопотання про визнання доказів недопустимими, то суд за результатами дослідження документів, допитів, призначених експертиз може визнати такі докази недопустимими [6].

Розв'язати цю проблему, на наш погляд, можна також шляхом забезпечення усіх органів НПУ необхідною кількістю планшетними пристроями, фотоапаратами, носіями комп'ютерної інформації та іншими необхідними технічними засобами, приладами та спеціальним обладнанням, які слід поставити на баланс у певному органі НПУ.

Висновок: вирішення вищевказаних проблем забезпечить в Україні належну роботу СОГ.

Список бібліографічних посилань

1. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні : наказ МВС України від 07.07.2017 № 575 // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: http://zakon.rada.gov.ua/laws/show/z0937-17 (дата звернення: 31.10.2019).
2. Калатур М. В. Шляхи підвищення взаємодії слідчих підрозділів з іншими суб'єктами кримінального провадження України. *Актуальні проблеми вітчизняної юриспруденції.* 2017. № 6, Т. 4. С. 121–125. URL: http://apnl.dnu.in.ua/6_tom_4_2017/28.pdf (дата звернення: 31.10.2019).
3. Мировська А., Патик Л. Роль деяких учасників слідчо-оперативної групи в діяльності щодо збору криміналістично значущої інформації під час огляду місця події. *Підприємництво, господарство і право*. 2018. № 10. С. 204–208. URL: http://pgp-journal.kiev.ua/archive/2018/10/41.pdf (дата звернення: 31.10.2019).
4. Про затвердження Інструкції з організації реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події та оперативного інформування в органах (підрозділах) Національної поліції України : наказ МВС України від 16.02.2018 № 111 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/z0371-18 (дата звернення: 31.10.2019).
5. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» : наказ МВС України від 03.08.2017 № 676 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/z1059-17 (дата звернення: 31.10.2019).
6. Кримінальний процесуальний кодекс України : закон України від 13.04.2012 № 4651-VI // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 31.10.2019).

Одержано 01.11.2019

УДК 343.985.7

Айтадж Ідріс Кизи Мурадли,
аспірант Харківського національного університету внутрішніх справ

Криміналістична характеристика торговців людьми

До основних елементів криміналістичної характеристики торгівлі людьми відносять: особу злочинця, жертву злочину, обстановку вчинення торгівлі людьми, механізм учинення злочину.

Характеристика особи злочинця включає такі дані: а) соціальні – соціальний стан, освіта, національність, сімейний стан, професія; б) психологічні – світогляд (світосприйняття), переконання, знання, навички, звички, емоції, почуття, темперамент; в) біологічні – стать, вік, особливі прикмети, фізичні дані: сила, зріст, вага та деякі інші [1, с. 120].

Аналізуючи особу злочинця в рамках криміналістичної характеристики даного виду злочину, треба відмітити деяку специфіку, зумовлену тим, що торгівля людьми здебільшого являє собою транснаціональну організовану злочинність.

За соціальним статусом торговців людьми можна розділити на дві групи: явно кримінальні елементи, члени злочинних угруповань, з одного боку, і зовні законослухняні співробітники комерційних структур, іноді високопоставлені співробітники банків, правоохоронних органів, туристичних фірм, засобів масової інформації – з іншого.

Пособниками злочину виступають безробітні, соціально неадаптовані громадяни, багатодітні й навіть психічно хворі особи, які можуть перебувати під наглядом психіатра чи невропатолога.

У вчиненні торгівлі людьми часто беруть спільну участь громадяни України і іноземні громадяни або особи без громадянства. Причому продавцями, як правило, виступають громадяни України, а покупцями навпаки – іноземні громадяни [3, с. 174–175].

Можна стверджувати, що кваліфікуюча ознака ч. 3 ст. 149 КК України (вчинення злочину організованою групою) є обов'язковою для кожної справи, що розслідується, оскільки злочин, пов'язаний з торгівлею людьми поодинці не вчиняється, а вчиняється саме організованими

злочинними групами з налагодженими каналами збуту на території інших держав. Усі члени груп чітко виконують певні функції і діють за узгодженим планом, переслідуючи при цьому єдину мету. Загальну характеристику торговців людьми визначити дуже складно, оскільки неможливо виділити характерні особливості – загальні для всієї категорії злочинців. Дуже великий віковий діапазон (від 15 до 50 років), різний рівень освіти (від незакінченої середньої

до вищої), громадянство, національність також є дуже різноманітними. Ніхто не займається цими злочинними діями самостійно – злочини вчиняються виключно злочинними групами, а також більшість злочинців не мають легального місця роботи, а займаються тільки цим злочинним бізнесом. Таким чином, більш розширена характеристика злочинця в цьому випадку залежить від того, яку функцію він виконує.

Як правило, спеціалізована злочинна група по торгівлі людьми зосереджує в собі такі ланки:

1. Організатори – в їх функції входить вирішення фінансових питань, зв'язок з корумпованими співробітниками місцевої поліції, участь в торгах привезеного «живого» товару, постачання в публічні будинки жінок. Найчастіше це виконують і громадяни інших країн, тобто країн призначення (зазвичай це чоловіки, хоча зустрічаються випадки, коли ці функції виконують жінки – громадянки України). Ще їх називають сутенерами, замовниками, покупцями, які потім і експлуатують жертву в області секс-індустрії, порно-індустрії як дешеву робочу силу і т. п.

2. Помічники – основними їх функціями є налагодження зв'язків, розміщення замовлень, зустріч жертв з подальшим «працевлаштуванням», організація процесу вербування. Як правило, це жінки, які були в свій час в ролі жертви, але побачивши прибутковість цього бізнесу, почали займатися ним самі (у літературі це явище отримало назву «друга хвиля»). Займаються цим жінки віком від 20 до 30 років, які найчастіше мають дітей віком 2–5 років. Помічники іноді виконують основні функції в механізмі експортування жінок.

3. Вербувальники – в їх функції входить «обробка жертви», вербування для вивозу, а саме – надання неправдивої інформації щодо місця і умов роботи, проведення співбесід. Працівники правоохоронних органів зустрічаються з такою ситуацією, коли функцію вербувальників дуже часто виконують матері жінок «другої хвилі» (приблизний вік 42 – 57 років).

4. Кур'єри – особи, які перевозять жінок і гроші. Іноді «посада» кур'єра відсутня в ланцюзі, а функції перевезення може виконувати помічник, а іноді і сам організатор. Існування споріднених зв'язків в злочинному ланцюзі (дочка – мати; чоловік – дружина) є дуже характерним для даного виду злочину. Така сімейність підвищує рівень організованості цих груп, додає їм велику оперативність при вирішенні поточних завдань і збільшує рівень конспірації [2, с. 269–270].

Таким чином, криміналістичною особливістю торгівлі людьми є те, що злочин вчинюється злочинними групами з чітким розподілом ролей, до складу яких входять: організатори, помічники, вербувальники, кур'єри. Узагальнену характеристику особи злочинця визначити складно, оскільки неможливо виділити характерні особливості – загальні для всієї категорії, саме тому соціальні, біологічні та психологічні дані різноманітні.

Список бібліографічних посилань

1. Весельський В. К., Пясковський В. В. Торгівля людьми в Україні (проблеми розслідування) : навч. посіб. Київ : КНТ, 2007. 266 с.
2. Карпов Н. С. Криміналістична характеристика торгівлі людьми. *Університські наукові записки*. 2005. № 3 (15). С. 268–273.
3. Волкова А. І. Структура криміналістичної характеристики торгівлі людьми. *Актуальні проблеми держави і права*. 2006. Вип. 27. С. 174–181.

Одержано 01.11.2019

УДК 343.9

Роман Русланович Орлов,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

Володимир Анатолійович Євтушок,
старший викладач кафедри тактичної
та спеціальної фізичної підготовки
Харківського національного університету внутрішніх справ

Застосування поліграфа в діяльності поліції

На сьогоднішній день на ринку представлено багато різних за призначенням та технічними можливостями технічних засобів аналізу інформації, як українського так і закордонного виробництва. При цьому періодично на ринку з'являються нові розробки та нові технічні засоби які орієнтовані на вияв інформації яку приховує людина, але поліграф завжди буде актуальним і корисним у різноманітних галузях. Поліграф як багатоцільовий прилад набуває все більшого поширення в Україні. Він використовується у медичних, комерційних цілях, для вимірювання психофізичного стану людини та у інших галузях.

Поліграфи за способом фіксації даних поділяють на два типи: аналогові(пір'яні, чорнильно-пишучі) та цифрові (електронні). Для отримання фізіологічних даних людини використовують датчики верхнього і нижнього дихання, серцево-судинної активності, електропровідності шкіри, відео- та аудіофіксація процесу перевірки. Поліграф використовують для вияву у кандидата на роботу наявність алкогольної залежності, наркотичної залежності, наявність хронічних захворювань травм і т. ін.

Достовірність досліджень з використанням поліграфа безпосередньо залежить від умінь поліграфолога та його наукового і практичного базису. Сертифікованих поліграфологів готують виключно в навчальних закладах. Експерт-поліграфолог це професія, яка офіційно була затверджена ще в 2010 році у Національному класифікаторі професій України (код професії – 2144.2), але зараз існує велика кількість приватних шкіл і поліграфологів, які, не маючи ліцензії на освітні послуги, пропонують сумнівні курси з навчання навикам роботи з поліграфом.

У сфері правоохоронної діяльності поліграф використовують, згідно з Інструкцією про порядок використання поліграфів у Національній поліції України яка затверджена наказом МВС України від 13.11.2017 № 920, у наступних випадках: під час вступу кандидатів на службу до поліції; у разі проведення атестування поліцейських; перевірка з власної ініціативи особи, яка виявила бажання бути опитаною з використанням поліграфа, у тому числі під час проведення службових розслідувань; здійснення оперативно-розшукової діяльності і багатьох інших випадках.

При створенні Національної поліції України можливість використання поліграфів була закріплена на рівні законодавства, а саме згідно з ч. 2 ст. 50 (перевірка кандидата на службу в поліції) Закону України «Про Національну поліцію» «громадяни України, які виявили бажання вступити на службу в поліції, за їхньою згодою проходять тестування на поліграфі».

Також поліграф можуть використовувати не тільки для розслідування злочинів та відбору персоналу але й у напрямі організації моніторингу за принципом зворотного зв'язку при навчанні персоналу поліції навичкам психологічної саморегуляції, клінічної експертизи наявності у співробітника поліції посттравматичного стресового розладу, психолого-фізіологічної діагностики агресивності і тривожності особистості та інше.

Перевірка на детекторі брехні є одним з найбільш недорогих, легких, але дуже надійних способів дізнатися правду про ту чи іншу людину. Поліграф сприяє більш глибокому і ретельному вивченню людини, ніж всі інші методи, які можуть використовувати в роботі фахівці. Але не зважаючи на це поліграфи іноді можуть давати хибні значення в розрахунках і не виключні випадки коли люди обманювали детектори для підробки отриманих даних.

Одержано 27.10.2019

УДК 004.056.53

Роман Русланович Орлов,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

Юрій Миколайович Онищенко,
кандидат наук з державного управління, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4
Харківського національного університету внутрішніх справ

Web-сервери: безпека використання та застосування

На сьогодні уразливості в Web-застосуваннях, як і раніше, залишається одним з найбільш поширених недоліків забезпечення захисту інформації. Загроз занадто багато, і потрібно щось закласти в основу ієрархії захисту. Інтернет вже давно не просто мережа html-сторінок. Це складні додатки, скрипти, транспортна мережа, телеконференції, електронна пошта і багато іншого. Звичайно, корпоративний firewall вже не вирішує всіх проблем безпеки. Адже рівний і узагальнений підхід до забезпечення безпеки даних кожного співробітника компанії неминуче призводить до наявності проломів в захисті. Через це страждають потреби того чи іншого працівника, коли виявляються закритими критичні для виконання роботи ресурси. Більш того, багато систем безпеки відокремлюють від загального доступу тільки життєво важливі дані (наприклад, бухгалтерський облік), в той час як інші відомості, які вважаються менш важливими, доступні всім. Звичайно, це не означає, що співробітники сусіднього підрозділу вивчають дані своїх колег. Але така відкритість робить дані всіх працівників вразливими до атаки через одну-єдину лазівку в мережі. Тому замість псування даних на 1-2 комп'ютерах страждають усі.

Вірус Code Red вивів з ладу саме ті сервери, які були захищені від елементарних атак з Мережі і не стежили за своєю зростаючою уразливістю (через відсутність подібних прецедентів). Мала місце вразливість, але у зв'язку з тим, що раніше подібні атаки не проводилися, ніхто про неї не думав. У підсумку така безпечність коштувала мільйонів доларів. Узагальнимо основні причини уразливості веб-серверів.

Більшість зростаючих підприємств регулярно змінює конфігурацію

своїх мереж, додаючи нові робочі станції (іноді і сервери), забуваючи при цьому тестувати ЛВС на безпеку. Зрозуміло, заборонити підключати нових користувачів неможливо, але варто задуматися про розширення мережі заздалегідь. Позначити її сегменти, які здатні до розширення, і проводити попереднє тестування на безпеку. Більшість веб-майстрів мають кореневий або адміністраторський доступ до сервера. Розумніше прописати кожному користувачеві свою політику доступу, що обмежує його права прямими обов'язками. Наприклад, співробітник працює тільки з одним каталогом сервера, але має доступ на всі інші. Тим самим він ставить під загрозу не тільки свій сектор робіт, але і всі дані сервера. Звичайно, статус веб-майстра має не кожен користувач, хоча обмежити доступ з міркувань безпеки слід і самим високим за професійною ієрархією професіоналам.

Програмне забезпечення веб-серверів (суміш піратських, ліцензійних, shareware- і freeware-програм) робить систему вразливою. Найбезпечніший підхід – сумісне програмне забезпечення від одного виробника.

Безпека веб-серверів зводиться до управління ризиками. Але не кожна компанія має потребу у вищому ступені захисту своєї інформації. Питання рівня безпеки – це питання використання ресурсів мережі. Якщо веб-сервер існує, наприклад, тільки для потреб маркетингу, то особливо складну систему захисту встановлювати не варто. Проте системи забезпечення електронної комерції, електронних платежів вимагають потужних заходів безпеки. Тому прийнято розділяти рівні захисту веб-серверів.

Безпека – це люди, процеси, програми, безперервний пошук уразливих місць системи, налагоджена структура ліквідації загрози і контроль над виконуваними програмами. На теперішній час нормальне функціонування Web-сервера, підключеного до мережі Internet, практично неможливе, якщо не приділяти належну увагу питанням забезпечення його безпеки. Ця проблема може бути вирішена шляхом використання комплексного підходу до захисту ресурсів сервера від можливих атак. Для цього до складу комплексу засобів захисту сервера повинні входити системи антивірусного захисту, контролю цілісності, виявлення вторгнень, розмежування доступу, криптографічного захисту, а також підсистема управління. При цьому кожна з систем повинна бути оснащена елементами власної безпеки.

Одержано 27.10.2019

УДК 343.1:65.012.8+004

Іван Вікторович Панасюк,
аспірант Харківського національного університету внутрішніх справ

Робота з великими текстовими масивами у правоохоронних органах

Під час проведення розслідування нерідко доводиться справу з великими текстовими масивами, які представлені в різних форматах. Вказані дані окрім захисту [1, 2] також потребують належної обробки. Для їх приведення до зручного формату потрібно користуватися спеціальними програмними інструментами.

Якщо великі дані зберігаються у текстовому вигляді, то переглянути їх за допомогою неспеціалізованих програмних засобів є достатньо складним завданням. Алгоритм роботи стандартних засобів перегляду передбачає першочергове завантаження всього об'єму файлу до оперативної пам'яті. Якщо такий файл має розмір декілька гігабайт, то його відкриття триватиме довго. З метою перегляду змісту таких документів слід користуватися спеціалізованими програмами. Однією з таких програм є редактор EmEditor. За його допомогою досить зручно переглядати великі текстові документи, здійснювати в них пошук, розділяти їх на частини, вносити інші зміни. У разі потреби перетворення текстових файлів у формат бази даних, може знадобитися їх попередня обробка для приведення до певної форми. В цьому випадку спеціалізовані редактори можуть бути використані для швидкого перегляду файлу та вилучення з нього фрагменту даних для відпрацювання процесу перетворення.

Для імпорту текстових даних до якоїсь СУБД вони нерідко мають бути перетворені у певну форму, вимоги до якої визначаються алгоритмом роботи СУБД. З метою швидкого внесення відповідних змін можуть бути застосовані спеціалізовані інструменти, як от TextPipe.

Порядок роботи з вказаною програмою є достатньо простим. У лівому полі обирається відповідний фільтр, який налаштовується, а потім розміщується в тому порядку, в якому його слід застосувати до відповідного файлу. Для ефективного створення фільтрів потрібно знати головні шаблони для перетворень. З відповідними прикладами

можна ознайомитися, наприклад, за адресою datamystic.com/textpipe/manual/general_usage_easypatterns_reference.htm. По суті створення фільтру нагадує процес написання простої програми.

Існують випадки, коли імпортувати великі дані до СУБД є недоцільним, через суттєве зростання об'єму вихідних файлів банку. В такому випадку пошук можна здійснювати стандартними засобами або з використанням спеціалізованих утиліт.

У системі Windows, наприклад, для цього можна скористатися утилітою findstr з вказівкою потрібних параметрів. Наприклад,

findstr /s «що шукаємо» де_шукаємо

Крім того, з цією метою можна використовувати утиліти Grep, Folder Find Text, DocFetcher.

За результатами обробки великих текстових масивів, як правило, складається протокол, або експертний висновок, у якому в стислій формі наведено узагальнену інформацію, зрозумілу для суду та пересічних громадян. Але… Не є секретом наявність великих черг на проведення комп'ютерно-технічних експертиз. Інколи така черга може тривати більше ніж пів року. І це тільки до початку проведення експертизи. Якщо ж мова йде про огляд документів, то у багатьох підрозділах оперативні працівники або слідчі в ручному режимі вивчають документи, що, по-перше, сприяє виникненню помилок через потребу концентрації уваги, по-друге, великий час на проведення аналізу невиправдано збільшує тривалість розслідування.

Список бібліографічних посилань

1. Носов В. В. Манжай О. В. Організація та забезпечення інформаційної безпеки : навч. посіб. Харків : Вид-во Харків. нац. ун-ту внутр. справ, 2007. 216 с.
2. Манжай О. В. Правові засади захисту інформації : навч.-посіб. Харків : Ніка Нова, 2014. 104 с.

Одержано 25.10.2019

УДК 004.02

Олександр Вадимович Пилипенко,
судовий експерт відділу комп'ютерно-технічних та телекомунікаційних досліджень Харківського науково-дослідного експертно-криміналістичного центру МВС України

Методи фіксації інформації вебсайтів, які можуть бути використані в комп'ютерно-технічній експертизі

Особливістю сучасного періоду розвитку суспільства є інформатизація у всіх сферах людської діяльності. Стрімкий розвиток і вдосконалення інформаційних технологій постійно породжує нові способи вчинення і приховування злочинів. Одне із завдань правоохоронних органів є протидія тероризму, корупції та кіберзлочинності. Інформаційні системи все частіше стають не тільки об'єктом злочинного зазіхання, але і самі використовуються як знаряддя скоєння різноманітних злочинів, залишаючи при цьому своєрідні «інформаційні» сліди, які необхідно досліджувати. Подібні дослідження вимагають спеціальних інженерних знань в області комп'ютерних систем та комп'ютерної інформації та проводяться в рамках судової комп'ютерно-технічної експертизи.

Швидка інформатизація породила новий вид діянь, які несуть в собі суспільно-небезпечний характер, коли цифрова інформація використовується в якості об'єкта посягання або неправомірно використовується злочинцями. На жаль не всі талановиті люди займаються законною діяльністю, постійно з'являються люди, які свої знання та талант використовують для створення нових унікальних способів вчинення злочинів, це не обходить стороною і галузь інформаційних технологій. Глобальна мережа Інтернет надає великі можливості в якості розвитку як прогресу, так і злочинності.

Методи фіксації вебсайтів можна розглядати як візуальні та технологічні. У випадку візуальних методів – фіксується зображення, яке виводиться на екран монітора або пристрою, з якого проводиться візуальний огляд. До технологічних методів відноситься безпосередньо технічні аспекти функціонування вебсайту.

Візуальні методи фіксації вебсайтів

1) Знімок екрану (скріншот) – зображення, отримане комп'ютером, телефоном, планшетним ПК, що зображує те, що бачить користувач на екрані.

На нормативному рівні електронні докази отримали правове закріплення відносно нещодавно, відповідно до статті 76 Цивільного процесуального кодексу України [1] та статті 73 Господарського процесуального кодексу України [2], проте застосовуються вже доволі часто.

2) Збереження та/або роздрукування вебсторінки. Відповідно до п. 46 Постанови Пленуму Вищого Господарського Суду України від 17.10.2012 р. № 12 [3], роздруківки вебсторінок самі по собі не можуть бути доказом у справі, але якщо відповідні документи видані або засвідчені закладом або спеціально уповноваженою особою в межах їх компетенції за встановленою формою і скріплені офіційною печаткою на території однієї з держав-учасниць Співдружності Незалежних Держав, то згідно із статтею 6 Угоди про порядок вирішення спорів, пов'язаних із здійсненням господарської діяльності від 20.03.1992 вони мають на території України доказову силу офіційних документів.

3) Відеозапис вмісту вебсторінки. Відповідно до п. 46 Постанови Пленуму Вищого Господарського Суду України від 17.10.2018 р. № 12, як засіб доказування може бути використаний відеозапис процесу дослідження будь-якою заінтересованою особою вебсайту, стосовно якого є відомості використання його з порушенням авторських чи суміжних прав; такий запис, здійснений на цифровому носії інформації, подається до суду із зазначенням того, коли, ким і за яких умов цей запис здійснено і може бути речовим доказом у справі.

Технологічні методи фіксації вебсайтів

1) Фіксація вебсторінок за допомогою онлайн-ресурсів. Цей метод досить суперечливий, тому що фіксуються не сторінки вихідного сайту, а сторінки онлайн ресурсу, який зберігає кешовану копію сторінок вихідного сайту. Це створено для більш швидкого доступу до інформації, яка міститься на вихідному вебсайті.

2) Журнали хостингу, тобто файли с записами про події в хронологічному порядку (log файли), отримані від провайдерів. В цих файлах може зберігатись інформація про розміщену користувачем інформацію на веб-ресурсі, в залежності від налаштувань хостингу. В цьому методі є суттєвий недолік, в журналах хостингу фіксується тільки назва завантаженого файлу, а не його зміст.

Подальше збільшення користувачів інтернетом збільшує кількість потенціальних злочинців в мережі інтернет, тому це зазвичай впливає на кількість ошуканих осіб та впливає на кількість досліджень вебсайтів, або окремих сторінок сайтів, в комп'ютерно-технічній експертизі.

Список бібліографічних посилань

1. Цивільний процесуальний кодекс : Закон України від 18.03.2004 № 1618-IV // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/1618-15 (дата звернення: 16.10.2019).
2. Господарський процесуальний кодекс : Закон України від 06.11.1991 № 1798-XII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/1798-12 (дата звернення: 16.10.2019).
3. Про деякі питання практики вирішення спорів, пов'язаних із захистом прав інтелектуальної власності : Постанова Пленуму Вищого Господарського Суду України від 17.10.2012 № 12 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/v0012600-12 (дата звернення: 16.10.2019).

Одержано 17.10.2019

УДК 343.431(477+100)

Анна Сергіївна Політова,
кандидат юридичних наук, доцент кафедри кримінально-правових дисциплін та судових експертиз факультету № 1 Донецького юридичного інституту МВС України

Детермінанти торгівлі людьми

Серед найважливіших прав людини, закріплених практично всіма міжнародно-правовими документами у галузі прав людини, а також Конституцією України, є право на життя, свободу, особисту недоторканність, право вільно пересуватися, вибирати місце перебування і проживання, свобода праці та іншої не забороненої законом діяльності.

Торгівля людьми є однією з найжорстокіших форм порушення основних прав і свобод людини. Для України це кримінальне правопорушення є досить болючою проблемою. Це пов'язано з тим, що наша держава очолює список країн, котрі потерпають від торгівлі людьми. Згідно доповіді Державного департаменту США про нелегальну торгівлю людьми у світі, Україна належить до держав, де для боротьби з цим явищем докладається недостатньо зусиль.

За період 2018 року набрали законної сили судові вироки з такою кваліфікацією та характеристикою:

- за ч. 1 ст. 149 КК України було засуджено 3 особи, до 1 з них застосовано покарання у вигляді позбавлення волі на строк від 2 до 3 років та 2 особи звільнено від відбуття покарання з випробуванням;

- за ч. 2 ст. 149 КК України було засуджено 10 осіб, до 1 з яких застосовано покарання позбавлення волі на строк від 2 до 3 років, 1 особі призначено покарання від 3 до 5 років та 8 осіб звільнено від покарання з випробуванням;

- за ч. 3 ст. 149 КК України засуджено 2 особи, до 1 з яких застосовано покарання позбавлення волі на строк від 3 до 5 років включно та 1 особі призначено покарання від 5 до 10 років. До 1 засудженої особи застосовано конфіскацію майна [1, с. 35].

Причини торгівлі людьми – це система зовнішніх та внутрішніх чинників, серед яких є як позитивні (відкриття кордонів та спрощення можливості для українських громадян подорожувати по світу), так і

негативні (інтернаціоналізація тіньової економіки; зростання різниці між багатими та бідними державами; формування міжнародних кримінальних об'єднань; корумпованість працівників державних органів).

Вченими-дослідниками протидії торгівлі людьми виділяється багато факторів її існування. Ці причини є комплексними та взаємопов'язаними і кожний дослідник намагається їх систематизувати та визначити найбільш впливові.

Аналіз наукової літератури з проблем протидії торгівлі людьми дає підстави відзначити, що до найбільш розповсюджених відносяться:

- недієва система протидії торгівлі людьми, а саме корумпованість відповідальних органів, які забезпечують дотримання законності;

- попит на торгівлю людьми;

- наявність можливостей для торгівців людьми, тобто фінансові винагороди за дану діяльність;

- економічна та політична нестабільність у державі;

- погана обізнаність українських громадян щодо можливостей працевлаштування та перебування за кордоном та їх наслідки;

- відсутність належної системи захисту потерпілих на теоретичному та практичному рівні;

- наявність насильства в сім'ї;

- бідність та привабливість уявного кращого життя за кордоном;

- корумпованість влади;

- безробіття та інші фактори.

Також існує точка зору, що серед причин, що сприяють виникненню та поширенню торгівлі людьми, зокрема дітьми, в Україні вирізняються економічні (низький рівень заробітної плати та добробуту населення, високий рівень безробіття), політичні (низький рівень контролю за виконанням існуючих положень нормативно-законодавчої бази), психологічні (готовність до ризикованої поведінки, вікові психологічні особливості розвитку дитини), правові (посилення загальної криміналізації суспільства, недотримання існуючих законів), соціальні (гендерна дискримінація; порушення прав дитини, зокрема насильство та жорстоке поводження, експлуатація; наркотична чи алкогольна залежність батьків) [2].

Підводячи підсумок, можна відзначити, що за даними експертної оцінки, понад 2 мільйони людей в світі щороку потрапляють до ситуацій, пов'язаних торгівлею людьми За даними Міжнародної організації з міграції, з 1991 року понад 230 тисяч українців постраждали внаслідок торгівлі людьми. Разом з тим, причини, які «штовхають» українців до «білого рабства» можуть бути різними. Проте, відповідно до ч.1 ст. 149 КК України «Торгівля людьми» постраждалі особи дають згоду на їх експлуатацію та розуміють небезпеку. Це свідчить, на нашу думку, про переоцінку факторів, які сприяють вчиненню цього небезпечного кримінального правопорушення.

Список бібліографічних посилань

1. Никифоряк Л. П., Орлеан А. М. Аналіз судової практики з питань застосування законодавства України щодо протидії торгівлі людьми. Київ : Фенікс, 2019. 120 с.
2. Ситуація з торгівлею людьми в Україні: причини, сучасний стан // Інформаційний портал Сумської міської ради : сайт. 07.06.2017. URL: https://smr.gov.ua/uk/novini/podiji/6372-situatsiya-z-torgivli-lyudmi-v-ukrajini-prichini-suchasnij-stan.html (дата звернення: 30.10.2019).

Одержано 01.11.2019

УДК 343+621.3

Виктория Евгеньевна Рог,
старший преподаватель кафедры информационных технологий и кибербезопасности факультета № 4 Харьковского национального университета внутренних дел

Оксана Петровна Мелащенко,
старший преподаватель кафедры информационных технологий и кибербезопасности факультета № 4 Харьковского национального университета внутренних дел

Денис Лєбєдєв,
менеджер компанії Risk and Compliance Group InfoReach Inc, США

Следообразование при неправомерном доступе к компьютерной системе или сети

В данное время разработки ученых и инженеров – программистов ведут общество к новому качественному витку развития информационных услуг, а также определяют и обеспечивают основу его существования в информационном поле. Глобальные информационные сети и системы являются технологической основой всеобщего обмена информации. Таким образом, информационные ресурсы представляют огромную ценность, а несанкционированный доступ к этим ресурсам может привести к глобальным катастрофам если не будет достаточной защиты данных ресурсов. Данная ситуация может привести к не поправимым последствиям или, в условиях конкуренции, изменить ситуацию в пользу того, кто первый получил доступ к информации.

Пагубные последствия неправомерного доступа к компьютерной системе могут заключаться в хищении денежных средств или материальных ценностей, завладении компьютерными программами, а также информацией путем изъятия машинных носителей либо копирования. Это может быть также незаконное изменение, уничтожение, блокирование информации, выведение из строя компьютерного оборудования, внедрение в компьютерную систему компьютерного вируса, заведомо ложных данных и др.

Также можно отметить, что традиционная классификация следов совершения тех или иных преступлений не охватывает те ее виды, которые возникли при появлении новых видов преступлений.

Таким образом, к киберпреступлению может быть отнесено любое преступление, совершенное в электронной среде. Преступление, совершенное в киберпространстве – это противоправное вмешательство в работу компьютеров, компьютерных программ, компьютерных сетей, несанкционированная модификация компьютерных данных, а также другие противоправные общественно опасные действия, совершенные с помощью компьютеров, компьютерных сетей и программ.

Механизм следообразования – это своего рода форма протекания процесса в результате которого образуется след-отображение.

В результате чего можно сделать вывод, что основой процесса следообразования в компьютерной системе и главным следообразующим фактором является совокупность взаимодействующих программ и их настроек, которые существовали на момент совершения расследуемого события. Поскольку программа оставляет следы только тогда, когда она находится в активном состоянии, то есть выполняется в оперативной памяти компьютера, а выполнение программы является некоторым процессом, то программа является следообразующим процессом.

Основой любого криминалистического исследования, в том числе и выполняемого специалистом при расследовании преступлений в компьютерной сфере является исследование процесса следообразования. Важным вопросом в этой области является вопрос о природе следов в компьютерной системе, и ряд связанных с ним вопросов, в частности, являющихся объектами взаимодействия в компьютерных системах, свойства присущи этим объектам и их признаки находят свое отражение в следах, связанных с событием преступления.

При рассмотрении преступлений в сфере компьютерной информации мы сталкиваемся с особой группой следов – «виртуальными следами», т.е. следами, которые остаются в памяти технических устройств, в электронном поле, на носителях информации. К таким следам можно отнести файлы, магнитные носители, информация, передаваемая в эфире посредством магнитной волны.

Получаемые «виртуальные следы» не надежны, так как их можно неправильно считать. Таким образом, можно представить «виртуальный след» как любое изменение состояния киберпространства, связанное

с событием и зафиксированное в виде компьютерной информации на материальном носителе.

С технической точки зрения обнаружение и фиксация «виртуальных» следов проводится с использованием широкого спектра програмно-технических средств.

Таким образом, можно сделать вывод, что основой процесса следообразования в компьютерной системе и главным следообразующим фактором является совокупность взаимодействующих программ которые существовали на момент совершения расследуемого события. Поскольку программа оставляет след только в активном состоянии, а выполнение программы это некоторый процесс, то программу можно считать следообразующим процессом.

Получено 01.11.2019

УДК 004.946.5.056

Софія Михайлівна Сапужак,
студентка 2 курсу юридичного факультету
Тернопільського національного економічного університету

Кіберзлочинність: характеристика поняття та способи захисту

Стрімкий розвиток інформаційних технологій, інформатизація та комп'ютеризація, створення глобального інформаційного простору сформували принципово нові субстанції – інформаційне суспільство, інформаційний і кібернетичний простори, які мають невичерпний потенціал і відіграють провідну роль в економічному та соціальному розвитку країн світу. Однак, створення інформаційного суспільства може призвести і до виникнення багатьох інформаційних загроз. Повною мірою ми всі змогли це відчути 27 червня 2017 року, у день, який став «чорним вівторком» для кібербезпеки нашої країни. Протягом одного дня комп'ютерний вірус «Ransom:Win32/Petya» атакував приватний і державний сектори економіки України, зокрема банки, аеропорти, державну залізничну компанію, телекомпанії, телекомунікаційні компанії, великі мережні супермаркети, енергетичні компанії, державні фіскальні служби, органи державної влади та місцевого самоврядування тощо.

Вважаємо, що обрана тема є надзвичайно актуальною, оскільки вітчизняні реалії та кримінальна статистика свідчать про недостатню обізнаність пересічних громадян про кіберзлочинність та способи захисту від неї.

Теоретичною базою, послужили наукові публікації В. Гібсона, М. Камчатного, О. Манжая, Л. Бурячка, Б. Толубка, В. Хорошка, С. Гнатюка.

Метою даної роботи є дослідження феномену кіберзлочинності, аналіз основних її проявів, а також формулювання комплексу заходів, щодо захисту громадян від даних злочинних діянь.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України», поняття кіберзлочин (комп'ютерний злочин) трактується, як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом

України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [1].

Нині чинним Кримінальним кодексом України передбачено кримінальну відповідальність за:

1) несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361);

2) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1);

3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в комп'ютерах, автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2);

4) несанкціоновані дії з інформацією, яка оброблюється в комп'ютерах, автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (ст. 362);

5) порушення правил експлуатації комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (ст. 363);

6) перешкоджання роботі електронно-обчислювальних машин комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1) [2].

За даними ООН, найпоширенішим кіберзлочином у світі є крадіжка інформації при проведенні фінансових операцій через Інтернет (наприклад, дані кредитних карт або банківських рахунків). Типологія поширення даного типу злочинів досить проста, і жертвою на сьогодні може стати кожний активний користувач всесвітньої мережі.

Департамент кіберполіції зазначає, що найбільше проблем сьогодні виникає через Інтернет-магазини. Явище електронної комерції зростає щодня, так само зростає і грошовий обіг в мережі Інтернет, а тому відповідно збільшується кількість Інтернет-шахраїв. Злочинці швидко пристосовуються до нових технологій і активно використовують їх для реалізації схем по заволодінню коштами простих громадян. Водночас вражає різноманітність цих схем: від використання масштабних Інтер-

нет-аукціонів і торгових платформ до створення фейкових сторінок або груп з продажу неіснуючих товарів [3, с. 44–45].

І все ж є певний набір заходів, який мінімізує ризики, як для звичайних людей, як і для співробітників компаній, які хочуть захистити себе від різних кіберзагроз та кібезлочинів, а саме:

- дотримання «цифровий гігієни»: грамотно працювати з електронною поштою, не відкривати підозрілі вкладення, не переходити по посиланнях з листів з незнайомих джерел, не завантажувати неліцензійні файли, які можуть містити віруси, постійно оновлювати ліцензійне програмне забезпечення як на персональних комп'ютерах, так і на інших гаджетах, до приклади смартфони, планшети;

- ділитися своїми персональними даними тільки після того, як зможете переконатись, що будь-яка компанія або навіть держпідприємство, якому ви пересилаєте свої дані, дійсно несе за них відповідальність, вживає всіх заходів для їх збереження;

- не розголошувати конфіденційну інформацію про себе в мережі Інтернет, а також повідомляти її на будь-яких електронних ресурсах. Також не залишайте свої банківські або фінансові дані за запитом сайту під виглядом безпеки;

- всі важливі дані повинні мати резервні копії. Рекомендовано зберігати особливо цінні дані в сховищах, які не підключені до інтернету.

Отже, здавалося б такі елементарні правила, але як же ж важливо, щоб всі учасники Інтернет-мережі були ознайомлені та прислухалися до них, аби не потрапити у неприємну ситуацію. У разі, якщо ви все ж таки стали жертвою кіберзлочину – негайно звертайтеся до поліції.

Список бібліографічних посилань

1. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403.
2. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131.
3. Кравцова М. О. Запобігання кіберзлочинності в Україні : монографія / за заг. ред. О. М. Литвинова. Харків : Панов, 2016. 212 с.

Одержано 01.11.2019

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

УДК 327.84:004

Олексій Георгійович Барбашов,
курсант 4 курсу факультету № 4
Харківського національного університету внутрішніх справ

Денис Олександрович Грищенко,
старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Щодо заходів безпеки для запобігання кіберзлочинності

Протидія кіберзлочинності є сьогодні одним з першочергових завдань, яке стоїть перед правоохоронними органами не тільки України, але й світу. Практика засвідчує, що названий напрям злочинної діяльності перебувають в активній фазі розвитку. Більшість випадків кіберзлочинів виконуються за допомогою відомих уразливостей безпеки, таких як застаріла операційна система та відсутність антивірусних програм для початку атаки. Існує багато різних типів кіберзлочинів, більшість із яких здійснюються з очікуванням фінансових вигод зловмисників, незважаючи на те, що методи, які використовуються кіберзлочинцями для виплат, можуть відрізнятися. Деякі з цих типів кіберзлочинності включають:

Криптовалюта: Ці атаки використовують скрипти для видобутку криптовалют у веб-переглядачах без відома користувача. Атаки криптовалюти можуть мати справу з завантаженням програмного забезпечення для видобутку криптовалют у систему жертви. Однак кілька атак покладаються на код JavaScript, який здійснює майнінг в браузері, якщо в браузері користувача на шкідливому сайті відкрито вікно або вкладку.

Кіберешпіонаж: це трапляється, коли кіберзлочинці втручаються в мережі чи системи, щоб отримати доступ до конфіденційних даних, що належать уряду чи іншим подібним організаціям. Діяльність кіберресурсів може очікувати, що кожен тип кібератаки збирає, коригує або знищує дані, окрім використання підключених до мережі пристроїв, таких як камери чи вебкамери, шпигує за цільовою групою або окремими

особами та контролює комунікації, включаючи текстові повідомлення, миттєві повідомлення та електронну пошту.

Наведемо деякі ключеві кроки для зміцнення безпеки в мережі:

Зміцніть домашню мережу. Настійно рекомендується почати із сильного пароля шифрування та віртуальної приватної мережі (VPN). VPN може зашифрувати весь трафік, залишаючи ваші пристрої, поки він не прибуде до місця призначення. Навіть якщо кіберзлочинцям вдасться зламати вашу лінію зв'язку, вони не перехоплять нічого, крім зашифрованих даних. Завжди корисно використовувати VPN, коли ви користуєтесь загальнодоступною мережею WiFi.

Використовуйте надійні паролі. Ніколи не повторюйте свої паролі на різних сайтах і не змінюйте їх регулярно. Створіть складні паролі, комбінуючи щонайменше 10 букв, символів та цифр. Використання програми керування паролем допоможе зберегти ваші паролі.

Постійно оновлюйте програмне забезпечення. Оновлення програмного забезпечення особливо важливе для Вашого програмного забезпечення безпеки в Інтернеті та операційних систем.

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.

Одержано 22.10.2019

УДК 343.575

Олексій Михайлович Рвачов,
старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Владислав Володимирович Лактіонов,
курсант 3 курсу факультету № 4 Харківського національного університету внутрішніх справ

Денис Олегович Дацюк,
курсант 3 курсу факультету № 4 Харківського національного університету внутрішніх справ

Сучасні методи активного залучення населення до протидії збуту наркотичних засобів, психотропних речовин або їх аналогів через мережу інтернет

За результатами проведеного в 2019 році всеукраїнського опитування учнівської молоді в рамках міжнародного проекту «Європейське опитування учнів щодо вживання алкоголю та інших наркотичних речовин (ESPAD)» 18% опитаних підлітків повідомили про те, що вони хоча б один раз в житті вживали яку-небудь з наркотичних речовин: серед хлопців – 17,9%, серед дівчат – 18,1%. При цьому 12,3% учасників опитування заявили, що вони можуть отримати доступ до канабісу «дуже легко» та «скоріше легко» [1].

В останні роки як в Україні, так і в сусідніх країнах, великого поширення набув спосіб збуту та придбання наркотиків через мережу Інтернет при якому покупець і продавець залишаються незнайомими один для одного.

Так тільки упродовж перших семи місяців 2019 року підрозділи протидії наркозлочинності по всій Україні викрили 255 кримінальних правопорушень щодо збуту наркотичних засобів та психотропних речовин з використанням Інтернету [2].

В мережі діють різноманітні так звані «наркокрамниці», що спеціалізуються на збуті наркотиків, які надають змогу покупцям придбати товар, не виходячи з дому. Під час замовлення наркотиків через Інтернет, їх збут відбувається або через кур'єрські служби, або шляхом використання так званих «закладок». В останньому випадку кур'єр від продавця залишає в тайнику в легкодоступному місці сплачений покупцем наркотик.

Для пошуку потенційних покупців та збуту наркотиків зловмисники об'єднуються у організовані злочинні групи з чітко вираженими ролями: менеджери з продажу («оператори»), оптові кур'єри – постачальники («мінери»), роздрібні кур'єри («закладчики»), рекламщики («графітчики») тощо. Вони активної рекламують свої «наркокрамниці» для чого розміщують на фасадах будівель, стінах гаражів, парканах, дорожньому покритті написи («графіті») або наліпки із інтернет-адресами цих наркокрамниць [3].

Для того, щоб залучити нових «клієнтів», зберегти існуючих, заохотити постійних, менеджери наркокрамниць застосовують певні маркетингові прийоми (знижки, безкоштовна доставка «пробних» зразків, рулетки тощо) [4, с. 153].

Злочинці використовують сучасні телекомунікаційні технології, зашифровані мережні Інтернет ресурси, псевдоніми, кодові слова, дотримуються заходів конспірації, координують свої дії та здійснюють обмін інформацією за допомогою різних телекомунікаційних мереж і мобільних додатків (застосунків). Зазначені додатки мають властивості технології наскрізного шифрування, що дозволяє читати повідомлення лише учасникам листування або мають функцію «секретний чат», повідомлення в якому видаляються автоматично в залежності від часу, встановленого користувачем, та на серверах листування теж не зберігається [5, с. 12].

До таких мобільних додатків, що найчастіше використовують зловмисниками для збуту наркотиків, відноситься месенджер Telegram. Саме адреси в цьому месенджері найчастіше рекламують через розміщення «графіті». Такі посилання починаються позначкою «@» – це, зазвичай, акаунти, що обслуговують оператори чи спеціальне програмне забезпечення – «чат-боти».

Під час «спілкування» у формі чату з ботом клієнт обирає населений пункт, район міста, тип наркотику, його кількість та ціну. Здійснивши

свій вибір клієнт отримує від боту номер електронного рахунку на який необхідно переказати гроші за наркотики. Після підтвердження факту оплати бот надсилає клієнту адресу та фото з місцем, до сховано сплачений товар – «клад». Покупець шукає сплачені наркотики та забирає їх.

Дослідження свідчать, що більшість дорослого населення не звертає уваги на ці «графіті» і не знає, про що вони свідчать [6].

Одним із методів боротьби з незаконною наркоторгівлею є зафарбовування в населених пунктах «графіті» з рекламою та блокування акаунтів в Telegram.

Будь-який користувач Telegram може поскаржитися адміністрації месенджеру на акаунт за допомогою якого здійснюється розповсюдження спаму, порнографії, культу насильства, а також здійснюється незаконний збут наркотиків.

Блокування акаунтів у Telegram ефективне коли цим одночасно займається якомога більше користувачів.

З метою об'єднання зусиль громадян з активною громадською позицією в мережі Інтернет з'явилися громадські проекти типу «NarcoStop» та «CleanCity2018». Суть цих проектів полягає в тому, що вони за допомогою месенджерів Viber та Telegram об'єднали зусилля зацікавлених громадян для централізованого залишення скарг на адреси в месенджері Telegram (операторів, чати, ботів), що використовують зловмисники для незаконного розповсюдження наркотиків [7].

В Стратегії державної політики щодо наркотиків на період до 2020 року зазначено, що одним із напрямків діяльності правоохоронних органів у сфері боротьби з незаконним обігом наркотиків в Україні є «впровадження нових технологій отримання інформації про факти незаконного обігу наркотиків, зокрема їх продаж через Інтернет» [8].

З метою залучення громадськості до протидії збуту наркотичних засобів, психотропних речовин або їх аналогів через мережу Інтернет фахівцями Одеського державного університету внутрішніх справ в 2018 році був презентований програмний додаток до смартфонів на базі операційної системи Google Android «НаркоІнфо», який дозволяв правоохоронним органам якнайшвидше виявляти місця з рекламою наркотичних засобів.

За допомогою зазначеного додатку користувачі мали можливість:

1) ознайомитися із довідковими даними про різні наркотики та наслідки від їх вживання;

2) дізнатися про передбачену відповідальність за незаконне зберігання, виготовлення та придбання наркотичних засобів та психотропних речовин;

3) завантажити фотографію «графіті» із рекламою «наркокрамниць» та місце його виявлення [9].

19 вересня 2019 року під час засідання Координаційної ради з попередження наркоманії Харківської міської ради представниками факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ презентували спеціальний чат-бот «СтопНаркотик» (https://t.me/stopdrugsbot) для месенджеру Telegram [10].

Програмне забезпечення чат-боту «СтопНаркотик» складається з наступних частин:

1) підсистема накопичення, аналізу інформації, що надіслали користувачі, та формування відповідної бази даних, в якій зберігаються відомості:

- адреси наркокрамниць в месенджері Telegram;

- адреси наркокрамниць на Інтернет-ресурсах (сайти);

- фотографічні матеріали, що надсилаються користувачами з місць закладок або графіті з адресами наркокрамниць;

2) підсистема взаємодії користувачів із системою;

3) підсистема адміністрування системи;

4) доступ до програмного інтерфейсу додатку Telegram [11].

Чат-бот «СтопНаркотик» має наступні функціональні можливості:

- отримує від користувачів адреси в меседжері Telegram та вебсайтів, що використовують зловмисники для збуту наркотиків;

- підтвердження модераторами чату-боту, що посилання, яке було додано до бази, дійсно є наркокрамницею;

- веде базу посилань, що використовують зловмисники для збуту наркотиків;

- надає інструкцію користувачу щодо того як саме залишати скаргу на адресу наркокрамниці в месенджері Telegram;

- надсилає учасникам чату адреси наркокрамниць, на які необхідно надіслати скарги до адміністрації месенджеру Telegram;

- веде облік адрес наркокрамниць, що були заблоковані;

- здійснює облік на скільки адрес наркокрамниць користувач поскаржився та скільки з цих адрес вже заблоковані.

З метою більш активного залучення населення, громадських організацій тощо до протидії наркозлочинності пропонується:

1. Об'єднати функціональні можливості двох програмних продуктів:

- чат-бот для Telegram «СтопНаркотик»;

- програмний додаток під мобільні «НаркотикІнфо».

2. Розробити єдину базу даних, що буде містити наступну інформацію та наповнюватися за допомогою:

1) експертів:

- довідкові дані про різні наркотики та наслідки від їх застосування;

- дані про передбачену відповідальність за незаконне зберігання, виготовлення та придбання наркотичних засобів та психотропних речовин;

- електронний опитувач (підказувач) щодо визначення які наркотичні засоби, можливо, вживає особа, на підставі аналізу його фізичного стану та поведінки;

- контактні дані організацій, що надають допомогу наркозалежним особам;

- повідомлення від правоохоронних органів щодо ефективних випадків протидії наркозлочинності;

2) небайдужих громадян:

- фотографії «графіті» з «наркоадресами» із зазначенням GPS-координат або фізичних адрес, де вони були виявлені;

- адреси в меседжері Telegram та вебсайтів з продажу наркотиків;

- адреси точок продажу наркотиків та «наркопритонів» в населених пунктах;

- місця виявлення, фотографії та відеозаписи дій «закладчиків» та «графітчиків», які беруть участь у незаконному розповсюдженні наркотиків.

3. Розробити програмні продукти:

1) що будуть надавати доступ до єдиної бази даних та мати однаковий функціонал:

- окремний вебсайт (вебпортал) чи окрема розділ на сайті МВС чи Національної поліції;

- програмні додатки для мобільних пристроїв, що працюють під операційними системами: Google Android та Apple iOS;

- чат-боти для меседжерів: Telergam; Viber; Facebook Messenger.

2) кожен користувач обирає той програмний продукт яким йому простіше та звичніше користуватися.

4. Виявляти та заохочувати користувачів, які найбільше приклали зусиль у протидії наркозлочинності:

1) при визначенні переможців може враховуватися кількість:

- виявлених та зафарбованих кожним користувачем «графіті» із рекламою «наркокрамниць»;

- виявлених користувачем наркоадрес у меседжері Telegram та вебсайтів;

- скарг, що були відправлені користувачем адміністрації Telegram на виявлені наркоресурси в месенджері для їх блокування;

2) можна визначати кращих користувачів за певний період часу та в певному населеному пункті, районі чи області.

5. Розміщувати мурали на місцях де раніше була розміщена «наркореклама»:

- виявляти художників, які бажають намалювати мурали, та розміщувати ескізів пропонованих ними муралів;

- збирати інформацію про спонсорів, що бажають підтримати розміщення муралу в певному місці;

- місцевими мешканцями можуть обирати серед запропонованих муралів найкращий для подальшого його розміщення на обраному художником місці.

Список бібліографічних посилань

1. Європейське опитування учнів щодо вживання алкоголю та інших наркотичних речовин – ESPAD // Український інститут соціальних досліджень імені Олександра Яременка : сайт. URL: http://www.uisr.org.

ua/img/upload/files/ESPAD_Ukraine%20trends_UA.pdf (дата звернення: 28.10.2019).
2. Кіберполіція та підрозділи протидії наркозлочинності співпрацюватимуть для припинення розповсюдження наркотиків через інтернет // Єдиний портал органів системи МВС України : сайт. 06.09.2019. URL: https://mvs.gov.ua/ua/news/24152_Kiberpoliciya_ta_pidrozdili_protidii_narkozlochinnosti_spivpracyuvatimut_dlya_pripinennya_rozpovsyudzhennya_narkotikiv_cherez_internet.htm (дата звернення: 28.10.2019).
3. Мокляк С. В. Особливості збуту наркотичних засобів, психотропних речовин або їх аналогів, що вчиняється організованими групами. *Науковий вісник Херсонського державного університету.* 2018. Вип. 1, т. 2. С. 77–80.
4. Філіппов С. О. Протидія контрабанді наркотиків у США. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2018. Спецвип. С. 152–159.
5. Особливості розслідування злочинів, пов'язаних із незаконним обігом наркотичних засобів чи психотропних речовин із використанням сучасних телекомунікаційних та інших технологій : метод. рек. / О. О. Юхно, Т. П. Матюшкова, В. А. Коршенко та ін. ; за заг. ред. О. О. Юхна. Харків : Харків. нац. ун-т внутр. справ, 2018. 56 с.
6. Підлітки під прицілом: столиця розмальована Телеграм-каналами з наркотиками. Дилери – росіяни з «Хімпрому» // СТОПКОР : інформац. портал. 17.09.2019. URL: https://stopcor.org/pidlitki-pid-pritsilom-stolitsya-rozmalovana-telegram-kanalami-z-narkotikami-dileri-rosiyani-z-himpromu/ (дата звернення: 28.10.2019).
7. Шанойло О. Создание и тестирование линии по блокированию Телеграм-каналов и Сайтов распространяющих наркотики : проект. URL: https://drive.google.com/file/d/1YoVxaC4fbVi940VSPej6ZkoACOyXXZjf/view (дата звернення: 28.10.2019).
8. Про схвалення Стратегії державної політики щодо наркотиків на період до 2020 року : Розпорядження Кабінету Міністрів України від 28.08.2013 № 735-р // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/735-2013-р (дата звернення: 28.10.2019).
9. Захисти рідних та близьких від наркотиків // Телепрограма «LIVE STUDIO» / 7 канал (Одеса). 13.11.2018. URL: https://youtu.be/Q4P7UcU5X1Y (дата звернення: 28.10.2019).
10. У Харкові створили чат-бот для блокування інтернет-ресурсів з продажу наркотиків // Харківська міська рада, міський голова, виконавчий комітет : офіц. сайт. 19.09.2019. URL: https://www.city.kharkov.ua/uk/

news/u-kharkovi-stvorili-chat-bot-dlya-blokuvannya-internet-resursiv-z-prodazhu-narkotikiv-42760.html (дата звернення: 28.10.2019).

11. Чат-бот «СтопНаркотик» від фахівців ХНУВС лише за тиждень заблокував 10 наркокрамниць // Єдиний портал органів системи МВС України : сайт. 27.09.2019. URL: https://mvs.gov.ua/ua/news/24785_CHat_bot_StopNarkotik_vid_fahivciv_HNUVS_lishe_za_tizhden_zablokuvav_10_narkokramnic.htm (дата звернення: 28.10.2019).

Одержано 30.10.2019

УДК 004.62

Сергій Олександрович Бичков,
заступник завідувача відділу комп'ютерно-технічних та телекомунікаційних досліджень Харківського науково-дослідного експертно-криміналістичного центру МВС України

Штатні засоби криптографічного захисту інформації користувача в операційних системах Microsoft Windows та MAC OS

На сьогодні найбільш поширені операційні системи, які обирають користувачі для своїх персональних комп'ютерів це Windows 10 та операційна система Mac OS для комп'ютерів компанії Apple. З приводу захисту особистих даних користувачів операційних систем розробники вбудували в них програмне забезпечення, що дозволяє застосувати алгоритми криптографічного захисту. Для операційних систем Windows 10 це BitLocker, для операційних систем Mac OS – це FileVault 2. Підхід який пропонується для подолання встановленого криптографічного захисту в цих зазначених операційних системах у більшому схожий але має деякі особливості з використанням стороннього програмного забезпечення та послідовністю дій на активній операційній системі, які необхідно буде виконати особі, що проводить вилучення комп'ютерної техніки.

Дії що пропонується зробити для подолання криптографічного захисту в операційних системах Windows 10.

Розробники операційних систем сімейства Windows, починаючи з версії Microsoft Windows Vista Максимальна\Корпоративна додали у функціонал своїх продуктів можливість шифрування логічних розділів диску (томів) за допомогою вбудованого в операційну систему програмного забезпечення BitLocker, який підтримує наступні алгоритми шифрування:

- AES 128,
- AES 128 с Elephant diffuser (використовується за замовченням),
- AES 256,
- AES 256 с Elephant diffuser,

- XTS-AES (починаючи з Windows 10 версії 1511).

Для того щоб зрозуміти ввімкнено шифрування чи ні, на активній системі персонального комп'ютера чи ноутбука, що буде вилучатися для направлення на комп'ютерно-технічну експертизу, самий простий спосіб це увійти в меню провідник або увійти в «Цей комп'ютер» (російською «Этот компьютер»), на панелі де відображається список логічних дисків можна побачити іконки логічних дисків. Логічні диски до яких застосовано шифрування за допомогою BitLocker мають іконку у вигляді зображення диску та замку біля нього. Якщо замок відчинений це означає що диск замонтовано до системи, якщо зачинений – диск не замонтовано, та для того щоб отримати доступ до даних що на ньому зберігаються необхідно ввести пароль або використати апаратний ключ.

У разі, якщо застосовано шифрування функцією BitLocker, подальшим кроком, який є дуже важливим для успішного проведення дослідження у майбутньому є зняття дампу (копії) ОЗУ.

Дамп ОЗУ на комп'ютерах з операційною системою Windows можливо виготовити за допомогою спеціального програмного забезпечення, наприклад, «AccessData FTK Imager Lite Version», «Belkasoft Live RAM Capturer», «Magnet RAM Capture» та іншого. Наведене програмне забезпечення є безкоштовним та легким в користуванні.

Дуже важливо зробити дамп ОЗУ не даючи змоги власнику персонального комп'ютера його вимкнути, оскільки ОЗУ це енергозалежна пам'ять, та після вимикання комп'ютера більшість важливих даних, які містилися в неї, будуть очищені.

Таким чином, алгоритм дій має наступні ключові кроки:

1. Пересвідчитися чи застосовано до носіїв інформації комп'ютерної техніки функція шифрування даних BitLocker,

2. У разі якщо застосовано, виготовити дамп (копію) ОЗУ цього комп'ютера,

3. Надати судовому експерту для дослідження вилучену комп'ютерну техніку та виготовлений з неї дамп ОЗУ.

Дії що пропонується зробити для подолання криптографічного захисту в операційних системах Mac OS

На відміну від попередньої версії функції FileVault, яка могла захистити шифруванням лише розділ користувача, FileVault 2 здатна шифрувати як розділ диску, так і весь диск.

На стадії вилучення комп'ютерної техніки Apple, якщо вона знаходиться в активному стані (операційна система запущена, здійснений вхід до облікового запису користувача) необхідно виготовити дамп ОЗУ та надати його для подальшого дослідження експерту разом із комп'ютерною технікою, що вилучається.

Існує декілька сторонніх засобів для виготовлення дампів ОЗУ з комп'ютерів під керуванням операційною системою Mac OS, це:

1. Goldfish,

2. Mac Memory Reader,

3. OSXPMem,

які зможуть стати в нагоді при виготовленні дампів ОЗУ на версіях Mac OS до Mac OS X El Capitan 10.11.

Таким чином, у разі якщо виготовлення дампу ОЗУ з активної системи комп'ютера під керуванням операційної системи Mac OS завершилось успіхом, як і у випадку з операційними системами Windows, виготовлена копія пам'яті надається разом із технікою що вилучається на комп'ютерно-технічну експертизу для подальшого дешифрування та дослідження інформації судовими експертами.

Одержано 21.10.2019

УДК 004.056.53

Даніїл Сергійович Бєлік,
студент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Михайло Віталійович Цуранов,
старший викладач кафедри комп'ютерних систем, мереж та кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Методи боротьби з кібершахраями в магазинах цифрової дистрибуції

З розвитком телекомунікаційних мереж більшість звичайних магазині перейшли у онлайн режим роботи, це дозволило клієнтам не йти до магазина, а обирати потрібну їм річ у інтернет-магазині. В цей час почали набирати популярність такі магазини, як Aliexpress, Amazon (магазини, які продають звичайні речі, які потрібні для повсякденного користування), Apple Store, Google Play Market (магазини для мобільних додатків), Steam, Epic Games Store (магазини, які продають комп'ютерні ігри).

У зв'язку з тим, що компанія Apple, задала тенденцію що гарні мобільні ігри можуть коштувати не більше 30 грн, велика частина населення почала покупати ігри в онлайн магазині Apple Store, що і вплинуло і на інші компанії, які почали відкривати свої інтернет-магазини для продажу ліцензійних копій ігор. Магазини також почали надавати різні акційні пропозиції, що збільшило кількість активних користувачів. У Steam це традиційні розпродажі та різноманітні акційні пропозиції щодо ігор. У Epic Games Store безкоштовні ігри щотижня та тематичні розпродажі. А у Google Play Market великі знижки на ігри та акційні пропозиції на ігри.

Згідно з даних Steam, щоденно магазин відвідує близько 11 000 000 користувачів, у той час як у Epic Games Store приблизно 3 500 000 [1].

Магазини дозволяють не тільки проводити час за грою але отримати і зберігати різноманітні ігрові трофеї, які з часом можна буде продати на торговій площадці самого магазину. Спочатку це було маркетинговим

ходом ігрових магазинів, а з часом це набуло комерційної привабливості. Завдяки чому і виникли, люди які заробляють на перепродажі ігрових речей та обмінюються речами з іншими у вигоду собі. Така тенденція не могла, не зацікавити шахраїв, тому що в інвентарі деяких користувачів вартість трофеїв може досягати десятки тисяч доларів.

Зазвичай такі магазини мають недоліки у системі захисту. Наприклад, корпорація Valve (компанія, що створила сервіс Steam), опублікувала звіт, згідно якого майже 77 тисяч користувачів Steam, щомісяця втрачають гроші, ігрові предмети та навіть облікові записи, а також корпорація повідомляє, що ці жертви – далеко не завжди новачки або наївні користувачі, навпаки, від атак хакерів часто страждають професійні гравці, учасники спільнот на вебресурсі Reddit і торговці ігровими предметами [2].

Steam визнає, що торгівля краденими ігровими товарами і аккаунтами перетворилася в новий, вельми прибутковий підпільний бізнес. З кожним роком число таких кібершахраїв росте.

Існують наступні види шахрайств:

1. Фішинг – вид шахрайства, метою якого є виманювання у користувачів мережі персональних даних інтернет-магазинів. Шахраї вивчають профіль користувача та відправляють потенційній жертві повідомлення в якому міститься посилання, яке і повинен відкрити користувач [3].

2. Шкідливе ПЗ, найбільш поширені – кейлоггери. Кейлогери запам'ятовують все, що ви вводите з клавіатури, і передають цю інформацію зловмисникові. Природно, серед усього, що ви друкуєте, рано чи пізно опиняться і пароль з логіном. Подібного роду програми поширюються в середовищі геймерів під виглядом додаткових програм для ігор.

3. Уразливості клієнтів. Навіть у великих магазинах захист не є досконалим. Наприклад, у 2018 через проблеми з кешем Steam можна було випадковим чином потрапити в чужий аккаунт.

Останній скандал навколо платформи Steam розгорівся в лютому 2019 року – через некоректний XSS файл. Зловмиснику досить було залишити на своїй сторінці повідомлення з командою, наприклад, на JavaScript. Клієнт Steam виконував її автоматично, без будь-яких повідомлень – і міг перенаправити на сторінку, яка містить небезпечні віруси [4].

На сьогоднішній день проблема з крадіжкою цифрових аккаунтів є актуальною. Розвивається як засоби захисту цифрових магазинів, так

і можливі способи злому аккаунтів. Кожний магазин має засоби захисту від шахраїв, однак користувачі не завжди знають про їх наявність, тому магазинам треба більш активно інформувати своїх клієнтів про наявні засоби. Через неувагу користувачів та закордонної юрисдикції усіх цифрових-магазинів правоохоронним органам України дуже важко розслідувати такі порушення [5].

Список бібліографічних посилань

1. По данным Epic, количество ежемесячных игроков Fortnite достигло 78,3 млн // 3DNews : сайт. 21.09.2018. URL: https://3dnews.ru/975745 (дата звернення: 23.10.2019).
2. Valve раскрыла статистику кражи аккаунтов Steam и объяснила ужесточение правил обмена // 3DNews : сайт. 11.12.2015. URL: https://3dnews.ru/924979 (дата звернення: 23.10.2019).
3. Как крадут аккаунты Steam и как от этого защититься? // Pikabu : сайт. URL: https://pikabu.ru/story/kak_kradut_akkauntyi_steam_i_kak_ot_yetogo_zashchititsya_2437942 (дата звернення: 19.10.2019).
4. З легким паром: як шахраї заробляють на геймерах. URL: https://www.kaspersky.ru/blog/steam-scam/10879/ (дата звернення: 20.10.2019).
5. Против взлома есть приемы: как защитить игровой аккаунт от хакеров // PDA : сайт. 18.05.2017. URL: http://4pda.ru/2017/05/18/342232/ (дата звернення: 22.10.2019).

Одержано 25.10.2019

УДК 004.93

Владислав Олегович Воронько,
студент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Михайло Віталійович Цуранов,
старший викладач кафедри комп'ютерних систем, мереж та кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Біометрична ідентифікація як захист від несанкціонованого доступу

На сьогоднішній день кожна людина зберігає достатньо велику кількість критичної інформації на своєму смартфоні. З кожним роком зберігати конфіденційність все важче, тому що алгоритми і методи зловмисників розвиваються наряду із новітніми технологіями. Задля того, щоб надійно захистити особисті дані системи захисту використовують біометричну ідентифікацію.

Біометрична ідентифікація – засіб підтвердження особи, належності паспорта його власнику шляхом розпізнавання і зіставлення зафіксованих носіями біометричних даних (кольору очей, малюнка сітківки ока, відбитків пальців, геометрії руки, рис обличчя тощо) з особистими даними власника [1]. Біометричні системи ідентифікації досить поширені в системах безпеки.

Незважаючи на високий коефіцієнт надійності більшості методів біометричної ідентифікації, зареєстровано чимало випадків злому. У 2018 році зловмисники розробили 3D-форму голови власника банківського відділення на основі багатьох фотографій із соціальних мереж. Після цього вони створили гіпсову модель цієї форми й даної копії було достатньо для успішної ідентифікації особи. Загальна сума награбованого майна складала близько 2 мільйонів доларів США [2]. Задля захисту від подібного роду атак майже усі системи, котрі використовують ідентифікацію по 3D-формі голови, впроваджують сканування в інфрачервоному діапазоні.

Однією з не вирішених проблем захисту інформації є надійна ідентифікація користувача, який отримує доступ до конфіденційної інформації [3]. Компанія Google навіть опублікувала статтю на цю тему, де попереджувала користувачів класти смартфон дисплеєм донизу, щоб ідентифікація по формі обличчя ненароком не розблокувала телефон [1]. Традиційний парольний захист має ряд недоліків: підбір паролю методом перебору, низька надійність, якщо пароль було розгадано, то уся конфіденційність стає під загрозою. Як альтернатива парольній системі або її доповнення може розглядатися ідентифікація користувачів за біометричними характеристиками. Передовою в цій сфері є компанія Apple, яка першою почала розробляти та використовувати біометричні методи захисту у формі ідентифікації по формі обличчя (FaceID) й по відбитку пальця (TouchID). Біометричне підтвердження, а не проста перевірка пароля, який може бути вкрадений, перехоплений або вгаданий, є ключовим при розширенні Інтернет-торгівлі, створенні нових систем безпеки інформації в корпоративних мережах та системах дистанційного навчання та тестування.

Ідентифікувати людину можливо за ознаками, пов'язаними з її фізіологічними особливостями, які однозначно ідентифікують особу. До таких ознак можна віднести: геометричну будову руки, відбитки пальців, особливості малюнка сітківки ока, райдужну оболонку ока, портрет (наприклад, інфрачервону карту людини), характеристики і особливості мови, рукописний почерк, клавіатурний та комп'ютерний почерк та інші фізіологічні особливості людини, що робить її «особливою».

Методи біометричної ідентифікації діляться на дві великі групи:

- статичні методи, які ґрунтуються на фізіологічних характеристиках людини;

- динамічні методи, які ґрунтуються на особливостях поведінки людини – підсвідомих рухах в процесі виконання якої-небудь дії.

Основною перевагою статичних методів біометричної ідентифікації є їх відносна незалежність від психологічного стану користувача [2].

До сучасних статичних технологій ідентифікації відносять:

- відбиток долоні – в цій системі використовується розташування ліній на долоні людини, повністю аналогічно біометричній технології, що використовує відбитки пальців;

- судинні рисунки — розташування вен в різних частинах тіла людини, включаючи зап'ястя і тильну сторону долоні.

До сучасних динамічних методів відносять:

- ідентифікація особи за особливостями голосу. Досліджувані риси: частота, модуляція і тривалість голосового образу;

- ідентифікація за динамікою рукописного підпису. Досліджувані риси: швидкість, порядок ліній, тиск і зовнішній вигляд підпису;

- ідентифікація за клавіатурним почерком. Досліджувані риси: час затримки та час «польоту».

Біометричні методи не тільки ускладнюють доступ до пристрою, але і у випадку із правопорушником правоохоронним органам. На рахунок цього ведуться дискусії: чи буде згодна фірма надати доступ правоохоронним органам.

З точки зору безпеки найбільш зручним способом являється ідентифікація по термограмі обличчя. Оскільки за допомогою неї можна розблокувати телефон правопорушника навіть при його супротиву.

Список бібліографічних посилань

1. Иванов А. И. Биометрическая идентификация личности по динамике подсознательных движений. Пенза : Изд-во Пенз. гос. ун-та, 2000. 188 с.
2. Голубев Г. А., Габриелян Б. А. Современное состояние и перспективы развития биометрических технологий. *Нейрокомпьютеры. Разработка. Применение.* 2004. № 10. 40 с.
3. Як Google стежить за користувачами. КДБ і не снилося // Економічна правда : сайт. 02.07.2019. URL: https://www.epravda.com.ua/publications/2019/07/2/649257/ (дата звернення: 24.10.2019).
4. Borodavka V., Tsuranov M. Biometrics: Analysis and multi-criterion selection // 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). DOI: https://doi.org/10.1109/DESSERT.2018.8409152.

Одержано 25.10.2019

UDC 004.415.2:371.3

Andy David,
principal consultant, A2D Consultancy Ltd (Essex, United Kingdom)

Yurii Horelov,
Ph.D., associate professor of information technologies and cybersecurity chair of Kharkiv National University of Internal Affairs

Olexandr Horelov,
graduate student of Kharkiv National University of Radio Electronics

Some aspects of security in adaptive systems of distance learning

Distance Learning (DL) is an educational service delivery system that involves the widespread use of new information technologies to enable students to access educational resource, to interact and engage actively with teachers and colleagues while working with educational material. The capabilities of computer-aided presentation and information technology, as well as networked telecommunication technologies, can improve the quality of learning and create a comfortable environment for students as they have the ability to adjust their work with the material according to their current level of knowledge, needs, capabilities, skills and cognitive parameters of personality.

One of the ways to solve the problem of increasing the DL effectiveness is to develop educational Web courses that realize the principles of adaptation and interactivity. The implementation of adaptability provides a means to take into account the individual characteristics of the user (level of knowledge, goals, needs, cognitive characteristics, etc.), to plan the learning process, and offer them the most appropriate educational material in the most suitable form. An application with a high level of interactivity will allow the implementation of more productive scenarios of user interaction with the system, with the study material, and with colleagues.

Advantages of adaptive learning systems include:

- differentiation and individualization of training;

- optimization of the learning processes and knowledge assessment based on prognostic analysis;

- accounting for any previous level of knowledge;

- regulation of the course content by the degree of difficulty;

- students, themselves, define their own learning path, as the real-time response on process of working with the study course provides detailed feedback for self-improvement;

- adaptive systems encourage students' interest in learning through automated feedback cycles, encouraging them to take action and move forward regardless of the course teacher;

- adaptive systems increase the capacity of the teaching staff; a rich analysis of data on student performance allows teachers to constantly improve the course.

However, the spread of DL is not possible without solving a number of problems, one of which is information security. Information security in this context can be considered in two aspects:

1. Ensuring confidentiality, integrity and readiness of information in the learning process.

2. Protecting students from inaccurate, distorted and harmful information.

In the first case, we are dealing with the technical problem of protecting information from the following threats: unauthorized access to digital content, breach of integrity and inadequacy of training resources, disruption of the normal functioning of services and resources, breach of security of testing procedures, as well as unauthorized access to personal information.

A comprehensive approach to the solution of the problem of information security in the DL involves the implementation of a number of procedures. It uses the registration and authentication of the user, the implementation of access control, monitoring and detection of intrusion, the protection of network communications, and the protection of digital data storage.

Security is of particular importance for adaptive learning systems, since in this case it is possible to gain unauthorized access to a student's personal characteristics that are used to construct his model and implement an adaptation mechanism. Usually, the student model contains information about his level of knowledge, hierarchy of learning goals, cognitive, mental and psychological characteristics of the individual. This significantly increases the risk of continued use of social engineering technologies to commit illegal acts.

The second problem – protecting the user from malicious content – has become especially relevant with the advent of the Web 2.0 concept, which

significantly changes the model of user interaction with the network. The main features of the new concept include syndication, socialization, collaboration, interactivity and openness. The Internet becomes a means of interaction and communication, community building, and the realization of accessibility to the full range of services in the learning process, rather than just an instrument of access to the learning resources.

Blogging and microblogging, social networking and social presentation systems, wiki projects, social bookmarks, multimedia dissemination systems, shared editorial systems, syndication and notification technologies and more are available to the user.

In these circumstances, the solution to the problem of information security depends largely on media education, professional competence of the teacher, analysis, selection, preparation and systematic verification of information and educational resources, organization and management of student interaction. The teacher should be able to implement pedagogical technologies by means of information and communication technologies, ensuring the integrity and effectiveness of the learning process.

Одержано 21.10.2019

УДК 004.415.24

Ігор Олександрович Дука,
студент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Володимир Якович Пєвнєв,
кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Способи виявлення таємних комунікацій кіберзлочинців

Міжнародними експертами з кібербезпеки Cybersecurity Ventures підраховано, що в 2019 році в світі кібератаки відбуваються кожні 14 секунд [1]. До 2020 року у світі також продовжиться зростання кількості випадків шахрайства з використанням технологій соціальної інженерії – за підсумками 2018 року фахівцями BNP paribas вже відзначено зростання цього виду злочинів на 6%.

Зі збільшенням числа кібератак зростає і заподіяний ними збиток. Якщо в 2018 році збитки компаній різних секторів економіки склали 1,5 трлн доларів, то в 2019 році, за прогнозом BNP paribas, вони досягнуть вже 2,5 трлн. До 2022 року, за прогнозом Всесвітнього економічного форуму, сума планетарного збитку від кібератак може зрости до 8 трлн доларів [1].

Для того, щоб дії хакерів були скоординованими і точними необхідно добре налагоджений і безпечний канал зв'язку. Спілкування між хакерами проходить на форумах із обмеженим або закритим доступом, доступ до них має невелика кількість людей, усі повинні мати високу позитивну репутацію, що підтверджує надійність хакера [2]. Якщо необхідно залишити повідомлення у відкритому доступі, для цього правопорушники публікують відео, аудіо, фотографії в соціальних мережах, відкритих віртуальних дисках, в цих матеріалах приховується таємне повідомлення. Для приховування інформації в графічних зображеннях

використовуються алгоритми: LSB, метод приховування інформації: в коефіцієнтах дискретного косинусного перетворення, молодших біт палітри, в службових полях формату, в коефіцієнтах спектральних перетворень файлу, широкосмуговий.

В продовж 2017 року, за приблизним підрахунком InfoTrends було зроблено 1,2 трильйона фотографій [3] на смартфонах, фотоапаратах, тощо. Реальна кількість цих фотографій значно більша, такий об'єм інформації спец. службам неможливо перевірити, тому стеження проводиться тільки за суб'єктами, котрі привертають увагу.

Проаналізуємо методи виявлення факту наявності прихованого повідомлення в графічних зображеннях [4]:

- візуальні методи – базуються на здатності людини візуально аналізувати і виявляти істотні відмінності в порівнювальних зображеннях;

- метод візуального аналізу бітових зрізів. Основна ідея методу полягає в порівнянні зображення в цілому з зображеннями його бітових зрізів;

- статистичні методи – базуються на понятті «природного» контейнера. Суть методів полягає в оцінюванні ймовірності існування стеганографічного вкладення з невідомої стеганографічні системи на основі критерію оцінки близькості досліджуваного контейнера до «природного»;

- метод оцінки числа переходів значень молодших біт в сусідніх елементах зображення. У методі використовується знання, що між молодшими бітами сусідніх елементів і між ними та іншими бітами природних контейнерів є кореляційні зв'язки;

- метод оцінки частот появи k-бітових серій в потоці незалежних бітових елементів контейнера. Метод дозволяє оцінити рівномірність розподілу елементів у досліджуваній послідовності на основі аналізу частоти появи нулів і одиниць, і серій, що складаються з k біт;

- метод аналізу гістограм, побудованих за частотами елементів зображення. Метод дозволяє оцінити рівномірність розподілу елементів зображення, а також визначити частоту появи конкретного елемента;

- метод перевірки розподілу елементів на монотонність. Метод дозволяє оцінити рівномірність розподілу елементів зображення за результатами аналізу довжин ділянок не зростання і не спадання елементів послідовності;

Боротьба із стегоконтейнерами – є актуальною проблемою для спец. служб з точки зору складності, бо перевірити графічні зображення дуже важко, задача доказу того, що файл є контейнером секретного повідомлення – не так просто. Складність в тому, що для добре відомих алгоритмів і його варіацій існують методи атак, на відміну до рідких або зовсім невідомих, що використовують не очевидні конструкції, або принципи. Одного методу доказу наявності стегоконтейнера недостатньо для комплексної перевірки, бо для кожного типу файлів необхідна модифікація – пов'язано із алгоритмом формування зображення.

У представленій доповіді розглядаються можливі варіанти пошуку і відстеження прихованої інформації в графічних зображеннях із використанням приведених методів.

Список бібліографічних посилань

1. Потери организаций от киберпреступности // TADVISER : сайт. 29.08.2019. URL: http://www.tadviser.ru/index.php/Статья:Потери_организаций_от_киберпреступности (дата звернення: 25.10.2019).
2. Эксперты рассказали, как хакеры взаимодействуют друг с другом // Федеральное агентство новостей : сайт. 29.04.2019. URL: https://riafan.ru/1174326-eksperty-rasskazali-kak-khakery-vzaimodeistvuyut-drug-s-drugom (дата звернення: 25.10.2019).
3. Here's How Many Digital Photos Will Be Taken in 2017. URL: https://focus.mylio.com/tech-today/heres-how-many-digital-photos-will-be-taken-in-2017-repost-oct (дата звернення 25.10.2019).
4. Швидченко И. В. Методы стеганоанализа для графических файлов. *Штучний інтелект.* 2010. № 4. С. 697–705. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/58671/81-Shvidchenko.pdf?sequence=1 (дата звернення: 25.10.2019).

Одержано 29.10.2019

УДК 004.414.22:004.056:004.413.4

Петро Сергійович Клімушин,
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

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

Безпека національної інфраструктури електронних підписів

Побудова інформаційного суспільства спирається насамперед на довіру. Основою довіри в сучасній концепції інформаційного суспільства є інфраструктура відкритих ключів (PKI) та її юридичне вдосконалення у ЄС кваліфікована інфраструктура відкритих ключів (QPKI) [1].

Вітчизняна національна система електронних підписів (НСЕП) не є інтероперабельною до ЄС, тому актуальним завданням дослідження має бути зведення її до Європейської еталонної моделі QPKI.

Метою дослідження є забезпечення довірчих відносин за рахунок механізму крос-сертифікації, тобто транскордонного визнання сертифікатів відкритих ключів ЕП, виданих у різних країнах.

Розвиток національної інфраструктури центрів сертифікації ключів (ЦСК) пов'язаний з удосконаленням організаційної її структури, а саме моделі удосконалення сертифікаційних шляхів між різними державними відомствами (установами, агентствами) та недержавними організаціями, в тому числі банківським сектором, таким чином, щоб забезпечити високу надійність та високий рівень довірчих відносин, інтеграцію і одночасно криптографічну самостійність кожного з відомств/організацій.

Треба зазначити, що удосконалення національної інфраструктури ЕП є не тільки організаційно-технічним питання, а й питанням національної безпеки. Існуючі світові моделі інфраструктури ЕП можна поділити на ізольовану, ієрархічну, мережну, шлюзову [2].

Ізольований – це ЦСК, що має само-підписаний сертифікат, який не завіряється будь-яким іншим ЦСК вищого рівня. Тут ЦСК-домен складається тільки з ізольованого ЦСК та клієнтів-держателів сертифікатів, яким видано сертифікати цим ЦСК. Приєднати ізольований ЦСК-домен до деякої інфраструктури ЕП можна двома способами: через ієрархічні відносини, як Підпорядкований ЦСК; через відносини рівноправних ЦСК.

В першому випадку вимагається обов'язково перевипуск (заміна) АЦСК-сертифіката, а отже повний перевипуск усіх сертифікатів держателів. В другому випадку це не вимагається – усі сертифікати держателів залишаються чинними після приєднання ізольованого ЦСК до деякого довірчого ЦСК-домену через механізм кроссертифікації.

Ієрархічна модель – це об'єднання ЦСК-доменів в структуру зв'язного графа, тобто «дерева, що має одну головну вершину (кореневий ЦСК), з якої будується структура підпорядкованих ЦСК.

В ієрархічній моделі є один головний ЦСК, якому довіряють усі користувачі – це кореневий ЦСК, тобто для усіх держателів сертифікатів ієрархічної моделі шлях сертифікації починається є одного Кореневого ЦСК. Кореневий ЦСК не випускає сертифікатів для клієнтів, окрім виключно підпорядкованих ЦСК

Недоліки: компрометація «кореня» призводить до компрометації усього ієрархічного «дерева» та необхідності заміни усіх без виключення ключів держателів; єдиний кореневий ЦСК може бути неможливим із «політичних» міркувань – конкуренція, міжвідомчі перепони тощо.

Мережна модель – це модель встановлення довірчих відносин між окремими ізольованими та ієрархічними ЦСК-доменами без довірчого посередника. Довірчі відносини встановлюються через механізм крос-сертифікації.

Перевага: дуже еластична структура - VA=CT 1030B> B>G>: 4>2V@8 (=5 T48=0). 54>;V:: @>7H8@5==O H;OEC A5@B8DV:0FVW T 1V;LH A:;04=8< ?@>F5A><, =V6 2 VT@0@EVG=V9 <>45;V.

Шлюзова модель складається із окремих незалежних ізольованих та ієрархічних доменів, в тому числі інших структур зі шлюзовою моделлю, які об'єднані довірчими відносинами через довірчого посередника (шлюзовий ЦСК) за допомогою механізму крос-сертифікації. Така модель об'єднує переваги ієрархічної та мереженої моделей. Шлюзовий АЦСК не випускає сертифікатів для окремих користувачів, а тільки здійснює крос-сертифікацію між доменами на рівні однорангових відносин. Це

дозволяє встановити прості та прозорі відносини довіри між різними об'єднаннями користувачів.

Переваги шлюзової моделі в порівнянні з мережаною моделлю: можливість застосувати більш сувору процедуру реєстрації учасників, в тому числі з урахуванням вимог для ієрархічних ЦСК; при компрометації будь-якого з ЦСК-учасників, цей ЦСК інформує шлюзовий ЦСК і йому не потрібно «множити» інформацію на всіх ЦСК-учасників, так як цю функцію виконує шлюзовий ЦСК [3].

Національна ієрархічна інфраструктура ЕП повинна трансформуватися до шлюзово-ієрархічної моделі виходячи з питання національної безпеки та можливості забезпечення транскордонної взаємодії в світовому інформаційному просторі.

Список бібліографічних посилань

1. Про електронні довірчі послуги : Закон України від 05.10.2017 № 2155-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2155-19 (дата звернення: 30.10.2019)
2. Шевченко В. Л., Берестов Д. С., Зотова І. Г. Вибір моделі побудови інфраструктури відкритих ключів. *Збірник наукових праць Центру воєнно-стратегічних досліджень Національного університету оборони України.* 2014. № 1. С. 126–129. URL: http://nbuv.gov.ua/j-pdf/Znpcvsd_2014_1_21.pdf (дата звернення: 30.10.2019).
3. Бєлов С. В., Мартиненко С. В. Моделі побудови національної інфраструктури центрів сертифікації ключів та їх ризики // AMB Group : сайт. URL: http://www.itsway.kiev.ua/pdf/Model-CA_Risks.pdf (дата звернення: 30.10.2019).

Одержано 01.11.2019

УДК 681.3.06

Петро Сергійович Клімушин,
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Андрій Володимирович Білобров,
курсант 3 курсу факультету № 4 Харківського національного університету внутрішніх справ

Криптологія як провідний метод захисту інформації в сучасному суспільстві

У сучасних умовах захист інформації стає все більш актуальною і одночасно все більш складною проблемою. Це обумовлено як масовим застосуванням методів автоматизованої обробки даних, так і широким поширенням методів і засобів несанкціонованого доступу до інформації. Тому особливу роль в організації протидії потенційним загрозам займає підхід, при якому засоби захисту інформації використовуються комплексно, кожне у відповідності зі своїм призначенням. На сьогоднішній день існує багато алгоритмів шифрування, серед яких зустрічаються достатньо вдалі та широко використовувані, що розроблені не тільки спецслужбами, а й приватними особами.

Криптологія розділ науки, що вивчає методи шифрування і дешифрування інформації. Вона включає в себе два розділи: криптографію та криптоаналіз.

Криптографія займається розробкою методів шифрування даних, у той час як криптоаналіз займається оцінкою сильних і слабких сторін методів шифрування, а також розробкою методів, які дозволяють зламувати криптосистеми.

Шифруванням називається процес застосування шифру до повідомлення, що має бути захищеним. До основних характеристик сучасних методів шифрування можна віднести: довжину ключа, складність алгоритму перетворення даних, розмір даних, що обробляються, та ін.

Провідна роль у забезпеченні інформаційної безпеки в інформаційно-телекомунікаційних системах відводиться криптографії. До

найважливіших завдань, що вирішуються криптографією, відноситься забезпечення:

- конфіденційності відомостей, надаючи доступ до них лише з використанням спеціального ключа;

- цілісності інформації, що гарантує відсутність спотворень (видалення, заміни, модифікування) при передачі;

- автентифікації, перевіркою достовірності відправників і переданої інформації. Одним з найбільш поширених варіантів даної дії вважається доказ з нульовим дозволом, коли відправник підтверджує права, не надаючи одержувачу можливості використовувати отриману інформацію як особисту;

- ідентифікації, шляхом підтвердження суб'єктом, що передає відомості, своєї особистості. Доказ з нульовим розголошенням передбачає підтвердження особистих прав, без права розголосу одержувачем;

- нездійсненності відмови від авторства, для підтвердження обов'язків суб'єкта. Контракт, підписаний суб'єктами і підтверджений електронним підписом, має ті ж передбачені законодавством гарантії, що і підписаний звичайним способом.

Цілісність інформації та автентичність сторін досягається використанням хеш-функції та технології електронного підпису. Конфіденційність інформації забезпечується симетричним та асиметричним методами шифрування.

Методи симетричного шифрування – це метод, за яким ключі шифрування і розшифрування є або однаковими, або легко обчислюються один з одного, забезпечуючи спільний ключ, який є таємним.

Методи асиметричного шифрування – криптографічні алгоритми, в яких використовують пару ключів для кожного учасника протоколу – відкритий для шифрування і таємний для розшифрування, який не може бути обчислений з відкритого ключа за визначений час.

Для сучасної криптографії характерне використання відкритих алгоритмів шифрування, що припускають використання обчислювальних засобів. На сьогодні відомо більше десятка перевірених методів шифрування, які при використанні ключа достатньої довжини і коректної реалізації алгоритму, роблять шифрований текст недоступним для криптоаналізу.

Виділяють такі загальні вимоги для криптографічних методів захисту інформації: зашифроване повідомлення повинно піддаватися читанню тільки при наявності ключа; число операцій, необхідних для визначення використаного ключа шифрування по фрагменту повідомлення і відповідного йому відкритого тексту, повинно бути не менше загального числа можливих ключів; число операцій, необхідних для розшифрування інформації шляхом перебору можливих ключів повинно мати строгу нижню оцінку і виходити за межі можливостей сучасних комп'ютерів; знання алгоритму шифрування не повинно впливати на надійність захисту; незначна зміна ключа повинна призводити до значної зміни виду зашифрованого повідомлення навіть при використанні одного і того ж ключа; алгоритм має допускати як програмну, так і апаратну реалізацію, при цьому зміна довжини ключа не повинна призводити до якісного погіршення алгоритму шифрування.

В останні роки значний інтерес викликає квантова криптографія, вагоме місце в якій займає квантовий розподіл ключів. Квантова криптографія – метод захисту комунікацій, заснований на принципах квантової фізики. На відміну від традиційної криптографії, яка використовує математичні методи, щоб забезпечити секретність інформації, квантова криптографія зосереджена на фізиці, розглядаючи випадки, коли інформація переноситься за допомогою об'єктів квантової механіки. Процес відправки та прийому інформації завжди виконується фізичними засобами, наприклад, за допомогою електронів в електричному струмі, або фотонів у лініях волоконно-оптичного зв'язку.

Технологія квантової криптографії ґрунтується на принциповій невизначеності поведінки квантової системи – неможливо одночасно отримати координати і імпульс частинки, неможливо виміряти один параметр фотона, не спотворивши інший.

У результаті проведеного аналізу джерел з розглянутої проблеми виділені та розглянуті сучасні найбільш поширені методи криптографічного захисту інформації від несанкціонованого доступу. В новітніх інформаційних системах для шифрування повідомлень, які передаються, використовуються симетричні алгоритми шифрування, зважаючи на велику обчислювальну здатність асиметричних алгоритмів, їх застосовують для генерації та поширення сеансових ключів (використовується під час сеансу обміну повідомленнями). Усунути основні недоліки, властиві як симетричним, так і асиметричним методам криптографічного

захисту інформації, дозволяє їх комбіноване використання. Як відомо, у сучасних реальних криптосистемах шифрування даних здійснюється за допомогою «швидких» симетричних блокових алгоритмів, а завданням «повільних» асиметричних алгоритмів стає шифрування ключа сеансу. В цьому випадку зберігаються переваги високої секретності (асиметричні) та швидкості роботи (симетричні).

Таким чином, можна зробити висновок, що криптологія є незамінним фактором підтримання інформаційної безпеки як конкретної особи так і держави в цілому.

Одержано 01.11.2019

УДК 004.492

Ігор Володимирович Кобзев,
кандидат технічних наук, доцент, доцент кафедри природознавчих наук Харківського національного університету радіоелектроніки

Катерина Костянтинівна Петрова,
студентка групи ВПС 17-1
Харківського національного університету радіоелектроніки

Кібербезпека та відкриті дані

Відкриті дані (або open data) – підхід до зберігання інформації, згідно з яким набір даних має бути у вільному доступі, вільно використовуватися та розповсюджуватися. При цьому такі дані можуть використовувати як неприбуткові організації, так і комерційні установи [1].

Відповідно до Закону України «Про доступ до публічної інформації» публічна інформація у формі відкритих даних (відкриті дані) оприлюднюється для вільного та безоплатного доступу до неї. Відкриті дані дозволені для їх подальшого вільного використання та поширення [2].

У 2016 році Україна взяла на себе зобов'язання виконувати принципи Хартії відкритих даних: перш за все, робити урядові дані відкритими за замовчуванням. Відповідальним органом стало Державне агентство з питань електронного уряду.

В процесі реформування державні органи України публікують все більше відкритих даних з різних сфер діяльності. І ці дані допомагають зробити державний апарат прозоріше і посилити економіку країни.

Згідно з рейтингом Global Open DataIndex, який становить неурядова організація Open Knowledge International, в 2018 году Україна зайняла 31 місце (на 23 позиції вище в порівнянні з 2016-м) [4]. У рейтингу Open Data Barometer від World Wide Web Foundation Україна посіла 17 місце за 2017 рік, які підписали Міжнародну хартію відкритих даннях [3].

Для функціонування будь-якого сервісу необхідні дані. Велика кількість даних знаходиться у власності у держави, і держава не завжди поспішає ними ділитися.

Не все просто і з питаннями кібербезпеки відкритих даних. На жаль, сучасні цифрові технології розвиваються настільки стрімко, що архі-

тектори і розробники забувають пропрацювати ризики кібербезпеки і впровадити ефективні заходи їх зниження.

У звіті з кібербезпеки від компанії Cisco відзначається що хакери та держави створюють зловмисне програмне забезпечення із безпрецедентним рівнем складності та впливу; відбувається використання у військових цілях та на користь спецслужб хмарних сервісів та інших технологій, що використовуються зазвичай для законних цілей; для деяких творців шкідливого програмного забезпечення завдання полягає не в отриманні фінансової вигоди, а у руйнуванні інфраструктури та блокуванні систем цілих держав [1].

Фізично можливо два варіанти архітектури: Semi-automatic- дані завантажуються на портал відкритих даних вручну (через веб-інтерфейс) та Real-time – дані динамічно завантажуються з порталів відкритих даних органів державної влади або з інших веб-сервісів.

Архітектура Semi-automatic зазнає трьох ризиків:

- фальсифікація відкритих даних – зламавши портал, зловмисник може підробити відкриті дані, вплинувши тим самим на роботу цифрових сервісів, котрі їх використовують;

- підробка порталів – зловмисники можуть створити підробки порталів відкритих даних, представившись довіреним джерелом даних для цифрових сервісів.

- атака на бренд «відкриті дані» – розсилка спаму з пропозиціями отримати доступ до «розширених відкритих даних» в рамках «бета-тесту» або за невелику плату. Насправді листи міститимуть віруси і експлойти.

Архітектура Real-time зазнає трьох вищеописаним і двом специфічним ризикам:

- DDoS-атаки – відмова в обслуговуванні може привести до недоступності цифрових сервісів;

- комплексні цільові атаки – веб-сервіс може бути використаний як «точка входу» (entry point) в IT-інфраструктуру органу влади.

Вищеописані ризики можуть призвести до значних негативних соціальних і фінансових наслідків. Це може привести до нелегітимного використання відкритих даних в неправомірних цілях.

Сама наявність відкритих даних дозволяє бізнесу і суспільству звіряти новинні публікації і дослідження з незалежним офіційним джерелом, що істотно підвищує інформаційну безпеку.

Відсутність в відкритому доступі відомостей про архітектуру кібербезпеки відкритих даних не означає, що система заснована на відкритих даних цифрових сервісів може бути скомпрометована, а відповідні можливості для економічного зростання країни – втрачені.

Список бібліографічних посилань

1. Що таке відкриті дані та як ними користуватися. *Na chasi* URL: https://nachasi.com/2018/06/12/vidkryti-dani/ (дата звернення: 08.10.2019).
2. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2939-17 (дата звернення: 08.10.2019).
3. Україна вийшла на 17 місце в рейтингу відкритості даних // Українська правда : сайт. 21.09.2018. URL: https://www.pravda.com.ua/news/2018/09/21/7192760/ (дата звернення: 08.10.2019).
4. Place overview // Global Open Data Index. 2018. URL: https://index.okfn.org/place/ (дата звернення: 08.10.2019).

Одержано 10.10.2019

УДК 004.056.223

Ілля Сергійович Казмірчук,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

Володимир Анатолійович Євтушок,
старший викладач кафедри тактико-спеціальної
та фізичної підготовки факультету № 2
Харківського національного університету внутрішніх справ

Штучні нейронні мережі, їх використання у кіберзлочинності та боротьбі з нею

Останні роки ознаменувалися значним ривком у розвитку штучних нейронних мереж. І хоча перші спроби створити штучну нейронну мережу були ще у 40-х роках 20 ст., але саме останні події, пов'язані із ними, змусили суспільство широко говорити про них.

Для початку з'ясуємо, що ж таке нейронна мережа. Це математична програмна модель, побудована за принципом функціонування біологічних нейронних мереж – мереж нервових клітин живого організму. Головною особливістю таких мереж є те, що вони не програмуються в звичайному сенсі цього слова, а «навчаються» подібно до людського мозку. В процесі навчання нейронна мережа здатна виявляти складні залежності між вхідними даними й вихідними, а також здійснювати узагальнення.

Нейронна мережа під назвою Deepfake показує можливості даної технології та як саме їх можуть використовувати у кіберзлочинності. Наприклад, відео 2018 року, де показується екс-президент США Барак Обама та його слова змінені на ті що він ніколи не говорив, наприклад різко негативне звертання на адресу чинного президента США Дональда Трампа. При цьому мова та міміка людини відтворена нейронною мережею є надзвичайно правдоподібною та майже неможливо помітити підміну неозброєним оком. Таким чином, будь-яка людина коли-небудь знята на відео може стати ціллю злочинців, особливо політики, слова яких можуть викликати надзвичайно різку реакцію у суспільстві.

Так, зімітувавши лише голос людини, зловмиснику вдалося за допомогою нейронної мережі викрасти майже чверть мільйона доларів. Злочинець скопіював голос керівника потерпілої особи та вона, не запідозривши підміни, зробила переказ грошей. Це лише один з подібних випадків використання технології для злочинних дій, проте уже зараз можна сказати що вона ставить під сумнів доцільність використання технологій верифікації та ідентифікації за допомогою голосу особи.

Також нейронні мережі можуть значно спростити та прискорити роботу правоохоронних органів. Так звані Face detectors мережі здатні майже із сто відсотковою вірогідністю знайти людину за її фото у базі даних. При чому алгоритм дуже стійкий до змін – людині необов'язково дивитися в камеру, навіть можуть бути присутні деякі загороджуючі предмети: окуляри, борода або медична маска. Так вже у 2015 році китайська влада запустили проект по створенню національної бази даних на основі системи розпізнавання осіб. У країні будують мережу камер відеоспостереження, яку у Китаї називають найбільшою в світі: 176 мільйонів камер вже встановлені, та ще близько 450 мільйонів планується встановити до 2020 року. За задумом влади, до 2020 року штучний інтелект зможе за три секунди дізнатися в обличчя кожного з майже 1,4 мільярда жителів країни.

Отже, зважаючи на значний розвиток нейронних мереж, можна сказати що вони внесли свій вплив як на повсякденне життя людей, так і на розвиток кіберзлочинності й боротьби із нею. На мою думку правоохоронним органам України потрібно використати китайський досвід, та використовуючи такі мережі значно полегшити виконання деяких завдань, таких як пошук зниклих осіб, або ідентифікація особи у натовпі.

Одержано 28.10.2019

УДК 340:004

Вадим Анатолійович Коршенко,
кандидат юридичних наук, завідувач науково-дослідної лабораторії з проблем розвитку інформаційних технологій
Харківського національного університету внутрішніх справ

Гаджети – прихована загроза

Слово «гаджет» щільно ввійшло в наш побут. Ми живемо в часи коли нікого не здивуєш функціональним смартфоном, смарт телевізором, розумним порохотягом, холодильником чи годинником. Деякі автори навіть стверджують що ми живемо в епоху гаджетів [1; 2]. Що означає це модне слово зможе пояснити навіть дитина – це портативний пристрій, який об'єднує в собі кілька функцій. У перекладі з англійської gadget – пристосування, технічна новинка. Тож щоб перетворити звичайну річ на гаджет потрібно додати їй новітніх функцій, інтелектуальності, електронної функціональності, іншими словами коп'ютерізовати її. Тобто щоб стати гаджетом, звичайна річ (годинник, дитяча іграшка, телефон, лампа освітлення тощо) повинна бути оздоблена власним процесором що перетворює її на мікрокомп'ютер. З розвитком технологій ці вбудовані мікрокомп'ютери стають дедалі потужнішими, обладнуються телекомунікаційними модулями, що надає їм можливість отримувати та передавати інформацію. З'явився термін «Інтернет речей», як концепція комунікації та взаємодії гаджетів між собою та з навколишнім середовищем.

Здавалось би від цього людство отримає тільки вигоду. Однак ця тенденція несе дуже серйозні потенційні загрози. Брюс Шнайер, консультант з безпеки, який досліджує так звані «дірки» в інтернеті речей та описує їх, у своїй книзі «Натисніть сюди, щоб вбити усіх» зазначає, що він не налаштований цілком песимістично, але тут складно зберігати спокій, адже економічні та технічні цілі індустрії інтернету речей, не відповідають тим заходам безпеки які необхідні для забезпечення конфіденційності суспільства. Вбудувавши комп'ютер у звичні нам речі, компанії перетворюють весь світ у суцільну загрозу [3].

Проблема полягає в тому, що бізнес-моделі більшості бюджетних гаджетів не передбачають того рівню безпеки, який розповсюджується на традиційні інтернет пристрої. Бюджетні виробники гаджетів не

мають ані досвіду ані стимулу підтримувати достатній рівень безпеки своєї продукції. Тому інтернет речей – це синонім до словосполучення «погана безпека» [4].

Погана безпека несе в собі як ризики витоку особистих даних користувача гаджету, таких як стану здоров'я, місця знаходження, фотографій, відеозаписів, телефонних та навіть звичайних побутових розмов, особистої переписки, фінансових даних, тощо, так і створення на базі заражених гаджетів ботнетів, проведення ними DDoS-атак, незаконного видобутку криптовалюти та ін. За оцінками спеціалістів компанії ТрендМікро, світового лідеру в області рішень для захисту корпоративних даних і кібербезпеки для бізнесу, переважна більшість всіх зафіксованих атак в 2018 році були або спрямовані на гаджети, або виконані з їх допомогою.

Сьогодні існує велика кількість інтернет-ресурсів для пошуку вразливих гаджетів підключених до інтернету, і пошук та використання таких вразливостей набуває все більшої популярності між зловмисників які спеціалізуються на злочинах у кіберпросторі та в сфері високих технологій. Більшість людей навіть гадки не має яку загрозу можуть нести сучасні гаджети. Дуже велика частина гаджетів, особливо бюджетних гаджетів китайського виробництва, вже на етапі завантаження на них базового програмного забезпечення мають або серйозні «діри» в безпеці, або містять потенційно небезпечний програмний код. Необхідно доносити до пересічних громадян інформацію про зазначену небезпеку. Потрібно запроваджувати інформаційні програми державного рівня для донесення до населення інформації про потенційні загрози. Водночас з тим вже пройшли ті часи коли відносна безпека досягалась встановленням антивірусу на конкретний пристрій. В теперішніх умовах неможливо досягти успіху в забезпеченні безпеки локальним програмним забезпеченням, адже для більшості гаджетів воно не існує, а самі гаджети переважно не передбачають можливість його встановлення взагалі. Досягти безпеки у світі гаджетів та в інтернеті речей можна тільки використовуючи глобальні програмно-технічні комплекси захисту, які досить коштовні, та можуть бути встановлені переважно на телекомунікаційних вузлах. Звісно великі корпорації можуть дозволити собі встановлення корпоративних систем захисту. Захист від атак на гаджети пересічних громадян та відслідковування підозрілої активності таких гаджетів повинні здійснюватися на рівні операторів та провайдерів телекомунікаційних послуг. Законодавчо досить важ-

ко врегулювати такі відносини, однак існує можливість проводити заохочувальну політику в сфері захисту інформації і кібербезпеки, та надавати певні пільги чи преференції компаніям, які будуть встановлювати такі системи безпеки. В подальшому, в процесі підвищення обізнаності населення в сфері загроз в інтернеті речей та неминучому зростанні кількості гаджетів в кожному окремому домогосподарстві, наявність функцій програмно-технічного захисту на рівні оператора/провайдера буде напряму впливати на конкурентоспроможність його послуг серед населення, водночас підвищуючи безпеку в сфері захисту і кібербезпеки в цілому в Україні.

Список бібліографічних посилань

1. Мірошнікова А. Чому безграмотність стає нормою? Освіторія : сайт. URL: https://osvitoria.media/experience/chomu-bezgramotnist-staye-normoyu/?fbclid=IwAR2dTgAczAcVHUOfTo1ZtvHYahp-HDVEc132M8YA8diVrD9A0joUCMMkav8 (дата звернення: 22.10.2019).
2. Коптюг Н. Эпоха гаджетов // Учительская газета : сайт. 30.05.2017. URL: http://www.ug.ru/method_article/1165 (дата звернення: 22.10.2019).
3. Shnayyer B. Click Here to Kill Everybody : Security and Survival in a Hyper-connected World. W. W. Norton & Company, 2018. 288 p.
4. Manjoo F. A Future Where Everything Becomes a Computer Is as Creepy as You Feared// The New York Times. Oct 10, 2018. URL: https://www.nytimes.com/2018/10/10/technology/future-internet-of-things.html (дата звернення: 22.10.2019).

Одержано 23.10.2019

УДК 343.9

Микола Володимирович Мордвинцев,
кандидат технічних наук, доцент, провідний науковий співробітник науково-дослідної лабораторії з проблем розвитку інформаційних технологій Харківського національного університету внутрішніх справ

Олексій Володимирович Хлєстков,
старший науковий співробітник науково-дослідної лабораторії з проблем розвитку інформаційних технологій Харківського національного університету внутрішніх справ

Сергій Павлович Ницюк,
старший науковий співробітник науково-дослідної лабораторії з проблем розвитку інформаційних технологій Харківського національного університету внутрішніх справ

Стан і перспективи розвитку інформаційно-аналітичних систем для вирішення завдань правоохоронних органів

В Україні інтенсивна впроваджуються різні інформаційно-аналітичні системи для вирішення завдань правоохоронних органів. Наприклад, в Харкові з 2015 року ефективно використовується інтелектуальна система кримінального аналізу в реальному масштабі часу RICAS (Real-time Intelligence crime analytics system) [1]. Робота якій дозволила знизити рівень злочинності в Харківській області, збільшити розкриваність злочинів, дозволила прогнозувати криміногенну обстановку в регіоні. Система дозволила збільшити рівень розкриття злочинів по гарячих слідах, автоматизувати процес розкриття злочинів, виявити зони концентрації вуличної злочинності, збільшити швидкість реагування співробітників поліції, підвищити ефективність профілактичних заходів, оптимізувати маршрути патрулювання, здійснювати контроль за пересуванням і проводити координацію дій патрулів.

Система інтелектуального відеоспостереження в складі Єдиного аналітично-сервісного центру (UASC) в Головному управлінні Національної поліції в Донецькій області сприяє розкриттю злочинів, пошуку злочин-

ців та безвісно зниклих, протидії терористичним загрозам, проведенню оперативного налізу та прогнозуванню оперативних явищ, усуненню причин та умов аварійності на дорогах, контролю трафіку, фіксації порушенню правил дорожнього руху, оцінки загроз життю населення, своєчасне інформування екстрених служб про події [2].

Система дистанційного контролю психоемоційного стану людини (віброзображення) [3]. Ця система розроблялася на основі технології віброзображення компанією «Елсіс» (Санкт-Петербург) в ході виконання роботи «Створення системи дистанційного безконтактного сканування та ідентифікації психофізіологічного стану людини» за програмою «Антитерор» і «Розробка технології та створення засобів виявлення приховано переносяться людиною небезпечних предметів і контролю його психоемоційного стану». Системи віброзображення успішно експлуатуються на різних об'єктах транспортної інфраструктури Російської Федерації, Ізраїлю, Республіці Кореї. Застосовуються для забезпечення безпеки в метро, аеропортах, а також в місцях великого скупчення людей (торгово-розважальних центрів та ін.).

Принцип роботи системи віброзображення є накопичення міжкадрової різниці зображень, що характеризує енергетику рухів людини. Система працює в двох режимах. Це аналіз мікропереміщення голови людини, або аналіз всієї фігури людини, як єдиного об'єкта, що має фізичну та фізіологічну енергетику. Завдання аналізу зображення в режимі всієї фігури полягає в тому, щоб отримати максимальну інформацію про рухи всього тіла людини: його рук, ніг, тулуба і голови. Інформативним при цьому є, перш за все, динаміка його рухів, за весь час контролю.

Фіксоване розташування телевізійних камер передбачає, що порівнянню підлягають люди, які вчиняють приблизно однакові руху, наприклад, що йдуть прямо (в метро), що пред'являють квиток (на вокзалі), що ставлять багаж на контроль (в аеропорту) т. і. Якщо при цьому людина перебуває в аномальному стані (агресія, стрес, тривожність, ...), то динаміка його рухів помітно відрізняється від динаміки рухів людей в нормальному психоемоційному стані. Сукупність таких признаки і їх обробка комп'ютерною програмою є приводом задля ідентифікації об'єкта як небезпечного.

Розробка та встановлення подібних камер є перспективним напрямком для забезпечення безпеки населення України.

Список бібліографічних посилань

1. Узлов Д. Ю., Власов О. В., Онищенко Ю. М. Інтелектуальна система кримінального аналізу даних RICAS // Актуальні питання забезпечення публічної безпеки, порядку в сучасних умовах: поліція та суспільство – стратегії розвитку і взаємодії : тези доп. Всеукр. наук.-практ. конф. (м. Маріуполь, 18 трав. 2018 р.) / МВС України, ДВНЗ «Приазовський державний технічний університет», Донецьк. юрид. ін-т. Маріуполь : ДВНЗ «ПДТУ», 2018. С. 365–367.
2. Пефтієв О. В. Єдиний аналітичний сервісний центр головного управління Національної поліції в Донецькій області // Актуальні питання забезпечення публічної безпеки, порядку в сучасних умовах: поліція та суспільство – стратегії розвитку і взаємодії : тези доп. Всеукр. наук.-практ. конф. (м. Маріуполь, 18 трав. 2018 р.) / МВС України, ДВНЗ «Приазовський державний технічний університет», Донецьк. юрид. ін-т. Маріуполь : ДВНЗ «ПДТУ», 2018. С. 345–351.
3. Минкин В. А., Бунев Е. Г., Эргешова А. В., Титов В. Б. Виброизображение – система дистанционного контроля психоэмоционального состояния человека // DOCPLAYER : сайт. URL: http://docplayer.ru/28477871-Vibroizobrazhenie-sistema-distancionnogo-kontrolya-psihoemocionalnogo-sostoyaniya-cheloveka-minkin-v-a-bunev-e-g-ergeshova-a-v-titov-v-b.html (дата звернення: 13.10.2019).

Одержано 16.10.2019

УДК 004.382.001.25.343.3/7

Максим Анатолійович Ведмідь,
студент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Аналіз методів захисту інтернет- і мобільного банкінгу

Українці все частіше використовують безготівковий метод оплати, про що свідчить статистика Національного банку України. Так, за останні 9 місяців 2019 року частка безготівкових розрахунків в загальному обсязі операцій з використанням платіжних карток, емітованих українськими банками, зросла з 5% – до 44,3% [1].

За 2019 рік кількість операцій з використанням платіжних карток склала 2,8 млрд грн, а їх обсяг – 2 трлн грн. Ці показники, якщо порівнювати з минулим роком, зросли на 27,2% і 38,5% відповідно.

Кількість безготівкових операцій склало більше 2,2 млрд шт., З яких 1,1 млрд операцій (51,7%) припадало на розрахунки в торговельних мережах [1].

На сучасному етапі розвитку України є дуже велика кількість варіантів безготівкового розрахунку: смартфон, платіжна система, блокчейн систем. Більшість з вище перерахованих платіжних систем для оплати використовують банківські карти, та мають власні методи захисту платіжних даних.

Головна перевага для клієнтів, котрі використовують банківські картки це їх зручність. Головним недоліком стає велика кількість протиправних дій по відношенню до тримачів карт, карти постійно стають мішенню для зловмисників. За даними Асоціації членів платіжних систем ЕМА, в 2018 році шахраї вкрали в українців 669,6 млн гривень, з яких близько 160 млн гривень було викрадено за допомогою банкоматів. Більш 509 млн гривень шахраї отримали використовуючи соціальну інженерію. У кіберполіції відзначають, що в 2018 році в порівнянні з 2017 роком на 70% зросла кількість заяв про крадіжки з банківських карт. Всього у 2017 році було зареєстровано 3820 звернень [3].

Жодна фінансова установа не має в своєму розпорядженні універсального способу або технічного пристосування, здатного забезпечити 100-відсотковий захист карт від зазіхань зловмисників. Більшість банків фінансово не спроможні організувати власні процесингові центри, які зможуть підтримувати достатній рівень безпеки. В зв'язку з цим банки використовують сторонні процесінгові центри, в наслідок чого операції з платіжними картками більш захищені та правоохоронним органам легше викрити шахрайські операції.

Найбільш поширені фінансові злочини з банківськими картами умовно можна розділити на дві категорії. Перша – це крадіжка даних банківської карти за допомогою стороннього технічного забезпечення. Друга – це використання зловмисниками соціальної інженерії для отримання обманним шляхом даних банківських карт та інших даних, котрі допоможуть в скоєнні противоправних дій.

Методи шахрайства, котрі можна віднести до першої категорії.

1. Крадіжка даних банківської карти при здійсненні операцій в банкоматі шляхом установки зчитувальних пристроїв (скіммінг, шиммінг).

2. Отримання доступу до картрахунку шляхом фішингу, вивідування даних обманним шляхом.

3. Використання спеціальних пристосувань для блокування пластикової карти в банкоматах (траппінг).

Методи шахрайства, котрі можна віднести до другої категорії.

1. Зловмисники телефонують власнику карти представляючись працівниками банку. Дзвінок може бути здійснений як з звичайного незарезервованого банком номеру так і з банківського. Шахраї застосовують методи підміни номера за допомогою SIP/VOIP телефонії. Зловмисники зазвичай повідомляють клієнта про блокування його карти, або про «Підозрілу транзакцію». Іноді, коли зловмисник співробітник банку, він має доступ до приватних даних клієнтів, а саме:кількість грошей на рахунку, номери телефонів, що прив'язані до рахунку та інше. У наслідок чого зловмисники вимагають повідомити їм дані банківської карти, чи даних онлайн кабінету для ідентифікації користувача та урегулювання проблеми.

2. За допомогою підміни номеру зловмисники здійснюють дзвінки безпосередньо з різних фінансових організацій. Крім того, попутно вам навіть можуть приходити «підтверджуючі» легітимність співрозмов-

ника СМС. Ввічливий співробітник повідомляє, що з вашої карти були списані кошти і система безпеки банку маркувала його «підозрілим». Раптово з'ясовується, що на скасування переведення у вас є всього 10 хвилин і для скасування потрібно назвати код, який вам прийде за допомогою СМС. Звичайно, цей код – для проведення транзакції, тільки він зловмисникам і потрібен.

3. Також є повністю автоматизований спосіб здійснення противоправних дій по відношенню до клієнтів банку. Клієнт завантажує різні додатки з непідтверджених джерел, в наслідок чого заражає свій смартфон вірусом. Вірус в свою чергу виконує крадіжку платіжних даних та організовує переадресацію СМС та дзвінків з пристрою жертви на пристрій зловмисника. Такі дії вірусу дають змогу зловмисникам використовувати платіжні інструменти без відома власника рахунків.

Щоб мінімізувати ризики попадання фінансових даних до рук шахраїв та в перспективі викрадення даних з картки, розглянемо способи захисту цієї інформації:

1. Використання технології SMS-інформування власників. При використанні цього методу клієнт має можливість відстежувати всі операції з його банківською карткою і відмовити у вчиненні несанкціонованого трансакції. Недоліками SMS-інформування є те, що не всі клієнти усвідомлюють його ефективність і виявляють бажання на підключення даного сервісу, а у банку відсутні законні права підключити клієнта примусово.

2. Впровадження технології додаткової ідентифікації користувача системи дистанційного банківського обслуговування, використання надійних алгоритмів шифрування електронно-цифрового підпису для підтвердження фінансових операцій.

3. Застосування чіпових технологій VSDC в процесі випуску міжнародних банківських карт, найефективнішого способу захисту від скіммінгу (крадіжки персональних даних при обслуговуванні в банкоматі).

4. Управління емітентськими обмеженнями (автоматичну відмову в операції на стадії авторизаційного запиту) за операціями, проведеними в торгово-сервісній мережі та Інтернет-магазині, які відносяться банком до ризикових точках.

5. Використання спеціальних програмних систем Fraud-моніторингу, що дозволяють за допомогою критичних правил проводити аналіз і

виявляти шахрайські операції в процесі обігу банківських карт з більшою ймовірністю [4].

Запропоновані методи не можуть гарантувати стовідсоткової безпеки платіжних даних, але можуть значно знизити ризик противоправних дій по відношенню до клієнтів банку. Також подібні заходи дають змогу правоохоронним органам отримати більш повний обсяг інформації про зловмисників.

Список бібліографічних посилань

1. Украинцы стали чаще использовать безналичный расчет // delo.ua : сайт. URL: https://delo.ua/econonomyandpoliticsinukraine/za-9-mesjacev-ukraincy-rasschitalis-po-beznalu-n-348030 (дата звернення: 24.10.2019).
2. Мошенничество с банковскими картами, что такое кардинг, скимминг и шимминг // Fingramota.org : сайт. 11.06.2013. URL: http://www.fingramota.org/bezopasnost/v-bankakh-i-s-kred-kartami/item/88-moshennichestvo-s-bankovskimi-kartami-chto-takoe-karding-skimming-i-shimming (дата звернення: 24.10.2019).
3. Как с вашей карты могут украсть деньги: пять актуальных схем // Лига.Финансы : сайт. 01.02.2019. URL: https://finance.liga.net/personal/article/kak-s-vashey-karty-mogut-ukrast-dengi-pyat-aktualnyh-shem (дата звернення: 24.10.2019).

Одержано 25.10.2019

УДК 004.492.3

Микита Андрійович Єременко,
студент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Метод двофакторної автентифікації як засіб боротьби з шахраями в мережі інтернет

Завдяки розвитку мережі Інтернет, глобального покриття бездротовими мережами, а також збільшенню їх швидкості, кількість користувачів мережі Інтернет значно зростає кожного року. В Україні, за даними дослідження, станом на 2019 рік проживає 25,6 мільйонів Інтернет-користувачів, що складає 58% всього населення [1].

У наш час, майже у кожного користувача банківських послуг є доступ до онлайн-банкінгу, а деякі навіть зберігають увесь свій капітал на банківських рахунках до яких є доступ через мережу Інтернет. У вересні 2019 року обсяг грошей на гривневих рахунках в українських банках виріс на 3,1% – до 571,8 млрд грн [2]. Люди зберігають більше 290,78 млрд грн на своїх поточних банківських рахунках, до яких є доступ за допомогою Інтернет-банкінгу або мобайл-банкінгу [3]. У 2019 році зареєстровано близько 6000 злочинів, скоєних в сфері використання високих інформаційних технологій. З них майже тисяча – злочини, скоєні в сфері кібербезпеки [4]. Для захисту від несанкціонований доступу до банківського акаунту через Інтернет або мобільний банкінг передбачено багато систем ідентифікації користувача. Ці системи забезпечують достатній захист від доступу шахраїв, але зазвичай вони не включені без завдання. Для значного зменшення можливості кібератак шляхом фішингу, брутфорсу, соціальної інженерії та ін. дієвим рішенням стане встановлення двофакторної автентифікації.

Двофакторна автентифікація – це різновид багатофакторної автентифікації, яка полягає у підтвердженні особистості користувача за допомогою двох, незалежних один від одного, факторів. Першим фактором зазвичай є пароль або PIN-код[5].

Розглянемо існуючі фактори автентифікації:

1) знань – що знає користувач (ПІН, пароль, кодове слово, відповідь на секретне питання і т. д.);

2) власності – що належить користувачеві (ключ, паспорт, смарт-картка, маркер безпеки, USB флеш, смартфон та інший мобільний пристрій);

3)біометрії – це частина користувача (відбитки пальців, райдужна оболонка, голос, геометрія обличчя);

4) розташування – місцеперебування людини (наприклад, IP-адреса або супутникова навігаційна система);

5) часу – певний період часу під час якого ви можете увійти в систему.

Двофакторна автентифікація у багатьох сучасних сервісах встановлена за замовчуванням. На великій кількості криптогаманців її неможливо вимкнути.

Багато людей вже стикалися з двофакторною перевіркою, наприклад, коли користувач спробує увійти у свою сторінку в соціальній мережі з іншого комп'ютера або телефону і в цей момент, служба, підозрює, що це спроба несанкціонованого доступу, та вимагає у користувача ввести код, який був надісланий на телефон.

Слід розуміти, що двофакторона автентифікація це не завжди гарантія повної безпеки. Є досить багато методів взлому двофакторної автентифікації, деякі з них складні і дорогі,а деякі достатньо примітивні.

Розглянемо найбільш вживані методи взлому:

1. Соціальна інженерія – маніпулювання людьми через виконання дій, або розголошення конфіденційної інформації іншим способом, ніж як через засоби технічного руйнування баз даних[6].

2. Фішинг – вид шахрайства побудований на надсиланні листа, ніби від банку чи іншої установи, в якому міститься посилання де пропонується ввести код двофакторної автентифікації чи надати біометричні данні.

3. Перехоплення смс чи дзвінка з кодом підтвердження – код автентифікації надходить до телефону користувача він перенаправляється на пристрій зловмисника.

4. Використання cookies-файлів – заволодіння cookies-файлами жертви та подальше їх використання. В cookies-файлах зберігається ідентифікаційна інформація. На багатьох ресурсах за наявністю cookies користувачу не потрібно вводити пароль чи код двофакторної автентифікації.

5. Крадіжка, підробка приладу чи іншого фактору автентифікації – метод який найчастіше використовується для обходу двофакторної автентифікації. Це може бути крадіжка телефону, ключ-картки, також можлива підробка біометричних даних людини.

В результаті аналізу були розглянуті методи двох факторної автентифікації, як засіб боротьби з шахраями в мережі інтернет. Був проведений порівнювальний аналіз найпопулярніших факторів та методів автентифікації.

В результаті роботи, було виявлено, що найбільш безпечний фактор це біометрія. Біометрія завжди знаходиться поряд зі користувачем і її важко викрасти. Її можливо підробити, але це достатньо складний процес яких потребує великих фінансових вкладань. Потрібно розуміти, що двофакторна автентифікація не забезпечує стовідсоткового захисту, але є найкращім засобом для запобігання несанкціонованого входу. Для більшої безпечності можливо встановити багатофакторну автентифікацію. Вона перевіряє одночасно три чи більше факторів. Тому для значного зменшення вірогідності несанкціонованого входу до особистих кабінетів з важливою інформацією, таких як онлайн чи мобайл банкінг, електронна поштова скринька, соціальні мережі, онлайн-кабінети різних фінансових організацій, потрібно використовувати усі вбудовані в ці системи засоби захисту, особливо багатофакторну автентифікацію. Розуміння принципів механізмів, недоліків і вразливостей роботи двофакторної автентифікаціі значно полегшать правоохоронним органам процес ідентифікації зловмисника, а також дасть змогу отримати доступ до їх акаунтів.

Список бібліографічних посилань

1. У 2018 інтернет-користувачів стало 4 млрд, з них понад 3 млрд користуються соцмережами – дослідження // hromadske : сайт. URL: https://hromadske.ua/posts/u-2018-internet-koristuvachiv-stalo-4-mlrd-z-nih-ponad-3-mlrd-koristuyutsya-socmerezhami-doslidzhennya (дата звернення: 08.10.2019).
2. В НБУ сообщили, сколько денег держат украинцы в банках // delo.ua : сайт. 10.10.2019. URL: https://delo.ua/econonomyandpoliticsinukraine/v-nbu-soobschili-skolko-deneg-derzhat-ukraincy-v-359118/ (дата звернення: 08.10.2019).

3. Сколько денег украинцы держат в банках (инфографика) // finance.ua : сайт. 23.10.2019. URL: https://news.finance.ua/ru/news/-/458606/skolko-deneg-ukraintsy-derzhat-v-bankah-infografika (дата звернення: 08.10.2019).
4. Кибератаки на Украину и разоблачение хакеров: полиция подвела итог за год. URL: https://www.segodnya.ua/ukraine/kiberataki-na-ukrainu-i-razoblachenie-hakerov-policiya-podvela-itog-za-god-1199708.html (дата звернення: 09.10.2019).
5. Двухфакторная аутетификация // ITpedia : сайт. URL: https://ru.itpedia.nl/2018/09/10/two-factor-authenticatie-2fa/ (дата звернення: 10.10.2019).
6. Немного о 2FA: Двухфакторная автентификация // habr : сайт. 25.02.2016. URL: https://habr.com/ru/company/1cloud/blog/277901/l (дата звернення: 10.10.2019).
7. Демчук В. П. Соціальна інженерія: виклики та перспективи боротьби в українському контексті // Українське право : сайт. 01.11.2017. URL: https://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_demchuk_Social_engineering_perspectives_of_the_struggle_in_ukrain/ (дата звернення: 10.10.2019).

Одержано 25.10.2019

УДК 004.492.3

Євгеній Романович Лоцман,
студент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Методи деанонімізації як засіб виявлення правопорушників

Звичайний користувач не підозрює наскільки глибоко Всесвітня мережа вбудована в суспільство, і що, крім усього корисного, Інтернет несе об'єктивні ризики для користувацької безпеки. Кожен намагається зберегти свої дані в недосяжному для інших вигляді, через це збільшується кількість методів анонімізації і людей які намагаються нею скористатися. Серед звичайних користувачів можуть бути і зловмисники, тому правоохоронним органам дуже важливо мати в своєму арсеналі інструмент для деанонімізації.

Якщо говорити про анонімізацію, то – це спосіб ухилення від автентифікації [1], а визначення для деанонімізація – процес встановлення особи користувача в мережі або справжнього місця виходу в мережу. Розкриття проявляється в публікації особистих даних, найчастіше під цим розуміється публікація реальних фотографій анонімуса, в інших випадках – це публікація повних відомостей про людину.

В мережі Інтернет зловмисники захищені програмними засобами забезпечення анонімності. Більшості користувачів це надає відчуття безпеки і впевненості в тому що, до них не дістатися правоохоронцям і вони не будуть покарані за їх проступки. Наступні методи деанонімізації допомогли правоохоронним органам спростувати теорію безкарності:

1. Фізичний доступ і комп'ютерна криміналістика – шляхом фізичного доступу можна отримати багато інформації про носії і власника інформації. Сучасні засоби дозволяють правоохоронцям відновлювати видалені дані з оперативної пам'яті. Далі в хід йде аналіз отриманих даних і зіставлення їх з уже наявними зачіпками з мережі.

2. Поштова система – головною проблемою чорного ринку донині залишається спосіб доставки. Придбані наркотики і зброю потрібно десь і якось забрати, що представляє в своєму роді велику проблему.

Відомо, що улюбленим поштовим сервісом Сноудена був Lavabit. Уряд США зажадав від творця Lavabit Ладара Левісона передати ключ шифрування за протоколом SSL, який використовувався для криптографічного захисту даних на серверах Lavabit. Творець сервісу Ладар Левісон зволів закрити Lavabit, а не виконувати вимогу американських правоохоронців про стеження за своїми користувачами [2].

3. Операції під прикриттям – завдяки стрімкому розвитку засобів анонімізації і головному правилу в даркнета – анонімність перш за все, визначити хто на тому, протилежному, кінці мережі представляє велику трудність. Ця трудність дозволяє силовикам займати позицію продавця або покупця в мережі і тим самим деанонімізувати зловмисника.

4. Хакерство – в мережі існують білі і темні хакери. Новим напрямком в боротьбі є – взяття під контроль сайту з продажу або наприклад сайту з дитячою порнографією. Найгучнішим прикладом є операція голландських поліцейських, які взяли під контроль майданчик торгівлі наркотиками і жили життям донорів протягом декількох місяців, це дозволило їм виявити велику кількість IP-адрес і деанонімізувати більшу частину як користувачів так і постачальників.

5. Відкрита інформація – жити повним життям в реальності і залишатися анонімним в мережі нереально. Кожна дія, кожен запит в браузері, кожен клік – все це фіксується особливо у соціальних мережах Instagram або Facebook.

6. Телеметрія – це спосіб збору інформації про користувача для поліпшення якості додатку. Тільки грань між телеметрією і кібершпіонажем занадто тонка. Телеметрія – це коли всі дані користувача збираються без прив'язки до особистих даних та геопозиціунування.

7. Трекінг – це визначення місця розташування рухомих об'єктів в часі за допомогою зібраних даних. Існують випадки коли відомий лише MAC-адрес ноутбука зловмисника. В такому випадку сильно допомагає трекінг пристроїв.

З причини мережної загрози і активності країн світових лідерів в Інтернет просторі, кіберполіція в Україні починає стрімко розвиватися. Цей орган має величезний потенціал і вже розкрив велику кількість злочинних організацій. Яскравим прикладомі є викриття міжнародного хакерського угрупування «Cobalt». Працівники Київського управління кіберполіції Департаменту кіберполіції встановили причетність 30-річ-

ного мешканця Києва до розробки вірусів, кібершпигунства та продажу персональних даних громадян з усього світу [3].

Деанонімізація є потужною зброєю в руках поліцейських та хакерів. Вона дозволяє викрити зловмисників, але також дозволяє зловмисникам красти і продавати дані користувачів мережі Інтернет. Уряд України вчасно усвідомив важливість даного напрямку і збільшив фінансування служб інформаційної безпеки, що призвело до часткової нормалізації Інтернет простору.

Кожен користувач бажає залишатися анонімним тим самим дозволяє зловмисникам ховатися в натовпі, це розсіює увагу кіберполіції. Більш тісне співробітництво з іноземними службами інформаційної безпеки дозволяє українським правоохоронцям перейняти досвід і навести лад у кіберпросторі власної держави.

Список бібліографічних посилань

1. Анонимность, безопасность и цензура в Интернете // SecureVPN : сайт. 16.02.2017. URL: https://www.securevpn.pro/rus/blog/view/4 (дата звернення: 24.10.2019).
2. Бонларэв О. До біса ЦРУ! Легендарний сервіс електронної пошти Lavabit воскрес і готовий стати кошмаром спецслужб // НВ : сайт. 24.01.2017. URL: https://techno.nv.ua/ukr/gadgets/do-bisa-tsru-legendarnij-servis-elektronnoji-poshti-lavabit-voskres-i-gotovij-stati-koshmarom-spetssluzhb-530178.html (дата звернення: 24.10.2019).
3. Кіберполіція викрила українського хакера у взламі комп'ютерів світових банків та готелів // Національна поліція : офіц. сайт. 26.03.2018. URL: https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-vikrila-ukrajinskogo-xakera-u-vzlami-komp-yuteriv-svitovix-bankiv-ta-goteliv/ (дата звернення: 24.10.2019).

Одержано 26.10.2019

УДК 004.728:519.87

Олександр Олександрович Можаєв,
доктор технічних наук, професор, професор кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Хазім Рахім Наєм,
Іракський дослідницький інститут, Багдад, Ірак

Метод розподілу мережного ресурсу гібридної комп'ютерної геоінформаційної мережі МВС України з використанням технології MIMO

Сучасний рівень розвитку систем моніторингу надзвичайних ситуацій, а також досить складна криміногенна і політична ситуація в країні вимагають значного покращення системи криміногенного моніторингу України. Ця система повинна включати в себе підсистему збору первинної інформації в Україні (відповідні стаціонарні і мобільні пости, вузли і центри), підсистему передачі інформації як в рамках підсистеми збору інформації, так і в основній системі криміногенного моніторингу, а також оперативно-аналітичний центр, в який надходить найбільш важлива первинна інформація з локальних і регіональних центрів збору і обробки інформації.

Найбільш перспективними методами обробки і засвоєння подібних об'ємів інформації, на сьогодні, являються методи, грунтовані на використанні комп'ютерних геоінформаційних технологій. Використання геоінформаційних систем (ГІС), що дозволяють проводити одночасний аналіз багатовимірних даних з використанням цифрових карт, спрощує процедури екологічного прогнозу і оцінку комплексної дії на природне середовище, робить можливим оперативне виявлення аномалій і вжиття необхідних заходів для їх усунення.

Система криміногенного контролю, що реалізовує завдання безпеки регіону, повинна базуватися на мережній обчислювальній системі (МОС), що управляє, побудованій із застосуванням ефективних програмних і технічних засобів. екологічного моніторингу. Усі результати вимірів в

автоматичному режимі передаються в центр моніторингу і контролю промислових викидів регіону. Обчислювальну систему екологічної і техногенної безпеки регіону, що управляє, можна представити, як мережний комплекс, що об'єднує вимірювальні пристрої і контролери пунктів моніторингу, робочі станції центру моніторингу між собою, а також з рівнем управління регіоном.

Особливістю мережної МОС частина підмереж є безпровідною, що обумовлено особливостями місцерозташування ділянок земної поверхні, що піддаються моніторингу. Попри те, що безпровідні мережі використовуються достатньо довго, все ж завдання підвищення якості обслуговування такими системами є актуальній.

Великі надії в рішенні цієї задачі пов'язані з використанням так званих MIMO- технологій (MultipleInput – MultipleOutput, множинний вхід – множинний вихід). MIMO- принцип дозволяє зменшити число помилок при радіообміні даними (BER) без зниження швидкості передачі в умовах множинних перевідбиттів сигналів.

У доповіді наводиться аналіз алгоритмів та методів обробки сигналів, які використовуються в MIMO технологіях. Пропоновані алгоритми дозволяють досягти значного (до 15–20 %) збільшення пропускної спроможності мережі передачі даних ГІС системи криміногенного моніторингу МВС України, особливо для ситуації поширення інформації в складних умовах, за рахунок зниження помилок передачі даних.

Одержано 01.11.2019

УДК 651.34

Сергій Геннадійович Семенов,
доктор технічних наук, професор, завідувач кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

Денис Геннадійович Волошин,
аспірант кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

В'ячеслав Вадимович Давидов,
кандидат технічних наук, доцент, доцент кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

GERT-мережа виконання польотного завдання БПЛА в умовах зовнішніх впливів

В даний час безпілотна авіація є одним з найбільш перспективних напрямків в авіації. Так за оцінкою аналітичної компанії Teal Group, до 2020 року, обсяг ринку безпілотних літальних апаратів (БПЛА) виросте до 15,1 мільярдів доларів США. У той же час, підвищення попиту на БПЛА, а також їх використання для вирішення ряду складних і важливих завдань, як у цивільній, так і у військових сферах, істотно підвищує інтерес до цих технічних комплексів з боку зловмисників. Особливо почастішали випадки кібератак активного спуфинга (перехоплення управління).

У доповіді представлена GERT-мережа виконання польотного завдання БПЛА в умовах зовнішніх впливів. Облік ряду найбільш важливих складових процесу виконання польотного завдання дозволило максимально наблизити прототип даного процесу до реальних умов виконання поставленої БПЛА завдання і підвищити точність результатів моделювання.

Розв'язана задача математичної формалізації GERT-мережі виконання польотного завдання БПЛА в умовах зовнішніх впливів. Результатами

формалізації стали вирази для розрахунку щільності і функції розподілу випадкової величини часу виконання завдання БПЛА.

Проведено аналіз і дослідження отриманих результатів моделювання. Виявлено, що практична цінність розробленої моделі полягає в можливості прогнозування процесу виконання польотного завдання БПЛА, виходячи із заданих характеристик зовнішніх впливів (інтенсивності, ймовірності та ін.).

Одержано 01.11.2019

УДК 651.34

Сергій Геннадійович Семенов,
доктор технічних наук, професор, завідувач кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

Єлизавета Владіславівна Мелешко,
кандидат технічних наук, доцент, докторант Центральнукраїнського національного технічного університету

Анушірван Рашидінія,
аспірант кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

Аналіз характеристик безпеки рекомендаційних систем і вдосконалення моделі прогнозування змін подоби їх користувачів

Рекомендаційні системи (РС) на сьогоднішній день є потужним інструментом для цифрового маркетингу товарів та послуг. Часто вони застосовуються на веб-ресурсах з великою кількістю користувачів та контенту. В такому разі в процесі роботи рекомендаційної системи може виникати дефіцит ресурсів та зменшення якості їх роботи.

Аналіз основних критеріїв оцінки РС дозволив представити основні характеристики якості їх роботи (див. рис. 1.).

Кожна з цих характеристик суттєвим чином впливає на якість рекомендаційної системи, однак слід зауважити, що у зв'язку зі збільшенням кількості кібератак за допомогою соціальним мереж та рекомендаційних систем суттєво збільшується актуальність забезпечення характеристик безпеки. Серед них визначимо робастність до атак накручування рейтингів в рекомендаційних системах.

Проведені дослідження показали, що на даний час існує ряд способів та засобів зменшення ризиків подобних кібератак, але теоретичного підґрунтя використання цих засобів, а також опису шляхів підвищення ефективності їх використання на даний час дуже мало.

Рисунок 1 – Основні характеристики якості роботи РС

Тому, актуальним стає питання розробки моделей та методів забезпечення захисту даних в рекомендаційних системах, зокрема моделей та методів оптимізації характеристик безпеки рекомендаційних систем.

В доповіді пропонується вдосконалена модель прогнозування змін подоби користувачів та адаптація РС до визначених трендів часових характеристик з метою підвищення характеристик робастності до атак накручування рейтингів.

Список бібліографічних посилань

1. Recommender Systems Handbook / eds: F. Ricci, L. Rokach, B. Shapira, P. B. Kantor. 1st ed. New York : Springer-Verlag New York, Inc., 2010. 842 p. DOI: https://doi.org/10.1007/978-0-387-85820-3.
2. Huba G. The Cold Start Problem for Recommender Systems. 2015. URL: https://www.yuspify.com/blog/cold-start-problem-recommender-systems/ (дата звернення: 30.10.2019).
3. Bernardi L., Kamps J., Kiseleva J., Mueller M. J. I. The Continuous Cold Start Problem in e-Commerce Recommender Systems. 2015. URL: https://www.researchgate.net/publication/280773072_The_Continuous_Cold_Start_Problem_in_e-Commerce_Recommender_Systems (дата звернення: 30.10.2019).
4. Мелешко Є. В., Семенов С. Г., Хох В. Д. Дослідження методів побудови рекомендаційних систем в мережі Інтернет. *Системи управління, навігації та зв'язку*. 2018. Вип. 1. С. 131–136. URL: http://nbuv.gov.ua/j-pdf/suntz_2018_1_29.pdf (дата звернення: 30.10.2019).
5. Мелешко Є. В. Проблеми сучасних рекомендаційних систем та методи їх рішення. *Системи управління, навігації та зв'язку.* 2018. Т. 4 (50). С. 120–124. DOI: https://doi.org/10.26906/SUNZ.2018.4.120.

Одержано 01.11.2019

УДК 651.34

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

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

Марія Євгенівна Сиротенко,
студентка Вроцлавського економічного університету (Польща)

Прогнозування часових витрат на розробку безпечного програмного забезпечення

Проведені дослідження показали, що в даний час на практиці для вирішення завдань прогнозування часових витрат на розробку безпечного програмного забезпечення (БПЗ) практично не використовуються сучасні методи інтерполяції та екстраполяції. Існуючі методики розрахунку пропонують тільки грубі оцінки, а необхідні для виконання завдань ресурси визначаються виключно на основі досвіду і суб'єктивної думки людей, що виступають в ролі експертів, які далеко не завжди є фахівцями в цій області. Крім того, при описі методології «дбайливого виробництва» (Kanban). Це часто призводить до незадовільної точності отриманих результатів оцінки термінів виконання (закінчення) різних етапів в рамках проекту розробки БПЗ.

Одним із шляхів вирішення поставленого завдання прогнозування є використання підходу, заснованого на оцінці часових витрат на окремі етапи розробки БПЗ, з урахуванням функцій залежно поточного числа активних дефектів додатка від часу, отриманих експериментальним шляхом, а також за допомогою математичного моделювання. Таке комплексне використання апріорних та апостеріорних даних має дозволити врахувати специфіку сучасних методик розробки БПЗ з можливою динамічною зміною (розширенням) рамок проекту за бажанням замовника або з інших причин.

Одержано 01.11.2019

УДК 651.34

Віталіна Миколаївна Сергієнко,
завідувач навчальною лабораторією кафедри «Обчислювальна техніка та програмування» Національного технічного університету «Харківський політехнічний інститут»

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

Михайло Олександрович Можаєв,
кандидат технічних наук, завідувач сектору комп'ютерно-технічних та телекомунікаційних досліджень Харківського науково-дослідного інституту судових експертиз ім. Засл. проф. М. С. Бокаріуса

Розробка протоколів розподілу доступу для захисту даних на основі можливих сценаріїв роботи системи обробки й управління запитами

На основі реальних вимог кінцевих користувачів (служб) до роботи центрів управління запитами (ЦУЗ), у результаті досвідів, розроблено п'ять можливих сценаріїв роботи кінцевих користувачів (служб). У вартість комплексного рішення ЦУЗ входить один (на вибір) з нижчеперелічених сценаріїв: прийом замовлень; довідкова інформація; прийом скарг/пропозицій; секретарська підтримка; віддалений секретар/віртуальний офіс.

Залежно від конкретних вимог кінцевих користувачів (служб) до роботи ЦУЗ, по окремій домовленості, можливо комбінувати дані сценарії, або розробити нові.

Сценарій роботи «Прийом замовлень» передбачає прийом, запис всіх даних, що відносяться до замовлення з наступним перенесенням даних на сторону підприємства (служби). Сценарій роботи «Довідкова інформація» передбачає пошук і надання інформації про продукти й послуги підприємства (служби) в зручному для клієнта вигляді, а також

підтримка гарячих ліній і рекламних акцій. Сценарій роботи «Прийом скарг/пропозицій» передбачає прийом і запис скарг/пропозицій клієнта, а також його контактної інформації. Секретарська підтримка є зручним програмним додатком для роботи секретаря. Здійснює прийом і розподіл вхідних повідомлень по необхідних відділах/співробітниках підприємства (служби). Сценарій роботи «Віддалений секретар/віртуальний офіс» є програмним додатком по роботі зі списком для обзвону (Preview dialing).

Все актуальніше стає подальше підвищення швидкості передачі даних в таких застосуваннях.

Великі надії в рішенні цієї задачі пов'язані з використанням так званих MIMO- технологій (MultipleInput – MultipleOutput, множинний вхід – множинний вихід). І хоча існуючі втілення MIMO- ідеї доки не завжди помітно прискорюють трафік на невеликих відстанях від точки доступу, вже доведено, що на великих видаленнях вони дуже ефективні. MIMO- принцип дозволяє зменшити число помилок при радіообміні даними (BER) без зниження швидкості передачі в умовах множинних відлунень сигналів.

Одержано 01.11.2019

УДК 004.056.5

Віталій Анатолійович Світличний,
кандидат технічних наук, доцент, доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Вразливість операційної системи Android

Американська компанія Nightwatch Cybersecurity (https://wwws.nightwatchcybersecurity.com), яка займається дослідженнями в області кібербезпеки, виявила критичну уразливість в операційній системі Android, причому у всіх її версіях старше 6.0. Як заявляють фахівці з компанії, знайдена в системі Android вразливість дозволяє отримати досить докладну інформацію про встановлених на мобільному пристрої додатках, конфіденційну інформацію про користувачів. Розкриття таких даних, як ім'я мережі Wi-Fi, BSSID, локальні IP-адреси, інформація про DNS-сервері і MAC-адресу пристрою відбувається без будь-якого дозволу з боку користувача і навіть без його відома. На перший погляд подібні дані здаються нешкідливими, проте з їх допомогою зловмисники можуть стежити за активністю користувачів в інтернеті і дізнаватися їх адреси проживання. Використовуючи ці дані, зловмисники за допомогою шкідливого програмного забезпечення можуть відстежити смартфон і навіть влаштувати атаку на бездротову мережу і інші підключені до неї пристрої. Завдяки уразливості Android хакерам також буде доступний весь вхідний і вихідний трафік на мобільному пристрої, логіни і паролі до облікових записів, а також особисті дані власника смартфона.

Вразливість пов'язана з внутрішньою функцією Android під назвою intents – «наміри», які використовуються для абстрактного опису операцій і дозволяють додаткам і операційній системі транслювати загальносистемні повідомлення, які можуть бути прочитані будь-якими додатками або компонентами. Ця функція дозволяє додаткам і самій операційній системі розсилати внутрішні повідомлення, доступні для читання всіма додатками і функціями на Android – пристрої. Як виявилося, мобільна операційна система від Google розкриває інформацію про Wi-Fi підключенні і Wi-Fi мережі через дві окремі функції intents – NETWORK_STATE_CHANGED_ACTION класу WifiManager і WIFI_P2P_

THIS_DEVICE_CHANGED_ACTION класу WifiP2pManager. Встановлені на пристрої додатки можуть прослуховувати ці intents і перехоплювати пов'язану з Wi-Fi інформацію, навіть якщо у них немає права на доступ до функції Wi-Fi. Фактично, дана вразливість дозволяє обійти систему дозволів Android. Зловмисники здатні обманом змусити користувача встановити невинне на перший погляд додаток, що збирає дані про Wi-Fi підключенні, а потім використовувати зібрані відомості для пошуку ідентифікаторів BSSID (таких як WiGLE або SkyHook) в доступних базах даних і виявлення домашньої адреси користувача.

Дана вразливість (CVE-2018-9489 докладніше тут: https://wwws.nightwatchcybersecurity.com/2018/08/29/sensitive-data-exposure-via-wifi-broadcasts-in-android-os-cve-2018-9489 /) зачіпає всі версії Android, в тому числі такі спеціалізовані операційні системи на зразок Amazon FireOS (для Kindle). Дослідники повідомили про неї компанії Google в березні поточного року, і компанія вирішила виправити вразливість, але тільки лише в версії Android 9.0 Pie. Згідно зі статистикою Google, вона встановлена поки на 0,1% всіх пристроїв на «Андроїд», а іншим користувачам, мабуть, доведеться змиритися – з більш старими версіями нічого робити не планується, так як, це буде серйозною зміною API. Звідси випливає практична рекомендація: для усунення даної уразливості користувачам слід виконати оновлення операційної системи до Android 9.0 Pie або більш пізньої 10 версії.

Одержано 25.10.2019

УДК 519.859

Andrii Mykhailovych Chuhai,
Doctor of Technical Sciences, senior scientific researcher, senior scientific researcher of the department of mathematical modeling and optimal design, A. Pidgorny Institute of Mechanical Engineering Problems of the National Academy of Sciences of Ukraine

Serhii Borysovych Shekhovtsov,
Candidate of Technical Sciences (Ph.D.), associate professor, associate professor of the department of information technology and cybersecurity, Kharkiv National University of Internal Affairs

Rogelio Corrales Diaz,
faculty of mechanical and electrical engineering, postgraduate division in systems engineering, Nuevo Leon State University (Monterrey, Mexico)

Application of parallel calculations in large scale optimization problems

In large-scale optimization problems of artificial intelligence, cybersecurity, robotic, as a rule, a feasible region is described by a huge number of nonlinear inequalities and variables. One of the important issues is developing state-of-the-art technologies that allow increasing the solution algorithm efficiency. The basic idea of the proposed technique is based on the decomposition algorithm that reduces the large-scale problem to a sequence of the sub-problems with significantly smaller dimension. The optimization strategy involves the following stages: generating of feasible starting points, sequential construction of feasible sub-regions; forming of the system of active ε-inequalities; searching for local extrema in the selected feasible sub-regions. It should be noted that, depending on the value of the decomposition parameter, a sequence of sub-problems can be quite large, and the computational time is also significant. This is because of forming sub-problem requires substituting the obtained starting point into the inequality system, which describes the original large-scale problem, and to separate from it a new sub-system of inequalities. Since the system of inequalities describing feasible region is determined by a large number of nonlinear inequalities, it takes a long time to calculate such inequalities and form a new sub-system.

The computational costs have been sought in the application of modern parallel computing technologies. Simply migrating a sequential program algorithm to a system with many processors without substantially reworking it does not generally accelerate the computation. An analysis of the subtask formation algorithm when searching for a local extremum showed that it supports both task parallelism and data concurrency.

The basic principle of the developed algorithm of parallelization of calculations in the formation of sub-tasks of local optimization is based on the fact that the used functions are max-min functions.

An algorithm for forming a subsystem that specifies the area of admissible solutions of each subtask can be represented as a graph in a tier-parallel form having four tiers. The tasks of the first three tiers support data parallelism, since they use the same computational procedures to execute them, but over different data sets. The fourth tier tasks support task parallelism, since the tasks of this tier are implemented by separate procedures.

In order to perform parallel calculations of the algorithm, it is necessary to ensure synchronization of the execution of parallel tasks of the second and third tiers, since the results of the procedures of these tiers depend on the results obtained on the third and fourth tiers, respectively.

To implement the presented scheme of parallel computing, modern parallel computing tools are used that provide the program with mechanisms for automatic generation of parallel computations, problem scaling, and synchronization.

Received 01.11.2019

УДК 651.34

Кассем Халіфе,
доктор філософії,
дослідник Сарептського технічного інституту (Ліван)

Удосконалений спосіб оцінки вразливості системного програмного забезпечення

У доповіді наводяться результати порівняльних досліджень та оцінки ефективності методу проектування програмних засобів комп'ютерних систем критичного застосування.

Удосконалено спосіб оцінки вразливості системного програмного забезпечення (СПЗ). Його відмінною рисою є врахування можливості масштабування процесу розробки програмного забезпечення шляхом впровадження фахівців безпеки (PersonNon, SecDev). Методика дослідження ефективності розробленого методу на основі ігрової моделі включає:

Крок 1. Аналіз ймовірних загроз СПЗ. Змістовна постановка задачі дослідження.

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

Крок 3. Складання рівнянь для чисельностей станів в диференційній формі відповідно до методу динаміки середніх.

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

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

Крок 6. Обчислення показників ефективності методу розробки СПЗ.

Кількісно ефективність розробленого методу можна визначити за допомогою показника втрат ΔZ_i по кожному засобу Z_i. Цей показник визначає величину відносної шкоди, заподіяної засобу Z_i в результаті зловмисних атак на СПЗ. При цьому, показник відносної шкоди може бути обчислений за формулою

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

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 та підготовка рекомендацій щодо вибору структури методології розробки СПЗ та стратегії її використання в фірмах.

Стан динамічної системи «ПЗ – ЗЛОВМИСНИК» в цілому з кожного моменту часу $t \in [t_0, t_N]$ характеризується системою звичайних лінійних диференціальних рівнянь, в якій, як змінні, розглядаються чисельності станів z_i, $i = 1 \ldots 6$.

Одержано 01.11.2019

УДК 343.13

Владислав Ігорович Школьніков,
викладач кафедри інформаційних технологій та кібербезпеки навчально-наукового інституту № 1 Національної академії внутрішніх справ (м. Київ)

Використання можливостей прикладного програмного інтерфейсу для аналізу криміналістичної інформації

Великі масиви даних, що містяться в правоохоронних органах, а також у відкритих джерелах (наприклад, в мережі Інтернет), потребують обробки та аналізу можливостями мов програмування.

Ми живемо в епоху, коли все записується, оцифровується та зберігається на чисельних серверах. Правоохоронним органам за згодою із уповноваженими особами доступні «великі дані», володільцями яких є гіганти соціальних медіа та інші державні або приватні організації. Злочинець є звичайною людиною, яка також використовує всі можливості сучасного інформаційного суспільства, а тому роль алгоритмів машинного навчання та штучного інтелекту у попередженні злочинності стає актуальним питанням. Створення таких алгоритмів можливе на основі якісних та кількісних даних, а також на ефективних припущенням вченого або програміста.

З розвитком національних баз даних правоохоронних органів, розвитком соціальних мереж з'явилася можливість об'єднувати та аналізувати у взаємозв'язку таку інформацію. На основі цього можливо будувати точні моделі злочинної діяльності (наприклад, звичайні люди будуть здійснювати гугл-пошук або розміщувати інформацію в соціальних мережах, яка опосередковано може свідчити про ризики злочинної діяльності).

На жаль, такі програми як Microsoft Excel, IBM i2 Analyst`s Notebook та інші подібні аналітичні продукти, які здебільшого використовуються в діяльності правоохоронних органів, мають обмежені можливості в питанні об'єму інформації, що обробляється та аналізується. Більш того,

практично неможливо автоматизовано отримувати інформацію, що міститься в мережі Інтернет, за допомогою даних аналітичних продуктів.

Тому для таких завдань – обробка та аналіз великого масиву даних, а також отримання інформації з мережі Інтернет – аналітики використовують спеціально створені для виконання таких завдань мови програмування, на кшталт Python.

Окрім аналізу даних та веб-скрапінгу за допомогою мов програмування також можливо отримувати інформацію з API вебсайтів.

Багато вітчизняних реєстрів мають API інтерфейс, що значно полегшує процедуру здобуття та аналізу відомостей, що містяться в них. Наприклад, API інтерфейс мають Єдиний державний реєстр юридичних осіб, фізичних осіб-підприємців та громадських формувань, Державний реєстр речових прав на нерухоме майно, Єдиний державний реєстр декларацій, Єдиний державний вебпортал відкритих даних, Єдиний вебпортал використання публічних коштів, портал відкритих даних Верховної Ради України тощо.

Прикладний програмний інтерфейс (англ. Application Programming Interface, скорочено API) – це сукупність засобів та правил, що вможливлюють взаємодію між окремими складниками програмного забезпечення або між програмним та апаратним забезпеченням. Простими словами це спеціальний алгоритм, який дозволяє власникам сайтів автоматично завантажувати інформацію.

На сьогодні Кабінетом Міністрів України прийнята Постанова від 21.10.2015 № 835 «Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних». Постановою КМУ від 20.12.2017 № 1100 були внесені зміни до вищевказаної Постанови.

Зокрема в даній Постанові зазначено перелік наборів даних, які підлягають оприлюдненню у формі відкритих даних (додаток № 4). В даних наборах міститься великий обсяг інформації, що може бути використаний правоохоронними органами під час досудового розслідування кримінального провадження.

Відповідно до Постанови КМУ від 21.10.2015 № 835 «Про затвердження Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних» розпорядник інформації протягом одного робочого дня після оприлюднення (оновлення) наборів даних на своєму офіційному вебсайті оприлюднює такі набори даних на своїй вебсторінці на Єдиному державному вебпорталі відкритих даних.

Крім того, за адресою www.spending.gov.ua розташовано Єдиний вебпортал використання публічних коштів, який є офіційним державним інформаційним ресурсом у мережі Інтернет, на якому оприлюднюють інформацію відповідно до вимог Закону «Про відкритість використання публічних коштів». За допомогою цього ресурсу можливо відслідковувати онлайн транзакції державних підприємств: Укрзалізниці, Укрпошти, Нафтогаза України, Київпастранса, Міжнародного аеропорту «Бориспіль» та ін.

В мережі інтернет створено Єдиний державний реєстр декларацій (https://public.nazk.gov.ua), який надає доступ до інформації про подані декларації у форматі JSON. Така можливість дозволяє оперативним працівникам в автоматизованому режимі виявляти осіб, в діях яких можливі ознаки корупційних правопорушень, а також оінювати корупційні ризики у певній сфері державного управління.

У даному контексті актуальним питанням боротьби з кіберзлочинами та торгівлею людьми є питання здобуття, обробка та аналіз інформації про транзакції з використанням криптовалюти з метою виявлення підозрілих операцій та ідентифікації кінцевих бенефіціарів (власників) криптовалюти, отриманої в результаті злочинної діяльності.

Список бібліографічних посилань

1. Школьніков В. І., Орлов Ю. Ю., Корнєйко О. В., Вознюк А. А. Здобуття доказової інформації з мережі Інтернет із використанням можливостей мови програмування Python : метод. рек. Київ : Нац. акад. внутр. справ, 2019. 52 с.
2. Зміни, що вносяться до Положення про набори даних, які підлягають оприлюдненню у формі відкритих даних : Постанова Кабінету Міністрів України від 20.12.2017 № 1100. *Офіційний вісник України*. 2018. № 15. Ст. 10.

Одержано 01.11.2019

УДК 004.056.57

Олександр Едуардович Шорский,
студент Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Володимир Якович Пєвнєв,
кандидат технічних наук, доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут»

Антивірусний захист локальної мережі як засіб боротьби з правопорушеннями в кіберпросторі

В умовах інформатизації суспільства, застосування засобів інформаційних і комунікаційних технологій стає все більш актуальною проблема забезпечення інформаційної безпеки (ІБ) людини, підприємства, організації, громади, суспільства та держави.

Згідно з [1], кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі.

Одночасно з розвитком комп'ютерної техніки виникли та продовжують розвиватися шкідливі програми, серед яких виділяються комп'ютерні віруси. Комп'ютерний вірус – це невелика, складна, ретельно складена і небезпечна програма, яка може самостійно розмножатися, переноситися на диски, прикріплюватися до програм, передаватися через мережу, порушують роботу комп'ютера. При цьому вона намагається виконати приховане самокопіювання в різні області виконуваних кодів інших програм, максимально захищається від виявлення і по завершенню «інкубаційного» періоду заявляє про себе не прогнозованими руйнівними діями [2].

В грудні 2015 року відбулася кібератака на енергетичні компанії України. Найбільше постраждали споживачі «Прикарпаттяобленерго»: було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин. Атака відбувалась із використанням троянської програми BlackEnergy. Водночас синхронних атак зазнали «Чернівціобленерго» та «Київобленерго», але з меншими наслідками. Загальний недовідпуск електричної енергії становив – 73 МВт•год (0.015 % від добового обсягу споживання України) [3].

Кібератака з використанням вірусу, який спочатку був названий Petya.A (пізніше – NotPetya), відбулася наприкінці червня 2017 року. Департамент кіберполіції стверджує, що хакерська атака за допомогою вірусу Petya почалася в Україні через оновлення програми M.E.Doc, яке вийшло о 10:30 27 червня[4]. За підрахунками спеціалістів збитки України в результаті кібератаки вірусу Petya склали 0,4 % ВВП України, що є більше за 300 млн. доларів [4].

З роками розвинулась індустрія антивірусного програмного забезпечення, і про вірусні атаки звичайним користувачам вже можна менше хвилюватися. Антивірус – це програма, яка виявляє й знешкоджує комп'ютерні віруси. Слід зауважити, що віруси у своєму розвиткові випереджають антивірусні програми, тому навіть у випадку регулярного користування антивірусів немає 100% гарантії безпеки [5].

Розробники антивірусів активно впроваджують нові технології антівірусобудування: Hostbased Intrusion Prevention System (HIPS), Sandbox, Virtual-based Intrusion Prevention System (VIPS). Ці технології дозволяють користувачеві активно моніторити процеси в системі і приймати рішення про допуск їх до різних функцій ОС.

На сьогодні все більш популярними стають методи проактивного захисту: HIPS та пісочниця. Ці дві конкуруючі технології активно інтегрують в своє ПЗ найпопулярніші антивіруси: NOD32 і Kaspersky Anti-Virus використовують HIPS, Avast Antivirus – пісочницю. Проактивні методи захисту є високоефективним засобом захисту від шкідливого ПЗ і можуть скласти вагому конкуренцію класичним, реактивним методам захисту, а в поєднанні з ними можуть значно підвищити ефективність антивірусних систем.

4 Cyberpolice Ukraine (2017-06-27): Це ПЗ має вбудовану функцію оновлення, яка періодично звертається до серверу http://upd.me-doc.com.ua за допомогою User Agent «medoc1001189». URL: https://twitter.com/cyberpoliceua/status/879772963658235904 (дата звернення: 20.10.2019).

В доповіді розглянуті проблеми захисту локальних мереж від вірусного програмного забезпечення. Антивірусний захист локальної мережі є складною проблемою, яка не зводиться до простого налаштування антивірусних продуктів. Як правило, потрібне створення окремої підсистеми. З технічної точки зору при розв'язанні даної проблеми особливу увагу слід приділити тестуванню придбаного антивірусного ПЗ, а також установці антивірусних пакетів на поштові сервери. Для забезпечення антивірусного захисту локальної мережі доцільно використовувати комбіновані системи (міжмережний екран, антивірус, пісочниця). Такий метод дозволить максимально зменшити вірогідність проникнення вірусів в локальну мережу та забезпечити безпеку даних, що зберігаються на персональних комп'ютерах.

Список бібліографічних посилань

1. Про основні засади забезпечення кібербезпеки України : ракон України від 05.10.2017 № 2163-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 20.10.2019).
2. Ленков С. В., Перегудов Д. А., Хорошко В. А. Методы и средства защиты информации : в 2 т. / под ред. В. А. Хорошко. Киев : Арий, 2008. Т. 1 : Несанкционированное получение информации. 464 с.
3. Zetter K. The Ukrainian Power Grid Was Hacked Again // Vice. Jan 10, 2017. URL: https://www.vice.com/en_us/article/bmvkn4/ukrainian-power-station-hacking-december-2016-report (дата звернення: 20.10.2019).
4. Аналіз регуляторного впливу // Державна служба спеціального зв'язку та захисту інформації України : офіц. сайт. 03.04.2018. URL: http://195.78.68.84/dsszzi/control/uk/publish/article?showHidden=1&art_id=288142&cat_id=38837&ctime=1522850564776 (дата звернення: 21.10.2019).
5. ТОП-10 комп'ютерних вірусів в історії. Ч. 2. URL: https://zillya.ua/top-10-kompyuternikh-virusiv-v-istori-chastina-2 (дата звернення: 21.10.2019).

Одержано 22.10.2019

РОЗДІЛ 4
КАДРОВЕ ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 343.1+004

Ірина Андріївна Манжай,
завідувач навчального відділу Харківського університету

Особливості використання web-квестів для навчання студентів

Під час проведення занять за різними дисциплінами науково-педагогічні працівники нерідко стикаються з проблемою слабкої активності студентської аудиторії, розсіюванням уваги через деякий час після початку викладення матеріалу, відволіканням тощо. Особливо це є актуальним для такої форми занять як лекція, а також в рамках розв'язання рутинних та складних завдань під час практичного навчання.

Для активізації пізнавальної діяльності під час навчання можуть бути застосовані ігри, і цей прийом вже достатньо давно відомий викладацькій спільноті. Разом з тим перенесення таких ігор у кіберсферу є достатньо рідкісним явищем в українських вишах. Одним з ефективних рішень, які можуть бути запроваджені для покращення навчання у досліджуваному контексті є застосування технології web-квестів. Особливо це є актуальним на заняттях, які передбачають навчання в комп'ютерних класах.

Особливостями практично відпрацьованої технології застосування веб-квестів є те, що під час їх проходження студенту:

1) дозволяється користуватися будь-якими джерелами інформації, що дозволяє нівелювати фактор простого копіювання інформації, оскільки завдання, подібні до квестових, в мережі знайти вкрай важко;

2) потрібно надати відповідь на конкретні питання, без яких неможливо пройти подальші завдання;

3) слід вирішити завдання, максимально наближені до конкретної життєвої ситуації, що дозволяє набути не тільки знання, але й навички;

4) засвоюються типові алгоритми дій в різних життєвих ситуаціях.

Таким чином, особа занурюється у віртуальну реальність та з використанням «тренажерів» засвоює майбутню професію.

Для створення веб-квестів можуть бути використані різні інструменти:

- спеціальні застосунки ігрового призначення (необхідність професійного програмування, негнучкість зміни сценарію);

- боти (необхідність мати базові знання та навички програмування, питання та декілька варіантів відповідей, які визначають розвиток сюжету);

- платформи для навчання (постійний розвиток виробником платформи, легкість зміни сценарію, можливості гнучкої оцінки курсантів /студентів, слухачів/).

Останній варіант, на нашу думку, є найбільш оптимальним, оскільки дозволяє за наявності базових знань та навичок роботи з комп'ютерною технікою при незначних затратах часу зробити цікавий та корисний для навчання продукт.

У якості прикладу описаної платформи можна назвати Google Classroom, яка об'єднує Google Drive, Docs, Sheets and Slides, Gmail, Calendar, спеціальний журнал оцінювання. Також вагомою перевагою цієї платформи є наявність спеціального мобільного застосунку для iOS та Android пристроїв, який може бути встановлено студентом для проходження квесту. Таким чином, сервіс Google Classroom є придатним для проведення дистанційного навчання, у тому числі для організації на його базі web-квестів.

Одержано 24.10.2019

УДК 343.1+004

Віталій Вікторович Носов,
кандидат технічних наук, доцент, професор кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Гейміфіковане навчання кібербезпеки та цифрових криміналістичних досліджень у виші

Стрімкий розвиток кіберпростору суспільства призвів до зросту потреби у фахівцях в галузі кібербезпеки. Аналіз [1] показав, що у 2019 році в Україні 51 виш здійснює підготовку бакалаврів за спеціальністю 125 Кібербезпека. Суттєва специфіка навчання прикладним дисциплінам за цією спеціальністю полягає у постійній необхідності швидкого оновлення великого масиву знань разом із швидким розвитком інформаційних технологій, і якщо теоретичні відомості більш-менш залишаються актуальними тривалий період, то практичні аспекти потребують переробки і нової розробки кожен семестр навчання.

Комплексний підхід до розробки навчальних практичних задач із пов'язаними між собою курсами з тестового проникнення до комп'ютерних систем і цифрових криміналістичних досліджень (digital forensics) потребує постійного створення і модифікації мережі спеціальних віртуальних машин з різними операційними системами та застосунками, які містять або актуальні вразливості, або сліди несанкціонованого доступу. І це є значною проблемою.

Ефективність практичного навчання в цій галузі, окрім іншого, також залежить від способу стимуляції пізнавальної, мотиваційної та поведінкової діяльності студентів (курсантів) і одним із найбільш підходящих саме в цій царині є гейміфікація (використання ігрових практик та механізмів у контексті розв'язання практичних задач) [2, 3], яка спирається на природні людські інстинкти [4]: конкуренція, досягнення, винагорода і таке інше.

Впровадження гейміфікації у навчанні кібербезпеці і цифровим криміналістичним дослідженням можна здійснювати двома способами (одночасно або на вибір):

а) локальне або хмарне розгорнення фреймворка (інфраструктури програмних рішень) ігрового середовища;

б) реєстрація у провайдера спеціалізованої ігрової послуги і віддалене використання у навчанні актуальних ігрових сценаріїв.

Кожен спосіб має взаємодоповнюючі переваги і недоліки відносно організації навчання у виші:

спосіб а):

- переваги:
- контрольована доступність;
- гнучка зміна функціональності і параметрів роботи;
- наперед відомі для викладача варіанти розв'язання задач;
- недоліки:
- значні витрати ресурсів на розгортання, адміністрування і оновлення середовища;
- значні витрати ресурсів на безперервну розробку і оновлення ігрових сценаріїв-завдань;

спосіб б):

- переваги:
- провайдер здійснює розгортання, адміністрування і оновлення ігрового середовища;
- провайдер забезпечує систему безперервного оновлення ігрових сценаріїв-завдань від необмеженої кількості зацікавлених сторін;
- недоліки:
- залежність доступності середовища від надійності провайдера;
- значні витрати ресурсів для знаходження викладачем наперед невідомих варіантів розв'язання задач.

Наявні складові для реалізації обох способів гейміфікації у вигляді асоціативної карти наведені в [5] – для курсу тестового проникнення до комп'ютерних систем, і в [6] – для курсу цифрових криміналістичних досліджень.

Для впровадження гейміфікації за способом б) можна використовувати британський ресурс hackthebox.eu, де вже зареєстровано біля 100 вишів світу, а за способом а) Capture The Flag framework [7] та актуальну базу підготовлених віртуальних машин із різними завданнями-сценаріями vulnhub.com.

Досвід впровадження гейміфікації показує, що доцільна комбінація обох способів.

Список бібліографічних посилань

1. Вступ.ОСВІТА.UA : сайт. URL: https://vstup.osvita.ua/spec/1-40-1/0-100-1513-0-0-50 (дата звернення: 27.10.2019).
2. Sailer M. Does Gamification of Learning work? URL: http://gamification-research.org/2019/08/does-gamification-of-learning-work (дата звернення: 27.10.2019).
3. Sailer M., Homner L. The gamification of learning: a meta-analysis. *Educational Psychology Review.* 2019. https://doi.org/10.1007/s10648-019-09498-w (дата звернення 27.10.2019).
4. Hamari J., Eranti V. Framework for Designing and Evaluating Game Achievements // Proceedings of Digra 2011 Conference: Think Design Play, Hilversum, Netherlands, September, 14–17. URL: http://www.digra.org/dl/db/11307.59151.pdf (дата звернення 27.10.2019).
5. Aman Hardikar. Penetration testing practice lab – vulnerable apps/systems. URL: https://www.amanhardikar.com/mindmaps/Practice.html (дата звернення: 27.10.2019).
6. Aman Hardikar. Forensic challenges. URL: https://www.amanhardikar.com/mindmaps/ForensicChallenges.html (дата звернення: 27.10.2019).
7. Repository Capture The Flag framework. URL: https://github.com/CTFd (дата звернення: 27.10.2019).

Одержано 28.10.2019

УДК 342.9

Оксана Олександрівна Панова,
кандидат юридичних наук, доцент, доцент кафедри поліцейської діяльності та публічного адміністрування факультету № 3 Харківського національного університету внутрішніх справ

Шляхи оптимізації кадрового забезпечення протидії торгівлі людьми

Не викликає сумнівів, що торгівля людьми, в умовах сьогодення, є реаліями нашого суспільства. Особливого характеру даному злочину надає його транснаціональних характер, адже для торгівлі людьми державні кордони не є перешкодами, а в деяких випадках, наявність протиріч в нормативно-правових системах різних країн виступають каталізатором для скоєння даного злочину.

Незважаючи на прийнятий масив, як вітчизняного так і закордонного законодавства з питань протидії торгівлі людьми, рушійною силою залишаються люди, які опікуються даною проблематикою, та створюють її кадрову базу.

У науковій літературі з цього приводу відзначено, що система роботи з кадрами спрямована на формування й організацію кадрового забезпечення оперативно-службових завдань і раціонального використання персоналу, оскільки тут розв'язується весь комплекс питань, пов'язаних з відбором, розстановкою кадрів, службовим просуванням співробітника, присвоєнням звань, атестаційною оцінкою його професійних і особистих якостей на всіх етапах проходження служби, з правовим регулюванням порядку умов служби, профілактикою порушень дисципліни, визначенням потреб у фахівцях для органів і підрозділів [1, с. 15; 2, с. 84].

Вважаємо за доцільне звернути увагу на позицію Т.Є. Кагановської, яка наголошує, що кадрове забезпечення полягає у діяльності уповноважених суб'єктів з реалізації кадрової політики держави з метою забезпечення функціонування державного управління соціальними, технічними, біологічними об'єктами, яке здійснюється в умовах ринкової економіки з урахуванням демократичних засад побудови нашої держави із пріоритетним забезпеченням прав, свобод та законних

інтересів особи, шляхом наповнення організаційних структур системи державного управління відповідними за професією та кваліфікацією кадрами, створення у них мотивації до ефективної праці, організації їх ефективного використання, професійного та соціального розвитку, досягнення раціонального ступеня мобільності персоналу, а також їх соціального захисту [1, с. 26–27; 3, с. 311–312].

В рамках нашого дослідження, кадрове забезпечення протидії торгівлі людьми полягає у формуванні організаційно-штатної, функціональної структури та механізму як діяльності, так і побудови механізму роботи з кадрами, на які покладено обов'язки та завдання щодо протидії торгівлі людьми.

Таким чином, основним завданням кадрового забезпечення протидії торгівлі людьми в Україні є планування комплексу заходів щодо формування якісного і кількісного складу працівників, спроможних ефективно виконувати свої функції, приймати обґрунтовані та неупереджені рішення. Вказані заходи мають бути спрямовані на упорядкування процедур підбору кадрів (у першу чергу забезпечення дотримання принципу прозорості) та проходження служби; визначення професійних та особистісних якостей, яким повинен відповідати кандидат на виконання функцій у сфері протидії торгівлі людьми; забезпечення ефективного функціонування системи підготовки майбутніх кандидатів на посади та підвищення кваліфікації осіб, що вже працюють; стимулювання керівників усіх рівні до використання нового управлінського досвіду та впровадження сучасних методів мотивації; вироблення оновлених підходів оцінювання ефективності діяльності [3, с. 314].

Отже, задля оптимізації кадрового забезпечення протидії торгівлі людьми, з урахуванням досвіду Європейського Співтовариства та власних вітчизняних здобутків, необхідним є виокремлення таких шляхів оптимізації у досліджуваній нами сфері:

1. Виокремлення стратегії перспективного планування кадрового забезпечення суб'єктів забезпечення протидії торгівлі людьми. При плануванні необхідним є врахування двох моделей:

по-перше, планування організаційно-штатної структури спеціальних суб'єктів з протидії торгівлі людьми, для яких таке завдання є першочерговим;

по-друге, особливої уваги потребує перерозподіл повноважень серед інших державних органів, з метою унеможливлення дублювання функцій, та уникнення плутанини.

2. З метою удосконалення наявних кадрів, необхідним є впровадження інноваційних методик підготовки кадрів для відповідних органів, та встановлення обов'язкових підвищень кваліфікацій, шляхом вдосконалення професійних навичок за рахунок відвідання тренінгів, семінарів, круглих столів, тощо.

3. Створення критеріїв оцінювання та запровадження рейтингу державних службовців, які опікуються питанням протидії торгівлі людьми. З урахування зазначено, вбачається за можливе створення кадрового резерву, для заміщення відповідних посад в органах державної влади, у встановленій сфері.

Список бібліографічних посилань

1. Кагановська Т. Є. Кадрове забезпечення державного управління в Україні : монографія. Харків : Харків. нац. ун-т ім. В. Н. Каразіна, 2010. 330 с.
2. Манжула А., Янко О. Кадрове забезпечення органів внутрішніх справ на тлі становлення демократичних процесів в Україні. *Підприємництво, господарство і право*. 2005. № 3. С. 82–85
3. Панова О. О. Забезпечення публічної безпеки в Україні: адміністративно-правовий аспект : монографія. Харків : ФОП Панов А. М. 510 с.

Одержано 01.11.2019

РОЗДІЛ 5
МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 349

Марія Геннадіївна Артамонова,
студентка 4 курсу юридичного факультету
Харківського національного університету імені В. Н. Каразіна

Ігор Сергійович Воєводін,
викладач кафедри міжнародного і європейського права
юридичного факультету Харківського національного
університету імені В. Н. Каразіна

Сутнісна характеристика поняття та міжнародний досвід протидії кібермобінгу

Передові досягнення у сучасному світі суттєво розширили спектр можливостей кожного члена суспільства, у тому числі в напрямку електронних комунікацій. Проте, незважаючи на існуючі позитивні здобутки, людство отримало нову сферу зловживання правами та здійснення інших незаконних операцій. Одним із видів зловживань є кібермобінг, як вид насильства.

Власне мобінг є одним із різновидів морального насильства. Його прояв полягає у систематичному приниженні, цькуванні, психологічному терорі співробітника в колективі, зазвичай з метою звільнення. Сама дефініція «мобінг» походить від англійського «mob» (натовп) [1, с. 42–43].

Кібермобінг (або як його ще називають «агресія он-лайн») є підвидом мобінгу, досить новітньою формою приниження, заподіяння страждань потерпілому (працівнику) за допомогою засобів електронних комунікацій (у тому числі мережі Інтернет) іншими співробітниками робочого колективу. Кібермобінг характеризується специфічними засобами вчинення насильницьких дій. На практиці такими засобами можуть виступати мобільні телефони, ноутбуки, планшети, електронна пошта, акаунти соціальних мереж, програми незаконного отримання інформації (у тому числі піратський контент) та інші пристрої.

Підвищена небезпека кібермобінгу полягає у тому, що фактично діяння вчиняються в межах віртуального простору, проте наслідки

мають місце в реальному світі та приниження зазнає реальна людина. Крім того, така небезпека підкріплюється доступом до мережі Інтернет майже в будь-якому місці земної кулі та можливістю доступу до неї широких верств населення, що в перспективі може надати більш масштабні обсяги поширення інформації (порівняно із поширенням інформації у вербальній формі).

В Україні напрям протидії кібермобінгу, в рамках здійснення урядової політики, не є таким актуальним, як в інших країнах світу. Будь-яке законодавче врегулювання (у тому числі законодавче закріплення кібермобінгу як правопорушення) з цього питання є відсутнім. Тобто фактично наразі в Україні не існує правового механізму захисту працівників від мобінгу на робочому місці.

Серед країн Східної Азії новелу до свого законодавства щодо протидії кібермобінгу включила Південна Корея. У 2007 році її парламентом був розроблений законопроект, спрямований на боротьбу проти мобінгу в Інтернеті [2].

Серед країн Європи особливою активною державною політикою щодо протидії кібермобінгу відзначилася Німеччина. Кібермобінг у Німеччині не має об'єктивної сторони як окремого складу злочину, але разом із тим, окремі його прояви є караними.

Щодо Сполучених штатів Америки, то в штаті Міссурі в 2008 році був прийнятий закон щодо протидії кібермобінгу, прийняття якого було викликано самогубством працівника одного з підприємств, що мало широкий суспільний резонанс [3].

В 2011 році у Вашингтоні відбувся антимобінг-саміт, активну участь в якому брали представники Facebook Результатом проведення цього саміту стало прийняття рішення керівниками соціальної мережі Facebook про створення відділу медіації у спорах.

Власне сама співпраця урядів держав із керівниками світових соціальних мереж буде ефективним засобом здійснення заходів протидії кібермобінгу, оскільки більшість випадків кібермобінгу відбувається у площині соціальних мереж, а значна частина населення, що працює в колективах, і є користувачами цих соціальних мереж.

Отже, проблема кібермобінгу є, для України, відносно новою в тому образі, в якому вона постає перед нами зараз. Проте, як бачимо, на прикладі інших країн світу, навіть, своєчасне законодавче закріплення певних стратегій протидії кібермобінгу не дає гарантії того, що про-

блема викориниться. Центральним стрижнем концепції, у тому числі законодавчого регулювання та міжнародного співробітництва, має бути морально-психологічний підхід до явища кібербулінгу.

Список бібліографічних посилань

1. Трюхан О. А. Захист працівників від мобінгу на робочому місці: теоретико-правовий аспект. 2017. № 4. С. 42–46.
2. Südkorea: Gesetze gegen Cyber-Mobbing. URL: https://www.silicon.de (дата звернення: 30.10.2019).
3. Straffreiheit für Cyber-Bullying. URL: https://www.spiegel.de/netzwelt/web/online-haeme-wird-straftat-weltweit-erstes-gesetz-gegen-cybermobbing-a-563115.html (дата звернення: 30.10.2019).

Одержано 01.11.2019

UDC 342.738(477)

Oleksii Barbashov,
cadet of faculty No. 4 of Kharkiv National University of Internal Affairs

Foreign experience in combating cybercrime as exemplified by the USA and Japan

Cybercrime – a catch-all term loosely defined as any offence committed using a computer or network – has exploded over the past five years. It now costs the world economy between $100bn and $500bn a year, according to the US Center for Strategic and International Studies, as more and more services are offered online, increasing the volume of sensitive data held electronically. According to the World Economic Forum's Global Risks 2012 report, cyber-attacks are now one of the biggest threats faced across the globe. Cybersecurity is becoming more important to the economic, security, and social well-being of both the United States and Japan. Cybersecurity-related solutions will need significant amounts of public-private cooperation. This includes education for citizens, the workforce, and management. Despite pronouncements by senior officials, many still do not see cybersecurity as a priority. However, people in both countries understand the need for counterterrorism and disaster preparedness, and cybersecurity can be related to these.

U.S. Government (USG) activities and its organization for cyberspace operations are based on a strong set of recent foundational cybersecurity documents, which cover both steady state and crisis response approaches. These include:

1. The Cybersecurity National Action Plan (CNAP), issued in February 2016;

2. Presidential Policy Directive-41 (PPD-41) United States Cyber Incident Coordination, of July 26, 2016;

3. A draft National Cyber Incident Response Plan (NCIRP), mandated by PPD-4110;

Current USG Divisions of Responsibility: There is a National Cybersecurity Coordinator who has regular access to the President. National policy coordination on specific issues is done through the Principals and Deputies Committees of the National Security Council (NSC). The Department of

Homeland Security (DHS) is responsible for cybersecurity on most USG networks (the Intelligence Community protects its most sensitive networks and Department of Defense (DoD) protects some of its own). The Federal Bureau of Investigation (FBI), part of the Department of Justice (DOJ), has the responsibility for prosecuting cybercrimes. The National Security Agency (NSA), reporting both to the Secretary of Defense and the Director of National Intelligence (DNI), has the greatest technical capability of any organization in the USG on cybersecurity. It provides intelligence concerning potential and actual cyberattacks that it gathers outside the United States, as well as providing technical support to other government departments and agencies when requested.

It should be mentioned, to date, Microsoft has focused most of its energies on fighting botnets: networks of computers infected with malicious software that are controlled remotely. In December, the DCU successfully partnered with Europol's European Cybercrime Centre and Germany's Bundeskriminalamt's Cyber Intelligence Unit to crush the notorious botnet ZeroAccess. The takedown marked Microsoft's eighth anti-botnet action in three years.

Several innovative initiatives are underway to improve U.S. and Japanese collaboration on military networks. Today there is connectivity on several channels, such as NIPRNET (Non-Classified Internet Protocol Router Network), SIPRNET (Secret Internet Protocol Router Network), CENTRIXS-J (Combined Enterprise Regional Information Exchange System-Japan) and others. The United States is establishing a Mission Partner Environment (MPE) to promote multinational information sharing (MNIS) globally with allies and coalition partners within communities of interest (COI).

In sum, the next few years offer great opportunities to improve cybersecurity in both Japan and the United States, but also add significant risks if the chances to fix weaknesses are ignored. So, sticking to these measures above, countries like Ukraine can take a new level of fighting cybercrime.

Received 29.10.2019

УДК 341.456:004

Марія Володимирівна Бойко,
студентка 4 курсу юридичного факультету
Харківського національного університету імені В. Н. Каразіна

Євгеній Борисович Тітов,
кандидат юридичних наук, доцент,
доцент кафедри європейського і міжнародного права
Харківського національного університету імені В. Н. Каразіна

Діяльність інтерполу в боротьбі з кіберзлочинами

Кіберзлочинність – одна з найбільш швидко зростаючих форм транснаціональної злочинності, з якою стикаються держави-члени Інтерполу. Відсутність будь-яких кордонів кіберзлочинності означає, що правоохоронні органи стикаються з проблемами ефективного реагування через обмежене транскордонне розслідування злочинів, юридичні виклики та нерівні можливості поліції у всьому світі.

Інтерпол допомагає державам-членам проводити розслідування кіберзлочинів та забезпечує національну поліцію актуальною інформацію про загрозу задля здійснення ефективних та скоординованих дій. Наприклад, у результаті обміну оперативними даними і ресурсами між Європолом і державами-членами Європейського союзу був заарештований злочинець, відомий тим, що продавав фальшиві банкноти номіналом 50 євро на незаконних ринках в даркнеті.

У вересні 2014 р. уряд Сінгапуру офіційно передав Інтерпол будівлю Глобального комплексу інновацій Інтерпол (The Interpol Global Complex for Innovation).

Сучасний Глобальний комплекс інновацій забезпечує Інтерпол інструментами для кращого подолання загроз кіберзлочинності XXI століття, адже він являє собою спеціалізований передовий центр для боротьби з кіберзлочинністю, проведення досліджень та розробок із виявлення кіберзлочинів та злочинців, а відтак може краще захистити громадян як онлайн, так і офлайн.

Глобальний комплекс інновацій складається з Cyber Fusion Centre, лабораторії цифрової криміналістики та інноваційного центру.

Cyber Fusion Centre об'єднує кібер-експертів із правоохоронних органів та промисловості, які збирають та аналізують всю наявну інформацію про злочинну діяльність в кіберпросторі та надають державам-членам цілісну розвідувальну інформацію. Як керівний центр Interpol з розвідки кіберзагроз та координації операцій, Cyber Fusion Centre сприяє обміну інформацією між національною поліцією та надає надійні розвідувальні данні щодо виявлених загроз у кіберпросторі.

Центр публікує звіти, щоб попередити країни про нові, неминучі кіберзагрози або такі, які можуть статися. До них відносяться зловмисне програмне забезпечення, фішинг, компрометовані урядові вебсайти, шахрайство із соціальним інженерією тощо.

У рамках системи цифрової безпеки в структурі Глобального комплексу інновацій створена криміналістична лабораторія, яка також сприяє розробці практичних рішень у співпраці з поліцією, науково-дослідними лабораторіями, науковими колами, а також із державним та приватним секторами задля боротьби з кіберзагрозами.

Отже, Інтерпол допомагає країнам зрозуміти, як виявити та використовувати цифрові докази, допомагає аналізувати шкідливі програми, вивчає цифрові пристрої. Оскільки злочинці постійно розвиваються та пристосовуються до нових методів та технологій Інтерпол перевіряє нові цифрові криміналістичні інструменти з метою їх використання правоохоронними органами держав-учасниць, працює над розробкою нових способів протидії кіберзлочинам, консультуючись з партнерами в кіберіндустрії.

Одержано 01.11.2019

УДК 341.231.14

Кароліна Андріївна Варнавська,
аспірантка кафедри міжнародного і європейського права юридичного факультету Харківського національного університету імені В. Н. Каразіна

Деякі питання захисту жінок-журналістів у мережі Інтернет: міжнародно-правовий аспект

Жінки-правозахисники відіграють важливу роль у захисті і заохоченні прав і свобод людини, гарантованих міжнародно-правовими актами в галузі прав людини у різних сферах суспільного життя. При цьому, суттєве значення має діяльність журналістів, які виконують задачу збору інформації і доведення її до відома громадськості через друковані засоби масової інформації, Інтернет-видання, телебачення тощо. Журналісти в межах здійснення означеної діяльності сприяють забезпеченню прозорості та підзвітності здійснення державної політики, підвищення рівня обізнаності населення про права людини та вирішенню інших питань, що становлять суттєвий інтерес для суспільства. Саме через цю важливу роль журналісти можуть стати жертвами порушень основних прав людини [1]. Жінки-журналісти при виконанні своїх професійних обов'язків нерідко стають жертвами сексуального насильства або у формі цілеспрямованого статевого насильства або в покарання за свою діяльність; сексуального насильства з боку натовпу щодо журналістів, які висвітлюють публічні події; сексуального насильства над журналістами, які знаходяться в місцях позбавлення волі або в полоні. Вони стикаються зі зростаючою небезпекою, яка наголошує на необхідності взяття на озброєння підходу, що враховує гендерну перспективу [2].

Важливо зазначити, що жінки регулярно стикаються з надмірними проявами насильства за ознакою статі на робочих місцях і за їх межами, в Інтернеті та в інших сферах. Глобальне дослідження «Насильство та утиски щодо жінок у засобах інформації: стан справ у світовому масштабі», яке було проведено в 2014 році, показало, що майже дві третини опитаних журналістів-жінок піддавалися залякуванню в тій чи іншій формі, зазнавали погроз або наруги в зв'язку з їх роботою [3].

Інтернет та інші засоби масової інформації стали важливим джерелом новин. Зростає число журналістів, які працюють у режимі «онлайн», як професійних, так і «громадських», які не мають спеціальної освіти, але при цьому відіграють істотну роль у документуванні та поширенні інформації [1].

Верховним комісаром ООН з прав людини у доповіді A/HRC/35/9 було акцентовано увагу на тому, що жінки-активісти, включаючи жінок-правозахисниць, все частіше використовують інформаційно-комунікаційні технології в цілях пропаганди, комунікації, мобілізації, захисту, доступу до інформації та популяризації своєї діяльності. Однак у той же час інформаційно-комунікаційні технології можуть сприяти розширенню видів спостереження, цензури та утисків, з якими вони можуть стикатися. Спеціальний доповідач з питання щодо заохочення і захисту права на свободу думок і їх вільне вираження також зазначив, що стеження в мережному середовищі здійснює істотний вплив на свободу вираження думок широкого кола вразливих груп, таких як, зокрема, журналісти, а жінки в цих групах стикаються з гендерними ризиками і загрозами (п. 23) [4].

Вказаному вище питанню було приділено увагу в межах ЮНЕСКО, зокрема, в документі 39C/61 (Зміцнення провідної ролі ЮНЕСКО в здійсненні Плану дій ООН щодо забезпечення безпеки журналістів і проблеми безкарності), Генеральна конференція зазначила, що у зв'язку зі збільшенням випадків нападу на жінок-журналістів Організація буде сприяти застосуванню агентствами новин гендерно-орієнтованих протоколів безпеки, які передбачають боротьбу з насильством і домаганнями щодо жінок-журналістів в Інтернеті. ЮНЕСКО також буде прагнути до збільшення штату співробітників, які безпосередньо займаються питаннями безпеки жінок-журналістів і цифрової безпеки (п. 11). Крім цього, в резолюції, що міститься у додатку до документа 39C/61 було запропоновано Генеральному директору зміцнити заходи по боротьбі з особливими погрозами, з якими стикаються жінки-журналісти онлайн (п. 5) [5].

Так, хоча у мережному просторі жінки можуть обходити обмеження, які є однією з характерних рис друкованих засобів масової інформації та телебачення, а також уникати впливу гендерних забобонів і множинних і пересічних форм дискримінації, які заважають жінкам брати участь в роботі ЗМІ, разом з тим мережний простір також є новою платформу для

нападок на жінок. Крім того, журналісти-жінки більшою мірою і частіше піддаються в Інтернеті загрозам насильства, включаючи сексуальне насильство, цькування, доксінг (незаконне розголошення особистих даних в Інтернеті) і сваттінг (помилковий виклик груп оперативного реагування). Жінки, які висвітлюють такі теми, як політика, право, економіка, спорт, права жінок, гендерна проблематика і фемінізм, в особливій мірі схильні до ризику стати об'єктом насильства в мережному середовищі (п. 10) [6].

Спеціальний доповідач з питання про заохочення і захист права на свободу думок також висловив глибоке занепокоєння у зв'язку з переслідуванням журналістів онлайн-ресурсів, наприклад незаконним зламом їх акаунтів, відстеженням їх діяльності в мережі, довільними арештами і затриманнями, а також блокуванням вебсайтів, що містять критику на адресу влади. Такі дії являють собою залякування і застосування цензури (п. 63). Крім цього, Спеціальний доповідач зазначив, що журналістам, які публікують свої матеріали в Інтернеті, має забезпечуватися такий самий захист, який передбачено в статті 19 Загальної декларації прав людини 1948 р. і Міжнародному пакті про громадянські і політичні права 1966 р. [4].

Таким чином, виходячи з вищезазначеного, можемо зробити висновок, що жінки-журналісти відіграють важливу роль у захисті основоположних прав і свобод людини, проголошених міжнародно-правовими актами у галузі прав людини. З урахуванням стрімкого розвитку інформаційно-комунікаційних технологій зросла кількість журналістів, які працюють в мережі Інтернет, та одночасно збільшилась кількість нападів на них. Разом з тим, журналісти-жінки більшою мірою і частіше піддаються в Інтернеті загрозам насильства, оскільки переслідування в Інтернеті найчастіше є анонімним і має надзвичайно інвазивний характер. З огляду на вказане, мають бути розроблені заходи спрямовані на попередження та недопущення порушень прав журналістів (злам аккаунтів, блокування вебсайту тощо) в мережі Інтернет з урахуванням особливих потреб жінок.

Список бібліографічних посилань

1. Резолюция Генеральной Ассамблеи ООН. URL: https://documents-dds-OpenElement (дата звернення: 18.10.2019).
2. Безопасность журналистов : доклад Управления Верховного комиссара Организации Объединенных Наций по правам человека от 01.07.2013

A/HRC/24/23 // Организация Объединенных Наций : офиц. сайт. URL: https://undocs.org/ru/A/HRC/24/23 (дата звернення: 18.10.2019).
3. План действий ООН по обеспечению безопасности журналистов и проблеме безнаказанности // Объединенные Нации права человека : сайт. URL: https://www.ohchr.org/Documents/Issues/Journalists/UN_plan_on_Safety_Journalists_RU.pdf (дата звернення: 18.10.2019).
4. Безопасность журналистов и проблема безнаказанности : доклад Генерального секретаря от 04.08.2017 A/72/290 // refworld : сайт. URL: http://www.refworld.org/cgi-bin/texis/vtx/rwmain/opendocpdf.pdf?reldoc=y&docid=59c114e14 (дата звернення: 18.10.2019).
5. Поощрение, защита и осуществление прав человека в Интернете: пути устранения межгендерного цифрового разрыва с точки зрения прав человека : доклад Верховного комиссара Организации Объединенных Наций по правам человека от 05.05.2017 A/HRC/35/9 // Электронная подписка на документы Организации Объединенных Наций : сайт. URL: https://undocs.org/ru/A/HRC/35/9 (дата звернення: 18.10.2019).
6. Укрепление ведущей роли ЮНЕСКО в осуществлении плана действий ООН по обеспечению безопасности журналистов и проблеме безнаказанности : от 02.11.2017 39C/61 // UNESDOC : сайт. URL: http://unesdoc.unesco.org/images/0025/002599/259913R.pdf (дата звернення: 18.10.2019).
7. Доклад Специального докладчика по вопросу о поощрении и защите права на свободу мнений и их свободное выражение Франка Ла Руе : от 07.06.2012 A/HRC/20/17 // Организация Объединенных Наций : офиц. сайт. URL: https://undocs.org/ru/A/HRC/20/17 (дата звернення: 18.10.2019).

Одержано 01.11.2019

УДК 342.727

Тетяна Іванівна Гудзь,
кандидат юридичних наук, доцент, професор кафедри конституційного і міжнародного права факультету № 4 Харківського національного університету внутрішніх справ

Принцип вільного руху інформації як основний принцип європейської аудіовізуальної політики

У сучасному світі свобода думки і слова, вільне вираження своїх поглядів і переконань визнається невід'ємним правом кожної людини. Проте розвиток сучасних технологій, наукові винаходи, інновації у сфері зв'язку досить суттєво трансформували можливості осіб передавати та отримувати інформацію, у тому числі масову. В умовах сьогодення можна з впевненістю говорити про те, що електронні засоби масової інформації (далі – електронні ЗМІ), а саме телебачення, радіо і Інтернет, здійснюють суттєвий вплив на суспільство, а отже – і на державу в цілому. Вони можуть як стимулювати розвиток країни, так і гальмувати його.

У цьому контексті набувають актуальності питання щодо засад поширення інформації. При цьому, утвердження в українському суспільстві свідомої підтримки членства України в Європейському Союзі, інтеграції в європейський економічний, культурний та політичний простір і здійснення процесу внутрішніх реформ і перетворень у бік більш вільного, справедливого, демократичного, успішного і прозорого суспільства, що спирається на засадничі права та свободи людини, передбачає дослідження принципів діяльності засобів масової інформації, у першу чергу електронних, оскільки саме з їх допомогою існує можливість оперативно отримувати будь-яку інформацію у будь-якому місці, і у будь-який час за умови наявності технічних можливостей.

Базові принципи діяльності електронних ЗМІ знайшли своє закріплення в основоположних документах європейських інституцій, таких як Рада Європи, Європейський Союз, ОБСЄ, ПАРЄ. Цими міжнародними організаціями було прийнято низку документів, у яких було закріплено відповідні принципи, а саме: Декларацію про свободу виразу думки та інформації (1982 р.), Рекомендацію Комітету міністрів Ради Європи

«Про заходи щодо прозорості засобів масової інформації» (1994 р.), Рекомендацію «Про заходи стимулювання плюралізму ЗМІ» (1999 р.) тощо.

Одним із основних принципів європейської аудіовізуальної політики, що знайшов своє відображення у щойно згаданих документах, є принцип вільного руху інформації. Даний принцип є базовим принципом європейської аудіовізуальної політики, який спрямований на створення єдиного комунікаційного медіа простору, і базується на наступних обов'язкових елементах.

Забезпечення свободи думки і слова, вільного вираження своїх поглядів і переконань. Право людини на інформацію, свободу думки і слова гарантовано Конвенцією про захист прав людини і основоположних свобод та Декларацією Комітету міністрів Ради Європи «Про свободу вираження поглядів та інформації». Саме ці документи встановлюють, що кожен має право на свободу самовираження. Водночас, у цих же документах зазначається, що в інтересах національної безпеки, територіальної цілісності або суспільного спокою законом передбачені обмеження щодо поширення й отримання такої інформації. Крім того, процес ліцензування електронних ЗМІ розглядається не як прояв обмеження свободи вираження, а як засіб забезпечення безпеки медіа простору.

Обов'язковою умовою забезпечення реалізації принципу вільного руху інформації є забезпечення загального доступу до інформації. Вона передбачає, що у Європейському Союзі усі громадяни мають доступ до інформації, яка представляє суспільний інтерес, за допомогою електронних ЗМІ, що функціонують на рідній мові населення. Водночас, відкритість інформаційного простору автоматично заохочує населення підвищувати власний рівень медіа грамотності (зокрема, це стосується вразливих верст населення, меншин, осіб з обмеженими можливостями тощо) – люди мають можливість отримати допомогу задля розвинення навичок щодо пошуку і використання інформації, а отже й забезпечення її вільного руху.

Відкритість державного управління відіграє важливу роль у процесі забезпечення вільного руху інформації. Вона забезпечується, насамперед, за допомогою сайту Європейського Союзу, який демонструє громадянам увесь спектр діяльності ЄС на всіх мовах держав-членів. Крім того, забезпечення відкритості державного управління як невід'ємного елементу принципу вільного руху інформації, регламентовано у Білій

книзі про європейське управління, що закріплює обов'язок інститутів Європейського Союзу публікувати результати роботи.

Водночас, Європейський Союз визначає, що вільний рух і свобода інформації передбачає наявність медіаплюралізму. Оскільки засоби масової інформації виконують важливу роль у процесі поширення економічної та політичної інформації, слід перешкоджати їх використанню як зброї політичними та економічними групами. Також Європейський Союз активно протидіє медіаконцентрації, як гальмуючому елементу у системі вільної циркуляції інформації. Концентрація у медіасфері провокує обмежену кількість медіамагнатів й автоматично блокує доступ для нових «гравців» інформаційної сфери.

Європейська політика також широко протидіє відсутності плюралізму медіаконтекту. Наразі, існує проблема, коли різноманітні ЗМІ пропонують одну й ту саму інформацію/фотографії/відео. Це викликано тим, що медіа компанії не виробляють власну продукцію через відсутність ресурсів (зокрема, журналістів).

Ще одним елементом принципу вільного руху інформації виступає вільна конкуренція на інформаційному ринку, забезпечення якої регламентовано Директивою Комісії 2002/77/ЄС від 16 вересня 2002 року «Про конкуренцію на ринку електронних телекомунікаційних мереж та послуг» і Директивою «Телебачення без меж». Суть механізму забезпечення вільної конкуренції передбачає відкритість інформаційного суспільства для нових членів, як у сфері вироблення медіапродукту, так і у сфері його поширення та надання інших медіапослуг на всій території Європейського Союзу незалежно від національних кордонів. Водночас, Директива «Телебачення без меж» вимагає, щоб електронні ЗМІ резервували основну частину свого мовного часу для передачі європейського медіапродукту. А це виступає, з одного боку, як обмеження плюралізму медіапродукту та провокує «інформаційний застій», а з іншого – як інструмент забезпечення збереження культурного різноманіття.

Отже, європейська інформаційна/аудіовізуальна політика формується й розвивається паралельно зі світовою глобалізацією. Принцип вільного руху інформації як основний принцип європейської аудіовізуальної політики складається із системи таких обов'язкових функціональних складових, як: забезпечення свободи думки і слова, вільного вираження своїх поглядів і переконань; загального доступу до інформації; відкри-

тість державного управління; медіаплюралізм, протидія медіаконцентрації та плюралізм медіаконтенту; вільна конкуренція у медіасфері.

Україна визнає міжнародно-правові стандарти у сфері засобів масової інформації, у т. ч. й електронних, як основоположні для демократичного розвитку суспільства і держави. Водночас, реалізація принципу вільного руху інформації в Україні потребує вироблення дієвого механізму гарантування безпеки національного сегменту кібернетичного простору, зокрема щодо діяльності у сфері мас-медіа. Це пов'язано з тим, що певна інформація може бути використана як активний елемент інформаційної війни і, відповідно, стати загрозою виникнення порушень демократичних цінностей, прав та свобод людини, що є неприпустимим.

Одержано 01.11.2019

УДК 341:[343.346.8:004]

Сергій Миколайович Гусаров,
доктор юридичних наук, професор, професор кафедри адміністративного права та процесу факультету № 1 Харківського національного університету внутрішніх справ

Міжнародна співпраця у сфері протидії кібертероризму

Сучасний етап світового цивілізаційного розвитку характеризується стрімким розвитком інформаційних технологій, які охоплюють усі сфери діяльності сучасного соціуму, створюють можливості для зростання ефективності виробництва, кардинально змінюють механізми функціонування державних інституцій і приватного сектора. Однак разом із позитивними явищами з'явилися і негативні – це, зокрема, так звана комп'ютерна злочинність або кіберзлочинність, яка посідає значне місце серед сучасної кримінальній діяльності.

Дослідники, які займаються проблемою кіберзлочинності, пропонують різні класифікації кіберзлочинів. Кіберзлочини поділяють на види залежно від об'єкта і предмета посягання. Найпоширенішим варіантом є поділ на комп'ютерні злочини та злочини, що здійснюються за допомогою комп'ютерів, комп'ютерних мереж та інших пристроїв доступу до кіберпростору. Такою класифікацією користується Організація Об'єднаних Націй, поділяючи цей вид злочинної діяльності на кіберзлочини в широкому та вузькому розумінням. У такому контексті комп'ютерні злочини – це злочини, основним об'єктом посягання яких є конфіденційність, цілісність, доступність і безпечне функціонування комп'ютерних даних і систем. Решта кіберзлочинів, крім комп'ютерних систем, зазіхає на інші об'єкти: безпеку суспільства і людини (кібертероризм), майно та майнові права (крадіжки, шахрайства, скоєні за допомогою комп'ютерних систем або в кіберпросторі), авторські права (плагіат і піратство).

Кібертероризм можна визначити як комплексну модель, що проявляється в навмисній, політично вмотивованій атаці на інформацію, яка обробляється комп'ютерами та комп'ютерними системами, що створює небезпеку для життя чи здоров'я людей або настання інших тяжких

наслідків, якщо такі дії були вчинені з метою порушення громадської безпеки, залякування населення, провокації військового конфлікту.

Джерела кібератак фахівці з кібербезпеки поділяють на кілька категорій (особи й організації, які здійснюють атаки). Однак між цими категоріями не існує досить чіткої межі. Наприклад, багато експертів наголошують на можливості залучення до терористичних дій хакерів-одинаків і груп хакерів, які не мають уявлення про те, до якого результату можуть призвести їх дії. Таким чином, поділ на групи можна вважати в певному сенсі умовним.

Проблема кіберзлочинності та кібертероризму є відносно новою для міжнародної спільноти. Саме тому на нинішньому етапі будь-які серйозні висновки про її стан і подальші перспективи зробити досить складно. Зрозуміло одне – це явище, що виникло лише кілька десятиліть тому, охоплює все нові сфери діяльності людини, зростає швидкими темпами та вимагає вжиття адекватних і своєчасних заходів реагування як на національному, так і на міжнародному рівнях. Вирішення проблеми кібертероризму є важливим для забезпечення міжнародної інформаційної безпеки. Існують труднощі щодо створення і збереження коаліцій у процесі міжнародного співробітництва. З початком серйозного акту інформаційного тероризму (кібертеракту) міцність коаліцій держав піддається великому випробуванню, оскільки союзники деякий час перебувають в «інформаційному тумані». Можуть виникнути і гострі проблеми з реалізацією спільних планів дій проти транснаціональної кримінальної або терористичної організації.

З упевненістю можна сказати, що всі провідні міжнародні організації визнають небезпеку кіберзлочинності та її транскордонний характер, обмеженість одностороннього підходу до вирішення цієї проблеми і необхідність міжнародного співробітництва як у вжитті необхідних технічних заходів, так і у виробленні міжнародного законодавства. ООН, НАТО, Інтерпол, ОБСЄ, ЄС та багато інших міжнародних організацій відіграють важливу роль у координації міжнародних зусиль, побудові міжнародної співпраці в боротьбі зі злочинами у сфері високих технологій, зокрема кібертероризмом.

Одержано 01.11.2019

УДК 341.4

Володимир Анатолійович Євтушок,
старший викладач кафедри тактичної
та спеціальної фізичної підготовки
Харківського національного університету внутрішніх справ

Боротьба з торгівлею людьми на міжнародному рівні та її наслідки

Метою роботи є аналіз міжнародного співробітництва у сфері торгівлі людьми та особливості боротьби з нею.

Міжнародна торгівля людьми залишається важливою соціальною проблемою. Ця тема є актуальною не тільки для сучасної України, а й для усього світу. Торгівля людьми є прибутковим нелегальним бізнесом, тому злочинці вигадують все нові й нові методи з метою експлуатації людини та для власного збагачення.

На жаль торгівля людьми не обійшла жодну країну світу. Об'єктом цього злочину може бути будь-яка особа, незалежно від статі та віку. Торгівля людьми у світі постійно видозмінюється залежно від того, як економічні, демографічні та інші геополітичні фактори впливають на зміни в структурі країн.

Вплив міжнародного товариства все більше поширюється на нові засоби боротьби, зокрема ухвалення міжнародних актів, що забороняють торгівлю людьми. Але їх ухвалення не означає розв'язання проблеми, для вирішення кожна держава має чітко дотримуватись обов'язків, що зазначені в актах, повинна співпрацювати в різноманітних формах, не тільки в прикордонних контактах, але і на регіональному та універсальному рівні. Боротьба з торгівлею людьми – система заходів, що здійснюються в рамках протидії торгівлі людьми, спрямованих на виявлення злочину торгівлі людьми, в тому числі незакінченого, осіб, які від цього постраждали, встановлення фізичних / юридичних осіб – торгівців людьми та залучені їх до відповідальності. Боротьба з торгівлею людьми є невід'ємною складовою діяльності органів Національної поліції по боротьбі зі злочинністю, яка, зокрема, здійснюється шляхом реалізації організаційних, оперативно-розшукових, адміністратив-

но-правових, процесуальних, аналітично-дослідницьких, інформаційних та інших заходів.

До завдань у сфері боротьби з торгівлею людьми належать:

- виявлення причин та передумов, що сприяють торгівлі людьми, та вжиття заходів щодо їх усунення;

- забезпечення безпеки осіб, які визнані потерпілими від торгівлі людьми, свідків та інших осіб, які що беруть участь у кримінальному судочинстві у справах щодо торгівлі людьми;

- виявлення та розслідування злочинів, пов'язаних з торгівлею людьми;

- притягнення до відповідальності, у тому числі кримінальної, осіб, причетних до торгівлі людьми;

- забезпечення відновлення прав постраждалих від торгівлі людьми

- інформування суб'єктів, які здійснюють заходи у сфері протидії торгівлі людьми, та громадськості щодо результатів діяльності у сфері боротьби з торгівлею людьми.

Для того, щоб знайти шляхи розв'язання цієї проблеми міжнародне товариство повинно мати чітке уявлення про таке поняття, як торгівля людьми. На даний момент визначення цього поняття містить Протокол з попередження торгівлі людьми, особливо жінками та дітьми, який доповнює Конвенцію ООН про боротьбу з транснаціональною організованою злочинністю. Протокол є основним сучасним документом, спрямованим на боротьбу з цим злочином. Він визначає торгівлю людьми як: Здійснення з метою експлуатації вербування, перевезення, передачі, приховання чи отримання людей шляхом погрози силою або її застосування чи інших форм примусу, викрадення, шахрайства, обману, зловживання владою чи вразливістю стану або шляхом підкупу у вигляді платежів чи вигод для одержання згоди особи, яка контролює іншу особу.

На доповіді про торгівлю людьми в США визначили, що основними факторами, що сприяють цьому явищу, є: зростання безробіття, зменшення асигнувань на програми соціального захисту, зубожіння населення. Низький рівень доходів штовхає громадян на пошуки роботи за кордоном навіть без знання мови і правових знань, без кваліфікації, на нелегальних умовах, що водночас зумовлює їх перехід до груп ризику.

Протидія торгівлі людьми полягає в створенні великої кількості організацій, як урядових: Міжнародна організація з міграції (МОМ), та неурядових, наприклад: Всесвітня організація за Виживання (The Global Survival Network), Фонд проти торгівлі людьми (The Foundation against), та багато інших. Також є багато міжнародних правоохоронних організацій: Інтерпол та Європол, для координації зусиль у протидії торгівлі людьми. Проте національна стратегія протидії торгівлі людьми, особливо жінками та дітьми, на цей момент не передбачає приділення належної уваги врегулюванню проблеми забезпечення відшкодування та компенсації жертвам торгівлі людьми, натомість, розв'язує проблеми реабілітації жертв досліджуваного злочину.

На міжнародному рівні співробітництво у досліджуваній сфері ефективно проводиться не лише на міжурядовому рівні, але і на рівні залучення неурядових організацій. На національному рівні у більшості із напрямів реалізації положень. Державної цільової соціальної програми спостерігається поступове зростання ефективності імплементаційних заходів. Проте необхідно зазначити, що загальна національна стратегія боротьби з досліджуваним злочином потребує удосконалення та характеризується низкою недоліків. Проблема торгівлі людьми є дуже важливою та актуальною на даний час. З такими злочинами міжнародного характеру світові організації намагаються боротися давно, тож співробітництво держав на різних рівнях є надзвичайно важливими для захисту прав та свобод суспільства.

Одержано 25.10.2019

УДК 341.231.14

Вероніка Вікторівна Оніщенко,
аспірант кафедри криміналістики, судової медицини та психіатрії Дніпропетровського державного університету внутрішніх справ

Деякі питання торгівлі людьми в бізнес-сфері: міжнародно-правовий аспект

Питання щодо захисту і заохочення прав і основоположних свобод людини, гарантованих міжнародно-правовими актами універсального і регіонального рівнів у галузі прав людини перебуває в полі зору міжнародної спільноти. Разом з тим, у сучасному світі люди стають жертвами специфічних порушень прав людини в контексті підприємницької діяльності і часто непропорційно від них страждають. При цьому слід зазначити, що жінки можуть ставати жертвами множинних форм дискримінації та відчувати додаткові перешкоди на шляху до ефективних засобів правового захисту через їхній вік, колір шкіри, етнічну приналежність, релігію, мову, грамотність, доступ до економічних ресурсів, сімейний стан, сексуальну орієнтацію, гендерну ідентичність тощо. Як зазначено в Доповіді Робочої групи з питання про права людини і транснаціональні корпорації та інші підприємства внесок жінок в економіку або не визнається (наприклад, домашня робота), або недооцінюється (наприклад, у фемінізованих професіях і виробництві). Жінки виконують більшу частину роботи по догляду (наприклад, сімейний догляд за дітьми, людьми похилого віку, хворими та інвалідами), але не отримують плати за цю працю. У всьому світі жінки переважно представлені на неформальних і випадкових роботах або на роботах у режимі часткової зайнятості та виробничо-збутових ланцюжках численних виробництв, де вони відрізняються більшою вразливістю до експлуатації і зловживань. Крім цього, у всьому світі жінки стикаються з дискримінацією через вагітність і материнство, недостатньо представлені на управлінських посадах і отримують заробітну плату у середньому приблизно на 20% менше, ніж чоловіки [1].

Крім цього, нерідкими є випадки, коли жінки стають жертвами торгівлі людьми в аспекті здійснення підприємницької діяльності. Спеціальний доповідач з питання щодо торгівлі людьми, особливо жінками і дітьми при здійсненні свого мандата відзначив, що торгівлею людьми в

більшості випадків займаються недержавні суб'єкти та що підприємства часто прямо або побічно отримують економічну вигоду з праці жертв торгівлі людьми або з наданих жертвами послуг, у тому числі на рівні ланок своїх ланцюжків поставок [2].

Сучасна економіка значною мірою спирається на систему, засновану на експлуатації вразливих трудящих. Торгівля людьми, що є вираженням найбільш кричущих порушень на робочому місці, є однією з крайніх точок у континуумі експлуатації. Експлуатація, а отже, і торгівля людьми, починається зі створення сприятливих умов для порушення основних трудових прав, таких як обмеження прав на вступ до профспілок або їх створення, ведення колективних переговорів, також для ігнорування основних прав трудящих, таких як право на безпеку. У повсякденній діловій практиці часто зустрічаються незначні порушення трудових відносин, такі як затримки у виплаті заробітної платні, надмірна понаднормова робота, неоплачувана відпустка тощо. Нормалізація зловживань у сфері праці на цьому рівні безпосередньо впливає на ймовірність виявлення більш серйозних форм експлуатації [3].

Означене вимагає вироблення низки заходів, спрямованих на попередження та викорінення існуючої негативної практики та притягнення винних осіб до відповідальності.

Так, Генеральна Асамблея Організації Об'єднаних Націй у своїй резолюції A/RES/67/145, присвяченій питанню торгівлі жінками і дівчатками закликала уряди проводити за необхідності огляди і забезпечувати дотримання на своїх територіях і в межах своєї юрисдикції відповідних норм трудового та іншого законодавства, що передбачають або вимагають, щоб підприємства, в тому числі агентства з працевлаштування, запобігали торгівлі людьми в ланцюжках поставок і боролися з нею та періодично проводили оцінку адекватності такого законодавства і усували будь прогалини. Крім цього Генеральна Асамблея висунула пропозицію підприємницькому сектору розглянути питання про прийняття етичних кодексів поведінки з метою забезпечення гідної роботи і запобігання практики експлуатації, що сприяє торгівлі людьми (п. 25, 26) [4].

Підсумовуючи викладене вище, доходимо висновку, що випадки торгівлі людьми, особливо жінками і дітьми в аспекті здійснення підприємницької діяльності не є поодинокими. Корпорації можуть несвідомо ставати учасниками злочинів торгівлі людьми, коли їх постачальники,

підрядники або партнери надають матеріали або продукцію, вироблену жертвами торгівлі людьми. Така ситуація вимагає розробки та застосування державами та корпораціями ефективних правових заходів, направлених на припинення порушень прав людини жертв торгівлі людьми.

Список бібліографічних посилань

1. Гендерные изменения Руководящих принципов предпринимательской деятельности в аспекте прав человека : доклад Рабочей группы по вопросу о правах человека и транснациональных корпорациях и других предприятиях от 23.05.2019 A/HRC/41/43 // Организация Объединенных Наций : офиц. сайт. URL: https://undocs.org/ru/A/HRC/41/43 (дата звернення: 30.10.2019).
2. Торговля людьми, особенно женщинами и детьми : записка Генерального секретаря от 07.08.2012 A/67/261 // Организация Объединенных Наций : офиц. сайт. URL: https://undocs.org/ru/A/67/261 (дата звернення: 30.10.2019).
3. Торговля людьми, особенно женщинами и детьми : записка Генерального секретаря от 18.07.2019 A/74/189 // Организация Объединенных Наций : офиц. сайт. URL: https://undocs.org/ru/A/74/189 (дата звернення: 30.10.2019).
4. Резолюция Генеральной Ассамблеи ООН A/RES/73/146. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/445/38/PDF/N1844538.pdf?OpenElement (дата звернення: 30.10.2019).

Одержано 01.11.2019

УДК 341.215.4

Алла Ігорівна Предибайло,
аспірант кафедри міжнародного і європейського права юридичного факультету Харківського національного університету імені В. Н. Каразіна

Міжнародно-правові механізми протидії торгівлі особами похилого віку

Питання щодо налагодження взаємодії держав у галузі протидії торгівлі людьми є вкрай актуальним, а тому міжнародне співтовариство активно впроваджує нові засоби боротьби за рахунок прийняття міжнародних актів, які забороняють торгівлю людьми. Відповідно до Статуту Організації Об'єднаних Націй «Організація Об'єднаних Націй сприяє: а) підвищенню рівня життя, повній зайнятості населення й умовам економічного та соціального прогресу і розвитку... б) загальній повазі і дотриманню прав людини і основних свобод» (ст. 55) [7].

Особливу увагу слід приділити комплексу міжнародно-правових актів, створених світовим співтовариством з метою подолання торгівлі людьми, серед яких слід виокремити наступні:

- Загальна декларація прав людини, де підкреслюється, що «ніхто не повинен утримуватися в рабстві або підневільному стані; рабство і работоргівля забороняються у всіх їх видах» (ст. 4) [2]. Однак, Декларація за своїм характером є документом рекомендаційним та не є обов'язковою для виконання, а отже встановлює виключно універсальні механізми протидії торгівлі людьми.

- Міжнародний пакт про економічні, соціальні та культурні права, відповідно до якого «жодна людина не повинна піддаватися випробуванням, примусовій праці і незаконному утриманню чи утиску таких свобод як свобода на пересування, вираження та асоціацію з іншими», а також встановлює низку прав громадян країн-учасниць Пакту, які разом можуть забезпечити певний захист від торгівлі людьми. Наприклад, ці права включають в себе право на працю (ст. 6), освіту (ст. 13), справедливі та сприятливі умови праці (ст. 7), рівну оплату рівної за цінністю праці (ст. 7) та відповідні життєві стандарти (ст. 11) [6]. Стаття

8 Міжнародного Пакту про громадянські та політичні права забороняє рабство та работоргівлю державами або приватними суб'єктами [5].

- Конвенція про боротьбу з торгівлею людьми і з експлуатацією проституції третіми особами, де в преамбулі підкреслюється, що «проституція і зло, яке супроводжує її, яким є торгівля людьми, що має на меті проституцію, несумісні з гідністю і цінністю людської особи і загрожують добробуту людини, сім'ї і суспільству» [4].

Хоча Нью-Йоркська конвенція консолідує базисні положення серед діючих конвенцій ООН з цього питання, у той же час ключовим напрямом постало правове регулювання та протидія сексуальній експлуатації, хоча сьогодні існують інші форми експлуатації, які Конвенція цього ж не передбачає.

Таким чином, можна зробити висновок, що загальні стандарти з прав людини містять задекларовані принципи заборони рабства, примусової праці та формують базисні механізми контролю за виконанням державами цих положень, проте вказані приписи обов'язкової сили не мають і виконуються державами лише в силу такої потреби.

Проте торгівля людьми є більш широким поняттям, що включає в себе також торгівлю особами похилого віку, зокрема, через фінансові зловживання зацікавленими особами щодо однієї з найбільш вразливої категорії суб'єктів.

Правовим базисом в цьому аспекті слугують приписи загального характеру Віденського Міжнародного плану дій з проблем старіння, де рекомендується розробляти і здійснювати спеціальну політику і заходи, а також передбачати системи, що дозволяють людям похилого віку вільно переміщатися (п. d 19 рекомендація) [1].

Водночас у Мадридському Міжнародному плані дій з проблем старіння зазначено про доцільність надання правової консультативно інформаційної допомоги літнім людям в тих випадках, коли вони стають переміщеними особами або позбавляються належної їм землі та іншого виробничого та особистого майна (п. 56 розділ II) [3].

Таким чином, аналізуючи зазначені вище акти вбачається тенденція до загального (декларативного) забезпечення прав осіб похилого віку, тому, проблема щодо питання торгівлі вказаною категорією осіб є вкрай актуальною з огляду на відсутність правового механізму, який міг сформулювати сучасні стратегії боротьби та забезпечити належний

захист для осіб похилого віку з метою запобігання торгівлі людьми, не порушуючи при цьому прав людини.

Список бібліографічних посилань

1. Віденський Міжнародний план дій з проблем старіння : від 06.08.1982 // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: http://zakon.rada.gov.ua/laws/show/995_870 (дата звернення: 31.10.2019).
2. Загальна декларація прав людини : прийн. і проголош. резолюцією 217 А (III) Ген. Асамблеї ООН від 10.12.1948 // БД «Законодавство України». / ВР України. URL: https://zakon.rada.gov.ua/laws/show/995_015 (дата звернення: 31.10.2019).
3. Доклад второй Всемирной ассамблеи по проблемам старения : от 08-12.04.2002 // Организация Объединенных Наций : офиц. сайт. URL: https://www.un.org/esa/socdev/documents/ageing/MIPAA/political-declaration-ru.pdf (дата звернення: 31.10.2019).
4. Конвенція про боротьбу з торгівлею людьми і з експлуатацією проституції третіми особами : від 02.12.1949 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/995_162 (дата звернення: 31.10.2019).
5. Міжнародний пакт про громадянські та політичні права : від 16.12.1966 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/995_043 (дата звернення: 31.10.2019).
6. Міжнародний пакт про економічні, соціальні і культурні права : від 16.12.1966 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/995_042 (дата звернення: 31.10.2019).
7. Статут Організації Об'єднаних Націй і Статут Міжнародного Суду : від 26.06.1945 // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/995_010 (дата звернення: 31.10.2019).

Одержано 01.11.2019

УДК 343.2/.7;347.1

Микола Миколайович Перепелиця,
кандидат юридичних наук, професор, професор кафедри оперативно-розшукової діяльності та розкриття злочинів факультету № 2 Харківського національного університету внутрішніх справ

Зарубіжний досвід розшуку безвісти зниклих осіб

Якщо вибірково проаналізувати досвід деяких країн, можемо побачити, що розшук осіб, безвісти зниклих, різниться. Так, у США в 2006 р. була створена національна пошукова електронна система NAMUS, яка містить файли про всіх зниклих, і ці файли перебувають у відкритому доступі. Користувач може сам шукати через систему зниклу людину за ознаками: зростом, кольором шкіри, статтю, віком, татуюванням [1, с. 168].

Створення схожої системи пошуку, передбачено в Україні Законом України «Про правовий статус осіб, зниклих безвісти» – це Єдиний реєстр осіб, зниклих безвісти за особливих обставин. Проблемою на сьогодні залишається те, що такий Реєстр, як визначено у вищевказаному законі, не є загальнодоступним, інформація про осіб, зниклих безвісти за особливих обставин, що міститься в Реєстрі, може надаватися родичам таких осіб, заінтересованим особам, заявнику, органам, уповноваженим на облік та/або розшук осіб, зниклих безвісти, у межах та обсязі законодавством, на підставі запиту про надання інформації, поданого до Комісії з питань осіб, зниклих безвісти за особливих обставин (ст. 15) [2]. Закон «Про правовий статус осіб, зниклих безвісти» вступив в силу ще 2 серпня 2018 року. Згідно з ним, вже у листопаді мав бути створений відповідний Реєстр. Втім, вимоги закону не реалізовані й досі. На сьогодні облік осіб, що зникли безвісти, веде відділ пошукової роботи Управління цивільно-військового співробітництва Міністерства оборони. Крім того, свої реєстри є в Міжнародного Комітету Червоного Хреста [3].

Генеральна прокуратура Мексики та Міністерство внутрішніх справ цієї країни створили спеціальний орган, який буде займатися роботою з пошуку зниклих безвісти людей. Так, створення нового відомства,

спрямовано на те, щоб привернути до своєї діяльності експертів, які вже працюють над пошуком зниклих людей, щоб результати їхньої роботи не зникли. Крім того, влада Мексики має намір залучати до роботи родичів зниклих, тому що найчастіше вони у своїх розслідуваннях отримують набагато більше результатів, ніж урядові організації [1, с. 168].

В Іспанії зниклими безвісти займаються як державні, так і різні некомерційні організації та асоціації. Існує велика некомерційна державна асоціація «Sosdesaparecidos», яка допомагає в пошуку рідним і близьким зниклих. У своїй роботі асоціація співпрацює з усіма державними правоохоронними органами та службами безпеки, а також з організаціями з пошуку зниклих безвісти з Польщі, Великобританії, Італії, Швейцарії, Франції, Литви, Нідерландів [1, с. 169].

Цей та інший міжнародний досвід, на нашу думку, є корисним для використання його в Україні. Так, вважаємо, що для нашої держави було б доцільно перейняти досвід США та створити реєстр осіб,

зниклих безвісти, вільний доступ до якого, мав би будь-хто, кому інформація з реєстру необхідна для професійної діяльності або для пошуку своїх рідних, близьких. Таким чином, вважаємо, що можна буде пришвидшити процес розшуку осіб, зниклих безвісти. Також, на нашу думку, для ефективної роботи з пошуку осіб, зниклих безвісти, в Україні, за прикладом Мексики, має бути розроблено та впроваджено «Програму з пошуку зниклих безвісти» в якій передбачити залучення до пошукових робіт їхніх родичів. Національній поліції України доцільно було б налагодити співпрацю із Іспанською некомерційною державною асоціацією «Sosdesaparecidos».

Список бібліографічних посилань

1. Кличков А. О. Окремі аспекти врегулювання правового статусу безвісно зниклих осіб у діяльності правоохоронних органів. *Науковий вісник публічного та приватного права*. 2017. Вип. 3. С. 166–171.
2. Юридична енциклопедія : в 6 т. / редкол.: Ю. С. Шемшученко (голова редкол.) та ін. Київ : Укр. енцикл., 1998. URL: http://leksika.com.ua/13500424/legal/bezvisna_vidsutnist (дата звернення: 24.07.2019).
3. Скачко І. Зниклі безвісти – закон, що не діє // Права людини в Україні. Інформаційний портал Харківської правозахисної групи : сайт. 12.04.2019. URL: http://khpg.org/index.php?id=1555066354 (дата звернення: 24.10.2019).

Одержано 31.10.2019

УДК 341.215.4

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

Міжнародні спеціалізовані інституції у сфері протидії торгівлі людьми

З моменту створення універсальної міжнародної організації ООН та таких регіональних організацій, як Рада Європи, ОБСЄ, права людини стали наріжним питанням у їхній діяльності та діяльності створених під їх егідою структур. Безумовно, значний внесок у становлення і розвиток цієї співпраці роблять статутні органи, інституції, посадові особи означених організацій, які «персоніфікують» їх правозахисну діяльність та визначають головні вектори співпраці держав-членів в означеному напрямку. Статутні органи, що створюються на основі положень установчих актів, мають широкі мандати, звертаються до широкої аудиторії і приймають рішення більшістю голосів. Разом із тим слід констатувати, що різноманітні виклики в галузі прав людини, зокрема таке негативне явище як торгівля людьми, вимагають створення спеціалізованих інституцій (призначення відповідальних посадових осіб) з чітко визначеною компетенцією.

У цьому зв'язку слід означити, що в межах ООН створено механізм спеціальних процедур метою якого є розгляд конкретних ситуацій в країні, або тематичних питань в усіх частинах світу. Зокрема, на універсальному рівні запроваджено посаду Спеціального доповідача з питання торгівлі дітьми, дитячої проституції і дитячої порнографії (далі – Спеціальний доповідач) на підставі резолюції 1990/68, яка уповноважила його розслідувати випадки експлуатації дітей в усьому світі, аналізувати першопричин торгівлі та сексуальної експлуатації дітей, виявляти нові форми цього явища, обмінюватися успішними практиками у боротьбі з ним і розробляти рекомендацій щодо реабілітації дітей, які стали жертвами торгівлі і сексуальної експлуатації й надавати Генеральній Асамблеї ООН і Комісії з прав людини доповіді та рекомендації стосовно захисту відповідних прав дітей. З тих пір мандат Спеціального доповідача неодноразово змінювався (резолюції Ради з

прав людини A/HRC/RES/7/13, A/HRC/RES/16/1, A/HRC/RES/25/6). Наразі він є єдиним мандатом у рамках системи спеціальних процедур ООН, що зосереджений виключно на правах дітей.

У своїй резолюції A/HRC/RES/7/13 Рада з прав людини поклала на Спеціального доповідача такі повноваження: проводити аналіз корінних причин торгівлі дітьми, дитячої проституції і дитячої порнографії; розглядати всі фактори, що сприяють цим явищам; виявляти приклади передової практики з метою прийняття заходів по боротьбі проти торгівлі дітьми, дитячої проституції і дитячої порнографії, здійснювати обмін прикладами такої практики і пропагувати їх; докладати зусилля задля пропаганди всеосяжних стратегій і заходів щодо попередження торгівлі дітьми, дитячої проституції і дитячої порнографії тощо. Рекомендації Спеціального доповідача в першу чергу стосуються урядів, органів ООН, підприємницького сектору та неурядових організацій.

На регіональному міжнародному рівні, зокрема в межах Ради Європи, було створено Групу експертів із заходів стосовно протидії торгівлі людьми (далі – ГРЕТА) на підставі Конвенції Ради Європи про заходи щодо протидії торгівлі людьми від 16 травня 2005 р. (СЄД № 197) (далі – Конвенція 2005 р.), що здійснює моніторинг за виконанням Конвенції сторонами. Група складається з 15 членів, які обираються Комітетом Сторін строком на 4 роки з можливістю переобрання на повторний строк.

Оціночна процедура стосується сторін Конвенції 2005 р. і поділяється на раунди, тривалість яких визначає ГРЕТА. З метою проведення належного оцінювання ГРЕТА визначає найдоцільніші засоби для здійснення оцінювання; може запитувати інформацію від громадянського суспільства; може додатково організовувати візити до країн тощо; готує свій звіт і висновки стосовно заходів, ужитих відповідною стороною для виконання положень Конвенції, які надсилаються заінтересованій стороні й Комітетові сторін. Звіт і висновки ГРЕТА оприлюднюються з моменту їхнього ухвалення разом з можливими коментарями відповідної сторони.

Комітет сторін може прийняти на основі звіту й висновків ГРЕТА рекомендації, адресовані цій стороні: a) стосовно заходів, яких слід ужити для виконання висновків ГРЕТА, і b) що мають на меті сприяння співробітництву з цією стороною для належного виконання Конвенції 2005 р. (Розділ VII).

ОБСЄ заснувала Бюро Спеціального представника і координатора по боротьбі з торгівлею людьми ОБСЄ (2003 р.) з метою підвищення інформованості суспільства про торгівлю людьми в усіх її формах і сприяння зміцненню політичної волі до боротьби з нею. На прохання держав-учасниць Бюро допомагає у виконанні прийнятих у межах ОБСЄ зобов'язань і рекомендацій. Бюро координує зусилля ОБСЄ по боротьбі з торгівлею людьми та співпрацює з іншими міжнародними організаціями, а також з відповідними суб'єктами громадянського суспільства.

Бюро наділено компетенцією щодо: співпраці з урядами, надання їм допомоги в розумінні поставлених перед ними завдань з приборкання торгівлі людьми і в прийнятті заходів для реалізації цих завдань; надання урядам допомоги у виробленні рішень і політики та пропозиції рекомендацій з питання про організацію боротьби з торгівлею людьми з метою виходу на рішення, що відповідають потребам окремих країн і міжнародними стандартами; надання урядам допомоги у створенні національних структур по боротьбі з торгівлею людьми, необхідних для ефективного внутрішньодержавного і транснаціонального співробітництва; підвищення обізнаності з метою акцентування уваги на складності цієї проблеми і необхідності пошуку всеосяжних рішень; розгляд усіх вимірювань торгівлі людьми, а саме торгівлі з метою сексуальної експлуатації, торгівлі з метою використання примусової і підневільної праці, включаючи внутрішньодержавне рабство, торгівлю з метою примусу до насильницького шлюбу, торгівлю органами і торгівлю дітьми; забезпечення ефективної взаємодії всіх агентів і зацікавлених сторін, що беруть участь у боротьбі з торгівлею людьми.

Спеціальний представник і координатор по боротьбі з торгівлею людьми ОБСЄ відвідує країни з метою стимулювання політичної волі до здійснення стратегій по боротьбі з торгівлею людьми та оцінки практичного стану справ у галузі боротьби з торгівлею людьми. Його завдання полягає в наданні державам-учасницям, на їхній запит, підтримки в реалізації законів і загального курсу з протидії торгівлі людьми та у просуванні заснованих на правах людини підходів при розробці стратегій та створення відповідних структур, а також у виконанні обґрунтованих рішень по боротьбі з торгівлею людьми.

Під егідою ОБСЄ також створено Альянс проти торгівлі людьми – неофіційна партнерська мережа, що являє собою широкий міжнародний форум, до складу якого входять міжнародні міжурядові та неурядові

організації (МОП, МОМ, Європол, Рада Європи, СНД, Хьюман Райтс Вотч (HRW) Міжнародний центр розвитку міграційної політики (МЦРМП), Міжнародний центр зниклих та експлуатованих дітей (ICMEC), Міжнародна організація кримінальної поліції (Інтерпол) тощо), що об'єднують сили для запобігання торгівлі людьми та боротьби з нею. Він допомагає розробляти ефективні спільні стратегії, об'єднує індивідуальні зусилля та надає державам-учасницям ОБСЄ і партнерам по співробітництву інноваційні та скоординовані підходи для посилення запобігання торгівлі людьми і боротьби з нею. Щороку Спеціальний представник проводить конференцію Альянсу високого рівня і два засідання Координаційної групи експертів Альянсу.

Виходячи з вищеозначеного слід констатувати, що міжнародне співтовариство в особі міжнародних міжурядових організацій, відповідно реагує на виклики і загрози в галузі забезпечення прав людини та протидії порушенням, зокрема, торгівлі людьми, під їх егідою створено інституції, механізми, що мають за мету враховувати особливості тієї чи іншої категорії осіб, надавати своєчасну допомогу, ставити питання та виносити їх на обговорення на рівень органів відповідних організацій і прийняття ними раціональних рішень у цій галузі із залученням держав-членів.

Одержано 28.10.2019

УДК 341.783

Альона Леонідівна Шевченко,
викладач кафедри міжнародного і європейського права юридичного факультету Харківського національного університету імені В. Н. Каразіна

Забезпечення інформаційної безпеки потерпілих персоналом Міжнародного кримінального суду

Враховуючи необхідність забезпечення безпеки потерпілих, значимість їхньої участі у справі, Статут Міжнародного кримінального суду (далі – Статут МКС) і його процесуальні акти приділяють значну увагу означеному питанню.

Правовий статус жертв злочинів регламентовано Статутом МКС, Правилами процедури і доказування (далі – ППД), а також іншими нормативно-правовими актами. Правові акти Суду використовують одночасно два поняття – «потерпілі» та «жертви злочинів», які є тотожними. Відповідно до ППД жертви злочину – (а) фізичні особи, які зазнали шкоди від будь-якого злочину, що підпадає під юрисдикцію Суду, а також (б) організації або установи, які зазнали безпосередніх збитків щодо будь-якого майна, призначеного для релігійних, освітніх, наукових, благодійних цілей, або щодо їх історичних пам'яток, лікарень та інших місць і об'єктів гуманітарного призначення (правило 85) [2].

Слід зазначити, що незалежно від класифікації, усі жертви мають спеціальний правовий статус, який у юридичній літературі йменується «правовий статус потерпілого», і який визначається як «правове становище потерпілого у кримінальному процесі, що визначається сукупністю правових норм, які регламентують суспільні відносини, пов'язані з визнанням особи потерпілою, виникненням, строком дії та припиненням повноважень потерпілого, процесуальними гарантіями» [3, с. 292]. Серед прав потерпілого найбільше значення має право на захист (ст. 68 Статуту МКС), яке безпосередньо пов'язане із забезпеченням інформаційної безпеки про що свідчать положення нормативних актів Суду.

Так, Статут МКС значну увагу приділяє інформуванню потерпілих про їх права, незалежно від стадії судового процесу, і покладає обов'я-

зок інформування на органи та персонал МКС. Відповідно до положень Статуту і процедурно-процесуальних актів МКС, безпосереднє забезпечення прав жертв злочинів здійснюється Секретарем і Секретаріатом [1; 2]. Секретар створює у складі Секретаріату Групу з надання допомоги жертвам і свідкам (Victims and Witnesses Section), а також Групу з питань участі жертв і відшкодування шкоди (Victims Participation and Reparations Section). У випадку допуску потерпілих, а також їх законних представників до участі у справі, на Секретаря покладається обов'язок повідомлення означених осіб про: судовий розгляд, зокрема, дату слухань та їх перенесення, а також дату винесення рішення; прохання, подання, клопотання і про інші документи, пов'язані з такими проханнями, поданнями і клопотаннями (правило 92(5) ППД). Секретар також зобов'язаний інформувати осіб, яким загрожує небезпека стосовно їх прав, передбачених Статутом МКС і ППД, а також про функції Групи з надання допомоги жертвам і свідкам та про можливості звернення до неї. Секретар забезпечує своєчасне ознайомлення потерпілих з відповідними рішеннями Суду, які можуть зачіпати їхні інтереси, на умовах конфіденційності. Секретаріат зберігає у надійному місці в захищеній електронній базі даних інформацію стосовно потерпілих, які з'являються до Суду, та осіб, яким загрожує небезпека, а також осіб, які їх супроводжують, і членів їх сімей. Доступ до цієї бази даних мають лише призначені співробітники Секретаріат і, у випадку необхідності, особи, призначені Палатою та учасниками [2; 3, с. 320].

Група з надання допомоги жертвам і свідкам має вживати необхідних заходів з метою забезпечення захисту і безпеки, а також розробки довго- та короткострокових планів захисту всіх потерпілих, які з'являються до Суду, та інших осіб, яким загрожує небезпека через свідчення свідків; повідомляє їм про те, де можна отримати юридичну допомогу щодо захисту їхніх прав, зокрема, стосовно їх свідчень; надає допомогу під час виклику для свідчення у Суді [1].

Забезпечення інформацією жертв злочинів має на меті виключення ситуації, коли жертва відчуває себе безправною і беззахисною в системі кримінальної юстиції. На особливу увагу заслуговує інформаційно-просвітницька діяльність МКС, відповідальність за розробку і реалізацію якої здійснює Секція суспільної інформації і документації Секретаріату МКС [3, с. 377]. Крім того, Група з питань участі жертв і відшкодування шкоди відповідальна за проведення інформаційно-просвітницької кампанії в інтересах потерпілих. Група також надає консультації Секції

суспільної інформації і документації Секретаріату з питань підготовки матеріалів стосовно жертв злочинів у межах загальної програми МКС з питань інформування і зв'язку. Так, було підготовлено інформаційні матеріали про права потерпілих і про те, яким чином потерпілі мають отримувати доступ до Групи з питань участі жертв і відшкодування, а також інших джерел допомоги і підтримки [4].

Отже, Статут МКС і нормативно-правові акти Суду наділяють відповідні органи і персонал широкими повноваженнями щодо надання допомоги і захисту потерпілих на всіх стадіях судового процесу, зокрема, забезпечення надійного рівня інформаційної безпеки.

Список бібліографічних посилань

1. Rome Statute of the International Criminal Court. URL: https://www.icc-cpi.int/resource-library/Documents/RS-Eng.pdf (дата звернення: 30.10.2019).
2. Rules of Procedure and Evidence of the International Criminal Court. URL: https://www.icc-cpi.int/iccdocs/pids/legal-texts/rulesprocedureevidenceeng.pdf (дата звернення: 30.10.2019).
3. Сыроед Т. Л. Субъекты (участники) международных уголовно-процессуальных отношений: понятие, виды, специфика правового статуса : монография. Харьков : ФИНН, 2010. 584 с.
4. Representing Victims before the International Criminal Court : A Manual for legal representatives / The Office of Public Counsel for Victims. URL: https://www.icc-cpi.int/iccdocs/opcv/manual-victims-legal-representatives-fifth-edition.pdf (дата звернення: 30.10.2019).

Одержано 30.10.2019

Наукове видання

ПРОТИДІЯ КІБЕРЗАГРОЗАМ ТА ТОРГІВЛІ ЛЮДЬМИ

Збірник матеріалів
Міжнародної науково-практичної конференції,
(26 листопада 2019 року, м. Харків)

Українською, англійською та російською мовами

Відповідальні за випуск: *О. В. Манжай*
Редактор: *О. В. Манжай*
Корегування списків бібліографічних посилань: *О. В. Манжай, С. С. Тарасова, П. О. Білоус*
Комп'ютерне верстання: *О. В. Манжай*

Формат 60х84 1/16. Ум. друк. арк. 11,24 Обл.-вид. арк. 12,4.
Тираж 200 пр.