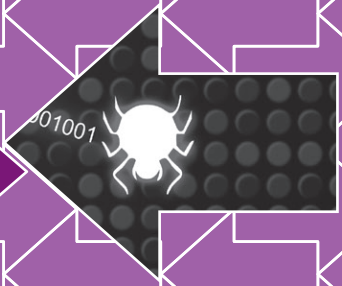
ПРОТИДІЯ



КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Матеріали Міжнародної науково-практичної конференції
27.05.2020 р. м. Харків

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

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ

Харківський національний університет внутрішніх справ

Canada

USOSCE U.S. Mission to the OSCE

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

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

Збірник матеріалів
Міжнародної науково-практичної конференції

(27 травня 2020 року, м. Харків)

Харків
Харківський національний університет внутрішніх справ
2020

УДК [351.74:343.85](062.552)
ББК 67.611.31я43
П83

Друкується згідно з рішенням оргкомітету за дорученням Харківського національного університету внутрішніх справ від 10.03.2020 № 41

П83 Протидія кіберзлочинності та торгівлі людьми : зб. матеріалів Міжнарод. наук.-практ. конф. (27 травня 2020 р., м. Харків) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. – Харків : ХНУВС, 2020. – 224 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. Досліджено використання інформаційних технологій і технічних засобів у протидії кіберзлочинності та торгівлі людьми.

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

Публікації наведено в авторській редакції.
Оргкомітет не завжди поділяє погляди авторів публікацій.
За достовірність наукового матеріалу, професійного формулювання, фактичних даних, цитат, власних імен, географічних назв, а також за розголошення фактів, що не підлягають відкритому друку, тощо відповідають автори публікацій та їх наукові керівники.

Електронна копія збірника безоплатно розміщується у відкритому доступі на сайті Харківського національного університету внутрішніх справ (http://www.univd.edu.ua) у розділі «Видавнича діяльність. Матеріали науково-практичних конференцій, семінарів тощо»), а також у репозитарії ХНУВС (http://dspace.univd.edu.ua/xmlui/)

Опубліковано Координатором проектів ОБСЄ в Україні в рамках проекту «Посилення кримінального переслідування торгівлі людьми з використанням інформаційних технологій в Україні», що впроваджується за фінансової підтримки урядів Канади та 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.
МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

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

УДК 004.7

Дмитро Володимирович ШВЕЦЬ,
доктор юридичних наук, доцент,
ректор Харківського національного університету внутрішніх справ

РЕАЛІЗАЦІЯ ПРОГРАМИ ІНФОРМАТИЗАЦІЇ СИСТЕМИ МІНІСТЕРСТВА ВНУТРІШНІХ СПРАВ УКРАЇНИ НА 2018–2020 РОКИ

Інформатизація діяльності, а саме підвищення ефективності роботи і взаємодії через максимальне використання інформаційно-комунікаційних технологій у реалізації завдань органами системи МВС є основним шляхом суттєвого покращення якості функціонування всієї системи правоохоронних органів. Розпорядженням Кабінету Міністрів України від 20 вересня 2017 р. № 649-р було схвалено Концепцію розвитку електронного урядування в Україні та запроваджено Єдину інформаційну систему МВС, а також розвиток сучасних електронних технологій у найбільш актуальних напрямах діяльності органів виконавчої влади, діяльність яких координується Кабінетом Міністрів України через Міністра внутрішніх справ України.

Концепція визначає напрями і механізми розбудови галузевої інформатизації з урахуванням кращих європейських практик. Метою є запровадження нової моделі спільного інтегрованого інформаційного середовища – базового інструменту для автоматизації інформаційних процесів у державі, побудованого за принципами технологічної незалежності, використання єдиних інтерфейсів і протоколів взаємодії та обміну інформацією у реальному часі, інтероперабельності електронних інформаційних ресурсів, а також повнофункціональна реалізація загальнодержавного сервісу електронної ідентифікації особи на базі єдиного «наскрізного» ідентифікатора з одночасним комплексним захистом інформаційних ресурсів.

Шляхи реалізації галузевої інформатизації, які пропонуються Концепцією, дозволять забезпечити економію витрат на виконання владних повноважень органами, які функціонують у сфері внутрішніх справ, за рахунок застосування сучасних інноваційних підходів, методологій і

технологій, у тому числі хмарної інфраструктури, Mobile-ID, просування методики опрацювання даних великих обсягів (Big Data), нормативно-правового врегулювання принципів «цифровий за замовчуванням», «одноразове введення інформації» та «сумісність за замовчуванням», а також розвитку публічно-приватного партнерства, у сферах відповідальності МВС.

Необхідність вироблення і закріплення нових концептуальних основ розвитку галузевої інформатизації виникає під час аналізу існуючого на цей час інформаційного простору Міністерства внутрішніх справ України. Він характерний тим, що обмін інформацією між ресурсами державних органів відбувається за принципом формування запиту і відповіді безпосередньо користувачем, тоді як доцільно забезпечити автоматизований доступ у межах повноважень і агрегацію даних.

До цього часу залишається неузгодженою архітектура взаємодії між автоматизованими інформаційними системами, бракує стандартизованих інтеграційних інтерфейсів для обміну даними. Крім того, нормативно-правова база у сфері інформаційно-телекомунікаційних технологій не відповідала сучасним вимогам і темпу розвитку, правове регулювання діяльності носило громіздкий, суперечливий і взаємодоповнюючий характер у різних нормативно-правових актах, тому вимагала уніфікації та гармонізації, в тому числі з нормами європейського законодавства. Організація ефективної електронної взаємодії інформаційних ресурсів і забезпечення їх належної якості потребує розробки та впровадження нового, системного, нормативно-правового й організаційно-методичного середовища.

Реалізація Концепції, передбачена на період до 2020 року, покликана забезпечити досягнення необхідного рівня оптимізації, ефективності та результативності виконання основних завдань із забезпечення формування державної політики щодо:

1) охорони прав і свобод людини, інтересів суспільства й держави, протидії злочинності, забезпечення публічної безпеки і порядку, а також надання поліцейських послуг;

2) захисту державного кордону та охорони суверенних прав України в її виключній (морській) економічній зоні;

3) цивільного захисту, захисту населення і територій від надзвичайних ситуацій та запобігання їх виникненню, ліквідації надзвичайних ситуацій, рятувальної справи, гасіння пожеж, пожежної і техногенної

безпеки, діяльності аварійно-рятувальних служб, а також гідрометеорологічної діяльності;

4) міграції (імміграції та еміграції), в тому числі протидії нелегальній (незаконній) міграції, громадянства, реєстрації фізичних осіб, біженців та інших визначених законодавством категорій мігрантів.

Реалізація Концепції сприятиме:

- створенню єдиного інтегрованого інформаційного середовища, побудованого за принципами наскрізної сумісності баз даних і технологічної незалежності, що поєднає ресурси апарату Міністерства та його територіальних органів з надання сервісних послуг МВС, Національної гвардії України, закладів, установ і підприємств, що належать до сфери управління МВС та центральних органів виконавчої влади, діяльність яких спрямовується і координується Кабінетом Міністрів України через Міністра внутрішніх справ України, для спільного контрольованого використання;
- впровадженню ефективної уніфікованої системи планування та управління інформаційними ресурсами з використанням сучасних європейських та євроатлантичних підходів і, відповідно, забезпеченню;
- консолідації ресурсів та підвищенню економічної ефективності їх використання;
- нормативно-правовому врегулюванню відносин у сфері галузевої інформатизації та електронної взаємодії на рівні державного апарату;
- створенню державного системного інтегратора, що одночасно забезпечить розробку та реалізацію високоефективних рішень щодо впровадження новітніх інформаційних технологій в діяльність системи МВС та інших центральних органів виконавчої влади;
- оптимізації технічних засобів та програмних комплексів, які автоматизують службові процеси суб'єктів системи МВС та інших центральних органів виконавчої влади з метою підвищення ефективності використання фінансових ресурсів.

Одержано 01.03.2020

УДК 340.13:004.056.5

Ольга Тимофіївна БАСАРАБ,
кандидат юридичних наук,
старший викладач кафедри теорії та історії держави і права та приватно-правових дисциплін Національної академії Державної прикордонної служби України імені Богдана Хмельницького

Олександр Корнійович БАСАРАБ,
кандидат технічних наук,
доцент кафедри зв'язку, автоматизації та кібербезпеки Національної академії Державної прикордонної служби України імені Богдана Хмельницького

Інна Тимофіївна ЛАРІОНОВА,
старший викладач кафедри тактичної та спеціальної фізичної підготовки Харківського національного університету внутрішніх справ

ДО ПИТАННЯ ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ ПРОТИДІЇ КІБЕРЗЛОЧИНАМ У КІБЕРПРОСТОРІ ДЕРЖАВНОЮ ПРИКОРДОННОЮ СЛУЖБОЮ УКРАЇНИ

В умовах ведення гібридної війни на сході нашої держави, проблема захисту інформаційно-телекомунікаційних систем органів державної влади, правоохоронних органів та військових формувань від кібернетичних злочинів, набуває особливого значення.

Віртуальний простір, у межах якого циркулює інформація, що обробляється з використанням інтегрованої інформаційно-телекомунікаційної системи «Гарт» являє собою окремий кібернетичний простір (кіберпростір) Державної прикордонної служби України (далі – ДПС України), який, з огляду на характер сучасних кіберзагроз також потребує надійного захисту [1].

Відповідно до статті 1 закону України «Про основні засади забезпечення кібербезпеки України» кіберзлочином (комп'ютерним злочином) вважається 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].

Правове регулювання протидії кіберзлочинам у кіберпросторі ДПС України здійснюють норми міжнародного права, Конституція України, закони України («Про захист інформації в інформаційно-телекомунікаціних системах» від 05.07.1994, «Про інформацію» від 02.10.1992, «Про Державну прикордонну службу України» від 03.04.2003, «Про телекомунікації» від 18.11.2003, «Про захист персональних даних» від 01.06.2010, «Про основні засади забезпечення кібербезпеки України» від 05.10.2017, «Про національну безпеку України» від 21.06.2018), укази Президента України (Концепція розвитку сектору безпеки і оборони України, від 14.03.2016 № 92/2016, «Про Стратегію кібербезпеки України» від 15.03.2016 № 96/2016, «Про затвердження доктрини інформаційної безпеки України» від 25.02.2017 № 47/2017), Постанови Кабінету Міністрів України («Про затвердження правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» від 29.03.2006 № 373, «Про затвердження порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури» від 23.08.2016 № 563, «Про затвердження загальних вимог до кіберзахисту об'єктів критичної інфраструктури» від 19.06.2019 № 518), накази та розпорядження Міністерства внутрішніх справ України та Адміністрації Державної прикордонної служби України (наказ Головного центру зв'язку, автоматизації та захисту інформації АДПСУ від 15.05.2018 №10од. «Про затвердження положення про центр кібербезпеки Головного центру зв'язку, автоматизації та захисту інформації», Концепція програми інформатизації системи Міністерства внутрішніх справ України на 2018-2020 роки від 05.11.2018 року № 18 КМ) та інші нормативно-правові акти.

Аналіз вищезазначеного законодавства дозволяє зробити висновок про наявність достатнього правового підґрунтя у сфері протидії кібернетичним злочинам у кібернетичному просторі ДПС України. Разом з тим, окремі питання правового забезпечення безпеки кіберпростору прикордонного відомства від злочинних посягань, на нашу думку, варті уваги нормотворців та потребують удосконалення.

Зокрема, у Стратегії кібербезпеки України, яка є основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України, практично відсутні положення

щодо організації кібербезпеки у ДПС України, як одного із суб'єктів сектору безпеки і оборони [3]. Схожа ситуація, також, з указом президента України «Про затвердження доктрини інформаційної безпеки України» від 25.02.2017 № 47/2017 та окремими актами уряду.

Таким чином, сучасний стан правового забезпечення протидії кіберзлочинам у кіберпросторі ДПС України потребує удосконалення, шляхом внесення змін та доповнень до низки нормативно-правових актів із обов'язковим урахуванням специфіки діяльності прикордонного відомства.

Список бібліографічних посилань

1. Басараб О. Т., Басараб О. К., Ларіонова І. Т. Щодо визначення поняття «кібербезпека Державної прикордонної служби України» – теоретико-правовий аспект. *Вісник Національної академії Державної прикордонної служби України. Серія: Юридичні науки*. 2019. Вип. 3. URL: http://nbuv.gov.ua/j-pdf/vnadpcurn_2019_3_5.pdf (дата звернення: 06.04.2020).
2. 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: 06.04.2020).
3. Про стратегію кібербезпеки України : Указ Президента України від 15.03.2016 № 96/2016 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 06.04.2020).

Одержано 07.04.2020

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 факультету № 1
Харківського національного університету внутрішніх справ

ЯК ПРОТИДІЯТИ НАВМИСНИМ ПІДПАЛАМ?

Останніми роками у засобах масової інформації України все частіше можна побачити новини, що стосуються підпалів автомобілів громадських активістів, приватних підприємців, чиновників, інших громадян.

Статистичні дані яскраво засвідчують контраст між зареєстрованою кількістю відповідних правопорушень (рис. 1) та числом осіб, яких реально було притягнено до відповідальності (рис. 2).

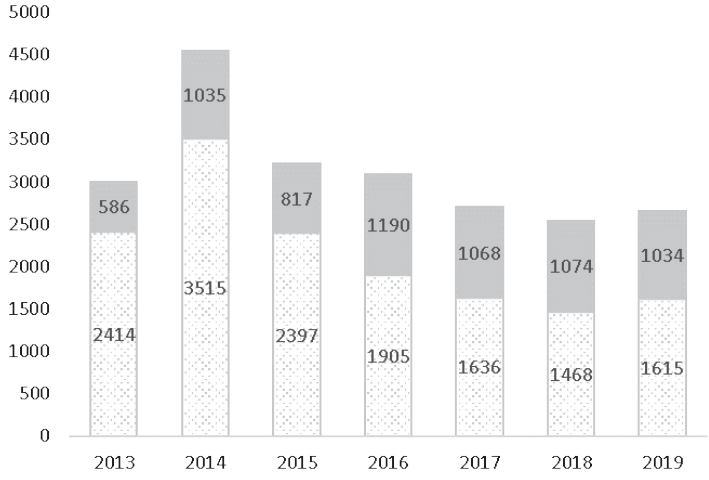


Рис. 1. Кількість зареєстрованих злочинів за ст. 194 Кримінального кодексу України (умисне знищення або пошкодження майна, у тому числі шляхом підпалу (відображено суцільною сірою фарбою)

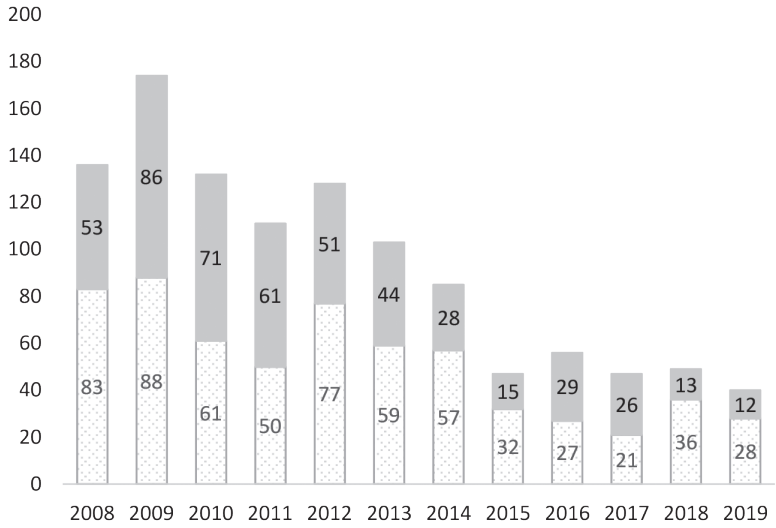


Рис. 2. Кількість засуджених осіб, до яких застосовано позбавлення волі на певний строк (відображено суцільною сірою фарбою) серед загальної кількості засуджених (ст. 194 Кримінального кодексу України)

Головні методи виявлення підпалювачів на сьогодні зводяться переважно до виставлення додаткових патрулів та вивчення результатів відеофіксації з камер спостережень, які встановлено недалеко від місць вчинення злочинів.

Указані заходи є вкрай затратними в частині людського ресурсу, а також часу. Водночас науковцями вже достатньо давно напрацьовано методики звуження місць пошуку підпалювачів у рамках географічного профілювання.

Для цього можуть бути застосовані різні підходи, серед яких методики:

1) М. Б. Ньютона 1980 рр. щодо звуження зони пошуку за спеціальною формулою, яка застосовується до серії злочинів. Передбачається, що після п'ятого випадку в серії зона пошуку злочинця може бути суттєво звужена;

2) Д. К. Росмо 1990 рр., який захистив дисертаційне дослідження та емпірично довів ефективність географічного профілювання, розробив-

ши свою унікальну формулу, запрограмовану в продукті Rigel Analyst компанії ECRI;

3) Д. Кантера 1990 рр., який експериментував з розрахунком експоненційних кривих у частині встановлення відстані до місця мешкання злочинця від місць вчинення злочину. Автор розробив свою методику географічного профілювання, подану в програмному комплексі Dragnet.

Крім наведеного, хотілося б також згадати вітчизняну розробку RICAS, яку збиралися впроваджувати в усіх регіональних підрозділах поліції, проте на сьогодні ця система використовується лише в м. Харкові і то в обмеженому вигляді.

Отже, хотілося б ще раз підкреслити важливість упровадження наукових досліджень у практичну діяльність поліцейських підрозділів, адже це може суттєво підвищити якісні показники роботи поліції та посилити довіру громадян до органів правопорядку.

Одержано 01.05.2020

УДК 343.9

Владислава Станіславівна БАТИРГАРЕЄВА,
доктор юридичних наук, старший науковий співробітник,
директорка Науково-дослідного інституту вивчення проблем
злочинності ім. акад. В. В. Сташиса
Національної академії правових наук України,
головний науковий співробітник Науково-дослідного інституту
інформатики і права Національної академії правових наук України

ІНФОДЕМІЯ ЯК УМОВА КРИМІНАЛІЗАЦІЇ КІБЕРПРОСТОРУ

У Стратегії національної безпеки України, затвердженій Указом Президента України від 26 травня 2015 року № 287/2015, до загроз інформаційній безпеці нашої країни віднесено ведення інформаційної війни проти України, відсутність цілісної комунікативної політики держави та недостатній рівень медіа-культури суспільства. Однак у цьому документі нічого не говориться про вплив на стан національної безпеки у країні такого явища, як інфодемії. І це недивно, адже інфодемія виявилася свого роду невідомою перемінною глобального масштабу, що виникла як феномен-сателіт пандемії COVID-19, яка спостерігається зараз у режимі реального часу по всьому світу.

Що ж розуміється під інфордемією, і чому вона є благодатним ґрунтом для криміналізації кіберпростору? Інфодемія – це свого роду масовий психоз в умовах глобалізації, при якому навіть незначний інформаційний поштовх стосовно ключової у конкретний момент проблеми здатний за короткий час обрушити весь світопорядок, що вже встиг перетворитися у подібність глобального соціального організму, до того ж ураженого чисельними соціально-економічними, військово-політичними та соціоморальними хворобами. Отже, інфодемія набуває вигляду, образно кажучи, дезінформаційного кванту, що в умовах сьогодення поширюється головним чином за допомогою кіберпростору, до того ж набагато швидше за будь-яку вірусну інфекцію або дію інших фізичних наслідків тих чи інших катаклізмів будь-якого масштабу. Не можна не погодитися з тим, що отримання, замість правдивої інформації, фейкової здатне погіршити шанси людства в цілому й окремо взятої людини на подолання існуючої загрози у вигляді нової небезпечної хвороби [1].

Дійсно, зараз у всесвітній павутині щохвилини з'являються як помилкові новини, так і відверто неправдиві інформаційні спекуляції щодо ситуації із коронавірусом. При цьому інфодемією може охоплюватися такі аспекти, як-от: а) причини виникнення вірусу COVID-19 (палітра щодо його походження надто значна – від реалізації теорій змови та підступів неземних цивілізацій до несанкціонованого виходу штамів вірусу з лабораторних умов); б) рівень захворюваності в цілому та в окремих регіонах світу та окремої країни (темпи поширення вірусу, кількість осіб, що захворіли, померли, вилікувалися, число непідтверджених випадків хвороби та ін.); 3) наслідки пандемії для економіки, політики, соціально-культурного життя та ментального здоров'я населення; 4) методи профілактики та лікування; 5) здатність національних систем охорони здоров'я протистояти пандемії; 6) стан кримінальної обстановки; 7) тощо.

Особливістю інфодемії є те, що правдивій інформації, яка розміщується в Інтернеті, надається надмірне емоційне забарвлення, або ж будь-яка інформація від самого початку генерується в дезінформаційному ключі. Хоча, повторимося, неможна виключати й ті випадки, коли інформація має суто помилковий характер. Поширення фейків, підняття градусу панічних настроїв, врешті-решт, загрожує продукуванням, з одного боку, небезпечної віктимної, а з другого боку, протиправної поведінки людей. Якщо вся увага людини в такі періоди масової інфодемічної істерії прикута до інформаційної сфери, то злочинці все частіше і частіше вдаються до вчинення протиправних діянь з використанням саме кіберпростору. До того ж це в значній мірі «убезпечує» їх злочину діяльність.

Отже, нескладно здогадатися, що будь-хто з нас є потенційною жертвою правопорушень у кіберпросторі, оскільки, кіберкримінал, що нерідко до того ж набуває організованих рис, в умовах пандемії та інфодемії, безсумнівно, намагатиметься збільшити прибутки від вчинення кібершахрайств, фінансових злочинів, реалізації контрафактних і нелегальних товарів, розквіту протиправних онлайн-індустрій (порнографія, незаконні казино та ін.) та скоєння інших видів кіберзлочинів. Відомості, одержувані з різних країн світу – з Китаю, США, Норвегії, Індії, Італії та Японії, – свідчать про те, що кіберкримінал, на відміну від традиційних видів організованих злочинних угруповань, стрімко зреагував на пандемію і використовує можливості, що відкрилися [2].

У березні 2020 р. Європол підготував доповідь, що має назву «Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis» («Пандемічний спекулянт: як злочинці експлуатують кризу COVID-19»), в якій стисло викладено позицію аналітиків Європолу щодо головних змін у кримінальній дійсності пандемічного періоду. Відмічається, що правопорушники швидко скористалися можливостями, які відкриває криза, адаптуючи до цього свою злочинну діяльність або вдаючись до вчинення нових злочинних дій. При цьому, ґрунтуючись на інформації, наданої державами-членами ЄС та власними експертами, Європолом робиться висновок про формування нового, так званого карантинного типу організованої злочинності, коли групи правопорушників реалізують цілі схеми, видаючи себе за представників органів влади та медиків із метою вчинення шахрайства і крадіжок [3].

Отже, пандемія та інфодемія несподівано вплинули на визначення вектора прогнозних розрахунків майбутнього кількісно-якісного стану злочинності (принаймні на найближчу перспективу) та розробку стратегій запобігання їй, виступивши специфічною умовою ще більшої криміналізації кіберпростору.

Список бібліографічних посилань

1. Ищенко Н. «Инфордемия» и как с ней бороться. *День*. 2020. № 37-38.
2. Овчинский В. Преступность COVID-19: как меняется криминал в период пандемии // Завтра : сайт. 31.03.2020. URL: http://zavtra.ru/blogs/prestupnost_covid_19 (дата звернення: 01.04.2020).
3. Pandemic Profiteering: How Criminals Exploit the COVID-19 Crisis // European Union Agency for Law Enforcement Cooperation. 27.03.2020. URL: https://www.europol.europa.eu/publications-documents/pandemic-profiteering-how-criminals-exploit-covid-19-crisis (дата звернення: 01.04.2020).

Одержано 07.04.2020

УДК 004.7

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

МОДЕРНІЗАЦІЯ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ «ІНФОРМАЦІЙНИЙ ПОРТАЛ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ»

Існуюча інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» (далі – ІПНП) призначена для інформаційно-аналітичного забезпечення діяльності Національної поліції України, наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних, що входять до Єдиної інформаційної системи МВС (далі – ЄІС МВС), забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, відносин документообігу та електронної взаємодії з МВС, іншими органами державної влади. Однак існуюча сьогодні система не цілком задовольняє зрослі вимоги щодо оперативності, надійності й захищеності. Тому виникає актуальне завдання модернізації системи ІПНП, яке досліджується в цій доповіді.

Метою модернізації (побудови) системи ІПНП є створення високонадійної, сучасної програмно-технічної інфраструктури поліції, що сприятиме захисту конституційних прав і свобод громадян та інтересів держави, суттєвому вдосконаленню інформаційного забезпечення поліції, інформаційній взаємодії правоохоронних та інших державних органів у сфері боротьби зі злочинністю, що забезпечить:

1) підвищення:

— надійності та ефективності;

— повноти й достовірності обліку інформації, утвореної у процесі діяльності поліції;

— оперативності інформаційної взаємодії між центральним та регіональними органами поліції;

2) формування інформаційних ресурсів ЄІС МВС;

3) надання безпосереднього оперативного доступу до інформаційних ресурсів ЄІС МВС та інших органів державної влади у випадках, визначених законодавством;

4) генерацію інтерфейсів та оброблення тимчасових наборів даних для здійснення інформаційної взаємодії органів (підрозділів) поліції, суб'єктів системи ІПНП з іншими органами державної влади, органами правопорядку іноземних держав, міжнародними організаціями;

5) надання пошукових та аналітичних сервісів для використання інформації з інформаційних ресурсів (баз даних) поліції, МВС та інших органів державної влади в межах службової діяльності відповідно до рівня доступу і повноважень за запитом або регламентом;

6) упровадження оброблення біометричних даних для можливості проведення портретної ідентифікації осіб, формування та використання дактилоскопічної інформації, в тому числі ДНК-профілів;

7) використання програмних компонентів геоінформаційних підсистем для візуалізації інформації у вигляді електронних карт, автоматичної зміни зображеного образу об'єкта залежно від зміни його характеристик, зміни масштабу та деталізації картографічної інформації в інформаційних ресурсах;

8) автоматизацію процесів управління силами та засобами поліції;

9) запровадження електронного документообігу в органах (підрозділах) поліції, обмін електронними документами з МВС та іншими органами державної влади;

10) захист інформації та розмежування доступу до інформації, що зберігається в базах даних системи ІПНП;

11) зниження витрат на експлуатацію та підтримку системи за рахунок уніфікації та спрощення використання її складових.

У доповіді розглянуто структуру системи ІПНП та основні вимоги до її функціонування.

Система ІПНП відповідно до Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» повинна включати: центральний ПТК; автоматизовані робочі місця; телекомунікаційну мережу доступу та комплексну систему захисту інформації з підтвердженою відповідністю.

Центральний ПТК ІПНП повинен включати територіально рознесені основний (ЦОД-1) та резервний центри обробки даних (ЦОД-2).

Автоматизовані робочі місця користувачів – робочі місця поліцейських та інших працівників поліції, обладнані комп'ютерною технікою, в тому числі планшетними комп'ютерами, що підключені до телекомунікаційної мережі доступу системи ІПНП і призначені для автоматизації службової діяльності, реалізації повноважень обробляти інформацію відповідно до наданого рівня доступу в системі ІПНП.

Телекомунікаційна мережа доступу – сукупність технічних і програмних засобів, призначених для обміну інформацією між складовими системи. Для захисту інформації в телекомунікаційній мережі (Єдина цифрова відомча телекомунікаційна мережа Міністерства внутрішніх справ України, канали передачі даних) використовуються засоби технічного та криптографічного захисту інформації з підтвердженою відповідністю.

Система ІПНП повинна забезпечити підвищення ефективності діяльності персоналу підрозділів за рахунок:

1) оперативності, достовірності, повноти, доступності та багатоваріантності автоматизованого обліку, оброблення, накопичення, передавання та подання облікової, оперативно-розшукової та довідкової інформації;

2) постійного автоматизованого контролю за виконанням службових обов'язків користувачами системи.

Одержано 02.03.2020

УДК 004.7

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

ПРОБЛЕМА ЗАБЕЗПЕЧЕННЯ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У БАЗАХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Третє тисячоліття по праву називають епохою інформатизації. ІТ-технології стали невід'ємною частиною практично всіх сфер життєдіяльності людства. Вони знаходять своє застосування у промисловій сфері, в державному і муніципальному управлінні, в соціальній сфері, економіці і навіть культурі.

Однак повсюдне використання ІТ-технологій несе в собі потенційні загрози і ризики не тільки для користувачів Інтернету і соціальних мереж. Значною мірою підвищується небезпека їх застосування як «інформаційної зброї» як проти державних, так і проти корпоративних та індивідуальних інформаційно-комунікаційних систем. Останнім часом тема використання і захисту персональних даних фізичних осіб набула особливої актуальності. Як відомо, Україна ратифікувала Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додатковий протокол до цієї Конвенції щодо органів нагляду та транскордонних потоків даних.

Відповідно до чинного законодавства персональними даними є будь-яка інформація про фізичну особу, яка дозволяє її ідентифікувати, зокрема про ім'я, дату і місце народження, місце роботи і проживання, освіту тощо. Персональними даними також можуть бути відомості про національність, освіту, сімейний стан, релігійність, стан здоров'я та ін. Крім того, згідно з рішенням Конституційного Суду України від 30 жовтня 1997 р. № 5-зп до персональних даних також належать дані про майновий стан і медична інформація (інформація про стан здоров'я, в тому числі з історії хвороби).

Шкода від кіберзлочинності має різноплановий характер: репутаційна шкода, що завдається компаніям у результаті витоку клієнтських даних, перебої в ланцюжках створення вартості, крадіжка інтелектуальної

власності хакерами тощо. Крім того, зростають витрати, пов'язані із судовими розглядами в рамках врегулювання позовів, поданих постраждалими від таких злочинів сторонами.

Стаття 5 Закону України «Про захист персональних даних» № 2297-VI визначає, що об'єктами захисту є персональні дані, які обробляються в базах персональних даних. У цій же статті визначено, що «Персональні дані, крім знеособлених персональних даних режимом доступу, є інформацією з обмеженим доступом». Таким чином, порушення конфіденційності доступу до персональних даних є порушенням і тягне за собою відповідальність, встановлену законом. Зараз в Україні вже застосовуються санкції за правопорушення та злочини, пов'язані з персональними даними фізичних осіб.

Аналогічні проблеми доступу можуть виникнути і в численних базах даних, які є підконтрольними Міністерству внутрішніх справ України. Тому проблема організації системи доступу до баз даних Національної поліції та Міністерства внутрішніх справ України є актуальною і визначає мету наукових досліджень, результати яких подані в цій доповіді.

Проведений аналіз поточного стану доступу до відомчих і суміжних баз даних показав, що поточна ситуація характеризується відсутністю стратегічних планів розвитку складових частин інфраструктури – серверного обладнання, систем зберігання даних, телекомунікаційного обладнання, систем захисту інформації.

Утворено велику кількість інформаційних баз (банків) даних і картотек та дрібних обчислювальних центрів, що значно ускладнює систематизацію, зберігання й аналітичну обробку інформації, наслідком чого є відсутність достовірних статистичних відомостей про ефективність реалізації підрозділами системи МВС завдань, віднесених до сфер їх відповідальності, що, у свою чергу, унеможливлює як належне перспективне прогнозування, так і оперативне прийняття дієвих управлінських рішень.

Таким чином, існує потреба у заходах з підвищення рівня кіберзахисту галузевих інформаційних ресурсів та впровадження і забезпечення функціонування систем управління інформаційною безпекою в підрозділах системи МВС та ЦОВВ, процеси із розбудови ІТ-інфраструктури повинні відбуватися у тісній взаємодії зі структурованою безпекою.

Актуальним для органів системи МВС є завдання з розширення спектру сервісних послуг для населення. Основою для вирішення цього

завдання є Концепція програми інформатизації системи Міністерства внутрішніх справ.

Реалізація Концепції передбачена на період до 2020 року та покликана забезпечити досягнення, через процеси інформатизації, необхідного рівня оптимізації, ефективності та результативності виконання основних завдань із забезпечення формування державної політики. У Концепції передбачено заходи організаційного забезпечення виконання програми. Можна виділити такі організаційні заходи:

1) розробка концептуальних засад розвитку ІТ-інфраструктури системи МВС та її інформаційної безпеки, забезпечення автоматизації, прозорості та контрольованості внутрішніх процесів;

2) впровадження захищеної телекомунікаційної інфраструктури МВС із метою забезпечення функціонування систем централізованого управління інформаційною безпекою в підрозділах системи МВС та Національної поліції;

3) забезпечення електронної взаємодії під час надання послуг населенню в електронному вигляді відповідно до вимог інформаційної безпеки в частині технічної сумісності засобів електронного підпису і спеціалізованого програмного забезпечення.

Одержано 25.03.2020

УДК 343.5

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

КІБЕРБУЛІНГ: КЛАСИФІКАЦІЯ ФОРМ ПРОЯВУ ТА СУЧАСНІ СВІТОВІ ТЕНДЕНЦІЇ

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 була 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 [1].

Пропонуємо визначення кібербулінгу, 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 особою, 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.

Кібербулінг хоча і походить від звичайного булінгу, але має ряд своїх особливостей, які значно підвищують його суспільну небезпечність у порівнянні з останнім. Тому світова спільнота акцентує свою увагу саме на дослідженні кібербулінгу та, навіть, криміналізації деяких його форм.

Існують різні підходи до класифікації кібербулінгу: Michael Nuccitelli виділяє 38 підвидів [5]; Laurie-ann M. Hellsten – 18 основних та 3 підвиди [4]; сайт Kaspersky – 10 видів [2], а Willard N. E. – 8 форм [3, с. 265-266]. Проаналізувавши наявну інформацію, пропонуємо схематично відобразити основні та похідні форми кібербулінгу.

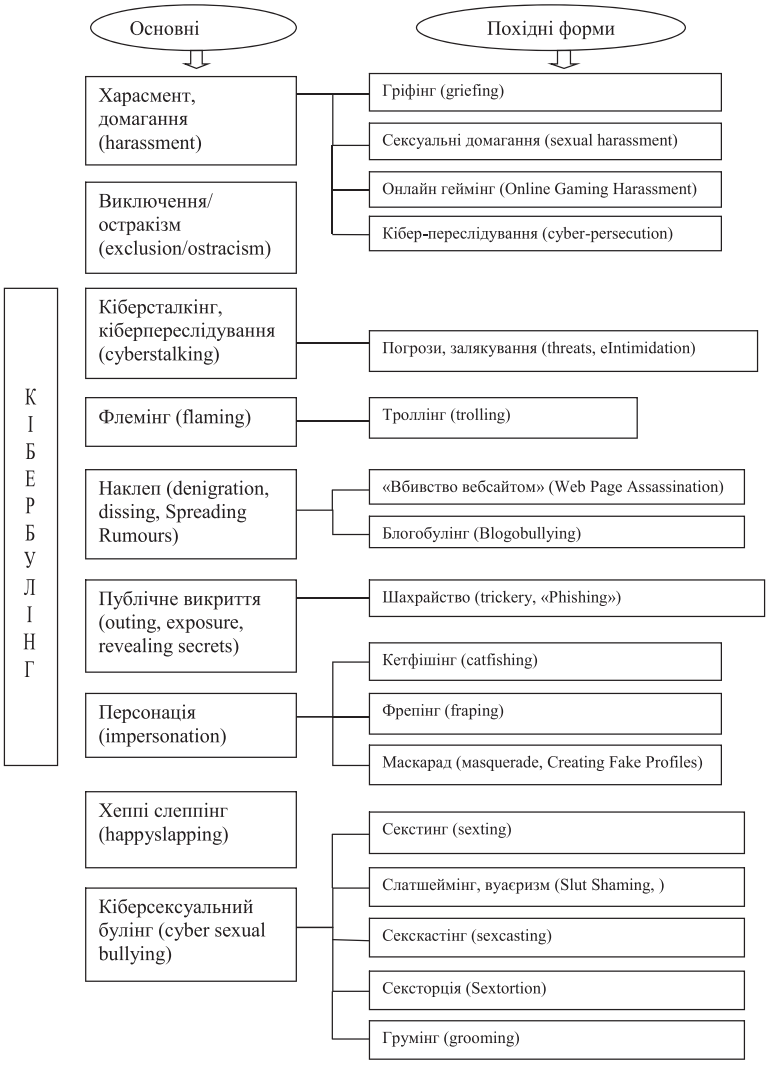


Рис 1. Класифікація форм кібербулінгу

Вважаємо, що основними формами кібербулінгу є: харасмент або домагання; соціальне виключення; кіберсталкінг або переслідування з загрозою завдання шкоди офлайн; флемінг або ворожі мовленнєві випади; наклеп; публічне викриття конфіденційної чи компрометуючої інформації; персонація або видавання себе за іншу особу; хеппі слеп-

пінг або фільмування проявів булінгу; кіберсексуальний булінг. Форми кібербулінгу, які зазначені у схемі праворуч, є похідними від основних, маючи вужчу специфіку, але не втрачаючи спільних рис. В Україні ці питання чітко не визначені законодавцем, хоча зарубіжний досвід свідчить, що саме кримінально-правовому регулюванню кібербулінгу та таким його підвидам, як харасмент та кіберсталкінг, секстинг, грумінг, приділяється велика увага. Наприклад, відповідальність за харасмент передбачена законодавством США, Великобританії, за кіберсталкінг – Іспанії, Франції, США, Великобританії, за секстинг – Австралії, США, Великобританії, за грумінг – США, Великобританії, за наклеп – Великобританії та Іспанії тощо.

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 [6].

Періодично у деяких країнах з'являються законодавчі ініціативи щодо криміналізації булінгу чи кібербулінгу (Бельгія, Кіпр, Ірландія, Італія, Португалія, Іспанія, Швеція, Великобританія, Австралія тощо). Однак більшість країн вважають ці явища достатньо охопленими чинними положеннями і немає конкретної потреби в додатковому нормативному регулюванні, особливо на кримінальному рівні.

В Україні кібербулінг регулюються ст. 173-4 КУпАП, а в разі значної суспільної небезпечності, відповідальність може наставати за ст. ст. 127 та 296 КК України. Однак, через законодавчу невизначеність, особливості суб'єкта правопорушення та складність доказування кібербулінг залишається безкарним.

Зважаючи на масштабність кібербулінгу вважаємо за необхідне через призму чинного Кримінального кодексу врегулювати механізм кримінально-правової відповідальності за це суспільно-небезпечне діяння. А відсутність законодавчого закріплення цього поняття та його видів, заважає належній реалізації наявних правових норм.

Список бібліографічних посилань

1. Опитування ЮНІСЕФ: понад третина молодих людей у 30 країнах світу потерпають від онлайн-булінгу // UNICEF : офіц. сайт. 04.09.2019. URL: https://www.unicef.org/ukraine/прес-релізи/опитування-юніcеф-понад-третина-молодих-людей-у-30-країнах-світу-потерпають-від-онлайн (дата звернення: 25.04.2020).
2. 10 Forms of Cyberbullying // Kids Safety by Kaspersky. 27.10.2015. URL: https://kids.kaspersky.com/10-forms-of-cyberbullying (дата звернення: 25.04.2020).
3. Parent Guide to Cyberbullying and Cyberthreats // Embrace Civility in the Digital Age. URL: http://www.embracecivility.org/wp-content/uploadsnew/2012/10/appK.pdf (дата звернення: 25.04.2020).
4. Laurie-ann M. Hellsten. An Introduction to Cyberbullying // University of Macerata. 23.03.2017. URL: http://docenti.unimc.it/alessandra.fermani/teaching/2016/15583/files/lh_slide-1-seminario (дата звернення: 25.04.2020).
5. Cyberbullying Examples and Types of Cyberbullying // iPredator Inc. URL: https://www.ipredator.co/cyberbullying-examples (дата звернення: 25.04.2020).
6. Sameer Hinduja, Justin W. Patchin. State Bullying Laws // Cyberbullying Research Center. November 2018. URL: https://cyberbullying.org/pdfs/2018_Bullying-and-Cyberbullying-Laws.pdf (дата звернення: 25.04.2020).

Одержано 30.04.2020

УДК 343.72:004.773+578.834.1

Сергій Миколайович ГУСАРОВ,
доктор юридичних наук, професор,
член-кореспондент Національної академії правових наук України,
заслужений юрист України, професор кафедри адміністративного права та процесу факультету № 1 Харківського національного університету внутрішніх справ

В'ячеслав Валерійович МАРКОВ,
кандидат юридичних наук, старший науковий співробітник,
декан факультету № 4 Харківського національного університету внутрішніх справ

НОВІ СХЕМИ КІБЕРШАХРАЇВ, ПОВ'ЯЗАНІ З ПОШИРЕННЯМ ГОСТРОЇ РЕСПІРАТОРНОЇ ХВОРОБИ COVID-19, СПРИЧИНЕНОЇ КОРОНАВІРУСОМ SARS-COV-2

У грудні 2019 року Муніципальна комісія охорони здоров'я м. Ухань, Китай, повідомила про виявлення групи випадків захворювання пневмонією у м. Ухань провінції Хубей. Згодом було встановлено, що збудником захворювання був новий коронавірус, який в подальшому отримав назву SARS-CoV-2.

11 березня 2020 року Всесвітня організація охорони здоров'я дійшла висновку, що спалах нового захворювання під назвою COVID-19 можна охарактеризувати як пандемію [1].

В Україні першу інфіковану особу було виявлено 03 березня 2020 року [2].

11 березня Кабінет Міністрів оголосив на всій території України карантин [3].

Майже з самого початку виявлення у Китаї нової короновірусної хвороби це широко висвітлювалося як закордонними, так і вітчизняними ЗМІ та медіа.

Мешканці багатьох країн світу, у тому числі українці, читаючи друковані видання та електронні джерела інформації, дивлячись новини по

телевізору чи в інтернет, та слухаючи їх по радіо, майже щодня чули про небезпеку поширення світом гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2.

У певної частини населення виникли побоювання, що вони або вже захворіли COVID-19, або можуть захворіти у будь-який момент.

Серед населення, через комп'ютерні соціальні мережі та інтернет-месенджери, почала поширюватися неправдива інформація про короновірус та протидію йому. Так на початку березня 2020 року в України швидко поширились неправдиві чутки про обробку в нічний час за допомогою вертольотів хімікатами вулиць населених пунктів для дезінфекції від короновірусу [4].

Серед певної частини українців виникла паніка, пов'язана з Covid-19, через що вони втратили пильність та стали більш вразливими та довірливими. Цим вирішили скористуватися аферисти, які для незаконного заволодіння коштами громадян почали використовувати сучасні цифрові комунікації та мережу інтернет для вчинення протиправних дій.

Так станом на 04 травня 2020 року працівниками підрозділів Департаменту кіберполіції Національної поліції України було перевірено 642 інформації щодо вчинення можливих протиправних дій, у тому числі онлайн-шахрайств, пов'язаних з коронавірусом. За результатами перевірок розпочато 58 кримінальних проваджень. Було ідентифіковано 166 осіб, які причетні до організації чи участі в шахрайських схемах, де використовувалась ситуація з COVID-19. Крім цього, за матеріалами українських кіберполіцейских складено 40 адміністративних протоколів за фактами порушення карантинних заходів та реалізації виробів медичного призначення та дезінфікуючих засобів.

Українська кіберполіція відзвітувала, що із початку запровадження в Україні карантинних заходів вони заблокували 9954 інтернет-посилання, що використовувалися шахраями в злочинних цілях, і 1945 шахрайських фінансових операцій за банківськими рахунками [5].

За даними Служби безпеки України станом на 04 травня 2020 року, за період дії карантинних заходів кіберфахівці СБУ заблокували понад 2,1 тисячі інтернет-спільнот із загальною аудиторією понад 900 тис. користувачів, викрили 301 інтернет-агітатора, які поширювали різноманітні фейки про епідемію COVID-19.

Фахівці Служби безпеки України нейтралізували 103 кібератаки на інформаційні ресурси державних органів влади протягом першого

кварталу 2020 року. Починаючи з березня, значна кількість атак відбувається проти відомств, що забезпечують боротьбу з COVID-19 – протидії таким атакам приділяється особлива увага.

Також СБУ зазначає, що з початку карантину хакерські угруповання, зокрема, масово направляють на поштові скриньки державних установ електронні листи на тематику коронавірусу. Насправді до цих листів прикріплені файли зі шкідливим програмним кодом, який активізується при відкриванні листа.

За оприлюдненою інформацією більшість хакерських атак скеровані російськими спецслужбами, що намагаються отримати віддалений доступ до комп'ютерів українських держорганів. Потім вони планують спотворювати чи знищувати дані, поширювати фейки нібито від імені держструктур, а також дискредитувати дії української влади. Загалом у січні-березні СБУ припинила роботу майже 2 тисяч вебресурсів, які хакери використовували для здійснення кібератак [6].

До речі, через зазначений вище спосіб поширення шкідливого програмного забезпечення, кібертерористи також можуть розповсюджувати віруси-шифрувальники, які знищують інформацію на зараженому пристрої [7].

Шахрайства пов'язані із поширенням COVID-19 скоюють не тільки в Україні. Так кіберспеціалісти поліції та спецслужб Федеративної республіки Німеччини виявили близько 90 шахрайських сайтів німецькою мовою, метою яких було привласнення державної фінансової допомоги для постраждалих підприємств від наслідків обмежувальних заходів щодо протидії епідемії COVID-19.

Так на початку квітня 2020 року було виявлено фішинговий вебсайт Міністерства економіки федеральної землі Північний Рейн-Вестфалія, який містив усі розділи і вбудовані елементи справжнього сайту Міністерства. Підробка мала один додатковий розділ – а саме онлайн-заявку на отримання субсидії для індивідуальних підприємців, які зазнають збитків через епідемію COVID-19 у Німеччині і заходи для боротьби з нею. Як вважають фахівці, від 3500 до 4000 осіб могли заповнити фейкову заявку, надавши шахраям усі конфіденційні дані, які ті, своєю чергою, використовують уже під час подавання справжніх заявок. Тільки банківські реквізити у цьому випадку будуть фейковими. Замість них будуть використовуватися так звані bankdrops – банківські рахунки, доступ до яких раніше отримали шахраї

Тільки з початку березня у світі зареєстровано близько 80 тисяч доменних імен зі словами Corona і COVID-19. Скільки з них призначені для добрих, а скільки – для злочинних цілей, ніхто навіть не береться оцінювати [8].

Для скоєння протиправних дій кібершахраї також надсилають фішингові електронні листи чи повідомлення у месенджерах та соціальних комп'ютерних мережах від імені, наприклад, Всесвітньої організації охорони здоров'я, Міністерства охорони здоров'я України, Центру громадського здоров'я МОЗ України, відомих лікарів тощо.

Зазвичай такі фейкові повідомлення та електронні листі містять або посилання на фішингові вебсайти, або вкладення із файлами, які шляхом застосування шахраями методів соціального інжинірингу, користувачі відкривають щоб ознайомитися із їх вмістом.

На сьогодні можна виділити за змістом наступні типи електронних шахрайських повідомлень та оголошень, пов'язані із поширенням гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2 [9, 10]:

1) від банківських установ про уточнення чи перевірку даних клієнта для:

— отримання ним соціальних виплат (по безробіттю, пенсіонерам та іншим категоріям громадян);

— уникнення ним штрафів за несвоєчасні платежі за кредитом;

2) від міжнародних організацій та благодійних організацій з проханням перевести кошти на боротьбу з вірусом;

3) від закордонних (наприклад, з азіатських країн) медичних організації чи дослідницьких центрів, які пропонують отримати чималі кошти за участь у анкетуванні щодо вивчення стану поширення короновірусу у певному регіоні;

4) від продавців товарів для боротьби із короновірусом:

— засобів індивідуального захисту (медичних та захисних масок, респіраторів, халатів тощо);

— медичних виробів (термометрів тощо);

— дезінфекторів;

— тестів на короновірус;

— неіснуючих ліків від короновірусу;

5) про начебто приховування органами державної влади:

– реальної кількість захворілих;
– способи поширення вірусу;
– ефективних способів лікування.

Зазвичай всі вищезначені шахрайські схеми направлені на незаконне отримання інформації про номер банківської картки, термін її дії та коду безпеки, для подальшого несанкціонованого списання коштів з банківського рахунку потерпілого, або на незаконне заволодіння коштами потерпілої особи під час продажу несправжніх або неіснуючих товарів та послуг.

Список бібліографічних посилань

1. COVID-19 – хронология действий ВОЗ // Всемирная организация здравоохранения : офиц. сайт. 27.04.2020. URL: https://www.who.int/ru/news-room/detail/27-04-2020-who-timeline---covid-19 (дата звернення: 10.05.2020).
2. В Україні підтвердили перший випадок зараження коронавірусом // РБК-Україна : сайт. 03.03.2020. URL: https://www.rbc.ua/ukr/news/ukraine-podtverdili-pervyy-sluchay-zarazheniya-1583227440.html (дата звернення: 10.05.2020).
3. Про запобігання поширенню на території України коронавірусу COVID-19 : Постанова Кабінету Міністрів України від 11.03.2020 № 211 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/211-2020-п (дата звернення: 10.05.2020).
4. СБУ спростувала фейк про нічне розпилення «хімікатів від коронавірусу» над Києвом // 5 канал : сайт. 17.03.2020. URL: https://www.5.ua/kyiv/sbu-sprostuvala-feik-pro-nichne-rozpylennia-khimikativ-vid-koronavirusu-nad-kyievom-210548.html (дата звернення: 10.05.2020).
5. Кіберполіція заблокувала майже 10 000 Інтернет-посилань, які шахраї використовували під час пандемії // Кіберполіція України : офіц. сайт. 04.05.2020. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-zablokuvala-internet-posylan-yaki-shaxrayi-vykorystovuvaly-pid-chas-pandemiyi-6499/ (дата звернення: 10.05.2020).
6. СБУ нейтралізувала 103 кібератаки і завадила російським хакерам отримати дані держустанов // Служба безпеки України : офіц. сайт. 06.05.2020. URL: https://ssu.gov.ua/ua/news/3/category/21/view/7559 (дата звернення: 10.05.2020).
7. Бєляєва Є. Г., Рвачов О. М. Віруси-шифрувальники як головна зброя кібертерористів // Актуальні питання протидії кіберзлочинності та торгівлі

людьми : зб. матеріалів Всеукр. наук.-практ. конф. (м. Харків, 15 листоп. 2017 р.) / МВС України, Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків : ХНУВС, 2017. С. 121–124.

8. Як шахраї в Німеччині використовують коронавірус у своїх цілях // Deutsche Welle : сайт. 20.04.2020. URL: https://www.dw.com/uk/a-53147244 (дата звернення: 10.05.2020).
9. Увага, шахраї! Коронавірус допомагає аферистам створювати нові шахрайські схеми // Незалежна асоціація банків України : сайт. 27.03.2020. URL: https://nabu.ua/ua/uvaga-shahrayi-koronavirus-dopomagaye-aferistam.html (дата звернення: 10.05.2020).
10. Засаднюк А. Ліки «від коронавірусу» та інші шахрайства. Як легко померти через власну довірливість // УНІАН : сайт. 27.04.2020. URL: https://www.unian.ua/society/liki-vid-koronavirusu-ta-inshi-shahraystva-yak-legko-pomerti-cherez-vlasnu-dovirlivist-novini-ukrajini-10975121.html (дата звернення: 10.05.2020).

Одержано 11.05.2020

УДК 347.77.025

Анастасія Олександрівна ДОРОШ,
курсантка 3 курсу факультету № 2
Харківського національного університету внутрішніх справ

Олександр Романович ШИШКА,
кандидат юридичних наук, доцент,
доцент кафедри цивільно-правових дисциплін факультету № 4
Харківського національного університету внутрішніх справ

ДОМЕННЕ ІМ'Я ЯК ОБ'ЄКТ ЦИВІЛЬНИХ ПРАВ

Сьогодні людські відносини все більше переходять у віртуальну площину, все більш інтенсивно розвиваються інформаційно-технологічні відносини, що супроводжується виникненням нових об'єктів у сфері ІТ-відносин, які потребують правового регулювання та належного правового визначення. У зв'язку із цим доменні імена як об'єкти цивільних прав потребують сьогодні чіткого правового встановлення через належне правове регулювання відносин (як абсолютних, так і відносних), що виникають з приводу таких благ, чіткого визначення правовою природою доменного імені, способів його захисту та відчуження тощо

Слід сказати, що для позначення певного сайту використовується доменне ім'я, яке створюється за допомогою доменів різних рівнів. На практиці все це має такий вигляд. Наприклад, Харківський національний університет внутрішніх справ володіє сайтом з IP-адресою – 185.67.1.153, де сайт має назву - «http://univd.edu.ua», при цьому доменним ім'ям є «univd.edu.ua», а доменами – «univd», «edu» і «ua».

Серед базових нормативно-правових актів, які встановлюють правовий режим доменних імен як об'єктів цивільних прав є ЦК України, Закони України «Про охорону прав на знаки для товарів і послуг» та «Про телекомунікацію», Постанова Кабінету Міністрів України від 12.04.2002 № 522 «Про затвердження Порядку підключення до глобальних мереж передачі даних» (далі – Постанова КМУ від 12.04.2002 № 522) тощо.

Вперше в Україні поняття «доменне ім'я» з'явилося у Постанові КМУ від 12.04.2002 р. № 522 під яким розуміється буквено-цифровий вираз, що ідентифікує будь-який комп'ютер абонента у мережі Інтернет. У

ст. 1 Закону України «Про охорону прав на знаки для товарів і послуг» вказано, що доменне ім'я – це ім'я, яке використовується для адресації комп'ютерів і ресурсів в Інтернеті, а в ст. 1 Закону України «Про телекомунікації» це позначення (словесне, цифрове, словесно-цифрове), яке використовується для ідентифікації діяльності юридичних і фізичних осіб в мережі Інтернет, з будь-якою метою.

Наведене демонструє, що чинне законодавство не містить єдиного правового підходу до розуміння правового поняття «доменне ім'я», що породжує проблеми при спробах визначення правової природи доменного імені, як і його правового режиму як об'єкту цивільних прав.

Слід також сказати, що сьогодні ведуться дискусії з приводу того, чи слід вважати доменне ім'я майном, і відповідно, об'єктом права власності, чи це є об'єкт права інтелектуальної власності. Деякі дослідники порівнюють доменне ім'я з товарним знаком.

Судова практика на сьогодні визначилась з тим, що доменне ім'я це сфера права власності. Так, Європейський суд з прав людини у своєму рішенні у справі «Паеффген проти Німеччини (PAEFFGEN GMBH v. Germany, № 25379/04, 21688/05, 21722/05, 21770/05, ECHR 2007)», вказав на те, що власник доменного імені вправі самостійно визначати способи його використання (розмістити рекламу, сайт про послуги і товари, зробити доступ платним або безкоштовним, здавати доменне ім'я в оренду, продати його). Тому виключне право на використання доменного імені має економічну цінність, а відповідно являється правом власності в змісті статті 1 Протоколу № 1 до Конвенції про захист прав людини і основних свобод.

Опосередковано на це звертає увагу і Постанова Пленуму ВСУ від 27.02.2009 № 1 «Про судову практику у справах про захист гідності та честі фізичної особи, а також ділової репутації фізичної та юридичної особи» де у п. 12 визначено: «Належним відповідачем у разі поширення оспорюваної інформації в мережі Інтернет є автор відповідного інформаційного матеріалу та власник веб-сайту».

Наведене демонструє, що доменне ім'я слід вважати різновидом майна, майновим правом та, відповідно, об'єктом права власності, а отже об'єктом цивільних прав. Воно цілком підпадає під охорону ст. 1 Протоколу № 1 Конвенції про захист прав людини і основоположних свобод. Тому вважаємо, що в науці цивільного права є потреба в проведенні ревізії на предмет встановлення місця доменних імен в системі об'єктів цивільних прав.

Одержано 11.05.2020

УДК 316.624

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

Станіслав Олександрович ЛАРІОНОВ,
кандидат психологічних наук, доцент,
начальник кафедри психології та педагогіки
Національної академії Національної гвардії України (м. Харків)

ПРОФІЛАКТИЧНА РОБОТА З ПРОТИДІЇ СЕКСУАЛЬНОМУ НАСИЛЬСТВУ ЩОДО ДИТИНИ

Сексуальне насильство та комерційна сексуальна експлуатація є одним з найбільш тяжких порушень прав дитини. За тяжкістю завданих травм і наслідків сексуальне насильство та експлуатація прирівнюються до тортур і катування. Проблема визнання посилення сексуального насильство щодо дітей залишається серйозною у більшості країн, часто оповитою секретами, стигмами і табу. Сексуальне насильство щодо дітей не просто поширена проблема, досить часто за дане злодіяння кривдник не несе покарання. По-перше, тому що в це неможливо повірити, тому батьки часто заперечують, не вірять розповідям дітей або намагаються якомога швидше про це забути. По-друге, тому що діти не розповідають про такий злочин. Першим кроком, на шляху подолання цього негативного явища, є своєчасне виявлення та усунення негативних факторів, що зумовлюють протиправну, злочинну поведінку людей.

Опрацювавши низку соціально-психологічних досліджень [1, 2, 3, 4] ми виокремили основні види і завдання профілактичної роботи з протидії сексуальному насильству щодо дітей.

Первинна профілактика сексуального насильства щодо дітей – це сукупність заходів спрямованих на інформування про наявність проблеми, попередження розвитку чинників ризику виникнення сексуального насильства щодо дітей; формування в суспільстві ненасильницького світогляду спрямованого на дотримання законослухняної позиції; не-

прийняття насильницької моделі виховання дітей та насильницької поведінки в сім'ї.

Основні завдання первинної профілактики:

1) інформування дітей, молоді, батьків, педагогічних працівників, працівників поліції і соціальних служб у справах дітей про причини, ризики, ознаки, наслідки сексуального насильства щодо дітей в сім'ї та комерційної сексуальної експлуатації дітей; про правила безпечної поведінки дитини; про законодавство, покарання кривдників, захист постраждалих;

2) поширення правової освіти населення; спростування міфів, стереотипів, викорінення упереджень, звичаїв щодо насильства в сім'ї;

3) формування негативного ставлення з боку суспільства до фактів насильства в сім'ї; формування у дітей ненасильницького світогляду;

4) статеве виховання дітей та молоді; забезпечення підлітків необхідною грамотною інформацією, що допоможе їм адаптуватися до змін у період статевого дозрівання; дошлюбна підготовка молоді, підготовка до відповідального батьківства;

5) здійснення постійно діючого навчання, підвищення кваліфікації для всіх категорій фахівців (поліцейських, вчителів, соціальних педагогів, психологів, служб у справах сім'ї тощо), які працюють у сфері захисту дітей та попередження насильства щодо дітей.

Вторинна профілактика сексуального насильства щодо дітей – це сукупність заходів, спрямованих на раннє виявлення, усунення та подолання чинників, які сприяють скоєнню сексуального насильства щодо дитини конкретними особами; виявлення сімей, що входять до «групи ризику», де зафіксовано чи спостерігається жорстоке ставлення до дітей, членів родини, домашніх тварин; роботу з дітьми «групи ризику»: формування у них умінь та навичок безпечної поведінки, уявлення про діяльність установ та організацій, які можуть допомогти в ситуаціях насильства; зміну ризикованої поведінки дитини на адаптивну.

Основні завдання вторинної профілактики:

1) розроблення та впровадження системи раннього виявлення ситуацій підвищеного ризику виникнення сексуального насильства щодо дитини в сім'ї та комерційної сексуальної експлуатації дітей;

2) виявлення та нейтралізація чинників, які сприяють скоєнню секснасильства щодо дитини конкретними особами;

3) підтримка сімей, які перебувають у складних обставинах, організація їх соціально-психологічного супроводу;

4) підвищення кваліфікації психологів, педагогів, працівників поліції, фахівців соціальних служб у справах дітей щодо методів своєчасного виявлення представників групи ризику; виховання дітей, які мають девіантну поведінку, психічні відхилення тощо; формування у дітей життєвих умінь і навичок безпечної поведінки.

Третинна профілактика сексуального насильства щодо дітей – це сукупність засобів втручання у ті ситуації, коли сексуальне насильство щодо дитини вже здійснено з метою недопущення рецидиву та реабілітації дитини, яка зазнала насильства і членів її родини. В основному третинна профілактика є індивідуальною і передбачає тривалу роботу і комплекс соціальних послуг різних фахівців і організацій, в тому числі й міжнародних.

Основні завдання третинної профілактики: 1) кризове втручання та вилучення дитини з ситуації секснасильства; 2) надання комплексної допомоги дитині, яка зазнала сексуального насильства, та членам її сім'ї; 3) вивчення і усунення чинників та умов вчинення сексуального насильства конкретною особою; 4) реабілітація потерпілих; 5) розробка та забезпечення ефективного функціонування реабілітаційних програм для дітей, які зазнали сексуального насильства в сім'ї та постраждали внаслідок комерційної сексуальної експлуатації.

Слід зазначити, що сексуальне насилля в сім'ї та комерційна сексуальна експлуатація дитини, в майбутньому призводять до зростання низки проблем, як для особистості так і для соціуму в цілому, а саме: алкоголізації, наркотизації, порушень порядку і закону, суїцидальної, агресивної, залежної поведінки тощо. Тому профілактична робота щодо проблеми сексуального насильства дітей повинна бути комплексна і системна, з координацією взаємодії різноманітних соціальних інститутів (психологів, вчителів, суддів, працівників поліції, прокуратури, соціальних служб захисту дітей, медичних працівників).

Список бібліографічних посилань

1. Максимова Н. Ю., Мілютіна К. Л. Соціально-психологічні аспекти проблеми насильства. Київ : Комітет сприяння захисту прав дітей, 2003. 342 с.
2. Підготовка працівників структурних підрозділів Національної поліції України у частині забезпечення та захисту прав дітей. Частина 1. :

навч.-метод. посіб. / за заг. ред. Т. В. Журавель, Л. В. Зуб, О. В. Ковальова, Ю. В. Пилипас. Київ : ФОП Буря О. Д., 2019. 515 с.
3. Сексуальне насильство над дітьми: причини, наслідки, профілактика : інформ.-метод. посіб. / авт.-упоряд. Т. П. Цюман, Ю. М. Малієнко ; за заг. ред. Т. П. Цюман. Київ : ФОП Пономаренко Я. М., 2011. 76 с.
4. Формування навичок безпечної поведінки дітей. Частина 1. Вчимо дитину захищатися : метод. посіб. / авт.-упоряд.: Т. П. Цюман, О. Л. Нагула ; за заг. ред. Т. П. Цюман. Київ : ФОП Буря О. Д., 2017. 52 с.

Одержано 29.04.2020

УДК 347.440.44

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

Владислав Вікторович ХРОМЕНКОВ,
курсант 3 курсу факультету № 4
Харківського національного університету внутрішніх справ

ПРОТИДІЯ КІБЕРЗЛОЧИНАМ В ДЕРЖАВНИХ ЗАКУПІВЛЯХ

В національному законодавстві основу публічних закупівель було закладено розпорядженням КМ України від 12 серпня 1993 р. № 604-р «Про заходи щодо підготовки і проведення Міжнародного тендеру з розв'язання проблеми перетворення об'єкта "Укриття" Чорнобильської АЕС в екологічно безпечну систему».

Наступним кроком було затвердження «Положення про порядок організації та проведення міжнародних торгів (тендерів) в Україні» від 21 жовтня 1993 р. № 871, відповідно до нього визначався порядок організації та проведення в Україні виключно міжнародних торгів (тендерів) для іноземних, а також українських підприємств, установ і організацій, що гарантувало замовникові виконання у межах погодженої вартості необхідних поставок товарів, обсягів робіт і послуг. Але вже з 1997 року процедура закупівель запроваджується і на внутрішньому ринку України відповідно до постанови КМ України «Про організацію та проведення торгів (тендерів) у сфері державних закупівель товарів (робіт, послуг)» від 28 червня 1997 р. № 694.

Прийнятий 19 вересня 2019 р. Закон України «Про внесення змін до Закону України «Про публічні закупівлі» та деяких інших законодавчих актів України щодо вдосконалення публічних закупівель» № 114-IX містить в собі квінтесенцію 23 років роботи законодавця над постійним і густо необґрунтованим ускладненням процедури закупівлі. Тобто стартувавши з першого (і єдиного) тендера викликаного глобальною техногенною катастрофою ми опинилися в ситуації, коли державні

установи абсолютно всі свої закупівлі здійснюють виключно публічно, а починаючи з 50 тисяч гривень – шляхом оголошення відкритих торгів.

З того часу відбулося багато як юридичних так і фактичних змін в природи тендерних відносин (економічних, цивільних, господарських, організаційних, адміністративних, кримінальних, технічних), що виникають у зв'язку зі здійсненням державних закупівель, та конкуренції серед нормативних актів, які ці відносини регулюють.

Резонансне затримання співробітниками НАБУ за підозрою у розтраті понад 149 млн грн державних коштів заступника Міністра оборони України та директора Департаменту державних закупівель та постачання матеріальних ресурсів Міноборони знову привертає увагу до державних закупівель.

Окрім цього були виявлені інші вразливості. Так у система Prozorro дозволяла отримати доступ до закритих даних, зокрема, про запропоновані учасниками ціни ще до старту торгів.

Згідно з розслідуванням видання, вразливим місцем у деяких типах тендерів став порядок використання його учасниками електронного цифрового підпису (ЕЦП).

Зазначається, що компанії не зобов'язані закріпляти ЕЦП свій пакет документів (лиш в деяких випадках замовник вимагає цього), але більшість із них роблять це автоматично. При перевірці дійсності ЕЦП на сайті Мін'юсту можна натиснути лише одну кнопку – «Зберегти» – та отримати доступ до всього підписаного ним файлу: збережений файл завантажуєте в стандартну програму «Блокнот» і отримуєте, зокрема, й інформацію про цінову пропозицію. Таким чином учасникам торгів на Prozorro почали надходити пропозиції продажу такої інформації про початкові ставки конкурентів[1].

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

1 https://www.the-village.com.ua/village/business/news/274923-u-sistemi-prozorro-viyavili-bag-scho-dozvolyae-otrimati-dostup-do-zakritih-danih-auktsionu

Як висновок можемо зазначити таке:

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

— законодавство з державних закупівель потребує уніфікації та удосконалення.

Одержано 11.05.2020

УДК 343.431

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

ОСНОВНІ ПРИЧИНИ ВЧИНЕННЯ ТОРГІВЛІ ЛЮДЬМИ В УКРАЇНІ

Торгівля людьми залишається актуальною проблемою для України. Зростання її масштабів та небезпеки обумовило прийняття спеціальної нормативно-правової бази щодо протидії цьому злочину. Так, Закон України від 20 вересня 2011 року «Про протидію торгівлі людьми» [1] визначив торгівлю людьми 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. Цим же Законом закріплені завдання у сфері попередження торгівлі людьми, до яких належать: дослідження стану, причин і передумов поширення явища торгівлі людьми; підвищення рівня обізнаності населення про причини та наслідки торгівлі людьми шляхом проведення інформаційних кампаній протидії торгівлі людьми серед населення, у тому числі серед дітей; забезпечення регулювання процесів зовнішньої та внутрішньої трудової міграції тощо (ст. 10). Одним із завдань у сфері боротьби з торгівлею людьми є, зокрема, виявлення причин та передумов, що сприяють торгівлі людьми, та вжиття заходів щодо їх усунення (п. 1 ч. 1 ст. 12).

Отже, у протидії торгівлі людьми об'єктивне визначення обставин, що породжують та сприяють вчиненню цього злочину має важливе значення.

Дослідники зазначають, що зростання переважної більшості негативних соціальних явищ обумовлюється економічними та політичними потрясіннями, зниженням рівня життя суспільства тощо [2, с. 16]. Це повною мірою стосується і торгівлі людьми.

Саме соціально-економічні фактори змушують торгувати своїм тілом, виступати донорами біоматеріалів тощо, а це, в свою чергу, дає можливість злочинцям, які експлуатують таких осіб, отримувати великі кримінальні прибутки. На нашу думку, до криміногенних детермінантів торгівлі людьми можна віднести: наявність тіньової економіки; економічну нестабільність; негаразди перехідного періоду, зокрема, низький рівень життя значної частини населення при слабкому соціальному захисті; разюче розшарування суспільства на багатих і бідних, відсутність середнього прошарку; матеріальну незабезпеченість більшої частини населення при наявності значних потреб і пропозицій матеріального характеру у вигляді різноманітних товарів, послуг тощо; обмежену кількість можливих способів отримувати високий заробіток, влаштуватися на високооплачувану роботу; високий рівень безробіття в державі та деякі інші.

Криміногенними факторами залишаються поширена корумпованість влади, наявність організованої злочинності, політична нестабільність, тривалий збройний конфлікт на Сході країни.

Фахівці зазначають, що велике значення має загальний рівень моральності суспільства, характер загальновизнаних моральних цінностей і правил поведінки у сфері сексуальних відносин. Відсутність у нашій країні протягом тривалого часу цілеспрямованого статевого виховання, формалізм, догматизм і демагогія в галузі ідеології не могли не викликати негативних зрушень у психології молоді. Відсутність ідеалів, високих моральних цінностей призвела до занепаду моралі, розвитку цинізму, прагматизму. Це створило сприятливе середовище для проявів негативних факторів у поведінці людей.

Крім того, бездуховність, поширення домашнього насильства та жорстокого поводження з дітьми, падіння престижу материнства, споживацьке ставлення до людини також призводять до торгівлі людьми.

Одним із основних факторів, який сприяє загостренню проблеми торгівлі людьми в Україні є той, що чинне законодавство не повністю приведене у відповідність до вимог норм міжнародного права з цього питання і не відповідає потребам захисту прав людини на внутрішньодержавному рівні. Але не лише правові прогалини, а й незнання громадянами наданих їм прав внаслідок відсутності системи правової пропаганди сприяють вчиненню щодо них злочинів.

Торгівлі людьми сприяють також оголошення в засобах масової інформації про надання високооплачуваних робочих місць за кордоном, оформлення документів і перевезення яких здійснюються за рахунок комерційних структур. Пропонуються навіть програми підготовки і навчання, а для тих, хто менше цікавиться роботою, – можливість вийти заміж за заможного іноземця. На наш погляд, такі повідомлення потребують проведення попередньої кримінологічної експертизи.

Є недоліки і в діяльності органів, покликаних вести боротьбу зі злочинністю. Не маючи повної кримінологічної характеристики злочину торгівля людьми, правоохоронні органи проводять профілактичні заходи не зовсім цілеспрямовано, як наслідок, не досягають очікуваних результатів.

Отже, можна зробити висновок, що основними причинами торгівлі людьми є: соціально-економічна ситуація в країні; низький моральний рівень частини населення; недосконаліть вітчизняного законодавства та неповна його невідповідність положенням міжнародно-правових норм; слабка профілактична робота щодо запобігання торгівлі людьми; віктимна поведінка потерпілих та ін. Зазначені обставини мають враховуватися при розробці заходів з протидії торгівлі людьми та суспільно небезпечним діянням, які з нею пов'язані.

Список бібліографічних посилань

1. Про протидію торгівлі людьми : Закон України від 20.09.2011 № 3739-VI // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/3739-17 (дата звернення: 07.04.2020).
2. Карпухин Ю., Торбин Ю. Проституция: закон и реальность. *Милиция*. 1992. № 11. С. 16–20.

Одержано 12.04.2020

УДК 354.32:351.745.5

Юрій Іванович ІГНАТУШКО,
кандидат юридичних наук,
старший викладач кафедри інформаційних технологій та кібербезпеки
Національної академії внутрішніх справ (м. Київ)

ІНФОРМАЦІЙНИЙ ПОРТАЛ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Суспільство стає інформаційним – підвищується роль інформації і знань, збільшується частка інформаційних продуктів і послуг у валовому внутрішньому продукті, удосконалюється вже розвинута інформаційно-комунікаційна інфраструктура, формується глобальний інформаційний простір.

Фахівці практично всіх сфер сьогодні працюють в умовах інформаційних перенавантажень. Єдиний спосіб впоратися з ними полягає у використанні нових інформаційних технологій.

Очевидно, що правознавець повинен знати, як можна застосувати інформаційні технології у своїй роботі та які правові інформаційні системи вже створено й упроваджено. Але незалежно від майбутнього місця роботи йому необхідні знання про комп'ютерні технології загалом, про тенденції комп'ютеризації та інформатизації, про інформаційні системи фірм, банків, органів державної влади та ін. Без цього співробітник поліції як і кожен юрист не може ефективно виконувати свої функції та завдання.

Вирішення великої кількості правових задач залежить від якості результатів інформаційного пошуку – вибору з усієї відомої сукупності документів, текстів, відомостей, фактів і даних тих елементів, які відповідають інформаційним потребам. За умов великих обсягів інформації, серед якої здійснюється пошук, стає доцільним і навіть необхідним використання інформаційно-пошукових систем.

Інформаційно-пошукова система (ІПС) – це сукупність методів і засобів, призначених для зберігання та пошуку документів, відомостей про них чи певних фактів.

Залежно від типу інформації, що зберігається, розрізняють документальні системи, в яких об'єктом зберігання і пошуку є документ,

та фактографічні, в яких зберігаються і розшукуються окремі дані, що характеризують деякі факти – події, процеси, явища.

Відповідно до статей 25 - 27 Закону України «Про Національну поліцію» [1], підпункту 40 пункту 4 Положення про Національну поліцію, затвердженого постановою Кабінету Міністрів України від 28 жовтня 2015 року № 877, з метою організації інформаційно-аналітичного забезпечення поліції 28 серпня 2017 р. в Міністерстві юстиції України зареєстровано наказ МВС України від 03 серпня 2017 р. № 676 «Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» [2].

Інформаційно-телекомунікаційна система «Інформаційний портал Національної поліції України» (далі – система ІПНП) – сукупність технічних і програмних засобів, призначених для обробки відомостей, що утворюються у процесі діяльності Національної поліції України та її інформаційно-аналітичного забезпечення. Система ІПНП є складовою частиною єдиної інформаційної системи МВС (далі – ЄІС МВС).

Основними завданнями системи ІПНП є:

- інформаційно-аналітичне забезпечення діяльності Національної поліції України;
- забезпечення наповнення та підтримки в актуальному стані інформаційних ресурсів баз (банків) даних, що входять до ЄІС МВС;
- забезпечення щоденної діяльності органів (закладів, установ) поліції у сфері трудових, фінансових, управлінських відносин, документообігу;
- забезпечення електронної взаємодії з МВС та іншими органами державної влади.

Система ІПНП призначена для:

- формування інформаційних ресурсів ЄІС МВС;
- обробки інформації, яка утворена в процесі діяльності поліції;
- надання безпосереднього оперативного доступу до інформаційних ресурсів ЄІС МВС;
- генерації інтерфейсів та оброблення тимчасових наборів даних для здійснення інформаційної взаємодії органів (підрозділів) поліції з іншими органами державної влади, органами правопорядку іноземних держав, міжнародними організаціями;

- здійснення пошукових та аналітичних функцій для використання інформації з інформаційних ресурсів (баз даних) поліції, МВС та інших органів державної влади в межах службової діяльності відповідно до рівня доступу і повноважень за запитом або регламентом;
- використання програмних компонентів геоінформаційних підсистем для візуалізації інформації у вигляді електронних карт, автоматичної зміни зображеного образу об'єкта в залежності від зміни його характеристик, зміни масштабу та деталізації картографічної інформації в інформаційних ресурсах;
- забезпечення автоматизації процесів управління силами та засобами поліції;
- забезпечення електронного документообігу в органах (підрозділах) поліції, обміну електронними документами з МВС;
- комплексного захисту інформації та розмежування доступу до інформації, що зберігається в базах даних системи ІПНП.

Інформаційними ресурсами системи ІПНП є інформація, що утворена в процесі діяльності поліції та використовується для формування:

- тимчасових наборів даних, що створюються в процесі діяльності поліції та використовуються для наповнення та підтримки в актуальному стані баз (банків) даних, які входять до ЄІС МВС та визначені статтею 26 Закону України «Про Національну поліцію»;
- баз даних у сфері управлінських відносин, необхідних для виконання покладених на поліцію повноважень;
- баз даних, необхідних для забезпечення щоденної діяльності поліції, у сфері трудових відносин, фінансового забезпечення, документообігу.

В інформаційних ресурсах системи ІПНП обробляється інформація, яка належить до державних інформаційних ресурсів. Така інформація не підлягає поширенню та передачі іншим особам, крім випадків, передбачених законодавством.

Бази даних поліції, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції, містять відомості, зокрема, стосовно:

- повідомлень про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, що надійшли технічними каналами зв'язку;

- щодобових переліків та складу нарядів поліції та слідчо-оперативних груп, що заступають на чергування;
- завдань та орієнтувань, що доводились до нарядів поліції для реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події;
- звітування нарядів поліції за результатами реагування на повідомлення про кримінальні та адміністративні правопорушення, надзвичайні ситуації та інші події, виявлення додаткових обставин на місці пригоди;
- пересувань нарядів поліції, які отримані із планшетних комп'ютерів (мобільних терміналів) та засобами GPS.

Поліція може створювати інші бази даних, необхідні для забезпечення щоденної діяльності органів (закладів, установ) поліції, відповідно до статті 25 Закону України «Про Національну поліцію».

Порядок формування та використання інформаційних ресурсів системи ІПНП регулюється окремими нормативно-правовими актами із дотриманням вимог Закону України «Про захист персональних даних» та інших актів законодавства у сфері захисту персональних даних.

Розпорядником ІТС ІПНП є Національна поліція України, адміністратором – Департамент інформаційно-аналітичної підтримки (далі – ДІАП) Національної поліції України, користувачами – посадові особи органів (підрозділів) поліції, яким в установленому порядку надано право доступу до інформації в цій системі.

Список бібліографічних посилань

1. Про Національну поліцію : Закон України від 02.07.2015 № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40–41. Ст. 379.
2. Про затвердження Положення про інформаційно-телекомунікаційну систему «Інформаційний портал Національної поліції України» : Наказ МВС України від 03.08.2017 № 676 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/z1059-17 (дата звернення: 23.04.2020).

Одержано 25.04.2020

УДК 351.95

Ірина Дмитрівна КАЗАНЧУК,
кандидат юридичних наук, доцент,
доцент кафедри адміністративного права та процесу факультету № 1
Харківського національного університету внутрішніх справ

Дар'я Олександрівна СЕЧАНЦИНА,
курсантка 4 курсу факультету № 1
Харківського національного університету внутрішніх справ

ПРАВОВІ АСПЕКТИ ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ У СФЕРІ ПОДОЛАННЯ ІНФОРМАЦІЙНИХ ВИКЛИКІВ І КІБЕРЗАГРОЗ У СУСПІЛЬСТВІ

Згідно Закону України «Про національну безпеку України» від 21.06.2018 року № 2469-VIII одним із важливих напрямків державної політики у сфері національної безпеки і оборони є забезпечення кібербезпеки України [1]. Проблема подолання інформаційним загрозам та кіберзлочинності турбує не лише Україну, а й увесь світ. Одним з аспектів тероризму є крадіжка і злом баз даних як закордонних, так і вітчизняних державних органів влади. Під загрозою злому можуть перебувати державні реєстри з персональними даними громадян. Сучасні хакери, використовуючи всі самі передові розробки в області ІТ-технологій, щодня зламують тисячі акаунтів. Зламати можна все: поштову скриньку, акаунт у соціальній мережі, медичну базу, номер банківської карти та кредитної історії тощо. Цікаво, що Україна вже давно асоціюється у світі з місцем, де процвітає кіберзлочинність. Яскравий приклад тому – викрита у серпні 2015 року у Сполучених Штатах Америки злочинна група, в якій були і українські хакери, що зламувала бази даних спеціалізованих біржових видань. Зловмисники завдали шкоди у десятки мільйонів доларів, торгуючи незаконно отриманою інсайдерською інформацією великих міжнародних компаній [2].

Стратегія кібербезпеки України передбачає, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення режимів роботи автоматизованих систем керування технологічними процесами на об'єктах

критичної інфраструктури. Більшого поширення набуває політично вмотивована діяльність у кіберпросторі у вигляді атак на урядові та приватні вебсайти в мережі Інтернет. Після атаки вірусу «Petya» наприкінці 2017-го, від якої постраждали енергетичні компанії, банки, урядові установи, Україна посідає 3 місце світовому рейтингу з ризику зіткнення з вебзагрозами. За оцінками фахівців у сфері загроз інформаційній безпеці характерні такі тенденції: неконтрольовані ризики, пов'язані з «Інтернетом речей» та поширенням мережевих з'єднань; стрімке зростання «кіберзлочинів як сервісу»; зростання правових ризиків у сфері регулювання мережевих комунікацій; хакерські атаки, спрямовані на підрив репутації політичних сил [3, с. 57-58].

Головна роль в подоланні різних видів злочинів, скоєних за допомогою застосування новітніх технологій, належить Національній поліції України.

Створена у рамках реформи системи МВС України кіберполіція здійснює оперативно-розшукову діяльність, а отже, забезпечує реалізацію державної політики у сфері протидії кіберзлочинності, займається захистом персональних даних громадян у віртуальному просторі, в тому числі, боротьбою з піратством, а також поліцейською допомогою онлайн [4]. При цьому на виконання положень Закону України «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 № 2824-IV [5] та з метою забезпечення міжнародної діяльності кіберполіції у структурі Департаменту кіберполіції діє сектор Національного контактного пункту з реагування на кіберзлочини. Відповідно до Положення про Департамент кіберполіції Національної поліції України, затвердженого наказом Національної поліції України від 10.11.2015 № 85, діяльність підрозділів кіберполіції спрямована на: 1) протидію кіберзлочинності, тобто протиправним діянням, що вчинені з використанням інформаційних технологій або пов'язані з втручанням в роботу комп'ютерів, програмного забезпечення, мереж, несанкціонованою модифікацією даних, а також інші протиправні діяння, вчинені за допомогою пристроїв доступу до інформаційного простору; 2) забезпечення кібербезпеки – стану захищеності прав та інтересів людини, суспільства, держави у кіберпросторі від протиправних посягань; 3) протидія правопорушенням у інформаційній сфері, яка стосується вирішення проблем реалізації інформаційної політики держави, її стратегічних напрямів [6]. Ця діяльність вимагає належної системи правових заходів, спря-

мованих на нейтралізацію, запобігання та припинення кіберзагроз і інформаційних викліків.

Крім того, відповідно до Рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» підтримання належного стану інформаційної безпеки визнано важливою функцією органів поліції щодо захисту прав та свобод людини і громадянина, закріплених Конституцією України [7]. Тому співробітники української кіберполіції борються з кіберзлочинністю і кіберзагрозами, а також здійснюють міжнародне співробітництво щодо знешкодження транснаціональних злочинних угруповань у цій сфері у відповідність з кращими світовими стандартами [4].

Зважаючи на викладене, можна дійти висновку, що удосконалення правових засад діяльності підрозділів Національної поліції в сфері протидії кіберзагрозам і інформаційним викликам, у першу чергу, спрямоване на:

- оптимізацію організаційно-функціональної структури кожного підрозділу поліції, у ході якої особлива увага повинна приділятися аналізу оперативної обстановки, визначенню базових вимог до їх діяльності, на основі чого вже повинні формулюватися конкретні функції;
- обґрунтований розподіл функцій і обов'язків між підрозділами і працівниками поліції, створення належних умов для налагодження якісно нового рівня взаємодії між ними та координації їх діяльності;
- запровадження нових підходів до формування переліку організаційно-правових форм та методів взаємодії усіх суб'єктів протидії правопорушенням в інформаційній сфері, та підвищення контролю за якістю їх реалізації;
- запровадження сучасних механізмів аналітичного і матеріально-технічного забезпечення правоохоронної діяльності, покращення системи заходів, спрямованих на підвищення рівня професіоналізму поліцейських.

Зважаючи на стрімкий розвиток інформаційно-комунікаційних технологій, тенденцію до активізації зусиль щодо розвитку глобального інформаційного суспільства надзвичайно актуальним є вироблення ефективного правового механізму подолання кіберзагрозам за допомогою адміністративних засобів.

Список бібліографічних посилань

1. Про національну безпеку України : Закон України від 21.06.2018 № 2496-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 22.04.2020).
2. США підозрюють українських хакерів у викраденні конфіденційної корпоративної інформації // ZN,UA : сайт. 12.08.2015. URL: https://dt.ua/WORLD/ssha-pidozryuyut-ukrayinskih-hakeriv-u-vikradenni-konfidenciynoyi-korporativnoyi-informaciyi-181425_.html (дата звернення: 17.04.2020).
3. Ткачук Т. Ю. Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір : монографія. Київ : АртЕк, 2018. 422 с.
4. Українська кіберполіція: протистояти найнебезпечнішим хакерам світу // Українська правда : сайт. 20.10.2019. URL: http://www.pravda.com.ua/inozmi/deutsche-welle/2019/10/20/7085458 (дата звернення: 11.04.2020).
5. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.2005 № 2824-IV. *Відомості Верховної Ради України*. 2006. № 5–6. Ст. 71.
6. Про затвердження Положення про Департамент кіберполіції Національної поліції України : Наказ Нац. поліції України від 10.11.2015 № 85 // Національна поліція України : офіц. сайт. URL: https://www.npu.gov.ua/uk/publish/article/1816252 (дата звернення: 11.04.2020).
7. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України : Рішення Ради нац. безпеки і оборони України від 01.05.2014 № 449/2014. *Урядовий кур'єр*. 2014. № 81.

Одержано 05.05.2020

УДК 343.9

Аліна Владиславівна КАЛІНІНА,
кандидат юридичних наук,
науковий співробітник відділу кримінологічних досліджень
Науково-дослідного інституту вивчення проблем злочинності ім. акад. В. В. Сташиса
Національної академії правових наук України

«КОРОНАВІРУСНИЙ» НАПРЯМОК У КІБЕРШАХРАЙСТВІ[2]

Збентеження населення новопосталою проблемою – потенційним зараженням вірусом SARS-CoV-2 (коронавірусом) та наслідками хвороби, яку він викликає, – більш, ніж благодатний ґрунт для різного роду маніпуляцій із людською свідомістю. Адже емоція страху – головна зброя в цьому випадку. До неї додаються ще і стресовий стан, в якому опинилася особа через введення карантинних заходів в Україні, острах за життя і здоров'я (як своє, так і близьких і рідних), недовіра до статистичних даних про кількість хворих та померлих саме від коронавірусної хвороби, різні сюжети у ЗМІ з цієї тематики (переважно негативного забарвлення) тощо. Отже, людина готова повірити у будь-що, аби убезпечити себе від загрози, що одразу ж намагаються використати зловмисники, у тому числі й ті, які «працюють» в Інтернет-просторі. Адже злочинність завжди чутлива до змін у суспільстві. Особливо, коли ці зміни – потенційне середовище для її продукування.

Життя сучасної людини важко уявити без Інтернету. Наразі для багатьох саме цей ресурс є першочерговим в отриманні інформації. Тому із появою нового фактора (загроза захворювання на коронавірус), який значно вплинув на життєдіяльність людини (у виді масштабних карантинних заходів, запроваджених у державі), Інтернет-простір став активно використовуватися і злочинцями. Значного поширення набуло вчинення діянь, які можна охарактеризувати терміном «кібершахрайство» – тобто, шахрайство, що вчиняється шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 3 статті 190 КК України). Зокрема, за даними Національної поліції на тлі

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

загального зниження рівня злочинності в державі рівень шахрайств з використанням мережі Інтернет протягом карантину збільшився на 15 % [1]. Тенденція до зростання кількості «кібершахрайств» прогнозована. Використання паніки серед громадян, пов'язаної із епідемічною ситуацією в Україні та світі, зміни в організації виробничих процесів, а також перехід на «дистанційний режим праці» деяких злочинців – головні умови для збільшення кількості таких злочинів. Необхідно підкреслити, що кібершахрайства, пов'язані із COVID-19, мають «інтернаціональний характер»: результат аналізу повідомлень у пресі та на інформаційних інтернет-ресурсах (у тому числі й державних і правоохоронних органів) підтверджує цю тезу [див., напр. 2; 3 та ін.].

За висновками зарубіжних дослідників 71 % з більше, ніж 400 опитаних експертів (спеціалістів у сфері IT та інформаційної безпеки) вказують на активне використання злочинцями змін в роботі багатьох організацій [3]. Як головну загрозу більшість респондентів називають спроби фішингу (55 %), на другому місці – існування шкідливих вебсайтів, що нібито містять інформацію про коронавірус (32 %); далі – збільшення кількості шкідливих програм (28 %) та вимагателів (19 %) [3]. Коронавірус став головною темою в злочинних схемах із використанням соціальної інженерії (знань про людську поведінку та фактори, які на неї впливають, для злочинного вивідування даних) [4].

«Кібершахрайства», що активізувалися під час пандемії COVID-19, можна умовно розподілити на:

1. *Фішинг* – діяльність злочинців, що заснована на «гачках» для користувачів Інтернету: даних про COVID-19, інформації про методи, засоби та способи лікування коронавірусної хвороби і її профілактику, різних видах компенсацій грошових коштів у зв'язку із карантинними заходами (як то: державна допомога, благодійна допомога, відтермінування виплат за кредитами; компенсація за білети на різного виду транспорт, рейси якого відмінилися тощо), участь в інтернет-опитуваннях тощо. Основна «зброя» фішингу – листи на електронну пошту, вебсайти та додатки для смартфонів. Мета фішингу – отримання персональних банківських даних особи задля доступу до коштів жертви [4]. У технології фішингу можуть використовуватися назви міжнародних організацій, державних органів та установ (наприклад, Всесвітньої організації охорони здоров'я, Міністерства охорони здоров'я тощо).

2. *Організація фальшивого продажу засобів індивідуального захисту та антисептиків, тестів на зараження COVID-19, медичних препаратів від коронавірусу та засобів його профілактики, інших продовольчих товарів та товарів особистого вжитку*, що полягає у створенні фейкових сайтів, сторінок у соціальних мережах, телеграм-каналів тощо із пропозицією продажу такої продукції [4; 5; 6 та ін.]. Наприклад, кіберполіція України за місяць карантину виявила та заблокувала діяльність 179 Інтернет-посилань, за якими шахраї ошукували громадян, продаючи неіснуючий товар, під час пандемії та встановила 236 осіб, що займалися вказаною вище діяльністю. Головна умова придбання таких товарів – стовідсоткова передплата їх вартості [6].

3. *Розповсюдження шкідливого програмного забезпечення під виглядом інформації про COVID-19*. Із цією метою використовуються доменні ім'я, пов'язані зі словами Coronavirus, COVID-19 тощо. Кінцева мета – завантаження користувачем шкідливого програмного забезпечення на його пристрій (наприклад, «троянів») під виглядом карти розповсюдження коронавірусу чи місць перебування хворих на нього, додатку чи спеціальної програми про COVID-19 тощо, метою якого є отримання доступу до фінансової (платіжної) інформації користувача [7].

Окрім зазначеного, можна ще додати про надшвидке поширення фейкової інформації про коронавірус та його лікування, у тому числі, й від імені офіційних установ.

Таким чином, в умовах світової пандемії COVID-19 активізувалися «дистанційні» форми злочинної активності, а саме вчинення шахрайств у мережі Інтернет. Головною рисою таких шахрайств є маніпуляція інформацією, що пов'язана із захворюванням на коронавірус. Це потребує підвищеної уваги з боку правоохоронних органів та посилення заходів боротьби зі злочинністю.

Список бібліографічних посилань

1. Продовження та пом'якшення карантину обговорили на нараді в Офісі Президента // Президент України : офіц. інтернет-представництво. 21.04.2020. URL: https://www.president.gov.ua/news/prodovzhennya-ta-pomyakshennya-karantinu-obgovorili-na-narad-60757 (дата звернення: 29.04.2020).
2. Coronavirus (COVID-19): advice on how to protect yourself and your business from fraud and cyber crime // United Kingdom public sector information website. 27.04.2020. URL: https://www.gov.uk/government/publications/

coronavirus-covid-19-fraud-and-cyber-crime/coronavirus-covid-19-advice-on-how-to-protect-yourself-and-your-business-from-fraud-and-cyber-crime (дата звернення: 30.04.2020).
3. Мельникова Ю. Коронавирус – друг кибермошенников // Comnews : сайт. 09.04.2020. URL: https://www.comnews.ru/content/205491/2020-04-09/2020-w15/koronavirus-drug-kibermoshennikov (дата звернення: 30.04.2020).
4. Маніпуляції та шахраї під час епідемії коронавірусу: хто і як виграє, коли інші страждають // Рубрика : сайт. 19.03.2020. URL: https://rubryka.com/article/koronovirus-manipulation-crooks/ (дата звернення: 30.04.2020).
5. COVID-19: Increasing Risk of Cyber Fraud // McCann FitzGerald. 21.04.2020. URL: https://www.mccannfitzgerald.com/knowledge/disputes/covid-19-increasing-risk-of-cyber-fraud (дата звернення: 30.04.2020).
6. З початку карантину кіберполіцейські перевірили 576 інформацій щодо можливих протиправних дій, пов'язаних з коронавірусом // Кіберполіція України : офіц. сайт. 17.04.2020. URL: https://cyberpolice.gov.ua/news/z-pochatku-karantynu-kiberpoliczejski-pereviryly--informaczij-shhodo-mozhlyvyx-protypravnyx-dij-povyazanyx-z-koronovirusom-6129/ (дата звернення: 30.04.2020).
7. Комаровская В. Коронабизнес: как на пандемии коронавируса зарабатывают мошенники // COMMENTS.UA : сайт. 01.04.2020. URL: https://comments.ua/news/it/Internet/649763-koronabiznes-kak-na-pandemii-koronavirusa-zarabatyvayut-kibermoshenniki.html (дата звернення: 30.04.2020).

Одержано 01.05.2020

УДК 004.056.5

Віктор Миколайович КРАСНОЩОК,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки
Національної академії внутрішніх справ (м. Київ)

Людмила Миколаївна СКАЧЕК,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки
Національної академії внутрішніх справ (м. Київ)

КРАЇНА У СМАРТФОНІ – ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ

В 2019 році влада України анонсувала впровадження концепції «Держава в смартфоні» – це концепція з переведення державних послуг у режим онлайн. «Держава у смартфоні» – це коли громадянин може вирішити будь-яку свою життєву чи бізнесову ситуацію онлайн в один клік і бажано зі смартфона. Така концепція надає багато переваг, а в умовах всесвітньої пандемії – є життєво необхідною. В ситуації обмеженого пересування громадян містом можливість онлайн замовити їжу, сплатити комунальні платежі, поповнити рахунки, розрахуватися за послуги, спілкуватися з колегами, проводити заняття та конференції – все це дозволяє продовжувати працювати навіть в умовах карантину.

Разом з тим, для плодотворної роботи необхідно багато персональних даних передати в загальне користування різним додаткам, які в свою чергу зберігають ці дані або в смартфоні, або в хмарних сервісах.

В Україні презентували мобільний додаток «Дія», який на сьогоднішній момент містить водійське посвідчення та техпаспорт та планується скоро додати цифрову ID-картку, біометричний закордонний паспорт та студентський квиток. Розробники додатку «Дія», представники компанії EPAM, стверджують, що "авторизація здійснюється через BankID, сам застосунок побудовано відповідно до кращих практик індустрії, усі дані передаються та зберігаються на смартфоні користувача виключно у зашифрованому вигляді, посилена процедура автентифікації між додатком та сервером".

В Міністерстві цифрової трансформації України декларують для зберігання даних про використання українського облака De Novo. Але разом з тим ip-адреса сайту diia.app вказує на німецький Франкфурт та містить в описі хмарні сервіси Amazon, які не мають українського атестату відповідності КСЗІ. Сама компанія EPAM (розробник «Дія») працює в 25 країнах світу, а міноритарний пакет акцій належить інвестиційному банку «ВТБ-Капітал» з головним офісом в Москві. «ВТБ-капітал» публічно називає EPAM своїм ключовим партнером [1].

В умовах карантину величезної популярності набувають онлайн конференції. Одним з лідерів на ринку програмного забезпечення для проведення відео-конференцій є компанія Zoom Video Communications. Її розробка Zoom – є доволі простою та зручною програмою для проведення відео-конференції. У січні 2020 р., після зросту популярності Zoom, команда дослідників Check Point опублікувала звіт, в якому довела, що сервіс відеоконференцій Zoom мав недоліки в області безпеки. Згідно з дослідженням, хакери могли прослуховувати виклики Zoom, генеруючи і вгадуючи випадкові числа, призначені URL-адресами конференції Zoom. Zoom був змушений усунути пролом в системі безпеки і змінити деякі функції безпеки, такі як обов'язковий захист запланованих конференцій паролем [2].

В сучасних смартфонах реалізована технологія NFC – це доволі безпечна технологія бездротового високочастотного зв'язку малого радіусу дії «в один дотик». Ця технологія дає можливість обміну даними між пристроями, насамперед смартфонами та безконтактними платіжними терміналами, що перебувають на відстані близько 10 см.

З використанням технологія NFC є можливість застосовувати технологію безконтактної оплати, яка була реалізована в Україні ще в 2011 році.

Технологія безконтактної оплати є максимально безпечною, оскільки має кілька ступенів захисту. Кожна транзакція захищена унікальною криптограмою або динамічним кодом. Використати безконтактну картку (смартфон) без згоди користувача практично неможливо.

Проаналізувавши три найбільш популярні дії, які роблять з використанням смартфонів сьогодні, можна зробити висновки, що перш за все треба використовувати загальні рекомендації щодо захисту гаджетів:

— здійснювати регулярне та своєчасне оновлення операційної системи та додатків;

- використовувати надійні паролі для запобігання несанкціонованого доступу до пристрою;
- завантажувати додатки тільки перевірених та відомих розробників, а також звертати увагу на відгуки про них, особливо негативні. Крім цього, спеціалісти ESET не рекомендують завантажувати невідоме програмне забезпечення або додаток з невеликою кількістю інсталяцій, оскільки така програма може мати ще певні помилки, а в гіршому випадку й шкідливий код;
- використовувати двофакторну аутентифікаціюдля покращення безпеки телефона за допомогою захисту облікових записів банківських додатків;
- уникати підключення до публічних Інтернет-мереж, які є менш захищеними та часто поширюють різні загрози;
- не переходьте за випадковими посиланнями та не натискайте на спливаючі вікна;
- уникати поширення конфіденційної інформації через електронну пошту та соціальні мережі;
- використовувати надійне рішення для безпеки телефона та захисту від різних загроз, зокрема фішингових атак, спрямованих на викрадення паролів, даних банківських карт, інформації для входу в облікові записи, а також програм-вимагачів, які блокують екрани пристроїв та вимагають викуп.

Список бібліографічних посилань

1. Лиховид И. Электронные документы в смартфоне – насколько надежна защита данных? // DATA.UA : сайт. 12.02.2020. URL: https://data.ua/news/top-tema/49570-elektronnie-dokumenti-v-smartfone-naskolko-nadezhna-zaschita-dannih (дата звернення: 04.04.2020).
2. Киберпреступники эксплуатируют возросшую популярность Zoom // КО. IT для бизнеса : сайт. 02.04.2020. URL: https://ko.com.ua/kiberprestupniki_jekspluatiruyut_vozrosshuyu_populyarnost_zoom_132478 (дата звернення: 04.04.2020).

Одержано 08.04.2020

УДК 343.98

Ілля Миколайович МЕЛЬНИКОВ,
старший викладач кафедри інформаційних технологій та кібербезпеки навчально-наукового інституту № 1 Національної академії внутрішніх справ (м. Київ)

СУЧАСНІ ВИКЛИКИ ТА ЗАВДАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

В наш час всі ми є свідками стрімкого прогресу та розвитку інформаційних технологій. Зараз до мережі Інтернет підключено кілька мільярдів комп'ютерів. Одночасно в Мережі розміщено кілька сотень мільярдів сайтів, сторінок і зображень. На інтернет-економіку в світі вже припадає значна частина валового продукту, приблизно 10-15 %. Щокварталу обсяг переданих через Інтернет даних подвоюється і зараз, як зазначалося на міжнародних конференціях, можна говорити про появу реальної залежності розвинених країн від надійності міжнародної інформаційної інфраструктури. Даний процес, природно, торкнувся і України. Через кілька років кожен другий фахівець у нас буде здобувати другу вищу освіту дистанційним шляхом. Особливої популярності та необхідності цей процес набув під час епідемії коронавірусу. Розпочато створення Національної електронної бібліотеки. Однак сьогодні, як відомо, Інтернет став не тільки світової скарбницею, але і, на жаль, «світовим смітником». Спами, неправомірна реклама і порнографія все більш нахабно нав'язуються користувачам. Криміналізація соціуму отримала своє специфічне переломлення і в криміналізації Інтернету, появі якісно нових загроз у вигляді інформаційних воєн і кіберзлочинності [1].

Фахівці називають п'ять основних напрямків (викликів) правового регулювання Інтернет-відносин: захист особистих даних і приватного життя в Мережі; регулювання електронної комерції та інших угод і забезпечення їх безпеки; захист інтелектуальної власності; боротьба проти протиправного змісту інформації і протиправної поведінки в Мережі; правове регулювання електронних повідомлень [2].

В даний час кіберзлочинність розглядається багатьма експертами як бурхливо зростаюча загроза безпеці, як для окремих держав, так і для світової спільноти в цілому. Ця загроза спонукала до пошуку адекватних заходів протидії. Після прийняття в 2000 р. Хартії глобального

інформаційного суспільства і в 2001 р. відомої Конвенції Ради Європи про боротьбу з кіберзлочинністю, в світі проведені спеціальні форуми з цієї проблеми. Так, в грудні 2002 р в Лондоні пройшов перший т. зв. Стратегічний конгрес по боротьбі з електронної злочинністю. У лютому 2003 року за підтримки Інституту вивчення проблем кіберзлочинності в Атланті (США) відбувся Перший міжнародний саміт з проблем кіберзлочинності. Проте, поки проблема загострюється, і так буде тривати ще досить довго.

Лідером за кількістю кібератак сьогодні є США, на рахунку яких 35,4% від світового коефіцієнта кіберзлочинів. Ця цифра постійно зростає. Друге місце в списку кіберзлочинів займає Південна Корея – 12,8%; за нею Китай – 6,9%; Німеччина – 6,7%; Франція – 4%, Великобританія – 2,2% від усього коефіцієнта кібератак. Найпоширенішими серед них є: програмні віруси, комп'ютерні віруси, що саморозмножуються та інші форми збоїв програмного коду. Той факт, що США лідирують в цьому списку, цілком закономірний, оскільки тут, в порівнянні з іншими країнами, спостерігається найбільше число користувачів [3].

Найбільш небезпечним видом кіберзлочинності стає кібертероризм. Головною мішенню кібертерористів в майбутньому можуть стати основні фінансові інститути, бо посягання на них здатні заподіяти дуже тяжка шкода. Так, якщо, наприклад, відключити всі засоби зв'язку Нью-йоркській біржі із зовнішнім світом, то їй буде завдано збитків більше, ніж від вибуху вибухового пристрою в її будинку [4, с. 11].

Також нагадаємо, що за характером використання комп'ютерів або комп'ютерних систем зазвичай виділяють три види кіберзлочинів: діяння, де комп'ютери є предметами злочинів – власне комп'ютерні злочини (викрадення інформації, несанкціонований доступ, знищення або пошкодження файлів і пристроїв тощо.); дії, де комп'ютери використовуються як знаряддя злочину (електронні розкрадання тощо.); злочини, де комп'ютери відіграють роль інтелектуальних засобів (наприклад, розміщення в Інтернет порносайтів) [4].

Примикають до кіберзлочинності і деякі дії, спрямовані на підтримку умов для її існування і розвитку (використання електронної пошти для комунікації, створення власних сайтів, спрямованих на поширення кримінальної та протиправної ідеології, а також обмін кримінальним досвідом і спеціальними знаннями). У всьому світі налічується десятки тисяч орієнтованих на злом і навчальних цим прийомам сайтів. Будь-

який підліток може купити за невеликі гроші книгу, навчальну його елементарним прийомам атаки на інформаційні системи. Ще однією проблемою є те, що комп'ютерна злочинність по-різному криміналізована в законодавстві країн світу. В даний час більше 100 країн, в тому числі 60% членів Інтерполу, не мають законів, призначених для боротьби з кіберзлочинами.

Ефективна боротьба з кіберзлочинністю передбачає адекватне з'ясування специфіки причин її розростання. В цілому злочинні прояви мають єдиний причинний комплекс, в основі якого знаходяться найглибші і гострі деформації в суспільстві у всіх його сферах (політичній, економічній, соціальній і духовній) та на всіх його рівнях, починаючи зі світового глобального і закінчуючи індивідуальним особистісним. Це такі деформації, які, по-перше, перш за все, висловлюють несправедливість соціального устрою, відкривають простір для сваволі одних суб'єктів на шкоду іншим; по-друге, обмежують права і свободи громадян і, по-третє, ведуть до дегуманізації і ущербності соціального статусу і менталітету частини населення. Особливості причинного комплексу кіберзлочинності пов'язані зі специфікою віртуального світу. Тут в не меншому ступені, ніж у світі реальному, потрібно гармонізація відносин.

Кіберзлочинність має специфічні причини, і боротьба з нею також передбачає застосування специфічних засобів. У світі вже накопичено певний позитивний досвід такої боротьби, який треба застосовувати і на Україні.

Список бібліографічних посилань

1. Дремин В. Н. Глобализация информационных систем как фактор глобализации преступности. *Інформаційні технології та безпека*. 2002. Вип. 1. С. 56–59.
2. Номоконов В. Актуальные проблемы борьбы с киберпреступностью // Computer Crime Research Center : сайт. URL: http://www.crime-research.org/library/Nomokon1.html (дата звернення: 07.04.2020).
3. Некоторые проблемы современного кибертерроризма. *Борьба с преступностью за рубежом*. 2001. № 12.
4. Батурин Ю. М., Жодзишский А. М. Компьютерная преступность и компьютерная безопасность. М. : Юрид. лит., 1991. 160 с.
5. Правовые аспекты борьбы с кибернетическими преступлениями в ЕС. *Борьба с преступностью за рубежом*. 2003. № 2. С. 37.

Одержано 28.04.2020

УДК 343.85(477)

Дарина Вадимівна МІЩЕНКО,
студентка 3 курсу Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

Олександр Ростиславович ХОМИЧ,
студент 3 курсу Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

ОСНОВНІ ЗАСАДИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ОРГАНАМИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Останнім часом в міжнародній юридичній практиці широко використовується термін «кіберзлочинність», під якою розуміють вид транснаціональної злочинної діяльності, що базується на використанні в якості засобів вчинення злочинів кіберпростору. В рамках Ради Європи було підписано Конвенцію про кіберзлочинність від 23.11.2001 та Додатковий протокол до неї від 28.01.2003, учасницею яких є й Україна. Нині кількість кіберзлочинів в світі неухильно збільшується, зростає їх питома вага за розмірами викрадених сум та іншими видами шкоди в загальній частці матеріальних втрат від звичайних видів злочинів. Аналіз міжнародної практики свідчить про те, що за останні тридцять років в числі виявлених корисливих злочинів широкого поширення набули саме кіберзлочини. Масового характеру набули електронні розкрадання грошових коштів у великих та особливо великих розмірах, заподіяння майнової шкоди в сфері інформаційно-телекомунікаційних технологій, неправомірний доступ до охоронюваної законом комп'ютерної інформації, підробка електронних і звичайних документів, поширення як незаконної, так і шкідливої інформації, незаконна діяльність в сфері надання послуг, порушення авторських прав та багато інших. В Україні кіберзлочинність – це п'ятий за значимістю вид економічної злочинності після незаконного привласнення майна, корупції та хабарництва, недобросовісної конкуренції та маніпуляцій з фінансовою звітністю. За результатами досліджень на кіберзлочинність в світ припадає 23% випадків шахрайства, а в Україні – 17% [1, с. 5]. Згідно з тими ж даними, кіберзлочини стають все більш складними та витонченими, що значно

ускладнює процес їх виявлення та попередження. Це може привести до ще більш значних збитків і втрат у майбутньому.

Розглянемо більш детально систему суб'єктів протидії кіберзлочинності в Україні. Так, у 1991 р. при Генеральному секретаріаті Інтерполу діє Робоча група з проблем комп'ютерної злочинності, яка вивчає цей вид злочинів у різних країнах світу, розробляє рекомендації, допомагає в стандартизації національних законодавств, напрацьовує методичний досвід запобігання й розслідування комп'ютерних злочинів [2]. Як наслідок, в Україні на базі Національного центрального бюро Інтерполу 17 вересня 1996 р. було створено Національний центральний консультативний пункт з проблем комп'ютерної злочинності [2]. Згодом в структурі МВС України були створені Департамент боротьби з кіберзлочинністю і торгівлею людьми МВС України та підрозділи боротьби з кіберзлочинністю і торгівлею людьми ГУМВС, УМВС, а пізніше на їх базі – Управління боротьби з кіберзлочинністю МВС України та підрозділи боротьби з кіберзлочинністю ГУМВС, УМВС.

Новим етапом в реформуванні системи органів по боротьбі з кіберзлочинністю стало створення постановою Кабінету Міністрів України «Про утворення територіального органу Національної поліції» від 13.10.2015 № 831 Департаменту кіберполіції як міжрегіонального територіального органу Національної поліції [3]. Основними завданнями нової Кіберполіції, за словами Міністра внутрішніх справ України Арсена Авакова, є:

1. Реалізація державної політики в сфері боротьби з кіберзлочинністю.

2. Протидія кіберзлочинів (здійснюється в різних сферах, а саме: у сфері використання платіжних систем, в сфері електронної торгівлі та господарської діяльності, в сфері інтелектуальної власності, у сфері інформаційної безпеки).

3. Своєчасне інформування громадськості про появу нових кіберзлочинів.

4. Впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини.

5. Реагування на запити зарубіжних партнерів, що надходять каналами Національної цілодобової мережі контактних пунктів.

6. Участь у підвищенні кваліфікації співробітників поліції в сфері застосування комп'ютерних технологій у боротьбі зі злочинністю.

7. Участь в міжнародних операціях і взаємодія в режимі реального часу. Забезпечення функціонування мережі контактних пунктів між 90 країнами світу [4].

Таким чином, можна зробити висновок, що протидія кіберзлочинності в Україні здійснюється в трьох основних напрямках діяльності: 1) попередження кіберзлочинів; 2) загальна організація боротьби з кіберзлочинністю та правоохоронна діяльність, спрямована саме на виявлення, запобігання та розкриття кіберзлочинів; 3) застосування заходів кримінальної відповідальності і покарання осіб, які вчинили кіберзлочини. Попередження як одна з форм боротьби зі злочинністю передбачає як загальнодержавні заходи економічного, ідеологічного, правового та виховного характеру, так і спеціальні організаційні, технічні, програмні та криптографічні. Пріоритетним напрямком також є організація взаємодії і координації зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх необхідною матеріально-технічною базою. На сьогоднішній день жодна країна не в змозі протистояти кіберзлочинності самостійно, що обумовлює необхідність активізації міжнародного співробітництва в цій сфері. Захист інфраструктури інформаційних технологій є першочерговим завданням для спеціалістів у сфері інформаційної безпеки. Але забезпечення порядку в кіберпросторі є не менш важливою, тому кіберполіція відіграє значну роль в цьому.

Список бібліографічних посилань

1. Украина. Всемирный обзор экономических преступлений // DOCPLAYER : сайт. URL: http://docplayer.ru/35182824-Ukraina-vsemirnyy-obzor-ekonomicheskih-prestupleniy.html (дата звернення: 30.04.2020).
2. Малій М., Біленчук П. Космічна й електронна кіберзлочинність: загрози і виклики нового тисячоліття // LexInform : сайт. URL: https://lexinform.com.ua/dumka-eksperta/kosmichna-j-elektronna-kiberzlochynnist-zagrozy-i-vyklyky-novogo-tysyacholittya/ (дата звернення: 30.04.2020).
3. Про утворення територіального органу Національної поліції : Постанова Кабінету Міністрів України від 13.10.2015 № 831 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/831-2015-п (дата звернення: 30.04.2020).
4. Аваков А. Кіберполіція (крок реформі) // Українська правда. Блоги : сайт. 11.10.2015. URL: https://blogs.pravda.com.ua/authors/avakov/561a92c183c27/ (дата звернення: 30.04.2020).

Одержано 01.05.2020

УДК 342:343.346.8

Леонід Володимирович МОГІЛЕВСЬКИЙ,
доктор юридичних наук, професор,
проректор Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ АНАЛІЗУ СОЦІАЛЬНИХ МЕРЕЖ ДЛЯ ПОПЕРЕДЖЕННЯ ЗЛОЧИНІВ

Сучасний світ стрімко вривається в епоху Четвертої промислової революції і, відповідно, в епоху докорінних змін у всіх сферах життєдіяльності, і в кримінальному світі в тому числі. Все доступніше і потужніше стають технологічні інструменти, використання яких надає суспільству принципово нові можливості, але в руках злочинців можуть заподіяти дуже великої шкоди.

Як мінімум останні 15-20 років боротьба з тероризмом ведеться на основі упереджувальної концепції, а боротьба зі злочинністю - на основі караючої концепції. Це обумовлено, як правило, істотно різними масштабами наслідків для суспільства. В контексті цієї концепції якщо стає відомо про скоєний терористичний акт, а потім винні в ньому караються, це все одно говорить про провал розвідслужб і правоохоронців. У зв'язку з цим в останні роки в ряді країн, в першу чергу в США, Великобританії здійснюються спроби перебудувати боротьбу зі злочинністю за образом і подобою боротьби з тероризмом. З 2016 року нью-йоркська поліція, ФБР і Офіс директора національної розвідки розробили і прийняли Третю стратегію боротьби з ОЗ. Суть її полягає в максимальному використанні даних для випереджаючого реагування на загрози.

У даний час відомий лише один спосіб вирішення цього завдання - побудова поліцейської діяльності не тільки на штабному, а й на оперативному рівнях на основі інтелектуального аналізу і прогнозу різнорідних даних. Головним в цій перебудові є перехід від реактивної до проактивної поліцейської позиції. Це, в свою чергу, вимагає наявності у поліцейських надійних предикативних методів, що дозволяють з достатнім ступенем релевантності не стільки розслідувати вже скоєні, скільки прогнозувати злочини на етапі їх підготовки. Це завдання набуває все більшої актуальності у країнах розвиненої демократії, в яких потреби розвідувальної діяльності поліції конфліктують з зако-

нодавчими нормами, які традиційно суворо захищають право недоторканності приватного життя. В цих обставинах особливо актуальними є можливості автоматичного (суто програмно-технічними засобами, без участі людини) дослідження соціальних мереж, як легального джерела цінної розвідувальної інформації.

У доповіді Європолу 2016 р. «Соціальні мережі: як з ними працювати правоохоронцям» вказується: «Згідно з даними, отриманими від правоохоронних органів країн ЄС, наукових доповідей і власними дослідженнями, не менше 70% членів високотехнологічних ОЗУ, в першу чергу кіберкріміналу, становить молодь у віці від 18 до 25 років. Ця демографічна група сформувалася як особистості вже в епоху інтернету. Для них немає чіткої і однозначної межі між фізичним і віртуальним. Планшет або смартфон є таким же звичним інструментом, як блокнот або ручка для більш старших поколінь».

Згідно з даними спільного дослідження Стенфордського, Джорджтаунського університетів, Університету Техніон в Єрусалимі і Цюрихського технологічного університету «Інтернет-залежності: міфи і реальність» більш ніж дві третини молоді відчувають інтернет-залежності. Вони не можуть в інтервалі більш ніж сім хвилин жодного разу не звернутися до комунікатора, месенджера, e-mail тощо. В тому ж дослідженні вказується, що більш ніж для 4/5 молодих людей не просто звичною, а єдино нормальною моделлю поведінки є безперервне викладання в соціальні мережі візуальної, текстової та іншої інформації про своє проведення часу. Приблизно половина обстежених робить це навіть тоді, коли з міркувань безпеки або внаслідок можливих колізій з законом викладати такого роду інформацію було б не треба.

Наведені вище відомості дозволяють зробити висновок, що вперше в історії правоохоронні органи мають справу зі злочинцями, які не в поодиноких випадках, а масово залишають сліди своєї злочинної діяльності, повідомляють про зв'язки, знайомства, звички і т. п. Це робить соціальні мережі воістину неоціненним джерелом інформування для правоохоронців.

Аналіз соціальних мереж став одним з головних напрямків в програмі SECILE (Безпека Європи і боротьба з тероризмом: вплив, легітимність і ефективність). Також аналіз соціальних мереж вставлений як окремий блок в програму загальноєвропейського відеоспостереження - INDECT (Інтелектуальна інформаційна система, що підтримує спостереження,

пошук і виявлення небезпеки в контекстному транзакційному і відео-средовищі для забезпечення безпеки громадян у мегаполісах). Уже в 2016 р. аналіз соціальних мереж як пріоритетний напрямок вказано у найважливішій темі Європолу CAPER (Збір, обробка, аналіз, прогноз та звітність по інтегрованій інформації для попередження терактів). Найважливішою розробкою в рамках CAPER стало створення прототипу системи ePOOLICE (Раннє розпізнавання загроз організованої злочинності на основі сканування інформаційного середовища).

У 2007-2011 рр. була створена і почала функціонувати комп'ютерна система поліції Нідерландів. Система використовує великі сховища даних, що включають кілька компонентів: загальнонаціональна поліцейська база даних, поєднана з базами даних Європолу та Європейської Комісії; сховище електронної документації голландської поліції на всіх рівнях - від міністерства до первинних поліцейських управлінь. Третій блок комп'ютерної системи поліції включає в себе потужну систему сканування інтернету, і, в першу чергу, соціальних мереж і соціальних медіа. Голландський уряд в звіті за 2016 р. вказав, що використання системи дозволило в рамках встановлених бюджетних обмежень більш ніж на 17% за період з 2013 по 2016 рр. знизити число серйозних і організованих злочинів на території Нідерландів. За винятком Голландії, в країнах ЄС подібних систем в даний час немає. У той же час подібні системи експлуатуються не тільки ФБР, але і поліціями ряду штатів.

Досягненням голландської системи стало раннє розпізнавання загрози здійснення терористичних актів у Франції і в Бельгії. Голландська система моніторить Twitter та інші платформи в масштабах Бенілюксу, Німеччини, Франції та Великобританії. На жаль, французькі та бельгійські правоохоронні органи належним чином не оцінили попередження голландських колег і не вжили запобіжних дій.

Транснаціональна злочинність не має фізичних кордонів, тому боротьба з нею може вестися тільки на загальноєвропейському рівні, тому для європейських правоохоронців немає іншого шляху, як співпрацювати в аналізі та прогнозуванні організованої злочинності, розвивати загальні технології і здійснювати спільні багатосторонні практичні операції. В цьому ж руслі повинні рухатися і правоохоронні структури України як на штабному так і на оперативному рівні, особливо підрозділі таких департаментів: Департамент стратегічних розслідувань (у складі кримінальної поліції), Департамент кримінального аналізу (у складі

кримінальної поліції), Департамент кіберполіції (у складі кримінальної поліції), Департамент превентивної діяльності, Департамент боротьби зі злочинами, пов'язаними з торгівлею людьми (у складі кримінальної поліції), Департамент протидії наркозлочинності (у складі кримінальної поліції).

Одержано 12.04.2020

УДК 004.7

Михайло Олександрович МОЖАЄВ,
кандидат технічних наук,
завідувач сектору комп'ютерно-технічних, телекомунікаційних досліджень Харківського науково-дослідного інституту судових експертиз ім. засл. проф. М. С. Бокаріуса

Володимир Олексійович ГОМОН,
науковий співробітник сектору комп'ютерно-технічних та телекомунікаційних досліджень Харківського науково-дослідного інституту судових експертиз ім. засл. проф. М. С. Бокаріуса

КОНТРОЛЬ ЯКОСТІ ФУНКЦІОНУВАННЯ ТЕЛЕКОМУНІКАЦІЙНОЇ МЕРЕЖІ ІНФОРМАЦІЙНОГО ПОРТАЛУ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ

Комплексна система захисту інформації системи ІПНП, як взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації, повинна забезпечити:

- блокування витоку інформації каналами мережі передачі даних;
- блокування несанкціонованого доступу до інформації чи її носіїв.

В процесі передачі інформації в комп'ютерній системі, в тому числі і в комп'ютерній мережі передачі даних, завжди існує проблема недостатньої синхронізації, яка викликана різними програмно-апаратними факторами. Синхронізація – це засіб підтримки роботи всього цифрового устаткування в мережі передачі інформації на одній середній швидкості, яке повинно існувати на трьох рівнях: бітова синхронізація, синхронізація на рівні канальних інтервалів (time slot) і кадрова синхронізація. Тактовий генератор мережі, розташований у вузлі джерела, управляє частотою передачі через цей вузол бітів, кадрів і канальних інтервалів.

Ці фактори можуть суттєво ускладнити виконання вимог щодо якості передачі інформації і доступу до даних в інформаційній системі.

Для вирішення цих складних задач потрібно проводити постійний моніторинг завантаження каналів зв'язку інформаційної системи. Тому

задача моніторингу завантаження каналів зв'язку є досить актуальною і методи рішення її є метою даного доповіді.

Для постійного моніторингу завантаження каналів в комп'ютерних системах необхідно використовувати відповідні обчислювальні комплекси, які повинні з високою швидкодією і точністю визначати поточну частоту генераторів в мережі. В даний час такими апаратними засобами є акустооптичні аналізатори спектра (АОАС) з просторовим інтегруванням.

У доповіді запропонований метод моніторингу телекомунікаційної мережі комп'ютерної системи критичного застосування. Метод заснований на підвищенні роздільної здатності вимірювальної системи на базі акустооптичного спектроаналізатора. Основними результатами даного дослідження є:

- в доповіді наведено результати аналізу факторів, що впливають на порушення стабілізації комп'ютерної мережі комп'ютерної системи критичного застосування. Встановлено якісні та кількісні показники синхронізації системи;
- в роботі проаналізовані функціональні можливості використання акустооптичних спектроаналізаторів для контролю якості синхронізації комп'ютерних мереж, представлені основні математичні співвідношення, що визначають параметри вихідного сигналу АОАС;
- в результаті проведених чисельних розрахунків було встановлено, що для розрізнення несучих частот вхідних імпульсів при середніх і малих величинах расстройки загальним необхідною умовою є досить велика (в порівнянні з сумарною тривалістю вхідного імпульсу і тимчасової апертури спектроаналізатора) час реєстрації;
- основним підсумком досліджень можливості підвищення роздільної здатності АОАС є те, що виникають теоретичні передумови для визначення синхронності роботи генераторів в комп'ютерній мережі інформаційної комп'ютерної системи критичного використання, що призведе до підвищення показників якості обслуговування (QoS);
- подальші дослідження в цьому напрямку бажано присвятити отримання квазіоптимальних і оптимальних методів підвищення роздільної здатності АОАС для визначення параметрів десинхронизации роботи комп'ютерної мережі.

Одержано 28.04.2020

УДК 004.491.42

Олександр Євгенійович ПАКРИШ,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки
Національної академії внутрішніх справ (м. Київ)

ШАНТАЖ З ВИКОРИСТАННЯМ ПРОГРАМ-ВИМАГАЧІВ І МЕТОДИ ЗАХИСТУ

Програма-вимагач (англ. ransomware) – тип шкідливого програмного забезпечення, яке блокує доступ до комп'ютерної системи або запобігає зчитуванню записаних в ній даних, а потім вимагає від жертви викуп для відновлення початкового стану.

Програми-вимагачі шифрують інформацію жертви, що потенційно може призвести до незворотної втрати даних.

Малий та середній бізнес найбільше вразливий щодо атак за допомогою ransomware. Статистика останніх років оцінює середній розмір викупу за кожен інцидент у 2500 доларів США [1]. Тільки у США атаки програм-вимагачів за 2019 рік коштували біля 7,5 мільярдів доларів.

Не зважаючи на те, що більшість фахівців з питань інформаційної безпеки вважають сплату викупу поганою ідеєю, майже 40% жертв вибирають цей шлях [2].

При цьому, згідно з дослідженнями [3], майже 33 відсотки компаній, які сплачують викуп, не отримують доступ до своїх даних.

Ускладнює проблему програм-вимагачів те, що розробка деяких з них (зокрема WannaCry та NotPetya) фінансувалась, можливо, на державному рівні [4]. Ці програми маскувались під ransomware, але мали на меті незворотнє знищення інформації, а не отримання фінансової вигоди.

Загальний алгоритм злочинного використання програми-вимагача становить послідовність наступних кроків:

1. Інфікування комп'ютера жертви під час відкриття шкідливого вкладення, що розповсюджується шляхом спам-розсилки, або під час відвідування вебсторінки, яка інфікована пакетами експлойтів.

2. Потрапивши на комп'ютер жертви, програма-вимагач зберігає себе на жорсткому диску та створює ключ автозавантаження в реєстрі

для забезпечення власного запуска під час старту системи. Після цього програма шукає на диску файли за певним шаблоном та здійснює їх шифрування.

3. Програма-вимагач встановлює зв'язок з командним центром (сервером C&C) та інформує жертву про факт шифрування її файлів та щодо розміру і порядку передачі викупу. Більшість програм-вимагачів використовує для зв'язку з C&C сервером анонімні мережі

4. Після переведення коштів, жертва, в ідеалі, отримує ключ для розшифровки файлів. Для оплати зазвичай використовують одну з криптовалют (найчастіше біткоін).

Використання анонімних мереж та криптовалют забезпечує анонімність зловмисника і робить проблематичним притягнення його до відповідальності.

Епідемія коронавірусу викликала велику кількість спам-розсилок, що містять ransomware, та тематично пов'язані з питаннями пандемії. Також кіберзлочинці масово реєструють домени, пов'язані з пандемією та використовують їх для кібератак. Наприклад, зовсім анекдотичний сайт antivirus-covid19.site пропонував завантажити і встановити на свій комп'ютер програмне забезпечення Corona Antivirus для захисту від зараження [5].

Таким чином, виходячи з вищезазначеного, основні зусилля щодо захисту від програм-вимагачів пропонується зосередити, по-перше, на створенні умов, в яких програма-вимагач не зможе інфікувати комп'ютер, по-друге, на забезпеченні резервного копіювання критичної інформації [6]. Цього можна досягти, виконуючи наступні заходи:

- своєчасне оновлення операційної системи, браузерів та антивірусних баз;
- упереджене ставлення до вкладень листів електроної пошти та невідомих вебсайтів. Використання ресурсу VirusTotal для перевірки підозрілих файлів та вебадрес;
- контроль за мережевими підключеннями і дозвіл мережевого обміну тільки довіреним програмам (деякі програми-вимагачі починають шифрування тільки після встановлення зв'язку з C&C сервером);
- присвоєння атрибуту «тільки для читання» файлам, які не повинні змінюватись;

– організація резервного копіювання засобами, які не входять до складу операційної системи. При цьому права доступу до резервних копій повинні мати тільки програми резервного копіювання (для виключення можливого шифрування файлів резервних копій).

Список бібліографічних посилань

1. Cook S. 2018-2020 Ransomware statistics and facts // Comparitech Limited. 24.01.2020. URL: https://www.comparitech.com/antivirus/ransomware-statistics/ (дата звернення: 26.04.2020).
2. Understanding the Depth of the Global Ransomware Problem : survey report // Osterman Research, Inc. August 2016. URL: https://www.malwarebytes.com/pdf/white-papers/UnderstandingTheDepthOfRansomwareIntheUS.pdf (дата звернення: 26.04.2020).
3. Paying for ransomware could cost you more than just the ransom // Trend Micro Incorporated. 22.03.2017. URL: https://blog.trendmicro.com/paying-for-ransomware-could-cost-you-more-than-just-the-ransom/ (дата звернення: 26.04.2020).
4. Hern A. WannaCry, Petya, NotPetya: how ransomware hit the big time in 2017 // Guardian News&Media Limited. 30.12.2017. URL: https://www.theguardian.com/technology/2017/dec/30/wannacry-petya-notpetya-ransomware (дата звернення: 04.04.2020).
5. Как киберпреступники используют пандемию коронавируса в своих целях // ХАБР : сайт. 24.04.2020. URL: https://habr.com/ru/company/trendmicro/blog/498854/ (дата звернення: 04.04.2020).
6. Дроботун Е. Б. Анализ активности и тенденций развития вредоносных программ типа «блокиратор-шифровальщик файлов». *Програмные продукты и системы*. 2016. № 2 (114). С. 77–81.

Одержано 27.04.2020

УДК 343.123

Сергій Іванович ПІЧКУРЕНКО,
кандидат юридичних наук, доцент,
доцент кафедри оперативно-розшукової роботи
Національної академії внутрішніх справ (м. Київ)

Ольга Валеріївна ЗЛАГОДА,
кандидат юридичних наук,
старший викладач кафедри оперативно-розшукової роботи
Національної академії внутрішніх справ (м. Київ)

ЩОДО ДЕЯКИХ ПИТАНЬ ПРОТИДІЇ ОРГАНІЗОВАНІЙ КІБЕРЗЛОЧИННОСТІ

На сьогоднішній день процес реформування кримінальної поліції Національної поліції України триває, тому до діяльності оперативних підрозділів приділяється значна увага як з боку органів державної влади, так і збоку суспільства. Сучасна соціально-економічна ситуація та зміни в структурі злочинності в Україні зумовили необхідність створення блоку кримінальної поліції України, оперативні підрозділи якого, в змозі протистояти сучасній злочинності, зокрема, організованій.

Серед науковців, які досліджують проблеми організованої злочинності, слід зазначити таких вчених, як: С. В. Албул, О. М. Бандурка, М. Л. Грібов, В. О. Глушков, Д. Й. Никифорчук, В. А. Некрасов, О. О. Дульский, О. Є. Користін, М. В. Корнієнко, М. А. Погорецький, Є. Д. Скулиш та інші.

Науковці наголошують, що організована злочинність на сучасному етапі все більше впливає на соціально – політичні та економічні процеси в державі. В результаті організована злочинність перетворилась на один з головних факторів, який дестабілізує соціальний, економічний та політичний розвиток суспільства [1, 2].

Нинішній стан криміногенної ситуації у сфері протидії кіберзлочинності свідчить про необхідність удосконалення організаційно-управлінських заходів, спрямованих на попередження та розслідування кіберзлочинів.

Протидії організованій злочинності, зокрема, у сфері, кіберзлочинності – це особливий інтегрований, багаторівневий об'єкт соціального управління, який складає різноманітна за формами діяльність відповід-

них суб'єктів (державних, недержавних органів та установ, громадських формувань та окремих громадян), які взаємодіють у вигляді системи різнорідних заходів, спрямованих на пошук способів, засобів та інших можливостей ефективного впливу на злочинність із метою зниження інтенсивності процесів детермінації злочинності на всіх рівнях, нейтралізації дії її причин та умов для обмеження кількості злочинних проявів до соціально толерантного рівня [3, с. 44-45].

Головну роль у протидії кіберзлочинності відіграє міжрегіональний територіальний орган Національної поліції України – Департамент кіберполіції [4].

Відповідно до наказу на Департамент кіберполіції покладено завдання, щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та сприяння в порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції України у попередженні, виявленні та припиненні кримінальних правопорушень.

Департамент кіберполіції у сфері протидії організованій злочинності відповідно до покладених завдань розробляє та забезпечує реалізацію комплексу організаційних і практичних заходів, спрямованих на попередження та протидію кримінальним правопорушенням у сфері протидії кіберзлочинності; у межах своїх повноважень уживає необхідних оперативно-розшукових заходів щодо викриття причин і умов, які призводять до вчинення кримінальних правопорушень у сфері протидії кіберзлочинності; визначає основні напрями роботи і тактики оперативно-службової діяльності у сфері протидії кіберзлочинності; уживає передбачених чинним законодавством заходів зі збирання й узагальнення інформації стосовно об'єктів, що становлять оперативний інтерес, у тому числі об'єктів сфери телекомунікацій, інтернет-послуг, банківських установ і платіжних систем з метою попередження, виявлення та припинення кримінальних правопорушень; проведення комплексних і цільових оперативно-профілактичних заходів на території держави чи окремих регіонів, у тому числі за участю правоохоронних органів інших країн.

В той же час, на нашу думку, слід у протидії кіберзлочинності використовувати можливості департаменту стратегічних розслідувань

який в змозі забезпечити реалізацію комплексу заходів, спрямованих на протидію кіберзлочинності шляхом використання системи пошукових, розвідувальних, інформаційно-аналітичних заходів, у т.ч. із застосуванням спеціальних оперативних та оперативно-технічних засобів.

Список бібліографічних посилань

1. Катеринчук І. П. Вступне слово // Кримінальна розвідка: методологія, законодавство, зарубіжний досвід : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 29 квіт. 2016 р.) / МВС України, Одес. держ. ун-т внутр. справ. Одеса, 2016. С. 3.
2. Некрасов В. А. Корупція як форма кримінального контролю тіньової економіки. *Науковий вісник Дніпропетровського державного університету внутрішніх справ*. 2014. № 1 (70). С. 265–275.
3. Бандурка О. М., Литвинов О. М. Протидія злочинності та профілактика злочинів : монографія. Харків : ХНУВС, 2011. 308 с.
4. Про затвердження Положення про Департамент кіберполіції Національної поліції України : Наказ Нац. поліції України від 10.11.2015 № 85.

Одержано 28.04.2020

УДК 004.7

Валерій Васильович СОКУРЕНКО,
доктор юридичних наук, професор, заслужений юрист України, начальник Головного управління Національної поліції в Харківській області

ДОСВІД ПОШУКУ КОМПРОМІСІВ У ПРОТИРІЧЧІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ І ПОТРЕБ ПОЛІЦЕЙСЬКИХ РОЗСЛІДУВАНЬ

Останніми роками у правоохоронній сфері розвинених країн світу активно реалізується нова стратегія діяльності поліцейських підрозділів, сутність якої полягає у перенесенні акцентів з реактивної діяльності в бік проактивної, що передбачає перехід від підвищення рівня розкриття злочинів до превентивного їх припинення вже на стадії планування. Ця стратегія є безальтернативною відповіддю на сучасні виклики з боку, в першу чергу, організованої злочинності, яка за даними експертів розвідувальних співтовариств активно використовує у злочинних цілях досягнення технологій Четвертої промислової революції. Озброєні сучасними технологічними інструментами злочинці у змозі завдати такої шкоди суспільству, масштаби наслідків якої не можуть йти ні в яке порівняння з максимально можливою мірою покарання.

У численних документах ООН, ЄС, НАТО, інших міжнародних організацій містяться пункти, які передбачають «активну позицію держави і міжнародного співтовариства щодо ризиків і загроз, включаючи нові непізнані ризики і загрози, пов'язані з тероризмом, організованою злочинністю, кіберкримінальними угрупованнями, міжнародною мережею тіньового банкінгу, корупції і відмивання грошей».

Все більше політиків, представників правоохоронних органів, розвідувального співтовариства, відповідальних мислителів доходять висновку, що тотальне цифрове спостереження стає невід'ємним компонентом політики безпеки у високоризикованому високотехнологічному цифровому суспільстві.

«У цих умовах перед демократичними державами постає завдання встановити відповідно до обстановки, що змінилася, новий баланс між

двома акторами безпеки – державами і громадянами. Цей новий баланс повинен дозволити не на словах, а на ділі реалізовувати проактивну, а не реактивну стратегію боротьби зі злочинністю».

Міжнародний досвід свідчить про те, що в авторитарних країнах, наприклад у Китаї, цієї мети досягти значно простіше. Інша справа, коли йдеться про розвинені демократії з глибокими традиціями недоторканості приватного життя. Однак і в демократичному суспільстві обставини спонукають уряди рухатися в напрямку сприяння проактивним діям правоохоронних органів.

Яскравим прикладом знаходження компромісу у протиріччі захисту конфіденційних персональних даних і потреб поліцейських розслідувань є цікавий досвід розробників відомої поліцейської платформи ePOOLICE.

З урахуванням особливо прискіпливого ставлення до конфіденційності особистих даних у систему ePOOLICE включено досить простий, але ефективний програмний модуль, що дозволяє примирити вимоги захисту персональних даних і потреби поліцейських розслідувань. По суті, модуль являє собою шифратор. Під час надходження персональних даних у систему модуль стирає такі ідентифікатори, як ім'я, прізвище, і замінює їх на довільно обрані номери. У результаті всі дані зберігаються не на громадян країн ЄС, які мають прізвище, ім'я, а на номери, що володіють певним набором ознак. У такий спосіб удалося повністю забезпечити вимоги європейського законодавства й одночасно включити до складу баз даних значні масиви персональної інформації. Експерти Європейського суду з прав людини ретельно вивчили проєктну документацію платформи. У підсумку вони винесли вердикт, що система ePOOLICE повністю відповідає суворим стандартам європейського законодавства.

Іншим прикладом компромісного вирішення протиріччя конфіденційності персональних даних і потреб поліцейських розслідувань може слугувати застосування гомоморфного шифрування під час використання правоохоронними органами хмарних платформ у цілях збереження та обробки даних.

Однак зауважимо, що технічні варіанти рішення повністю не розв'язують проблеми, оскільки питання про її кардинальне вирішення лежить у правовій площині. А оскільки організована злочинність в умовах глобальної цифровізації світового суспільства все більше і більше набуває транснаціонального характеру, то це, в першу чергу, є сфера міжнародного права.

Одержано 17.03.2020

УДК 343.97

Владислав Віталійович СТЕПАНЕНКО,
курсант 3 курсу факультету № 2
Харківського національного університету внутрішніх справ

КІБЕРБУЛІНГ ЯК ФОРМА АГРЕСІЇ У ВІРТУАЛЬНОМУ ПРОСТОРІ

Сучасний інтенсивний розвиток інформаційних технологій призвів до появи нових інтернет-загроз, які здійснюють дестабілізуючий вплив майже на всі сфери суспільного життя і головне, при цьому, завдають шкоди охоронюваним законом правам та інтересам громадян, особливо найуразливішій таким категоріям населення як діти.

Розповсюдженню кібербулінгу, як різновиду кримінальної агресії, в мережі Інтернет свого часу передувало явище булінгу, заходи протидії відносно якого були запроваджені в Україні 2019 року. За рік протистояння українського суспільства з цим суспільно небезпечним явищем суди розглянули понад 300 справ про булінг, де зі 122 – уже винесено судове рішення і визначено вид покарання. Деякі справи закрито за терміном давності чи за відсутністю складу правопорушення, інші – відправлено на доопрацювання [1]. В той же час, сьогодні маємо ситуацію, коли діти активно фільмують та розповсюджують факти булінгу в соціальних мережах, інших контентах віртуального простору, що свідчить про відсутність у дітей сформованої онлайн-культури.

Кібербулінг – це новітня форма агресії, що передбачає жорстокі дії з метою дошкулити, нашкодити, принизити людину з використанням сучасних електронних технологій: Інтернету (електронної пошти, форумів, чатів, ICQ) та інших засобів електронної техніки – мобільних телефонів чи ін. ґаджетів [2, с. 279; 3, с. 7]. Як зазначає І. Лубенець, особливістю цього виду насильства є те, що воно може відбуватися як виключно у віртуальному світі, так і включати в себе ще й насильницькі дії фізичного характеру (наприклад, зйомки бійок, знущань, цькувань тощо з подальшим розміщенням таких фото, відео в мережі Інтернет) [4, с. 178].

З точки зору заходів кримінально-правового впливу, факти кібербулінгу можуть бути кваліфіковані за такими статтями Кримінального Кодексу України (*далі – КК України*) як: заподіяння тілесних ушкоджень різного

ступеня тяжкості (ст.ст. 121, 122, 125 КК України), побої та мордування (ст. 126 КК України), за наявності спеціальної мети – катування (ст. 127 КК України), навіть доведення до самогубства (ст. 120 КК України) тощо. І тільки в одному випадку розміщення цих матеріалів у мережі Інтернет може бути кваліфіковано як злочин – коли має місце пропаганда культу насильства і жорстокості – ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300 КК України) [5, с. 132-133]. В той же час, однією із проблем кримінально-правової охорони дитинства є відсутність підстави кримінальної відповідності з урахуванням віку особи-кібербулера. Тому, наразі важливим є створення тих умов, які будуть сприяти підвищенню, в першу чергу, рівня правової свідомості та правової культури серед дітей та підлітків. При цьому, робота у вказаному напрямку має відбуватися на всіх рівнях: від формування та реалізації державної політики у сфері протидії кібербулінгу, до – заходів виховного характеру в межах окремої родини.

Так, наприклад, з метою формування толерантного ставлення дітей один до одного, започатковуються та проводяться різноманітні заходи, які мають на меті протидіяти проявам кібербулінгу. Влітку 2019 року Міжнародний фестиваль документального кіно про права людини Docudays UA спільно з Інститутом соціальної та політичної психології НАПН та Громадською спілкою «УАнімА» в межах Кампанії проти кібербулінгу провели Всеукраїнський конкурс для дітей, який зібрав історії про те, як їм, тобто дітям, вдалося впоратися із цькуванням у мережі Інтернет. Автори кращих сценаріїв, в основу яких лягли невигадані історії переможців дитячого конкурсу, створили те, чого в Україні ще не бачили, – документальну анімацію про кібербулінг [6].

Як висновок слід зазначити, що небезпека кібербулінгу підсилюється специфікою інтернет-середовища: анонімністю, можливістю фальшувати ідентичність, мати величезну аудиторію одночасно, тероризуванням жертви будь-де і будь-коли. Одночасно з цим, проведення роз'яснювальної роботи серед школярів не є достатнім. Фінальним напрямом запобігання та протидії кібербулінгу на державному рівні, на наш погляд має стати – запровадження концепції чи іншого нормативно-правового акту, який би містив положення щодо протидії кібербулінгу, механізму його реалізації, кола суб'єктів протидії та напрямків їх взаємодії.

Список бібліографічних посилань

1. За рік дії закону про булінг українські суди розглянули понад 300 справ // Аргумент : сайт. 19.01.2020. URL: http://argumentua.com/novosti/za-r-k-d-zakonu-pro-bul-ng-ukra-nsk-sudi-rozglyanuli-ponad-300-sprav (дата звернення: 10.04.2020).
2. Кочан І. Слова з компонентом кібер- у сучасній українській мові. *Вісник Львівського університету*. 2016. Вип. 63. С. 277–288.
3. Найдьонова Л. А. Кібер-булінг або агресія в інтернеті: способи розпізнання і захист дитини: методичні рекомендації. *На допомогу вчителю.* 2011. Вип. 4. 34 с.
4. Лубенець І. Кібернасильство (кібербулінг) серед учнів загальноосвітніх навчальних закладів. *Национальный юридический журнал: теория и практика*. 2016. № 3 (19). С. 178–182.
5. Васильєв А. А., Кравцова М. О. Кібербулінг як форма кримінальної агресії: напрями протидії // Актуальні питання протидії кіберзлочинності та торгівлі людьми : матеріали всеукр. наук.-практ. конф. (м. Харків, 23 листоп. 2018 р.) / МВС України, Харків. нац. ун-т внутр. справ. Харків, 2018. С. 131–134.
6. Мультики про кібербулінг: як боротися зі цькуванням у мережі // Громадське радіо : сайт. 23.12.2019. URL: https://hromadske.radio/podcasts/turboranok-donbas/mul-tyky-pro-kiberbulinh-iak-borotysia-zi-ts-kuvanniam-u-merezhi (дата звернення: 10.04.2020).

Одержано 01.05.2020

УДК 347.13

Ольга Сергіївна ШКУМАТ,
курсантка 4 курсу факультету № 1
Харківського національного університету внутрішніх справ

Світлана Вадимівна ЯСЕЧКО,
кандидат юридичних наук, доцент,
доцент кафедри цивільно-правових дисциплін факультету № 4
Харківського національного університету внутрішніх справ

ПРАВОЧИНИ З ІНФОРМАЦІЄЮ

Постановка проблеми, її загальний вигляд та її неперервний зв'язок з науковими і практичними завданнями, насамперед полягає у помітно зростаючій ролі інформації та загалом у проблемах інформаційної сфери життя. Одним із завдань, які ставляться перед наукою цивільного права є вирішення проблем у інформаційній сфері та пошук шляхів інформаційного забезпечення цивільно-правового обігу інформації.

Відомо, що відповідно ст. 202 ЦКУ правочином є дія особи, спрямована на набуття, зміну або припинення цивільних прав та обов'язків. У науці цивільного права правочин – це найважливіший та найпоширеніший вид юридичних фактів, який спрямований на зміну або припинення цивільних правовідносин.

Одним із видів правочину є договір. Особливу увагу треба приділити саме поняттю «договір з інформацією» лише як правочин. Слід зазначити, що під «договором з інформацією» слід розуміти поняття, яке досить точно зазначається у ч. 2 ст. 302 ЦКУ, що фізична особа, яка поширює інформацію отриману з офіційних джерел, не зобов'язана перевіряти її достовірність та не несе відповідальності в разі її спростування. У свою чергу фізична особа, яка поширює інформацію, зобов'язана переконатися в її достовірності.

Необхідність створення нормативної основи регулювання цивільних відносин щодо інформації природним чином виходить зі становлення суспільства до інформації та підходів регулювання приватних відносин, основним механізмом регулювання яких тепер виступає договір. Виділення в особливий підрозділ загальних положень про договори і збільшення нормативного масиву і видів окремих договорів важливе

також і для подальшої розробки правових та методичних основ для нетрадиційних видів і типів договорів, які не входять до встановленого чинним законодавством переліку.

Якщо ми звернемося до монографії М. І. Брагінського і В. В. Вітрянського правовідносинами щодо інформації, а також можливостями її отримання і використання, охорони прав на інформацію наразі приділяється велика увага, про що свідчить: а) низка загальних та спеціальних актів законодавства в інформаційній сфері, зокрема законів України «Про інформацію», «Про науково-технічну інформацію», «Про друковані засоби масової інформації»; б) загальнодержавними та галузевими програмами та завданнями досліджень у цій сфері; в) праці вчених-цивілістів у галузі інформаційних правовідносин (Ч. Н. Азімова, І. В. Аристова, І. Л. Бачило, О. В. Кохановської та ін.).

Хочеться звернути увагу на те, що в науці цивільного права використовується таке поняття як таємниця листування, право на особисті папери та право на таємницю кореспонденції. Звернувшись до таких статей ЦКУ як 303 та 306 стає зрозуміло, що будь які дії спрямовані на поширення, зберігання, користування, зокрема шляхом опублікування, допускається лише за згодою фізичної особи, якій вони належать, тобто втручання у правовідносини, які встановлені цивільно-правовим договором та в яких використовується будь-яка інформація, що стосується фізичної особи, не допускається втручання без згоди цієї самої особи.

Сьогодні в теорії цивільного права під предметом правочинів дослідники розуміють: дії сторін, саме матеріальне благо, з приводу якого укладається правочин, або дії та матеріальне благо у комплексі, або права та обов'язки, або і об'єкти цивільного права і права, або юридичні наслідки. Тобто єдиної точки зору наразі не існує.

Одержано 11.05.2020

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

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

ПРОБЛЕМИ ВИКОРИСТАННЯ ЕЛЕКТРОННИХ ДОКАЗІВ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

На тлі стрімкого розвитку і поширення в усьому світі інформаційних технологій і телекомунікаційних систем злочини у сфері використання інформаційних технологій набули глобального характеру. Створюються міжнародні злочинні угрупування, члени яких діють узгоджено, хоча й перебувають в різних країнах світу. При цьому кількість кіберзлочинів щорічно зростає.

Провідною міжнародною компанією з кібербезпеки Cybersecurity Ventures надано прогноз щодо збільшення глобальних збитків від кіберзлочинності від трьох трильйонів доларів США в 2015 році до шести трильйонів доларів США у 2021 р. [1]. В таких умовах жодна країна світу, державна чи приватна установа не в змозі самостійно ефективно протидіяти кіберзлочинності і спонукає різні країни світу до міжнародної взаємодії та співробітництва.

Команда CERT-UA Держспецзв'язку в період з 18 по 24 квітня 2020 р. зареєструвала 2882 кіберінциденти, зафіксувала 17 фактів DDoS-атак (в т.ч. на сайти Офісу Президента України, ДБР, Держспецзв'язку) та 10761 підозрілих дій у кіберпросторі. Серед них: спроби викрадення інформації – 9, мережеве сканування – 2803, виявлення мережевого трояна – 1574, Web-атаки – 458, виявлення нестандартних протоколів або подій – 4344, спроби отримання прав адміністратора – 1531, спроби отримання прав користувача – 42 [2].

Правопорушники у кіберпросторі залишають не лише матеріальні сліди, а й електронні (цифрові). Виявлення, фіксація і використання електронних доказів у процесі доказування викликає певні труднощі через стрімкий розвиток інформаційних технологій, швидкі зміни поко-

лінь цифрової техніки та відсутність визначення поняття «електронні докази» у Кримінальному процесуальному кодексі України (КПК). У ч. 2 ст. 99 КПК України зазначено, що електронні носії інформації вважаються документами.

Електронні докази відрізняються від інших джерел доказів (показань, речових доказів, документів, висновків експертів) тим, що вони створені за допомогою електронних пристроїв, зберігаються та розповсюджуються лише за допомогою електронних носіїв інформації та комп'ютерних або телекомунікаційних мереж. Вони стають доступними для сприйняття людиною лише після обробки засобами електронної техніки з відповідним програмним забезпеченням. Електронні докази легше змінити чи підробити, ніж традиційні форми доказів, тому питання забезпечення їх належності і допустимості є вкрай актуальними.

У законодавстві України чітко не визначені порядок збирання та забезпечення електронних доказів, способи їх дослідження, механізми ідентифікації особи, яка створила або поширила інформацію в електронній формі.

В усіх країнах світу час від часу виникають проблеми визнання електронних (цифрових) доказів судом [3]. Складність їх використання в суді виникає через те, що до моменту дослідження в суді інформація в електронній формі може бути видалена або змінена, що значно знижує шанси довести факт її достовірності.

Чимало проблем виникає при дослідженні у вітчизняному суді навіть копій електронних листів. Суд вважає, що роздруківка з електронної скриньки не може вважатися належним доказом, оскільки неможливо ідентифікувати автора електронного листа та незрозуміло, на яку електронну адресу було здійснено відправлення, а також неможливо визначити, чи був надісланий файл підписаним електронним цифровим підписом [4].

На відміну від України, у США згідно з правилом 901b (4) «Федеральних правил про докази для судів та магістратів США» ідентифікація автора електронного листа з метою визнання його належним доказом здійснюється за допомогою показань свідків, які бачили, як певна особа створювала та надсилала електронний лист. Допустимість електронного листа як доказу в США встановлюється за сукупністю таких ознак, як зовнішній вигляд, зміст, лінгвістичні та семантичні ознаки листа, наявність певних знаків, фірмових найменувань, написів тощо [5].

Тобто, в окремих країнах світу поступово розробляються підходи до спрощення вимог щодо визнання електронних доказів судом. Однак в Україні через ускладнений та недосконалий процесуальний порядок подання електронних доказів в суд, їх використання у судочинстві є проблематичним.

Подолання існуючих проблем щодо визнання допустимими доказами інформації у цифровій формі є можливим за умови внесення до Кримінального процесуального кодексу спеціальної дефініції – визначення поняття «електронні докази» та розроблення «спрощеного» процесуального порядку їх фіксації і подання до суду.

Список бібліографічних посилань

1. The 2020 Official Annual Cybercrime Report // Herjavec Group. URL: https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/ (дата звернення: 29.04.2020).
2. Команда CERT-UA Держспецзв'язку з 18 по 24 квітня зареєструвала 2882 кіберінциденти // Державна служба спеціального зв'язку та захисту інформації України : офіц. сайт. 27.04.2020. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?art_id=320629&cat_id=317163 (дата звернення: 28.04.2020).
3. Arshad Humaira, Bin Jantan Aman, Abiodun Oludare Isaac. Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. *Journal of information processing systems*. 2018. Vol. 14, No. 2. Pp. 346–376. URL: http://xml.jips-k.org/full-text/view?doi=10.3745/JIPS.03.0095 (дата звернення: 25.04.2020).
4. Постанова Львівського апеляційного господарського суду від 10.09.2018 : справа № 914/2505/17 // ZakonOnline : сайт. https://zakononline.com.ua/court-decisions/show/76542389 (дата звернення: 25.04.2020).
5. Зозуля Н. Електронні докази за кордоном: практика застосування // Українське право : сайт. 25.06.2018. URL: https://ukrainepravo.com/scientific-thought/naukova-dumka/elektronni-dokazy-za-kordonom-praktyka-zastosuvannya/ (дата звернення: 25.04.2020).

Одержано 01.05.2020

УДК 343:973

Сергій Олександрович ЗОЛОТАРЬОВ,
головний судовий експерт відділу комп'ютерно-технічних та телекомунікаційних досліджень
Харківського науково-дослідного експертно-криміналістичного центру МВС України

СУДОВА КОМП'ЮТЕРНО-ТЕХНІЧНА ЕКСПЕРТИЗА ТА ЇЇ РОЛЬ У БОРОТЬБІ З КІБЕРЗЛОЧИНАМИ

Стрімкий розвиток електронних носіїв, їх значення, яке вони відіграють на сьогоднішній день у житті людей сприяє розвитку цифрової криміналістики, а саме такого експертного напрямку як комп'ютерно-технічна експертиза, яка є одним із різновидів судових експертиз, призначення якої – отримання фактичних даних шляхом дослідження комп'ютерних засобів, електронних носіїв інформації.

Предметом комп'ютерної експертизи є закономірності формування і дослідження комп'ютерних систем і руху цифрової інформації, дослідження фактів і обставин, пов'язаних з проявом цих закономірностей за завданням судових та слідчих органів за кримінальними та цивільними справами, а також проведення досліджень за зверненням громадян згідно переліку платних послух МВС України (для Науково-дослідних експертних центрів МВС України) у чіткій відповідності з вимогами чинного законодавства, що дозволяє комплексно побудувати цілісну систему доказів.

Вдосконалення комп'ютерної-техніки (системні блоки комп'ютера, ноутбуки, сервери тощо), цифрових електронних носіїв інформації (жорсткі диски, твердотілі накопичувачі даних, карти пам'яті, планшетні комп'ютери, мобільні телефони, розумні годинники), а саме збільшення об'єму досліджуваних даних, використання захисту, вимагають від експертів цього різновиду судових експертиз використання аналітичного підходу, поглиблених знань, а також новітніх експертних програмних продуктів, апаратних пристроїв, задля досягнення максимального результату дослідження. Недостатньо розвинені навички аналізу даних, незабезпеченість програмними та апаратними комплексами експертів

цього напряму дослідження, а також неналежне упакування об'єктів дослідження оперативними та слідчими підрозділами при огляді місця події, можуть суттєво вплинути на результат не тільки дослідження, а розслідування протиправного діяння (правопорушення) у цілому, адже все частіше у практичній діяльності трапляються випадки, що необхідна інформація, яка може бути використана у якості доказової знаходиться серед пристроїв, дослідженням яких займаються саме судові експерти напряму дослідження 10.9 «Дослідження комп'ютерної техніки та програмних продуктів».

За завданням судових та слідчих органів по кримінальним справам, судові експерти комп'ютерно-технічної експертизи здатні досліджувати факти несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж (стаття 361 Кримінального кодексу України) [1], а також фактів несанкціонованих дій з інформацією, яка оброблюється 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 (стаття 362 Кримінального кодексу України). Згідно вищезазначених статей Кримінального кодексу висновок судового експерта відіграє одну із ключових ролей, що у свою чергу також є внеском у боротьбі з кіберзлочинністю у нашій державі, адже проведення експертом дослідження у деяких випадках також може висвітлити нові джерела інформації для досудового органу розслідування.

Слід зазначити, що злагодженість дій правоохоронних органів з експертними установами: консультації, обмін досвідом, поглиблений аналіз викликів сьогодення у цій специфіці, а також розборка нових механізмів дослідження фактів несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж, подання пропозицій щодо удосконалення правового регулювання у цій сфері, здатна позитивно вплинути на розслідування злочинів у сфері кіберзлочинів.

Список бібліографічних посилань

1. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III. *Відомості Верховної Ради України*. 2001. № 25–26. Ст. 131.

Одержано 27.04.2020

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

КРИПТОВАЛЮТА ЯК ПРЕДМЕТ І ЗАСІБ УЧИНЕННЯ ЗЛОЧИНІВ

Стрімкий розвиток інформаційних і фінансових технологій, глобалізація і, як наслідок, поява нового виду приватних віртуальних грошей – криптовалюти зумовили зміщення центру впливу держави в сфері регулювання грошового обігу. Відповідно, з появою нового виду фінансових взаємовідносин, виникають і нові загрози суспільству і державі в цілому.

В рамках теорії кримінального права посягання, що здійснюються з використанням криптовалют або здійснюються в сфері її обігу, не мають самостійного законодавчого визначення, також не закріплено і поняття самої криптовалюти. Відповідно на даному етапі в рамках кримінального закону можна сказати, що кріптовалютной злочинності в нашій державі юридично не існує. Разом з тим, кріптовалютная злочинність настільки динамічно розвивається в світових масштабах, в тому числі і в Україні, що її ігнорування є неможливим. Звісно ж, що без початкового законодавчого визначення базових понять неможливо розробити і ефективні заходи кримінально-правової охорони кріптовалютних відносин і повноцінних заходів відповідальності за злочини з її використанням

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, на основі якої функціонує найпопулярніша криптовалюта в світі - біткоін.

Криптовалюти є абсолютно новим економіко-правовим явищем, відмінним від традиційних фіатних або електронних грошей. Незважа-

ючи на різні підходи до визначення різноманітних ознак криптовалют, загальними їх ознаками є:

- відсутність централізованого емісійного центру, тобто їх децентралізований характер;
- анонімність учасників операцій (у мережі використовуються криптографічні методи асиметричного шифрування даних із застосуванням публічного та приватного ключів);
- відсутність реальної їх забезпеченості (вартість криптовалют є результатом співвідношення попиту та пропозиції на них серед користувачів);
- віртуальні валюти здатні переміщатися по світу без обмежень [3, с. 2].

Однією з головних переваг криптовалют називають їх якісний захист, а також безмежні можливості транзакцій, а саме: будь-який власник гаманця може платити кому завгодно, де завгодно і за що завгодно; їх неможливо проконтролювати або заборонити, так що можна здійснювати перекази в будь-яку точку світу, де б не знаходився інший користувач з гаманцем біткоін. Не потрібно платити комісії і мита банкам і іншим організаціям. У мережі немає єдиного керуючого центру, який би обробляв інформацію про транзакції, баланс програм-гаманців. Один з головних плюсів - анонімність - одночасно і мінус. Фізично неможливо повернути втрачені біткоіни. Система настільки анонімна і безпечна, у разі якщо учасник втрачає свій секретний ключ, який грає роль пароля для здійснення операцій, то відновити його неможливо.

На сьогодні, з одного боку не можна заперечити факту широкого розповсюдження операцій з криптовалютами та їх використання, а з іншого боку – факту відсутності поняття криптовалюти у національному законодавстві, визначення її правового статусу.

Віртуальній валюті притаманні функції фіатних валют. Вона є мірою вартості, може вимірювати вартість товарів як і реальна валюта. При цьому не можна сказати, що в економічному світовому співтоваристві є єдиний підхід до розуміння суті криптовалюти. Так, наприклад, Сінгапурське законодавство визначає біткоін товаром і прирівнює його купівлю до купівлі програмного забезпечення. У Німеччині це «приватні гроші», а в США - це децентралізована віртуальна валюта. У Болівії та Еквадорі заборонено використання киповалют. У США, Німеччині, Сінгапурі діють обмеження на обіг криптовалюти. В Японії біткоін визнається легальним засобом платежу. А КНР нещодавно розпочала

тестування цифрового юаня. Більшість розвинених країн адаптують своє законодавство для регулювання обігу криптовалют [4].

Таким чином, навіть на міжнародному рівні на сьогодні відсутня єдність щодо визначення поняття та правової природи криптовалюти. Вітчизняна правова теорія і практика, як і більшість зарубіжних країн, також не вирішила цю проблему. Так, через свої технологічні особливості Bitcoin не може бути визнаний «електронними грошима», оскільки він не містить зобов'язання емітента з його погашення, не має єдиного емісійного центру і не прив'язаний до жодних готівкових або безготівкових коштів.

З точки зору кримінального права, залишається невирішеним питання про місце криптовалюти серед ознак складу злочину. Чи можна визнати криптовалюту засобом або предметом злочину, а можливо як першим так і другим, або взагалі залишити за рамками складу злочину.

Аналіз правозастосовної практики свідчить, що визнання криптовалюти в якості засобу вчинення злочину здебільшого у судів не викликає сумнівів та заперечень. Суди не відчувають труднощів при кваліфікації діянь, в яких криптовалюта виступають як засіб вчинення злочинів, наприклад, пов'язаних із незаконним обігом зброї, наркотичних засобів, порнографії тощо. Операції з криптовалютою розглядаються як докази у кримінальній справі. Незважаючи на відсутність коштів ідентифікації користувачів криптовалют за номерами гаманців, інформація про транзакції використовується для перевірки підозр і уточнення обставин у справі. Також операції з використанням криптовалюти широко застосовуються при вчиненні злочинів щодо легалізації (відмивання) доходів, одержаних злочинним шляхом, фінансуванні тероризму.

Використовуючи розрахунки в криптовалютою, правопорушник максимально відсторонюється від контакту з потенційним покупцем, залишає мінімум слідів злочинного діяння, а виключаючи візуальний контакт і спілкуючись за допомогою інтернет-месенджерів, істотно ускладнює виявлення і розслідування такого виду злочинів.

Також криптовалюта може виступати і в якості предмету злочину.

На сьогоднішній день вона може бути як самостійним засобом платежу, так і засобом обміну на будь-яку іншу валюту. З урахуванням анонімності операцій криптовалюта є досить привабливою формою незаконної винагороди. Невизнання її предметом названих вище зло-

чинів може спричинити фактичну легалізацію незаконних винагород у цій формі.

Саме тому актуальним на сучасному етапі є питання визнання криптовалюти предметом злочинів проти власності.

Слід зазначити, що предмету злочинів проти власності традиційно притаманні певні ознаки, серед яких економічна (вартість), фізична (матеріальність), юридична (приналежність іншій особі). Що стосується економічної ознаки, то вважаємо, що вона властива криптовалюті, тому що існує певний її курс до офіційної валюти, на сьогодні криптовалюта може виступатиа засобом платежу за звичайні товари або послуги. Так, Subway, Amazon, Ebay і ряд інших організацій приймають до оплати біткоіни. Юридична ознака також притаманна криптовалюті, оскільки, незважаючи на анонімність гаманців, вони комусь належать, і якщо конкретний гаманець не належить певній особі, то для нього він чужий. Більш складне питання з фізичною ознакою. Предмет злочинів проти власності матеріально повинен бути окреслений в просторі (тобто повинен перебувати в твердому, рідкому або газоподібному стані, бути живим або неживим).

Проте в сучасній кримінально-правовій літературі все частіше піднімається питання питання про те, що об'єкти права власності в умовах сучасного інформаційного суспільства не обов'язково повинні мати матеріальну природу, тому як відносинам власності в юридичному та економічному сенсі схильні і нематеріальні блага.

Так, наприклад, О. Е. Радутний та О. Г. Ганжа вважають, що у широкому розумінні криптовалюту можливо розглядати як засіб вчинення злочину, або як його предмет, якщо під останнім розуміти не тільки речі матеріального світу, з певними властивостями яких закон пов'язує наявність ознак того чи іншого злочину, але й інші явища (сюди, крім самої криптовалюти, слід відносити електричну або теплову енергію, інформацію тощо) [2, с. 169].

На думку Ю. А. Дорохіної, хоча криптовалюти є одним із видів віртуальних фінансових інструментів, проте їм притаманні всі ознаки предмета злочинів проти власності, а саме: фізичні ознаки характеризуються можливістю вимірювати їх у певних одиницях, ними можна торгувати на електронній біржі, тобто такий предмет можна вилучити; щодо соціально-економічної складової, то криптовалюти мають певну мінову

і споживчу вартість, а з точки зору юридичної ознаки – криптовалюти є чужим для винного майном [1, с. 170].

На нашу думку, фізична ознака криптовалюти як предмету злочинів полягає у її специфічній формі – цифровому коді.

Таким чином, існує практична необхідність визнання криптовалюти як предмету злочинів проти власності. Так, часто мають місце випадки її незаконного заволодіння шляхом обману. Наприклад, аналоги банку, що надають послуги «електронного гаманця», зникають безслідно (так звані фейкові гаманці), деякі просто переводять кошти клієнтів на інші рахунки, використовуються фальшиві гаманці та інші способи незаконно заволодіння криптовалютою. У разі невизнання криптовалюти предметом злочинів проти власності, всі незаконні дії, що виникають у віртуальному просторі не зможуть отримати належної кримінально-правової оцінки, а винні особи не будуть притягнуті до відповідальності.

Список бібліографічних посилань

1. Дорохіна Ю. А. Злочини проти власності. Теоретико-правове дослідження : монографія. Київ : Київ. нац. торг.-екон. ун-т, 2016. 744 с.
2. Радутний О. Е., Ганжа О. Г. Криптовалюта як нова дотична фінансового і кримінального права // Вороновські читання (Співвідношення матеріального та процесуального в регулюванні фінансових відносин) : матеріали міжнар. наук.-практ. конф, (м. Чернівці, 4–5 жовт. 2017 р.) / редкол.: А. П. Гетьман, М. П. Кучерявенко, Т. А. Латковська та ін. Харків : Асоціація фінансового права України, 2017. С. 166–170.
3. Погрібний Д. І. Питання визначення правового статусу криптовалют та господарсько-правового забезпечення їх використання в Україні. *Теорія і практика правознавства*. 2018. № 2. С. 1–9.
4. Барский Р. Цифровой юань заменит доллар. Что известно о криптовалюте Китая // Наука и техника : сайт. 17.04.2020. URL: https://naukatehnika.com/cifrovoj-yuan.html (дата звернення: 19.04.2020).

Одержано 21.04.2020

УДК 343.132+343.98

Віталій Геннадійович КОЛЕСНИК,
завідувач відділу комп'ютерно-технічних та телекомунікаційних досліджень Харківського науково-дослідного експертно-криміналістичного центру МВС України

ПРОБЛЕМНІ ПИТАННЯ ЗБЕРЕЖЕННЯ, ФІКСАЦІЇ ТА ДОСЛІДЖЕННЯ ІНФОРМАЦІЇ В СУЧАСНИХ МОБІЛЬНИХ ТЕЛЕФОНАХ

Сучасне життя сьогодні неможливо уявити без мобільних телефонів. Будь-яка діяльність, комунікація, спілкування, планування роботи і дозвілля, так чи інакше будуть відображені у телефоні сучасної людини. Доступність на ринку та надзвичайне поширення мобільних пристроїв зробили мобільний телефон незмінним супутником людини. Широке різноманіття функцій та сервісів у мобільному телефоні, такі як фотографування, відеозапис, аудіозапис, фіксація географічних координат та переміщень, можливість миттєво обмінюватися у різноманітних програмах-месенджерах текстовими та голосовими повідомленнями, документами, графічними зображеннями, можливість здійснювати миттєве керування фінансами та робити грошові перекази, призводить до накопичування у пам'яті телефону значної кількості інформації, яка має суттєве, а іноді й вирішальне значення для з'ясування обставин та доказування в процесі досудового розслідування.

Очевидно, що виробники телефонів та розробники їх операційних систем приділяють значну увагу захисту даних користувача. Окрім коду розблокування телефону, захист даних у телефонах наразі забезпечується (в залежності від року випуску та моделі телефону): режимом Secure Startup, засобами повного дискового шифрування Full Disk Encryption (FDE), а на останніх моделях – засобами пофайлового шифрування File Based Encryption (FBE). Окрім того, з кожним роком ускладнюється доступ до завантажувача та звужується вікно можливостей для його модифікації. Переписка у месенджерах вже не заноситься до резервної копії, тому її можливо вилучити лише з повної дешифрованої фізичної копії пам'яті телефону, зробити яку є можливим далеко не з усіх моделей, присутніх на ринку. Навіть найсучаснішими техніко-криміналістични-

ми засобами не є можливим здійснити вилучення інформації з усіх без винятку моделей мобільних телефонів [1].

Таким чином, головним засобом отримати доступ до інформації з метою хоча б її візуального огляду, наразі є визначення слідчим паролю розблокування, який підозрюваний повідомляти, зазвичай, відмовляється. Окрім паролю, сучасні телефони також можливо розблокувати сканером відбитка пальця та системою розпізнавання обличчя, однак вони надають лише умовний доступ та не є повноцінною заміною визначеному паролю блокування.

Постійний розвиток засобів захисту у сучасних телефонах, та недостатня обізнаність слідчих та оперативних співробітників у особливостях їх функціонування, помилки під час вилучення пристроїв, призводять до негативних наслідків, що виражаються у втраті як можливості доступу до інформації у телефонах, так і до втрати самої інформації в цілому. До найбільш типових помилок при вилученні та упакуванні телефону слід віднести:

1. Не вмикання автономного режиму («режиму польоту») або незабезпечення його захисту від зовнішнього впливу через мережу мобільного оператора та мережі бездротового зв'язку. У разі залишення телефону у мережі, можливе його віддалене блокування та навіть стирання (скидання, очищення) користувачем через мережу Інтернет [2].

2. Вимикання телефону без його попереднього огляду. Якщо телефон вдасться розблокувати, до його вимкнення доцільно робити вибіркові фото або відеозаписи виявлених окремих відомостей, оскільки після вимкнення телефону доступ до них може бути втрачений назавжди [3].

3. Витягання SIM-карти прямо на ввімкненому телефоні, що призводить до його автоматичного перезавантаження та втрати можливості розблокування відбитком пальця або системою розпізнавання обличчя.

4. Втрата можливості дослідження телефону після його розблокування відбитком пальця або системою розпізнавання обличчя.

Як зазначається у міжнародних інструкціях для правоохоронних органів, на місці події доцільно використовувати лише два основних алгоритми дій правоохоронця по збереженню інформації у телефоні.

Перший – ввімкнення «режиму польоту» без витягання SIM-карти з одночасним постійним підтримуванням стану зарядженості батареї

(під'єднання power bank) та упакуванням телефону у пакет, блокуючий радіохвилі (т.з. «пакет Фарадея») [4, с. 153].

Другий алгоритм витікає з першого та виконується у разі можливості розблокування особою телефону відбитком пальця або системою розпізнавання обличчя – розблокований телефон переводиться у «режим польоту», після чого у його налаштуваннях дисплею та меню налаштувань безпеки встановлюються параметри: «Вимикання екрану» – «ніколи», «Блокування екрану/режим очікування» – «ніколи», яскравість екрану виставляється в мінімум з метою збільшення строку збереження заряду батареї, телефон під'єднується до зовнішнього носія живлення (power bank) та упаковується у пакет, блокуючий радіохвилі. Таким чином, екран телефону не буде гаснути, телефон буде знаходитись постійно у розблокованому стані та може вільно оглядатись до розряджання всіх джерел живлення. Вимкнути біометричний захист у сучасних телефонах неможливо, оскільки при спробі його вимкнення телефон запитає числовий пароль розблокування.

Вказаний другий спосіб наразі є найбільш ефективним, його застосовують навіть для розблокування телефону потерпілого при вбивстві, використовуючи палець чи обличчя вбитого прямо на місці події, звичайно із дотриманням усіх процесуальних та протокольних процедур. Діючи невідкладно, доки телефон не заблокований, існує можливість синхронізувати переписку з месенджерів та деякі інші відомості з телефону на комп'ютер.

Як ми можемо спостерігати на практиці, спираючись на стан мобільних телефонів, що находять на експертизу, переважної більшості слідчих та оперативних співробітників (окрім спеціальних технічних управлінь) вищевказані алгоритми не відомі, а заняття та підвищення кваліфікації на цю тему з ними майже не проводяться, що за підсумком призводить до непоодиноких випадків втрати важливої доказової інформації.

Список бібліографічних посилань

1. Afonin O. Challenges in Computer and Mobile Forensics: What to Expect in 2020 // Elcomsoft. Blog. 20.12.2019. URL: https://blog.elcomsoft.com/2019/12/challenges-in-computer-and-mobile-forensics-what-to-expect-in-2020/ (дата звернення: 28.04.2020).
2. Извлечение данных из устройств под управлением iOS. Физический и логический методы // Elcomsoft : сайт. https://www.elcomsoft.ru/presentations/ios_acquisition_ru.pdf (дата звернення: 30.04.2020).

3. Распространённые ошибки в мобильной криминалистике // Elcomsoft. Blog. 05.02.2020. URL: https://blog.elcomsoft.com/ru/2020/02/rasprostranyonnye-oshibki-v-mobilnoj-kriminalistike/ (дата звернення: 30.04.2020).
4. Sammons J. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Elsevier Inc, 2012. 208 p.
5. Reiber L. Mobile Forensic Investigations: A Guide to Evidence Collection, Analysis, and Presentation. McGraw-Hill Education, 2015. 480 p.

Одержано 30.04.2020

УДК 343.7

Вадим Анатолійович КОРШЕНКО,
кандидат юридичних наук,
завідувач науково-дослідної лабораторії з проблем розвитку інформаційних технологій
Харківського національного університету внутрішніх справ

ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ПОВ'ЯЗАНИХ ІЗ НЕЗАКОННИМ РОЗПОВСЮДЖЕННЯМ МЕДІЙНОГО КОНТЕНТУ В МЕРЕЖАХ ПРОВАЙДЕРІВ ПРОГРАМНОЇ ПОСЛУГИ ТА ІНТЕРНЕТ-ПРОВАЙДЕРІВ, МЕРЕЖІ ІНТЕРНЕТ

Технічний прогрес зробив можливим практично необмежений інформаційний обмін, зберігання, відтворення, розповсюдження, використання і передачу аудіо, відео творів, програм, текстових творів, баз даних будь-якого обсягу і складності. Враховуючи той факт, що багато подібних об'єктів охороняються авторським правом, виникла необхідність в додатковому захисті і регулюванні вказаних операцій в цифровому середовищі з метою захисту правовласників від нових загроз і посягань. Сучасні цифрові технології розвиваються нестримно і законодавство іноді не встигає адаптуватись під цей стрімкий розвиток, що тягне порушення прав законних правовласників об'єктів інтелектуальних прав. У зв'язку з вказаними обставинами правове регулювання в сфері розповсюдженням медійного контенту в мережах провайдерів програмної послуги та інтернет-провайдерів, мережі Інтернет необхідно покращувати, щоб воно не відставало від науково-технічного прогресу і відповідало наявним викликам.

Слід зазначити, що рівень обізнаності суспільства про культуру споживання медійного контенту і необхідність дотримання законодавства щодо захисту прав інтелектуальної власності є досить низьким, що також сприяє незаконному розповсюдженням медійного контенту та значно ускладнює розслідування таких злочинів та збір доказової бази. Кількість інтернет-ресурсів з нелегальним контентом постійно

росте. Окремі сайти навіть спеціалізуються під певний контент, інші поширюють весь медійний контент без розбору. З'являються інтернет-провайдери, що незаконно ретранслюють телеканали у власних мережах. Використання злочинцями комп'ютерно-технічних засобів та мережі Інтернет в якості інструменту вчинення злочину вимагає від слідчого, детектива і працівника оперативного підрозділу не лише якісного володіння навичками поводження з комп'ютерною технікою та програмами, але й навичками пошуку, виявлення, фіксації та копіювання інформації, що міститься у комп'ютерах, смартфонах, різноманітних телекомунікаційних засобах та носіях комп'ютерної інформації, на Інтернет-ресурсах тощо. Документування таких злочинів найбільш ефективне у рамках кримінальних проваджень із застосуванням усіх дозволених законом методів і засобів.

Досить суттєвий позитивний вплив на стан розслідування злочинів, пов'язаних із незаконним розповсюдженням медійного контенту в мережах провайдерів програмної послуги та інтернет-провайдерів, мережі Інтернет мав факт прийняття Закону «Про державну підтримку кінематографії» [1], положення якого визначили цілу низку термінів таких як електронна (цифрова) інформація, кардшейрінг, піратство у сфері авторського права і (або) суміжних прав, визначили порядок припинення порушень авторського права і (або) суміжних прав з використанням мережі Інтернет, внесли зміни в інші законодавчі акти, зобов'язали постачальників послуг хостингу забезпечувати захист авторського права і (або) суміжних прав з використанням мережі Інтернет, тощо.

Станом на сьогодні незаконне розповсюдження медійного контенту можна розділити на наступні форми:

- незаконне розповсюдження музичних, аудіовізуальних творів або комп'ютерних програм на окремих сайтах (приватні або публічні файл-сервери, централізована файлообмінна мережа);
- незаконне розповсюдження музичних, аудіовізуальних творів або комп'ютерних програм за технологіями P2P (частково централізована файлообмінна мережа – торент, DC, тощо);
- незаконне поширення VOD (video on demand) контенту – це поширення аудіовізуальних творів (чи їх частин) власниками інтернет-сайтів за індивідуальним замовленням;
- незаконне поширення програм шляхом ретрансляції телеканалів за технологією OTT – (Over The Top) і IPTV окремими особами або

провайдерами програмної послуги;

- кардшейрінг – забезпечення у будь-якій формі та в будь-який спосіб доступу до програми (передачі) організації мовлення, доступ до якої обмежений суб'єктом авторського права і (або) суміжних прав застосуванням технічних засобів захисту (абонентська карта, код тощо), в обхід таких технічних засобів захисту, в результаті чого зазначена програма (передача) може бути сприйнята або в інший спосіб доступна без застосування технічних засобів захисту;
- незаконна ретрансляція провайдерами програмної послуги телеканалів в аналогових та цифрових кабельних мережах телебачення;
- незаконний публічний показ передач/програм в закладах HoReCa (закладах громадського харчування, готелях, кінотеатрах і так далі).

Усі вказані форми незаконного розповсюдженням медійного контенту мають істотні власні особливості відносно технологій здійснення, осіб-порушників, методики документування і засобів захисту. Окремі види незаконного розповсюдженням медійного контенту можуть бути припинені в досудовому порядку, інші, такі як кардшейрінг, поширення передач/програм на інтернет-сайтах, IPTV та OTT-сервісах, вимагають судового захисту. Протидію розглядуваному виду злочинів, можна умовно поділити на два напрями.

Перший напрям полягає у здійсненні взаємодії з підрозділами протидії кіберзлочинності та оперативно-технічними підрозділами поліції. При цьому ініціатива у протидії даним злочинам переходить від слідчого, детектива, до вказаних підрозділів, які за допомогою використання можливостей технічних засобів здатні отримати додаткову інформації про злочинців, їх дії тощо та задокументувати їх причетність до злочину.

Другий напрям є класичним у діяльності оперативних підрозділів та полягає, насамперед, у використанні можливостей штатних та позаштатних негласних працівників.

Список бібліографічних посилань

1. Про державну підтримку кінематографії : Закон України від 23.03.2017 № 1977-VIII // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1977-19 (дата звернення: 01.05.2020).

Одержано 05.05.2020

УДК 004.9

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

МЕТОДИ ДОСЛІДЖЕННЯ JTAG ТА CHIP-OFF У КОМП'ЮТЕРНО-ТЕХНІЧНІЙ ЕКСПЕРТИЗІ

В комп'ютерно-технічній експертизі методи дослідження JTAG ТА CHIP-OFF все більше викликають великий інтерес та необхідність в їх застосуванні, оскільки ці методи дозволяють отримати прямий доступ до даних які можуть перебувати під захистом (наприклад, захист паролем) або даних що містяться в пам'яті пошкоджених пристроїв.

На поточний момент JTAG (Joint Test Action Group) – це промисловий стандарт яким оснащуються практично всі складні цифрові мікросхеми. Фізично він представлений на платі у вигляді точок або коннекторів для підключення спеціального обладнання. Використовується JTAG для прошивки мікросхем з пам'яттю та їх вихідного контролю на виробництві, тестування готових плат, відладочних робіт при проектуванні апаратури та програмного забезпечення.

Тобто JTAG являє собою апаратний інтерфейс для прямого зв'язку робочої станції (персонального комп'ютера) з материнською платою пристрою за допомогою програматорів, наприклад Z3X Easy-Jtag, RIFF Box, Octopus.

Для вилучення даних з пристроїв за допомогою методу JTAG експерт повинен бути забезпечений необхідним програмним та апаратним забезпеченням програматора-JTAG, паяльником або паяльною станцією, припоєм, дротовими з'єднаннями та схемою розміщення на платі мобільного пристрою точок JTAG.

У випадках коли методом JTAG немає можливості скористатись, внаслідок пошкодження плати пристрою, або відсутньою схемою розміщення точок стандарту на платі – є можливість у використанні не менш значимого методу CHIP-OFF.

Якщо розглядати метод CHIP-OFF з точки зору комп'ютерно-технічної експертизи – то це технологія, за якою мікросхема пам'яті вилучається з печатної плати пристрою, проводиться її підготовка для зняття фізичного дампу пам'яті та подальше вилучення цього дампу за допомого програматорів з подальшою обробкою отриманих даних за допомогою спеціального програмного забезпечення.

Наразі існує два види пам'яті NAND – це TSOP и BGA. Основна відмінність мікросхем пам'яті типу TSOP – наявність контактів, що розміщені по контуру мікросхеми та зпаюються з платою. Демонтаж таких мікросхем найпростіший, але потребує великої акуратності. Що до мікросхем типу BGA (Ball Grid Array – масив кульок) – то процес з ними значно важчий. У даному типу мікросхем контакти виконані у вигляді кульок на основі мікросхеми, які припаяні до плати. А ще мікросхеми BGA не мають єдиного стандарту та кожен виробник може розробити та використовувати власний тип мікросхеми зі своїм розміщенням контактів.

Для вилучення даних з пристроїв за допомогою методу CHIP-OFF експерт також повинен бути забезпечений паяльною станцією, припоєм, флюсом, програматорами, що зчитують пам'ять, адаптерами які відповідають топологіям розміщення контактів на мікросхемі, програмним забезпечення для зчитування та обробки даних.

Після зняття фізичного образу даних обох методів, дампи пам'яті обробляються за допомогою програмних продуктів Oxygen Forensics або Cellebrite UFED Physical Analyzer. У випадку вилучення інформації за методом CHIP-OFF, може знадобитись «збірка» дампу, що являє собою виключення службових областей та корекцію стиків сторінок пам'яті. Для цих цілей можна використовувати програмне забезпечення ACE Laboratory.

Важливо зазначити, що для використання методів JTAG та CHIP-OFF, експерт комп'ютерно-технічної експертизи повинен мати розуміння в організації даних на мікросхемах пам'яті, володіти навичками демонтажу та повторного. монтажу компонентів пристрою.

На теперішній час, більшість носіїв інформації які надходять на комп'ютерно-технічну експертизу – це мобільні телефоні та планшетні комп'ютери. До того ж, з кожним днем все більше зростають вимоги до якості та кількості даних що вилучаються з портативних пристроїв. Сьогодні вже недостатньо вилучення лише списку контактів, СМС та журналу дзвінків, а обов'язково стоїть задача у вилученні історії листу-

вання засобами мережі інтернет за допомогою месенджерів, вилучення ГЕО-даних, зображень та відео, відновлення видалених даних. Однак, не всі дані, навіть при наявності їх в мобільному пристрої, можуть бути вилучені. Це пов'язано з апаратними та програмними особливостями зберігання даних в конкретному мобільному пристрої конкретного виробника.

Вже зараз можна сказати, що методи JTAG та CHIP-OFF стають все більш необхідними в сучасній комп'ютерно-технічній експертизі, адже можуть вирішити важливі питання що потребують непростих рішень та вирішення яких звичними методами не виявилося можливим.

Список бібліографічних посилань

1. Cellebrite Advanced JTAG Extraction (CAJE) // Cellebrite. 14.01.2020. URL: https://www.cellebritelearningcenter.com/mod/page/view.php?id=11903 (дата звернення: 28.04.2020).
2. Elder B. Chip-Off and JTAG Analysis. Evidence technology magazine. June 2012. URL: http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=922 (дата звернення: 28.04.2020).
3. Макаров А. Получение данных из мобильных устройств с помощью интерфейса отладки JTAG // Anti-Malware : сайт. 18.04.2017. URL: https://www.anti-malware.ru/analytics/Technology_Analysis/Getting_data_from_mobile_devices_using_JTAG_debug_interface (дата звернення: 28.04.2020).

Одержано 30.04.2020

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

ІДЕНТИФІКАЦІЯ СЕРІЙНИХ ПРАВОПОРУШЕНЬ

У рамках здійснення поліцейської діяльності слід регулярно проводити порівняльний аналіз проваджень на районному, регіональному та загальнодержавному рівнях. Проведення такого аналізу є корисним у рамках оперативного, тактичного та стратегічного рівнів кримінальної розвідки. Серед іншого шляхом порівняльного аналізу матеріалів кримінальних проваджень досягається виявлення серій злочинів на території обслуговування. Дані, що стосуються виявлених серій, можуть бути використані в якості вихідних даних для різних алгоритмів географічного профілювання. При цьому вкрай важливо наголосити, що помилково внесені до серії епізоди можуть спотворити загальну картину та ввести в оману правоохоронців, що може повести розслідування хибним шляхом.

В українській правоохоронній науці порівняльному аналізу справ, на жаль, не приділяється належної уваги, про що свідчить брак відповідних публікацій. Натомість у США розроблено цілий проект, у рамках якого проводиться порівняльний аналіз справ з метою виявлення серійних убивств (www.murderdata.org).

Журналіст Т. Харгроув, який заснував проект, розробив спеціальний алгоритм та автоматизував порівняння справ про серійні вбивства на території США [1]. Завдяки його дослідженням у США вдалося ідентифікувати та затримати серійного вбивцю Даррена Деона Ванна, який душив жінок на протязі десятків років. Свої дослідження Т. Харгроув розповсюджує на безкоштовній основі, тому цей нескладний алгоритм міг би бути адаптований і в правоохоронних органах України.

Одразу слід відзначити, що порівняльний аналіз дозволяє виявити серійність не тільки у провадженнях щодо вбивств, але й стосовно інших категорій злочинів.

Для виявлення серійних злочинів використовується два головних методи:

1) матричний аналіз;

2) контент-аналіз.

Матричний аналіз передбачає представлення наявної облікової інформації про вчинені злочини у табличному вигляді для наступного вивчення.

Одним із методів матричного аналізу є IZE [2, с. 64], який отримав свою назву від закінчень назв його п'яти етапів:

1. Категоризація (Categorize) – обрання змінних для виявлення злочинних трендів, які будуть виступати в якості назв полів у таблиці (наприклад, час доби).

2. Генералізація (Generalize) – визначення можливих значень для змінних, обраних на першому етапі (наприклад, ранок, день, вечір, ніч).

3. Організація (Organize) – групування змінних та сортування даних для виявлення однотипних скупчень (кластерів).

4. Мінімізація (Minimize) – обмеження даних в таблиці виявленими кластерами

5. Максимізація (Maximize) – додатковий аналіз даних, які могли бути пропущені на попередніх етапах. Наприклад, всі ознаки збігаються але особи, які вносили дані, використовувані для аналізу, вказали неповні параметри або помилково внесли невірні дані, або взагалі не внесли частину даних при введенні.

Формування відповідних таблиць повинно відбуватися з урахуванням системи 5W+H. Після того, як сформовано попередні кластери, слід провести ретельний контент-аналіз матеріалів проваджень для виявлення інших спільних рис злочинів або спростування припущення про їх належність до серії. Контент-аналіз дозволяє виявити додаткові ознаки злочинних посягань, які не були доступні раніше. На цьому етапі можуть бути створені більш докладні таблиці порівняння за кожною змінною.

Список бібліографічних посилань

1. Murder Accountability Project's computer algorithm // Dropbox : сайт. URL: https://www.dropbox.com/s/49i2mw0caswn8y0/Algorithm.pdf?dl=0 (дата звернення: 05.04.2020).
2. Paulsen D. J., Bair S., Helms D. Tactical Crime Analysis: Research and Investigation. Boca Raton, FL : CRC Press, 2009. 240 p.

Одержано 30.04.2020

УДК 343.8:328:185

Олег Володимирович НОВІКОВ,
кандидат юридичних наук,
асистент кафедри кримінології та кримінально-виконавчого права Національного юридичного університету імені Ярослава Мудрого,
науковий співробітник Науково-дослідного інституту вивчення проблем злочинності ім. акад. В. В. Сташиса
Національної академії правових наук України

ПРО РИЗИКИ ЗАСТОСУВАННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ ТЕХНОЛОГІЙ У СФЕРІ ПРОТИДІЇ ТА ЗАПОБІГАННЯ КОРУПЦІЇ

На сьогодні «діджиталізація» стала новим трендом суспільного розвитку усіх сферах життєдіяльності. Не оминула вона й сферу державного управління в Україні. Так, п. 14.1 досі чинної Програми діяльності Кабінету Міністрів України, яка була затверджена постановою Верховною Радою України від 04.10.2019 №188-IX, передбачено переведення всіх публічних послуг в режим онлайн-доступу до 2024 р. Серед останніх новин, Кабінет Міністрів України та Європейський Союз 11 лютого 2020 р. підписали нову Програму підтримки електронного урядування та цифрової економіки в Україні на суму 25 млн євро [1].

Необхідність діджиталізації державного управління, в першу чергу, пов'язують із протидією та запобіганням корупції. І з цим, дійсно, можна погодитися. Окремі наукові дослідження в країнах ЄС встановили суттєві обернені зв'язки між наявністю електронного урядування й відсотком населення, що використовують послуги електронного уряду, та рівнем корупції в державі [2, с. 32–33]. Інформаційно-комунікаційні технології, насправді, дозволяють ефективно протидіяти та запобігати корупційним практикам шляхом: підвищення прозорості державного управління (процедур прийняття владних рішень), забезпечення доступу до публічної інформації, усунення безпосереднього зв'язку між чиновниками та громадянами, зменшення бюрократичних перешкод, прискорення адміністративних послуг, виявлення корупційних практик

через моніторинг публічних реєстрів та повідомлень у засобах масової інформації, ідентифікації змов під час публічних закупівель тощо [3, с. 2].

В цей же час, існують певні ризики у застосуванні інформаційно-комунікаційних технологій у сфері протидії та запобігання корупції, які можна об'єднати у дві групи.

Перша група включає в ризики, що пов'язані із впровадженням та застосуванням зазначених антикорупційних технологій. До них належать, зокрема:

- конфлікт між концепцією «відкритих даних» та правами людини на приватне життя та конфіденційність;
- складність використання «цифрових» державних послуг для громадян, що не мають відповідних навичок роботи чи цифрової освіти, та громадян, що не мають доступу до мережі Інтернет;
- посилення конспірації корупційних угод та належне маскування чиновниками своїх незаконних активів [4, с. 9];
- можливість тотального державного контролю за населенням;
- неякісна розробка антикорупційного програмного продукту, що може призвести до порушення принципів кібербезпеки та некоректної роботи програми.

Друга група включає ризики, пов'язані із кіберзагрозами та кіберзлочинністю. До них належать, зокрема:

- можливість несанкціонованого втручання у роботу антикорупційного програмного продукту;
- несанкціоновані дії з інформацією з обмеженим доступом, яка обробляється антикорупційним програмним продуктом;
- несанкціоновані збут або розповсюдження інформації з обмеженим доступом, що обробляється антикорупційним програмним продуктом;
- кібершпигунство та кіберсталкінг за допомогою антикорупційного програмного продукту.

Таким чином, потрібно звернути увагу на зазначені вище ризики під час розробки, впровадження та використання інформаційно-комунікаційних технологій у сфері запобігання та протидії корупції.

Список бібліографічних посилань

1. Діджиталізація: Кабмін і ЄС підписали нову програму на €25 мільйонів // Укрінформ : сайт. 11.02.2020. URL: https://www.ukrinform.ua/rubric-polytics/2874257-didzitalizacia-kabmin-i-es-pidpisali-novu-programu-na-25-miljoniv.html (дата звернення: 30.04.2020).
2. Mungiu-Pippidi A. The Good, the Bad and the Ugly: Controlling Corruption in the European Union. Working Paper № 35 // European Research Centre for Anti-corruption and State-building. April 2013. URL: https://www.researchgate.net/publication/296624715_The_Good_the_Bad_and_the_Ugly_Controlling_Corruption_in_the_European_Union (дата звернення: 30.04.2020).
3. Technology against corruption: the potential of online corruption-reporting apps and other platforms // U4 Expert Answers. U4 Anti-Corruption Resource Centre. URL: https://www.u4.no/publications/technology-against-corruption-the-potential-of-online-corruption-reporting-apps-and-other-platforms.pdf (дата звернення: 30.04.2020).
4. Kossow N., Dykes V. Embracing Digitalisation: How to use ICT to strengthen Anti-Corruption. Deutsche Gesellschaft für Internationale Zusammenarbeit. March 2018. 38 p. URL: https://www.giz.de/de/downloads/giz2018-eng_ICT-to-strengthen-Anti-Corruption.pdf (дата звернення: 30.04.2020).

Одержано 01.05.2020

УДК 343.1+004

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

РОЗПОДІЛЕНИЙ КРИПТОАНАЛІЗ ПРИ ОБМЕЖЕНИХ РЕСУРСАХ ДЛЯ ПОТРЕБ ПРАВООХОРОННИХ ОРГАНІВ

Перед оперативними підрозділами правоохоронних органів при здійсненні досудового розслідування деяких кримінальних правопорушень виникає задача розшифрування вилучених у підозрюваного в скоєнні злочину зашифрованих симетричними криптосистемами даних, які можуть стати доказом у скоєнні злочину.

На практиці, при очевидній відсутності спеціалізованих обчислювальних ресурсів, підвищити обчислювальну ефективність криптоаналізу зашифрованих симетричними криптосистемами даних можна тільки за рахунок паралельної розподіленої клієнт-серверної атаки на базі локальної мережі персональних комп'ютерів, де сервер здійснює періодичний розподіл виділених підмножин простору можливих ключів шифрування між клієнтами, які в свою чергу передають задачу локальній програмі перебору ключів (ЛППК).

З точки зору застосовності системи розподіленого криптоаналізу (СРК) в оперативних підрозділах правоохоронних органів можна сформулювати вимоги до її компонентів:

1) максимальна універсальність до типів зашифрованих даних;

2) відкриті вихідні коди і ліцензія вільного програмного забезпечення;

3) функціонування на різних платформах;

4) обчислення як на центральних, так і на графічних процесорах клієнтських персональних комп'ютерів;

5) операційна система Windows на клієнтських персональних комп'ютерах;

6) необмежена кількість клієнтів.

Максимальну універсальність до типів зашифрованих даних забезпечує вилучення гешу ключа шифрування із різних об'єктів зашифрованих даних (*.docx, *.pdf, *.zip, *.7z, *.rar, та ін.) і обчислення гешу від імовірних ключів для порівняння із вилученим.

ЛППК, що відповідають вище зазначеним вимогам, можуть бути або *Hashcat*[3], або *John the Ripper jumbo release (JtR)*[4]. Для них існують взаємно сумісні програмні рішення вилучення гешу ключа із багатьох типів зашифрованих даних [5,6]. У якості СРК, які використовують Hashcat або JtR і задовольняють встановленим вимогам, можуть бути: *Hashtopolis*[7], *Fitcrack*[8], *Cracklord*[9], *GoCrack*[10].Розробники Fitcrack в [1] навели результати експериментального дослідження ефективності свого рішення у порівнянні із Hashtopolis, де для кожного типу перебору ключів (повний перебір, за шаблоном, за словником, гібридний) запропонували різну стратегію розподілу завдань. Fitcrack в цілому показав більшу ефективність і більш високий рівень абстракції та автоматизації розподіленого криптоаналізу. Результати подібних досліджень ефективності та застосовності рішень Cracklord та GoCrack не знайдені.

Для оцінки застосовності СРК в локальної мережі із 21 ПК під управлінням ОС Windows 7 Professional у зв'язці з Hashcat був інстальований та перевірений на працездатність Hashtopolis. Серверна частина була розгорнута в ОС Kali Linux Light на віртуальній машині Oracle VM VirtualBox, а клієнтська в середовищі Python 3.7.2 ОС Windows. Результати тестування розподіленого перебору ключів для гешів, обчислених за різними алгоритмами, підтвердили працездатність Hashtopolis та показали, що зростання швидкості паралельних обчислень не є прямо пропорційним до кількості агентів із-за витрат часу на формування підмножин простору ключів, їх доставки агентам і отриманням результатів перебору.

З урахуванням [1] та проведеного тестування була ідентифікована задача із оптимального визначення для клієнтів розміру підмножини простору можливих ключів (chunk) в залежності від кількості агентів, їх

3 https://hashcat.net/
4 https://www.openwall.com/john/
5 https://github.com/stricture/hashstack-server-plugin-hashcat/tree/master/scrapers
6 https://github.com/magnumripper/JohnTheRipper/tree/bleeding-jumbo/run
7 https://github.com/s3inlc/hashtopolis
8 https://github.com/nesfit/fitcrack
9 https://github.com/jmmcatee/cracklord
10 https://github.com/fireeye/gocrack

поточної швидкості перебору, алгоритму гешу, типу перебору (повний перебір, за шаблоном, за словником, гібридний).

В подальшому, після порівняльної оцінки вище зазначених СРК, доцільна розробка набору різних конфігурацій найбільш ефективної СРК із методикою їх оптимального застосування оперативними підрозділами правоохоронних органів.

Список бібліографічних посилань

1. Hranický R., Zobal L., Ryšavý O., Kolář D. Distributed password cracking with BOINC and hashcat. *Digital Investigation*. 2019. Vol. 30, No. 1. Pp. 161–172. URL: https://www.fit.vut.cz/research/publication-file/11961/Distributed_password_cracking_with_BOINC_and_hashcat.pdf (дата звернення: 25.04.2020).

Одержано 26.04.2020

УДК 343.46:347.63

Анна Сергіївна ПОЛІТОВА,
кандидат юридичних наук, доцент,
доцент кафедри юридичних дисциплін
Донецького юридичного інституту МВС України (м. Маріуполь)

ТОРГІВЛЯ ЛЮДЬМИ ТА СУРОГАТНЕ МАТЕРИНСТВО: АКТУАЛЬНІ ПИТАННЯ КВАЛІФІКАЦІЇ

За даними ООН, у світі щорічно продається приблизно 4 млн. осіб, яких обманом чи насильством змушують до певного виду діяльності. Україна взяла на себе зобов'язання щодо виконання Конвенції ООН про заборону торгівлі людьми й експлуатацію проституції, а також доповнила КК України відповідною статтею. Однак «живий товар» з України надходить у різні країни світу. На превеликий жаль, згідно доповіді Державного департаменту США про нелегальну торгівлю людьми у світі, Україна належить до держав, де для боротьби з цим явищем докладається недостатньо зусиль.

27 квітня 2020 року на сайті МВС України було опубліковано інформацію «Верховна Рада має врегулювати питання сурогатного материнства, щоб унеможливити продаж немовлят за кордон, – Антон Геращенко», де повідомлялося про те, що «зловмисники упродовж тривалого часу, під прикриттям сурогатного материнства та шляхом укладення фіктивних шлюбів із іноземцями, переправляли новонароджених дітей не лише по Україні, а й в інші держави, зокрема в Китайську Народну Республіку» [1].

Законодавство України певною мірою захищає права та інтереси дітей при їх усиновленні (удочерінні) і перешкоджає торгівлі ними. Але у зв'язку з тим, що в Україні зростає кількість безплідних подружніх пар, стає актуальним питання сурогатного материнства – введення заплідненої яйцеклітини, отриманої від біологічних батьків дитини, яка після народження передається цим батькам. І найбільш гострим є законодавче врегулювання відносин, які виникають між біологічними батьками і сурогатною матір'ю, а також проблема захисту прав дитини, що народилася за таких обставин.

Сама ідея сурогатного материнства не є новою. Ще в Біблії говориться, що коли Рахіль не змогла народити дитину своєму чоловіку Іакову, вона запропонувала служниці народити їм дитину (Бит. 30) [2]. На думку Я. Дргонца та П. Холлендера, яскравим прикладом сурогатного материнства є розповсюджена до винаходу штучного материнського молока практика годування новонародженої дитини чужою жінкою. Вона брала на себе частину біологічної турботи про дитину, тоді, коли мати не мала можливості годувати її за станом здоров'я [3, с. 170].

В Україні сурогатне материнство має понад 30-річну історію [4, с. 168]. Проте скористатися програмою сурогатного материнства більшість українських сімей, що страждають від безплідності, а це 10-15%, не можуть через її високу вартість. Натомість така програма є привабливою для іноземних громадян через недосконале українське законодавство, що регулює відносини у сфері сурогатного материнства і стосовно доступну для іноземних громадян вартість цієї програми. Наведене вище призвело до того, що Україна сьогодні є однією із привабливих країн для «репродуктивного туризму», незважаючи на те, що правове забезпечення сурогатного материнства є одним із законодавчо неврегульованих і найскладніших питань у галузі сімейного права України та у сучасній юридичній практиці.

У юридичній літературі сьогодні запропоновані різні варіанти правового врегулювання відносин, що виникають при сурогатному материнстві [5]. Більшість же дослідників пропонують оформляти відносини між замінюючою і сурогатною матерями та біологічними батьками договором, відповідно до якого сурогатна мати після пологів зобов'язується передати дитину її біологічним батькам [3, с. 198]. Проте укладання такого договору не гарантує його належного виконання. Сам по собі договір хоча і вносить ясність у стосунки батьків, але не може усунути невпевненості у правовому становищі дитини, якщо її відмовляються прийняти біологічні батьки, а мати, що її народила, такою вважатися не буде.

При всій юридичній принадності «договірного материнства», навряд чи воно має бути єдиною правовою формою, впорядкування цих відносин. Справа у тому, що, як правило, при невиконанні обов'язків за договором однією стороною інша вправі вимагати їх примусового виконання. Проте як не можна змусити жінку переносити «чужу» вагітність, так і не можна її заставити віддати народжену дитину, навіть

якщо біологічними батьками є інші особи. Специфіка таких договорів полягає в тому, що не повинно бути примусового виконання у випадку, коли «замовники» відмовляються взяти свою дитину або «виконавець» не хоче її віддати.

Вважаємо, що правильною є точка зору, яка полягає у тому, що принципово важливим є не допустити перетворення жінки, яка виношує чужу дитину, у товар. Жінка не може розглядатись як платний інкубатор, що відтворює чужих дітей за відповідну винагороду [6, с. 25].

В Англії в середині 80-х років минулого століття був прийнятий закон, що забороняє рекламу і комерціалізацію сурогатного материнства. Мати, яка виношує чужу дитину, не вправі брати будь-яку плату з батьків, крім компенсації витрат, пов'язаних з операцією і вагітністю. Про заборону використання сурогатного материнства у комерційних цілях йдеться і в Брюссельській декларації Всесвітньої медичної асоціації 1985 р. [7, с. 23].

Голландський доповідач з питань торгівлі людьми опублікувала звіт, у якому довела, що «комерційне сурогатне материнство» може кваліфікуватися як торгівля людьми [8, с. 51]. Визначення торгівлі людьми наведене у ст. 3 Протоколу ООН про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї, включає: 1) дія – вербування, перевезення, передача, приховування або одержання людей; 2) засіб – шляхом загрози силою або її застосування чи 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; 3) мета – з метою експлуатації, що також включає послуги. Також у звіті розглянуто таке питання – яким чином комерційне сурогатне материнство підпадає під визначення торгівлі людьми.

Підводячи підсумок можна відзначити, що оскільки торгівля людьми, а особливо дітьми, є надзвичайно прибутковою справою, в українському законодавстві теж необхідно закріпити заборону сурогатній матері отримувати від біологічних батьків кошти за те, що вона виносила і народила дитину. Така норма позбавить ділків ще однієї можливості займатися торгівлею дітьми. Оскільки усиновлення (удочеріння) здійснюється стосовно лише неповнолітньої (малолітньої) людини, то вербування, переміщення, переховування, передача або одержання з метою

усиновлення (удочеріння) з метою наживи не може кваліфікуватися за ч. 1 ст. 149 КК України, а тільки за ч. 2 чи ч. 3 цієї статті.

Список бібліографічних посилань

1. Верховна Рада має врегулювати питання сурогатного материнства, щоб унеможливити продаж немовлят за кордон, – Антон Геращенко // Єдиний портал органів системи МВС України : офіц. сайт. 27.04.2020. URL. https://mvs.gov.ua/ua/news/30209_Verhovna_Rada_ma_vregulyuvati_pitannya_surogatnogo_materinstva_shchob_unemozhliviti_prodazh_nemovlyat_za_kordon___Anton_Gerashchenko.htm (дата звернення: 29.04.2020).
2. Біблія, або Книги Святого Письма Старого і Нового Заповіту : із мови давньоєврейської та грецької на укр. наново перекладена. Київ : Біблійні товариства, 1995. 296 с.
3. Дргонец Я., Холлендер П. Современная медицина и право / пер. со словац. М. : Юрид. лит., 1991. 336 с.
4. Аблятіпова Н. А. Проблеми сурогатного материнства в Україні. *Актуальні проблеми держави і права.* 2009. Вип. 51. С. 167–172.
5. Мискарян Е. Г. Правовые гарантии установления материнства и отцовства : автореф. дис. … канд. юрид. наук : 12.00.03. Тбилиси, 1979. 23 с.
6. Майфат А. В. Суррогатное материнство и иные формы репродуктивной деятельности в новом Семейном кодексе РФ*. Юридический мир*. 2000. № 2. С. 19–33.
7. Григорович Е. В. Суррогатное материнство: за и против. *Юрист*. 1999. № 4. С. 22–25.
8. Міжнародний досвід законодавчого регулювання питання використання репродуктивних технологій (включаючи сурогатне материнство) / уклад. А. Брашовяну. Київ, 2013. 60 с.

Одержано 30.04.2020

УДК 004.056.5:343.9.024:343.85(477;438)

Максим Юрійович ТРЕТЬЯКОВ,
студент 3 курсу групи Інституту прикладного системного аналізу Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

ВІДПОВІДАЛЬНІСТЬ ЗА ОКРЕМІ ВИДИ КІБЕРЗЛОЧИНІВ ЗА КРИМІНАЛЬНИМ ЗАКОНОДАВСТВОМ УКРАЇНИ, ФРАНЦІЇ ТА ПОЛЬЩІ (ПОРІВНЯЛЬНИЙ АНАЛІЗ)

За статистикою за останні 5 років кількість кіберзлочинів в Україні збільшилась удвічі. При цьому значне зростання кількості кіберзлочинів у 2017 р. пов'язано з вірусом «Petya» й дотепер кількість таких злочинів не знижається [1]. Очевидно, що кіберзлочини можуть мати тяжкі наслідки. Хоча кількість порушених кримінальних проваджень в Україні досить значна, але кількість реально покараних злочинців є дуже малою та покарання за такі злочини в Україні є значно меншим, ніж в інших країнах Європи. Оскільки Україна має наміри вступити до Європейського Союзу, проаналізуємо відмінності кримінального законодавства окремих держав-членів ЄС, щоб зрозуміти переваги та недоліки вітчизняного законодавства. Візьмемо декілька реальних прикладів кіберзлочинів та проведемо порівняння судових вироків, які могли б бути винесені за них в Україні, Франції та Польщі.

Зрозуміло, що найбільшу загрозу несуть середні та тяжкі кіберзлочини. Щоб розуміти ситуацію з кіберзлочинністю, яка склалась у цих країнах, проведемо аналіз статей, які відповідають вищезазначеним злочинам, що допоможе зрозуміти серйозність покарання даних дій у цих державах.

В КК України передбачено декілька статей (ст.ст. 361, 361-1, 361-2, 362, 363, 363-1), які встановлюють відповідальність за кіберзлочини. У цих статтях передбачено найсуворіше покарання в 3-5 років обмеження волі (ст. 361-362) при умові, що дії вчинені повторно або за змовою групи осіб. Менш тяжкі злочини (ст. 363) караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян (що може бути дуже малою сумою у порівнянні з збитками даних злочинів) [2].

У Франції відповідальність за кіберзлочини передбачають 9 статей КК (art. 323, 323-1, 323-2, 323-3, 323-3-1, 323-4, 323-4-1, 323-5, 323-6). Найсуворіше покарання (art. 323-3) – це 5 років позбавлення волі та 75000 євро штрафу. Менш тяжкі злочини (art. 323-1, 323-2) передбачають позбавлення волі на 2-3 роки та штраф у розмірі 30000-45000 євро відповідно [3].

У Польщі відповідальність за кіберзлочини передбачають 3 статті КК (art. 267-269). При цьому злочини середньої тяжкості караються 2-3 роками позбавлення волі (art. 267-268). Тяжкі ж злочини, в яких постраждала держава та її органи, караються позбавленням волі до 8 років (art. 269) [4].

Розглянемо відомий випадок хакера Каріма Баратова, який був заарештований у Канаді та був екстрадований до США, де визнав провину в змові з метою здійснення комп'ютерного шахрайства та розкрадання персональних даних при обтяжуючих обставинах. За допомогою вірусів він зламав близько 11000 аккаунтів електронної пошти, отримуючи по 100 доларів США за кожний. Загалом його дії зачепили близько 500 мільйонів користувачів сервісу Yahoo. Слідство також виявило, що одним з замовників був агент ФСБ (тобто це злочин за попередньої змовою групи осіб). Оскільки від даних дій могли, а може й постраждали аккаунти державних працівників, це можна розцінювати як загрозу державі. Суд в Каліфорнії присудив йому 5 років позбавлення волі та штраф в розмірі 2,25 мільйонів доларів США [5]. Порівняємо, який вирок він би отримав у державах, законодавство яких ми розглядаємо:

- в Україні за ці дії відповідальність встановлено в ст. 361-2 КК (значна шкода, попередня змова групи осіб – передбачає 2-5 років позбавлення волі). Зважаючи на ситуацію, суд виніс би вирок 5 років позбавлення волі.
- у Франції за ці дії відповідальність встановлено в art. 323-3-1 КК. (передбачає 5 років позбавлення волі та штраф у 75000 євро).
- у Польщі за ці дії відповідальність встановлено в art. 269 КК (передбачає від 6 місяців до 8 років позбавлення волі). Зважаючи на ситуацію, суд виніс би вирок 8 років позбавлення волі.

Таким чином, порівнявши законодавство вищезазначених держав у сфері кіберзлочинності, можна стверджувати, що кримінальне законодавство України передбачає найменше покарання серед усіх розглянутих. Це може буди одним з факторів, який провокує кіберзлочини на

території нашої держави, а тому потрібно збільшити розмір покарання за ст. 361-363 КК України відповідно до прикладу розглянутих держав.

Список бібліографічних посилань

1. За последние пять лет количество киберпреступлений в Украине выросло вдвое // Опендатабот : сайт. 21.10.2019. URL: https://opendatabot.ua/blog/ru/375-hackers (дата звернення: 30.04.2020).
2. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 30.04.2020).
3. Code pénal Français du 22 juillet 1992 // Legifrance. 25.03.2020. URL: https://www.legifrance.gouv.fr/affichCode.do?cidTexte=LEGITEXT000006070719 (дата звернення: 30.04.2020).
4. Poland Penal Code of 6 June 1997. URL: https://www.legislationline.org/download/id/4172/file/Polish%20CPC%201997_am%202003_en.pdf (дата звернення: 30.04.2020).
5. Хакеру з Канади дали 5 років за злом Yahoo на замовлення російських спецслужб // Укрінформ : сайт. 31.05.2018. URL: https://www.ukrinform.ua/rubric-world/2471550-hakeru-z-kanadi-dali-5-rokiv-za-zlom-yahoo-na-zamovlenna-rosijskih-specsluzb.html (дата звернення: 30.04.2020).

Одержано 02.05.2020

УДК 343(431+522)

Михайло Ігоревич ФІАЛКА,
кандидат юридичних наук, доцент,
доцент кафедри кримінального права і кримінології факультету № 1
Харківського національного університету внутрішніх справ

ОКРЕМІ ПИТАННЯ КВАЛІФІКАЦІЇ ТОРГІВЛІ ЛЮДЬМИ, ПОВ'ЯЗАНОЇ З ПІДРОБЛЕННЯМ ДОКУМЕНТІВ

Суспільно небезпечне діяння, яке пов'язане з торгівлею людьми, в будь-якому випадку, вчинюється з метою експлуатації цієї людини. Крім того, весь цей «комплекс» суспільно небезпечних проявів повинен відбуватись з використанням примусу, викрадення, обману, шантажу, матеріальної чи іншої залежності потерпілого, його уразливого стану або підкупу третьої особи, яка контролює потерпілого. І все це реалізується для отримання згоди від потерпілого на його експлуатацію [1].

В окремих випадках, для реалізації свого суспільно небезпечного діяння винна особа використовує підроблені документи. Так, наприклад, слідчий суддя Хмельницького міськрайонного суду ухвалив обрати запобіжні заходи у вигляді домашнього арешту породіллі, яка хотіла позбутися новонародженої дитини, та жінці, яка хотіла її забрати незаконним шляхом.

Крім того, було вручено підозру в торгівлі немовлям, розпочато кримінальне провадження та обрано запобіжний захід в.о. директора з медичного обслуговування населення КП «Хмельницький міський перинатальний центр», яка, на думку слідства, розпорядилася підробити відповідні документи.

Усіх трьох підозрюють у вчиненні злочинів, передбачених ч. 3 ст. 15, ч. 3 ст. 149, ч. 4 ст. 358 та ч. 1 ст. 366 КК України [2].

Даний приклад демонструє нам той факт, що в реальній дійсності існують випадки коли винні особи, для реалізації власних намірів з продажу людини, використовують підроблені документи. В цій ситуації виникає запитання: яким чином повинна відбуватись кримінально-правова кваліфікація такого діяння.

Спробуємо розставити всі крапки над «і». В перу чергу, необхідно чітко розуміти те, що використання підроблених документів, як правило, використовується або для введення в оману потерпілу особу, або для прикриття самого факту торгівлі людиною.

У випадку, коли мова йде про маскування суспільно небезпечного діяння, то в цій ситуації сумнівів не виникає – кваліфікація повинна відбуватись за сукупністю злочинів, а саме: за торгівлею людьми (ст. 149 КК України) та за те чи інше підроблення (або ст. 358 або ст. 366 КК України). Якраз такий приклад кваліфікації ми розглянули декілька раніше в ситуації з продажем немовля. Така остаточна кваліфікація пов'язана з тим, що особа, в межах суспільно небезпечного прояву, реалізує декілька суспільно небезпечних діянь, за які, в свою чергу, настає кримінальна відповідальність за різними кримінально-правовими нормами. Тобто, безпосередньо за факт торгівлі людьми – передбачається відповідальність за ст. 149 КК України, за підроблення документу – в залежності від статусу суб'єкту, або за ст. 358 КК України, або за ст. 366 КК України.

В певній мірі складніше полягають справи з кваліфікацією підроблення документа, коли він використовується як засіб обману потерпілої особи від торгівлі людьми. В даному випадку, винна особа для прикриття свого обману, або для введення в оману потерпілої особи, здійснює підроблення відповідних документів. Виникає запитання, чи є потреба кваліфікувати таке діяння за сукупністю злочинів чи такої потреби не має і кваліфікація повинна відбутись тільки за ст. 149 КК України. Кваліфікація дій, які пов'язані з торгівлею людьми безумовно реалізуються на підставі ст. 149 КК України. Що стосується самого діяння у виді підроблення, то в цій ситуації, на нашу думку, потрібно чітко розуміти що ми маємо на увазі під підробленням.

Свого часу нами наголошувалось те, що у науковому просторі підроблення документів як загальне явище розуміють як повне виготовлення сфальсифікованого документа, так і часткову фальсифікацію змісту справжнього документа. В останньому випадку (так звана переробка) перекручення істини відбувається шляхом внесення у документ неправдивих відомостей (виправлення, внесення фіктивних записів, знищення частини тексту, витравлення, підчистка, змивання, підроблення підпису, переклеювання фотографії, нанесення на документ відбитка підробленої печатки тощо). Підроблення документа становлять, наприклад, дії особи, яка, скориставшись бланком підприємства

або організації, на якому є підпис уповноваженої особи, заповнює його відповідним текстом. Поняттям підроблення документа охоплюється і внесення неправдивих відомостей у вже підроблений документ (наприклад, особа, придбавши підроблене посвідчення водія, вклеює у нього свою фотографію) [3, с. 79].

Іншими словами, вищезазначені суспільно небезпечні дії, а саме – підроблення документів, ні яким чином не охоплюється диспозицією ст. 149 КК України. внаслідок чого, враховуючи принципи кваліфікації діяння, ми зобов'язані здійснити таку кваліфікацію, яка в повному обсязі охопить вчинене. Тобто, в ситуації обману потерпілої з використанням підроблених документів сам факт підроблення необхідно додатково кваліфікувати за ст. 358 або ст. 366 КК України.

Підсумовуючи викладене вище необхідно наголосити на тому, що кваліфікація суспільно небезпечного діяння у виді торгівлі людьми за допомогою підроблених документів повинно реалізовуватись шляхом сукупності злочинів, передбачених ст. 149 КК України та ст. 358 КК України або ст. 366 КК України.

Список бібліографічних посилань

1. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 15.04.2020).
2. Суд обрав запобіжні заходи двом підозрюваним у торгівлі немовлям // Судова влада України : офіц. сайт. 27.04.2020. URL: https://court.gov.ua/archive/930796/ (дата звернення: 28.04.2020).
3. Фіалка М. І. Підроблення документів як спосіб ухилення від військової служби (кримінально-правовий аналіз). *Вісник Кримінологічної асоціації України*. 2018. № 2 (19). С. 77–86.

Одержано 01.05.2020

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

УДК 004.056.5:343.34

Єлизавета Георгіївна БЄЛЯЄВА,
курсантка 4 курсу факультету № 4
Харківського національного університету внутрішніх справ

Петро Сергійович КЛІМУШИН,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ТЕХНОЛОГІЯ BLOCKCHAIN ЯК ЗАСІБ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ

На сьогодні люди все більше і більше пов'язані з мережею Інтернет, вони не тільки шукають інформацію або спілкуються через соціальні мережі, але й вступають у правовідносини: купують різноманітні товари, користуються послугами інтернет-банкінгу, влаштовуються на роботу, і все це зазвичай супроводжується наданням персональних даних. Ризики порушень прав громадян або ускладнення їх реалізації стали можливими в сучасному світі через цифровізацію персональних даних.

До числа таких ризиків ставитися витік персональних даних більш ніж 87 мільйонів користувачів Facebook, які були використані в передвиборних кампаніях Теда Круза, Дональда Трампа, а також перед референдумом про вихід Великобританії з Європейського Союзу. Це стало переломним моментом - про необхідність захисту персональних даних заговорили буквально все і технологія блокчейн виявилася в центрі цих обговорень. Нерідко персональні дані стають об'єктом злочинів.

Метою досліджень є здійснення аналізу зарубіжного та вітчизняного досвіду використання блокчейн технологій в захисту персональних даних та визначення пріоритетних та перспективних напрямів їх подальшого застосування в Україні.

Наявність великої кількості досліджень із питань численних переваг блокчейн технологій, таких як децентралізація, анонімність, доступність, прозорість та аудитоспроможність, існування широкого спектру програмних блоків – від управління криптовалютами, фінансових послуг, управління ризиками, Інтернету речей до створення технологій

кібербезпеки, не виключає необхідності подальшого розроблення цієї теми з захисту персональних даних громадян України [1].

Зберігання даних на єдиному сервері не може бути достатньо безпечним, а отже сервер є основною вразливістю цієї системи. Крім того, важливу роль відіграє людський фактор, оскільки у більшості випадків інформація зберігається у відкритому та незашифрованому виді, недобросовісні працівники організації можуть незаконно розповсюджувати конфіденційну інформацію за певну винагороду.

Технологія блокчейн дозволить користувачам самостійно зберігати особисті дані і повністю контролювати їх передачу кому-небудь, завдяки чому необхідність сліпо довіряти корпораціям в збереженні даних просто відпаде. Персональні дані користувачів будуть зберігатися виключно на їх девайсах, а не на віддалених серверах третьої сторони. При цьому особиста інформація буде зберігатися під захистом, забезпеченої методами криптографічного шифрування. Користувачі зможуть самі вибирати кому передавати особисту інформацію, а також самостійно визначати рівень доступу до цієї інформації. Використання блокчейна дозволяє наділити користувачів повним контролем і уникнути формування централізованих сховищ персональних даних, які дуже схильні до хакерських атак [2].

Згідно дослідження проекту TAPAS в Україні діє більше ніж 135 державних реєстрів з персональними даними громадян. Серед ключових проблем дослідники виділяють дублювання даних, низький рівень взаємодії та обміну інформацією реєстрів між собою, а також відсутність законодавства, що регулює порядок ведення реєстрів.

Такий підхід призводить до збільшення фінансових видатків на утримання подібних реєстрів, а також до зобов'язання громадянина звертатись з подібною інформацією кілька разів в різні органи державної влади для отримання адміністративних послуг, які пов'язані між собою. Тобто в Україні взаємозв'язок реєстрів лишається на досить низькому рівні. Проте проблема дублювання одних і тих самих персональних даних призводить і до інших ускладнень, а саме до порушення принципу точності та достовірності персональних даних.

Важливим кроком для захисту персональних даних буде уніфікація нормативної бази в сфері державних реєстрів. Необхідно чітко визначити суб'єктів цих правовідносин та вимог до самих реєстрів. І подібна

ініціатива вже існує. Так, 10 вересня 2019 року було зареєстровано проект закону про публічні електронні реєстри за № 2110 [3].

На базі цього закону необхідно повністю переосмислити інфраструктуру функціонування державних реєстрів в Україні, та від розпорошеної, ієрархічної структури перейти до єдиного реєстру, який буде функціонувати в розподіленому вигляді.

Створення нового розподіленого державного реєстру повинно базуватися на міжнародному досвіді, він повинен містити інформацію з усіх державних реєстрів в Україні, при цьому інформація, яка буде вноситись в цей реєстр із попередніх реєстрів повинна перевірятися на достовірність з вирішенням конфлікту між персональними даними громадян.

Будь-який орган державної влади відповідно до своїх повноважень буде мати доступ відповідного рівня до тих даних, які йому необхідні для реалізації поставлених завдань. Таке розподілення рівнів доступу дозволить уникнути дублювання інформації, а також захистити персональні дані громадян від несанкціонованого втручання.

Таким чином, такий розподілений реєстр персональних даних буде не покращенням вже діючих реєстрів, а абсолютно новим інструментом і держава зможе уникнути необхідності переробки та покращення існуючих реєстрів, налагодження їх взаємодії та обміну інформацією.

Список бібліографічних посилань

1. Яковлєв Р. В. Принципи мінімізації та точності персональних даних під час використання технології розподіленого реєстру (адміністративно-правовий аспект). *ScienceRise: Juridical Science*. 2019. № 4 (10). С. 16–24.
2. Адамов О. С., Хаханов В. І., Чумаченко С. В., Абдуллаєв В. Г. Блокчейн інфраструктура для захисту кіберсистем. *Радиоэлектроника и информатика*. 2018. № 4. С. 64–85.
3. Проект Закону про публічні електронні реєстри : від 10.09.2019 № 2110 / ініціатори: М. В. Крячко, Р. В. Соха, О. П. Федієнко, Є. В. Чернєв // База даних «Законодавство України» / Верховна Рада України. URL: https://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=66772 (дата звернення: 25.04.2020).

Одержано 27.04.2020

УДК 343.1:65.012.8+0043

Андрій Володимирович БІЛОБРОВ,
курсант 3 курсу факультету № 4
Харківського національного університету внутрішніх справ

Петро Сергійович КЛІМУШИН,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ВИКОРИСТАННЯ ТЕХНОЛОГІЙ OSINT ДЛЯ ОТРИМАННЯ ІНФОРМАЦІЇ

Отримання інформації у відкритих джерелах в інтересах розкриття і розслідування злочинів – одне з актуальних напрямків вдосконалення діяльності правоохоронних органів [1].

Діяльність по отриманню розвідувальної інформації з відкритих джерел кіберпростору отримала назву OSINT – Open Source INTelligence (відкриті джерела розвідки). У сферу інтересів OSINT входить добування та аналіз офіційних документів, проектів статутів, відстеження нових наукових розробок, баз даних, комерційних і державних сайтів, мережевих щоденників і багато іншого.

Одним із різновидів інформаційних технологій збору та аналізу інформації з відкритих джерел є ще один напрямок розвідки – HUMINT (human intelligence), у дослівному перекладі - «розвідка по людям». До таких технологій відносяться: моніторинг соціальних мереж, опитування, соціальний інженірінг, залегендовані бесіди (під виглядом журналіста, клієнта, роботодавця тощо). У сучасному світі технології OSINT та HUMINT значно пов'язані між собою і використовують значну кількість технологічно подібних методів отримання необхідної інформації про об'єкт розвідки.

Важливим напрямком діяльності є зміцнення здатності розпізнавати внутрішні загрози у напрямку посилення вміння вживати ефективні дії для передбачення цих загроз та нейтралізації негативних явищ та процесів. Створення на національному рівні системи інтегрованої оцінки ситуації дасть можливість урухомити механізми моніторингу рівня реалізації стратегії та коригування її положень, з огляду на зміни у

безпековому середовищі. Ефективне реагування на динамічні політичні, економічні, соціальні та технологічні зміни є критерієм результативності системи внутрішньої безпеки з точки зору виявлення, ідентифікації та попередження загроз та джерел ризику. Це має теж прямий вплив на боротьбу зі злочинністю, зважаючи на врахування даних кримінальної розвідки при оцінці ситуації.

У правоохоронних органах західних держав існують спеціальні підрозділи, що здійснюють розвідку на основі відкритих джерел інформації. Наприклад, таку діяльність провадять: Scotland Yard OSINT, Royal Canadian Mounted Police OSINT, OSINT unit of New York Police Department, OSINT unit of the Los Angeles County Sheriff's Department, британська BBC Monitoring, ізраїльський Хатсав, австралійське Управління національних оцінок [2].

Відповідно до ст. 34 Конституції України, кожен має право вільно збирати, зберігати, використовувати й поширювати інформацію усно, письмово або в інший спосіб – на власний розсуд. У межах кримінального провадження здійснення аналізу відкритих джерел інформації регламентовано главою 21 Кримінального процесуального кодексу України, зокрема в контексті розкриття порядку проведення такої негласної слідчої (розшукової) дії, як зняття інформації з електронних інформаційних систем.

Спеціальне програмне устаткування, таке як i2 Analyst`s Notebook, Maltego CE, надає можливість аналізувати соціальні мережі та визначати особливості взаємодії особи, яку підозрюють у вчиненні корупційного злочину, з іншими особами.

На початку цього року вийшов у світ черговий лінукс-дистрибутив для проведення кібер-розслідувань і OSINT під ім'ям CSI Linux Investigator. Даний дистрибутив містить програмне забезпечення, необхідне для вирішення наступних завдань: OSINT, Digital Forensics, Incident Response, Malware Analysis.

Ще одним відомим дистрибутивом є Maltegoю. Цей інтелектуальний інструмент для відстеження слідів кожного об'єкта в Інтернеті з відкритим вихідним кодом в основному використовується для виконання значних досліджень різних цілей за допомогою декількох вбудованих перетворень.

Також, популярності на даний момент набуває GitHub - нова Open Source бібліотека для OSINT, сервіс Hunter.io як інструмент пошуку адрес корпоративної пошти, за допомогою якого можна отримати кон-

тактну інформацію відповідно до домену. Такі відомості необхідні, щоб далі перевірити знайдені email на компрометацію. Hunter.io здатний обробити і витягти необхідні дані з 67 мільйонів відкритих джерел за допомогою 5 ключових методів: Domain Search - пошук email по домену або назвою організації; Email Finder - пошук окремого співробітника на ім'я і компанії; Email Verifier - підтвердження працездатності та актуальності пошти; Email Count - дозволяє дізнатися кількість email для одного домену або для однієї компанії; Account Information - управління особистим обліковим записом.

Застосування OSINT дозволяє отримати відповідь на багато питань, а також зосередити зусилля розвідувальних органів на виконання більш складних і «вузьких» завдань, не розпорошуючи сили інших напрямків розвідки на добування того, що можна отримати з відкритих джерел [3].

Таким чином, технологія OSINT є однією з важливих технологій різнорівневої різноформатної інформації, а також формування на її базі принципово нових знань. Поширення і використання перевіреної інформації з відкритих джерел дозволяє здійснювати обмін такою інформацією, оскільки при її отриманні не використовуються приховані методи і секретні джерела.

Ключовими факторами для успішного аналізу є: чітке розуміння цілей аналізу; неупередженість; збір інформації з максимально можливої кількості відкритих джерел; застосування коефіцієнтів ваги до кожної інформації; грамотний аналіз отриманої інформації.

Список бібліографічних посилань

1. Ісмайлов К. Ю. Особливості кримінальної розвідки з відкритих джерел як інструмент збирання оперативної інформації. *Південноукраїнський правничий часопис*. 2016. № 2. С. 110–113.
2. Жарков Я. М., Васильєв А. О. Наукові підходи щодо визначення суті розвідки з відкритих джерел. *Вісник Київського національного університету імені Тараса Шевченка*. 2013. Вип. 30. С. 38–41.
3. Молоков В. В. Эффективные способы получения открытой информации в сети интернет. *NovaUm.Ru*. 2017. № 9. С. 6–14.

Одержано 01.05.2020

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

ОСОБЛИВОСТІ КІБЕРАТАК НА МІСЬКУ ІТ-ІНФРАСТРУКТУРУ

Автоматизовані системи управління досить широко використовуються для регулювання різних процесів в сучасному місті. Все більше он лайн сервісів впроваджуються в міську ІТ-інфраструктуру. Це стало причиною того, що останнім часом кіберзлочинні угруповання та хакери-одинаки все частіше обирають їх ціллю своїх атак.

В 2019 році близько 20 муніципалітетів в США зіткнулося з проблемою шифрувальників. Найбільш гучна атака сталася 7 травня у місті Балтімор, де спрацював кріптолокер «Робін Гуд» (RobbinHood). У той же день муніципалітет Балтімора повідомив ФБР і відключив частину своїх систем, вважаючи, що таким чином зможе зупинити поширення шкідливого програмного забезпечення, яке наразі вже встигло заразити голосову та електронну пошту, систему оплати штрафів, систему оплати рахунків за воду, систему відеоспостереження, а також систему оплати податків за нерухомість, через що більше 1500 угод з нерухомістю було зупинено. Зловмисники вимагали викупу в розмірі трьох біткоїнів за кожну з атакованих систем або 13 біткоїнів за повернення доступу до всіх систем відразу.

Шифрувальник почав своє поширення через фішингову атаку, спрямовану на одного зі службовців муніципалітету. Чи була віна цілеспрямованою або випадковою - невідомо. При цьому, частина ІТ-інфраструктури була розміщена в хмаровому сервісі Amazon, але муніципалітет і її майже

втратив, тому що на початку травня завершився контракт на підтримку, який не змогли продовжити через непрацюючі систем оплати рахунків.

Причиною усіх цих неприємностей, як вважають спеціалісти з ІБ, стали декілька чинників.

По-перше, за останні 7 років 4 CIO (Chief Information Officer) Балтімора були звільнені або пішли самостійно, двоє досі знаходяться під слідством (за неправомірні витрати і сексуальні домагання). Таким чином, нормально розвивати ІТ та ІБ в Балтіморі не вдавалося - майже кожні 1,5 року начальство, яке визначає шлях розвитку ІТ-інфраструктури міста, змінювалося. Ще у 2017-му році компанія Gartner розробила для Балтімора 5-річний план розвитку, але реалізувати його так і не вдалося.

По-друге, в бюджеті міста лише 2,5% виділялося на ІТ (включаючи витрати і на ІБ), що вдвічі нижче середніх цифр американських міських бюджетів. Менеджер по ІБ на бюджетному комітеті просив грошей на заходи по ІБ, але йому було відмовлено.

По-третє, пропозиції щодо підвищенні обізнаності муніципальних службовців теж не отримали підтримки через брак коштів.

На засіданні міського бюджетного комітету 29 травня чиновники Балтімора підрахували, що напад може коштувати місту 18,2 мільйона доларів. Близько 4,7 мільйона доларів на той момент було вже витрачено.

До речі, в 2018-му році в Балтіморі від шифрувальника вже постраждала одна з систем (служба 911). Сталося це через відключені в процесі підтримки внутрішніх систем правил на MCE (Machine Check Exception). Однак ніяких висновків зроблено не було.

Випадок в Балтиморі не є поодиноким. RobbinHood до Балтімора атакував ще одне американське місто - Гринвиль в Північній Каліфорнії. Плану реагування на інциденти в муніципалітеті не було, що досить дивно. План ручного відновлення був розроблений через два тижні після початку епідемії. Частково виправдати це можна тим, що мер міста вступив на посаду за кілька днів до епідемії RobbinHood (колишній мер пішов у відставку через звинувачення в зростаючій корупції) і багато посад в адміністрації були порожні, що і призвело до такого хаотичного стану.

Лейк-Сіті, штат Флорида, декілька днів відновлювався після атаки іншого шифрувальника TripleThreat 10 червня, який вразив його електронну пошту та онлайн-платіжні системи.

Хмарна компанія з кібербезпеки AppRiver повідомила про TripleThreat минулого січня, але на той момент вважалося, що це фішинг-схема, призначена для збору облікових даних, і про шифрувальний компонент було не відомо.

12 червня місто оновило свій статус, в якому сказано, що, хоча більшість систем все ще не працює, досягнуто прогресу у відновленні мережі та доступу до заблокованих даних. Системи, що обслуговують міську поліцію, пожежну та інші екстрені служби, не постраждали. Відправку електронні листів відновили протягом наступного дня. Намагання з відновлення даних теж були успішними, хоча потрібен певний час, щоб повернути їх у первісний формат.

Таким чином, ми бачимо, що атаки на міську ІТ-інфраструктуру будуть поширюватися і треба бути заздалегідь готовими до них. Забезпечення ІБ міста справа не з дешевих, але витрати на відновлення втрачених даних можуть набагато перевищити витрати на інформаційну безпеку.

Одержано 29.04.2020

УДК 004.056.53

Дмитро Іванович ЄВСТРАТ,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ЗАСТОСУВАННЯ ПРИНЦИПІВ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В ПРОЦЕСІ РОЗРОБКИ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

Сьогодні далеко не кожен проект може дозволити собі окремого фахівця з безпеки, тому питання реалізації принципів забезпечення кібербезпеки стає предметом особливої уваги не тільки для експертів, а й для звичайних розробників програмного забезпечення. Безпека - це найважливіша характеристика програмного забезпечення, особливо у випадках з системами з програмним управлінням, які можуть вплинути на життя і здоров'я людей, а також системами, які пов'язані з обробкою персональних даних. Безпека програмного забезпечення концептуально відрізняється від функціональних вимог і не настільки зрозуміла інтуїтивно. При цьому, бажана поведінка програми найчастіше сприймається як основна мета, в той час як головна мета безпеки полягає в запобіганні діям, які програма не повинна робити і уникати небажаної її поведінки.

Серед властивостей безпеки програмного забезпечення, існує три основних, відсутності яких необхідно запобігти: конфіденційність, цілісність і доступність. Порушення властивостей безпеки призводить до вразливості програмного забезпечення – пов'язаному з безпекою дефекту, який можна використовувати для досягнення небажаної поведінки.

В процесі розробки безпечного програмного забезпечення необхідно дотримуватися ряду загальних принципів, які можна розділити на наступні групи:

- запобігання (вичерпне усунення дефектів);
- пом'якшення (зменшення шкоди від експлуатації невідомого дефекту);
- виявлення (моніторинг атаки);

— відновлення (нейтралізація шкоди).

На основі цих принципів можна сформулювати рекомендації, яких важливо дотримуватися при розробці, впровадженні і супроводі програмного забезпечення:

— перевага простій архітектурі;
— застосування безпечного вибору за замовчуванням;
— врахування слабкого рівня користувача;
— простий користувальницький інтерфейс;
— обмеження користувача у виборі щодо безпеки;
— використання мінімальної довіреної обчислювальної бази;
— використання відкритих, стандартних для галузі протоколів і алгоритмів;
— максимальне обмеження повноважень для компонентів і користувачів;
— валідація вхідних даних;
— посилення конфіденційності (обмеження доступу до персональних даних);
— розподіл компонентів і операцій;
— об'єднання всіх механізмів безпеки;
— використання стандартних і відкритих рішень;
— збір логів і телеметрії;
— створення резервних копій і знімків стану.

Процес розробки безпечного програмного забезпечення передбачає введення необхідних дій і практик для кожного етапу розробки.

Так, на етапі розробки вимог необхідно визначити:

— вимоги до безпеки;
— необхідні властивості безпеки для компонентів системи;
— механізми безпеки для підтримки цих властивостей;
— моделі загроз.

На етапі розробки:

— визначити архітектуру, з урахуванням загроз безпеки;
— проаналізувати і дати оцінку архітектурним ризикам;

— застосовувати наведені вище принципи безпеки (запобігання, пом'якшення, виявлення, відновлення).

На етапі реалізації:

— дотримуватися кращих практик написання коду;

— проводити обов'язкові рев'ю коду;

— застосовувати інструменти автоматизації для забезпечення високої якості коду.

На етапі тестування проводити:

— тестування на основі ризиків;

— випробування на проникнення;

— навмисне введення в систему випадкових і некоректних даних.

Враховуючи те, що безпека є вторинною характеристикою і часто суперечить функціональності, тому при розробці програмного забезпечення, до якого пред'являються вимоги безпеки, важливим завданням є розробка не просто безпечного, а збалансованого продукту.

Одержано 07.05.2020

УДК 621.3.01+621.38

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

ДОСЛІДЖЕННЯ СЕРЕДОВИЩ МОДЕЛЮВАННЯ ЗАХИЩЕНИХ МІКРОПРОЦЕСОРНИХ СИСТЕМ

Становлення Інтернет речей є однією з основних причин трансформації ринку мікропроцесорних систем в напрямку розробки захищених, інтелектуальних систем, об'єднаних в єдину глобальну обчислювальну мережу. Для забезпечення зростаючих потреб ринку актуальним завданням є визначення найбільш ефективних середовищ проектування мікропроцесорних систем на мікроконтролерах з додатковими модулями криптографічного захисту інформації.

Сфера застосування захищених мікропроцесорних систем складається з забезпечення функцій інформаційної безпеки: автентіфікації суб'єктів і об'єктів інформа-ційної взаємодії, шифрування інформації, контроля цілісності, управління доступом, управління ключами [1].

Аналіз науково-дослідних робіт показує, що проблема використання програмних середовищ моделювання мікропроцесорних систем досконально ще ні досліджена і має мінливий характер в залежності від етапів їх розвитку та кон'юнктури ринку мікроконтролерів.

Обираючи інструментальні засоби моделювання, доцільно брати до уваги: підтримку можливо більшої кількості мікроконтролерів; різноманітність вбудованих інтерфейсів та додаткових компонентів, що розширюють функціональні можливості проектування.

Метою дослідження є визначення найбільш ефективних та доступних програм комп'ютерного моделювання мікропроцесорних систем та надання практичних рекомендацій щодо їх застосування.

Найбільш потужною системою автоматизованого проектування вважається програмний пакет Proteus VSM, який дозволяє віртуально змоделювати роботу різних мікропроцесорних пристроїв з підтримкою декількох сімейств мікроконтролерів від різних виробників. Програма Proteus VSM є симулятором наскрізного проектування, що має на увазі створення пристрою, починаючи з графічного зображення і закінчуючи виготовленням друкованої плати пристрою.

До переваг використання Proteus відносяться: виконання всіх етапів розробки електронного пристрою на основі мікроконтролера в єдиному середовищі; можливість написання, налагодження і тестування мікропрограмного забезпечення, ще до фізичного виготовлення дослідного зразка системи; генерування діагностичних повідомлень, що дозволяє виявити складні в пошуку помилки програмування; прискорення процесу розробки електронного пристрою; підтримка спільної роботи з апаратними пристроями, що підключені через порт комп'ютера [2].

Дослідження використання Multisim в навчальному процесі показало, що система дає можливість: переглядати і змінювати стан вмісту регістрів, пам'яті програм і даних, осередків стека і біта конфігурації, що сприяє розумінню і кращому засвоєнню принципів роботи і архітектури мікроконтролерів; візуалізувати результат виконання окремої команди або програми в цілому, підвищуючи наочність викладеного матеріалу; демонструвати практику спільного застосування мов С і Асемблер в одному проекті з метою оптимізації програми; вивчати основи роботи і особливості функціонування периферійних пристроїв. Проте обмежений набір мікроконтролерів в програмі NI Multisim накладає суттєві обмеження на можливість її використання при розробці реальних проектів.

В останні роки з'явилася нова ефективна програма комп'ютерного моделювання TINA, яка містить інтегровану частину для проектування друкованих плат, має значно простіший інтерфейс у порівнянні з Proteus VSM, який легко освоюється студентами. Крім того, вся інформація про створений проект укладена в одному файлі, який можна переслати і відкрити на іншому комп'ютері для продовження моделювання або перевірки роботи слухачів. Наряду з цім, програма має русифікований

інтерфейс, що значно підвищує ефективність засвоєння навчального матеріалу.

TINA є потужним інструментом для моделювання електронних схем та мікроконтролерів, дозволяє проводити дослідження схем при зміні параметрів, оптимізації, виконувати частотний і спектральний аналіз, досліджувати перехідні характеристики тощо. У порівнянні з Multisim бібліотека TINA містить значно більше моделей мікроконтролерів, більше 1000, які можна програмувати на Асемблері і на мові С, моделювати, налагоджувати в змішаних схемах. Вбудований програматор дозволяє модифікувати програми та спостерігати результати [3].

Таким чином, дослідження показало, що найбільш потужною системою проектування мікропроцесорних систем на мікроконтролерах з апаратною реалізацією захисту інформації вважається програмний пакет Proteus, який дозволяє змоделювати роботу захищених мікропроцесорних пристроїв з підтримкою декількох сімейств мікроконтролерів від різних виробників. Дослідження Multisim показало високу ефективність її використання в навчальному процесі. Програма TINA має значно простіший інтерфейс у порівнянні з Proteus VSM з можливістю укладення всієї інформації про створений проект в одному файлі. У порівнянні з Multisim бібліотека TINA містить значно більше моделей мікроконтролерів з додатковими модулями криптографічного захисту інформації.

Можливість використання безкоштовної версії TINA-TI та наявність онлайн-версії TINACloud з використанням хмарних технологій робить цю програму дуже корисною для освіти. Вебсервіс пропонує безліч освітніх ресурсів і надає можливість виконання дослідження з проектування захищених мікропроцесорних систем.

Список бібліографічних посилань

1. Совин Я. Р., Наконечний Ю. М., Опірський І. Р., Стахів М. Ю. Аналіз апаратної підтримки криптографії у пристроях інтернету речей. *Ukrainian Scientific Journal of Information Security*. 2018. Vol. 24, Iss. 1. Pp. 36–48.
2. Березняков С. В., Греков А. В. Моделирование микроконтроллера 80С51 в системе схемотехнического моделирования Proteus VSM. *Электротехника, информационные технологии, системы управления*. 2016. № 17. С. 104–120.
3. Алехин В. А. Развитие учебного комплекса по электротехнике, электронике и микроконтроллерам с моделированием в программной среде TINA. *Открытое образование*. 2017. № 6. С. 57–69.

Одержано 30.04.2020

УДК 004.056.2,004.5,336.744,339.72

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

Петро Сергійович КЛІМУШИН,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ПРИХОВАНИЙ МАЙНІНГ КРИПТОВАЛЮТИ Й ОБМЕЖЕННЯ БРАУЗЕРНОГО КРИПТОДЖЕКІНГУ

Зазвичай, ціллю кіберзлочинців є ресурси жертви, під якими мається на увазі не тільки конфіденційна інформація, а й потужності машин, що є носієм цієї інформації. Особливо гострою проблема крадіжки потужності робочих машин стала з появою криптовалют. Сьогодні жертвами криптоджекінгу стали мільйони звичайних користувачів і кожна п'ята бізнес-компанія в світі.

Проте не лише класичний криптоджекінг несе велику загрозу. Зараз популярності набуває ще один вид прихованого майнінгу – криптоджекінг на веб сторінках. Прихованих майнерів уже виявляли на YouTube, в тисячах інтернет-магазинах і в додатках для Android. Скрипти, що видобувають криптовалюту, ховаються під рекламою та за допомогою диспетчера тегів Google інтегровані в код безлічі сайтів, а популярні CMS і зовсім захлеснула хвиля атак, метою яких є саме встановлення майнінгових скриптів [1, с. 2].

Криптоджекінг набрав катастрофічних наслідків у наш час. На сьогодні кіберзлочинці дуже швидко знайшли можливість добувати криптовалюти, не витрачаючи при цьому майже ніяких ресурсів. Тому актуальність дослідження полягає в тому, щоб знизити випадки прихованого майнінгу.

Метою дослідження є висвітлення методів для виявлення прихованого браузерного майнингу.

Криптоджекінг – це несанкціоноване використання обчислювальних потужностей (комп'ютерів) інших людей для видобутку криптовалюти.

Браузерний криптоджекінг у свій час став проблемою, яку неможливо було ігнорувати. Тож усі браузери при наступному обновленні вжили заходи для обмеження майнингу на вебсторінках. Найбільш жорстку політику щодо прихованого браузерного майнінгу ввела Opera. Цей браузер повністю блокує будь-яку активність, що стосується криптоджекінгу, тому справедливо вважається найбільш захищеним від цього виду атак.

Природньо, що за обмеження браузерного криптоджекінгу відповідають браузерні розширення. Існує три підходи для виявлення прихованого браузерного майнингу.

Перший метод полягає у моніторингу так званого чорного списку. Якщо адреса сайту збігається з адресою з чорного списку, вважається, що сайт користується прихованим браузерним майнінгом. За підрахунками експертів цей метод дозволяє виявити криптоджекінг у 58% випадків.

Другий підхід передбачає пошук у коді підозрілих бібліотек. Якщо входження відбулось, вважається, що сайт заражений криптоджекінгом. За підрахунками, цей метод дозволяє виявити близько 23% прихованого майнінгу. Проте на відміну від першого методу він дозволяє виявляти нові сторінки, заражені криптоджекінгом. Доведено, що використання обох цих методів у зв'язці дає результат у 67%. Реалізація цих методів полягає, головним чином, у javascript-функції indexOf [2, с. 5].

Третій спосіб полягає у тому, що розширення слідкує за наявністю підозрілої поведінки машини. Підозрілим, наприклад, вважається випадок, коли різко збільшується навантаження на процесор. Цей метод є ефективнішим аніж перші два, проте займає набагато більше часу. Тому використовується, зазвичай, тільки у великих антивірусних продуктах або виключно для пошуку нових сторінок, заражених криптоджекінгом.

Взагалі розширення Google Chrome, що використовуються для обмеження криптоджекінгу поділяються на два види. Перший – це великі антивіруси, в яких функція боротьби із прихованим майнінгом є лише однією з опцій. До таких відносяться такі додатки, як Avast та McAfee. Інші – навпаки вузькоспеціалізовані, і обмеження криптоджекінгу для них є основною функцією. До таких відносяться noCoin, MINEBlock, Coin-Hive, AntiMiner. На жаль, деякі з них не обновлювались на протязі 2-3 років.

Таким чином, у результаті досліджень проаналізовано ефективність методів виявлення прихованого браузерного криптоджекінгу та визначено застосування кожного з них. Метод чорного списку та метод, який виконує пошук шкідливих бібліотек у коді програми застосовується беспосередньо для виявлення прихованого браузерного криптоджекінгу. Тертій метод, що відслідковує підозрілу поведінку, зазвичай, використовується для пошуку нових вебсторінок, що заражені бібліотекою для прихованого майнінгу криптовалюти.

Проаналізувавши вже існуючі рішення, було виявлено деякі проблеми. По-перше, усі програмні засоби одразу блокують сайт із браузерним криптоджекінгом, не враховуючи те, що деякі вебсторінки дають можливість на вибір: або погодитися на узгоджений криптоджекінг, або ж продивлюватися рекламні пропозиції. По-друге, на сьогоднішній день не було знайдено сервісів, які б давали можливість виявляти прихований криптоджекінг у розширеннях браузера.

Звідси випливає, що актуальним завдання подальших досліджень є розробка розширення браузера, яке можливо використовувати разом з іншими рішеннями для обмеження браузерного криптоджекінгу [3].

Список бібліографічних посилань

1. Eskandari S., Leoutsarakos A., Mursch T., Clark J. A First Look at Browser-Based Cryptojacking. University College London, 2018. 9 p.
2. Hong G., Zhang L., Yan M. How You Get Shotinthe Back: A Systematical Study about Cryptojacking in the Real World. URL.: http://www.cs.ucr.edu/~zhiyunq/pub/ccs18_cryptojacking.pdf (дата звернення: 26.04.2020).
3. Ілляшенко О. М. Виявлення прихованого криптоджекінгу на веб-сторінках : дипломна робота. Київ : Нац. тех. ун-т України «Київський політехнічний інститут імені Ігоря Сікорського», 2019. 57 с.

Одержано 27.04.2020

УДК 340.132+006.83+004.05

Вадим Анатолійович КУДІНОВ,
кандидат фізико-математичних наук, доцент,
професор кафедри інформаційних технологій та кібербезпеки
Національної академії внутрішніх справ (м. Київ)

ПРОБЛЕМА НОРМАТИВНО-ПРАВОВОГО ВИЗНАЧЕННЯ ПОНЯТЬ НАДІЙНОСТІ, ФУНКЦІОНАЛЬНОЇ БЕЗПЕКИ ТА ЖИВУЧОСТІ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ

Станом на сьогодні в різних законодавчих і підзаконних актах міністерств і відомств України можна зустріти посилання на надійність, функціональну безпеку та живучість інформаційно-комунікаційних систем.

Так, зокрема, в статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» у визначенні терміну «кібератака» використовується словосполучення щодо «порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем» (пункт 4 частини 1), у визначенні терміну «кіберзахист» використовується словосполучення щодо «відновлення сталості і надійності функціонування комунікаційних, технологічних систем» (пункт 7 частини 1) [1]. Серед напрямів досліджень Паспорту спеціальності 05.13.06 (Інформаційні технології) зазначено такий: «Розроблення й дослідження моделей і методів оцінювання якості і підвищення надійності, функціональної безпеки і живучості інформаційних та інформаційно-управляючих систем» [2].

Таким чином, виникає актуальне питання щодо з'ясування нормативно-правового визначення зазначених понять. Для його дослідження будемо використовувати розділ «Термінологія законодавства» вебпорталу Верховної Ради України, який станом на 29 квітня 2020 року містить 69 543 термінів [3], та інші джерела.

За запитом «надійність» пошукова система надає 10 відповідей: безпосередньо сам термін «надійність» та 9 словосполучень з цим терміном

(наприклад, надійність технічних засобів телекомунікацій, надійність техніки зв'язку, надійність авіаційного електрозв'язку, надійність радіолокатора тощо). Але жодної відповіді немає щодо надійності інформаційно-комунікаційної системи. Сам термін «надійність» зустрічається в 11 нормативно-правових актах (наказах, постановах) міністерств та відомств. Їх аналіз дозволяє зробити висновок, шо вони містять майже однакове визначення цього терміну, а саме: «надійність – властивість об'єкта зберігати у часі в установлених межах значення всіх параметрів, які характеризують здатність виконувати потрібні функції в заданих режимах та умовах застосування, технічного обслуговування, зберігання та транспортування», що відповідає, як нами було встановлено, ДСТУ 2860-94 [4]. У п. 1.1 цього стандарту зазначено, що його терміни та визначення основних понять у галузі надійності поширюються на технічні об'єкти, до яких відносяться технічні системи, програмні засоби, людино-машинні системи, апаратура, пристрої та елементи тощо [4]. Таким чином, зазначене визначення необхідно використовувати також для інформаційно-комунікаційних систем.

За запитом «функціональна безпека» пошукова система надає 1 відповідь: «функціональна безпека – властивість системи (компонента) атомної станції, що полягає у здатності виконувати всі потрібні функції, важливі для безпеки, зберігати потрібні властивості та відповідати заданим характеристикам в усіх передбачених проектом режимах й умовах експлуатації». У праці [5] автори зазначають, що система стандартів ГОСТ Р МЭК 61508-1-2007 регламентує вимоги до функціональної безпеки для всього життєвого циклу систем, що складаються з електричних і/або електронних та і/або програмованих електронних компонентів, які використовують для виконання функцій безпеки.

За запитом «живучість» пошукова система надає 6 відповідей, п'ять з яких пов'язана з живучістю судна та одна з живучістю енергосистеми. Автори роботи [6] «під живучістю розуміють здатність інформаційної системи зберігати і відновлювати виконання основних функцій в заданому обсязі і протягом заданого часу в разі зміни структури системи і/або алгоритмів і умов її функціонування внаслідок несприятливих впливів» [6, с. 38].

Відповідно до ДСТУ 2860-94 «живучість – властивість об'єкта зберігати обмежену працездатність в умовах зовнішніх діянь, що призводять до відмов його складових частин» [4].

Висновок. У роботі розглянуто нормативно-правові визначення понять надійності, функціональної безпеки та живучості об'єктів, які можна також використовувати для інформаційно-комунікаційних систем. Є також пропозиція включити зазначену термінологію до проекту Закону України «Про безпеку інформації та інформаційно-комунікаційних систем» [7].

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 затвердження Паспортів спеціальностей : постанова президії Вищої атестаційної комісії України від 14.06.2007 № 47-08/6 // Дебет-Кредит : сайт. URL: https://docs.dtkt.ua/uk/download/pdf/1155.575.1 (дата звернення: 28.04.2020).
3. Термінологія законодавства // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/main/termin (дата звернення: 29.04.2020).
4. ДСТУ 2860-94. Надійність техніки. Терміни та визначення // ДНАОП. Законодавча база : сайт. URL: https://dnaop.com/html/2273/doc-ДСТУ_2860-94 (дата звернення: 29.04.2020).
5. Дудикевич В. Б., Микитин Г. В., Рудник О. Я. Функціональна безпека інформаційних технологій: засади, методологія, реалізація. *Сучасна спеціальна техніка*. 2013. № 1 (32). С. 115–125.
6. Додонов А. Г., Ландэ Д. В. Живучесть информационных систем. Киев, 2011. 256 с.
7. Про безпеку інформації та інформаційно-комунікаційних систем : Проект Закону України // Державна служба спеціального зв'язку та захисту інформації України : офіц. сайт. 10.03.2020. URL: http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=319256&cat_id=38837&ctime=1583911712891 (дата звернення: 28.04.2020).

Одержано 29.04.2020

УДК 343.985.5:629.735

Дмитро Валерійович КУРІЛЬОНОК,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

Олексій В'ячеславович ПЕРЕЦЬ,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

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

ЩОДО ПИТАННЯ ЗАПРОВАДЖЕННЯ В МВС УКРАЇНИ ЄДИНОЇ СИСТЕМИ МОНІТОРИНГУ ПОВІТРЯНОГО ПРОСТОРУ

Дистанційно пілотовані авіаційні системи (далі – ДПАС), які ще називають «безпілотними літальними апарати» (далі – БпЛА), або «безпілотниками», «дронами» чи «мультикоптерами», розпочали застосовувати у різних галузях виробництва ще на при кінці минулого століття. Але з удосконаленням електронних, навігаційних систем, джерел енергії ДПАС масово почали застосовуватись останні 10 років. Їх удосконалення все більше прогресує. Обладнані GSP та РТК антенами літальні апарати мають можливість із точністю до 2 см рухатись по заданій траєкторії польоту дотримуючись заданої висоти [1].

Використання безпілотних літальних апаратів, у останні роки стрімко поширюється майже на всі сфери діяльності людини. На сьогодні БпЛА широко застосовують військові, правоохоронці, державні та комерційні установи, а також цивільні громадяни. Дрони застосовують повсюдно: від військових операцій, патрулювання кордонів до рятувальних місій та вирішення побутових питань – фото- відеозйомок свят чи доставки товарів.

Залежно від принципів керування є наступні різновиди БпЛА:

— безпілотні некеровані;

— безпілотні автоматичні;

— безпілотні дистанційно-пілотовані літальні апарати (далі – ДПЛА) [2].

В останні роки значної популярності як у світі, так і в Україні набули мультикоптери, зокрема квадрокоптери.

За оцінками вітчизняних експертів, ринок БпЛА в Україні складає близько $ 1 млн на місяць, з яких значна частина припадає на агросектор [3].

Але злочинці також активно використовують БпЛА. За допомогою дронів зловмисники здійснюю стеження за приватним життям осіб, відстеження руху мобільних об'єктів і проникнення в важкодоступні місця. Тепловізор, встановлений на безпілотник, дозволяє працювати і відстежувати ситуацію навіть вночі.

Відомі випадки використання дронів для стеження за приватними будинками на предмет відсутності господарів і подальшої крадіжки з них. У деяких випадках, грабіжники використовували БпЛА для виявлення та вчасного попередження своїм спільників про небезпеку, що наближається.

БпЛА також використовують під час хакерських атак для взлому стільникових станцій і Wi-Fi мереж – для перехоплення інформації.

Оптика з високою роздільною здатністю, будучи встановленою на БпЛА, дозволяє отримувати фото документів і красти технології навіть через вікна. Так, квадрокоптер над банкоматом знімав банківські платіжні картки і як користувачі вводять свої PIN-коди.

В останні роки безпілотники активно використовують наркодилери для прихованої доставки наркотиків в будь-яку точку населеного пункту. Великі музичні фестивалі зіткнулися з фактами перенесення на територію заходів за допомогою дронів алкоголю і наркотиків.

Активно використовують безпілотники контрабандисти для незаконного переправлення через кордон тютюнових виробів, смартфонів та інших дорогих виробів. Також фіксується багато випадків переміщення у в'язниці телефонів, зброї, наркотиків та інших предметів.

БпЛА використовують для псування майна і організації підпалів – на об'єкти скидаються легкозаймисті рідини. До важких і смертельних наслідків призводить розпорошення з повітря отрут, небезпечних отруйних і радіоактивних речовин

Зафіксовані випадки використання дронів у яких були вбудовані зброя і вибухівка, які використовувалися для скидання бомб і мінування територій [4].

Після серії широко відомих інцидентів з мультикоптерами в 2018 і 2019 роках ринок рішень боротьби із ними швидко ріс в 2019 році. Майже подвоїлась кількість доступних технологій по боротьбі з мультикоптерами. Країни почали розробляти стратегії боротьби з небезпечними запусками БпЛА, а спектр доступних рішень продовжує зростати [5].

Через підвищення кількості фактів використання мультикоптерів під час проведення масових заходів, для несанкціонованого втручання у приватне життя громадян, незаконного переміщення товарів та заборонених до обігу речовин, диверсійної діяльності постала проблема запровадження та використання правоохоронцями систем моніторингу повітряного простору.

Системи моніторингу повітряного простору можна поділити на:

1) мобільні – мають меншу дистанцію роботи (3-5 км) щодо виявлення БпЛА;

2) стаціонарні – мають більшу дистанцію роботи (5-20-50 км в залежності від антени) щодо виявлення БпЛА.

Мобільні системи моніторингу повітряного простору доцільно придбати для ГУНП в областях та м. Київ для використання в ході забезпечення публічної безпеки та порядку під час проведення масових заходів.

Стаціонарні системи моніторингу повітряного простору доцільно використовувати на об'єктах, що потребують постійного моніторингу повітряного простору над ними.

Із метою раціонального використання коштів доцільно:

1. Створити Єдину систему моніторингу повітряного простору МВС України.

2. Визначити місце розміщення центрального серверу Єдиної системи моніторингу повітряного простору МВС України.

3. Визначити перелік населених пунктів України та територій над якими необхідно здійснювати моніторинг повітряного простору.

4. У визначених населених пунктах України на територіях структурних підрозділів установ та організацій, що входять до структури МВС України та інших центральних органів виконавчої влади, діяльність

яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України, встановити необхідну кількість стаціонарних антен системи моніторингу повітряного простору (розраховується в залежності від площі та розмірів населеного пункту).

5. Через Єдину цифрову відомчу телекомунікаційну мережу МВС України або мережу Інтернет підключити усі стаціонарні антени системи моніторингу повітряного простору до центрального серверу Єдиної системи моніторингу повітряного простору МВС України.

6. Визначитися із необхідною кількістю робочих місць операторів Єдиної системи моніторингу повітряного простору МВС України (наприклад, у кожному відокремленому структурному підрозділі установ та організацій, що входять до структури МВС України та інших центральних органів виконавчої влади, діяльність яких спрямовується та координується Кабінетом Міністрів України через Міністра внутрішніх справ України).

7. Обладнати робочі місця операторів Єдиної системи моніторингу повітряного простору МВС України та підключити їх до Єдиної цифрової відомчої телекомунікаційної мережі МВС України.

8. Розробити необхідні нормативно-правові акти, що повинні регламентувати функціонування Єдиної системи моніторингу повітряного простору МВС України.

Аналіз існуючих систем моніторингу повітряного простору, які пропонують на комерційному ринку, показує, що на сьогодні систем моніторингу повітряного простору, які б виявляли всі існуючі види БпЛА (як фабричні, так і саморобні), не існує.

Закордонні та вітчизняні фахівці у сфері використання БпЛА та безпеки повітряного простору зазначають, що найбільш розповсюджені у світі та в Україні мультикоптери компанії «DJI», тому вважаємо доцільним використання системи моніторингу повітряного простору цієї ж компанії – програмно-апаратний комплекс «DJI Aeroscope».

13 липня 2018 року Український державний центр радіочастот сертифікував пристрої для моніторингу БпЛА в повітряному просторі: «DJI Aeroscope Mobile» та «DJI Aeroscope Stationary» [6].

В основі технології «AeroScope» лежить використання вже існуючої лінії зв'язку між БпЛА та його пультом дистанційного керування. Завдяки цьому відбувається збір інформації про апарат, включаючи його місце

розташування, дистанцію до оператора, польотний маршрут, серійний номер та інші телеметричні дані. Якщо система виявить проникнення БпЛА на обмежену для польотів територію, то це дасть правоохоронним і контролюючим органам можливість використовувати отриману інформацію для відповідних дій.

Оператор мобільного системи спостереження в змозі одночасно відстежувати до 50-ти БпЛА [7].

«DJI Aeroscope» може виявляти не лише мультикоптери компанії «DJI», але й значну частину мультикоптерів інших виробників:

- 10 % саморобних БпЛА;
- 25 % БпЛА, що використовують стандартний відкритий протокол Wi-Fi;
- 65 % БпЛА популярних виробників [8].

Можливість замовлення комплексів «AeroScope» надається виключно державним підприємствам, таким як аеропорти або аеродроми, спеціальним службам і службам оперативного реагування, підприємствам пенітенціарної системи тощо.

За результатами аналізу закупівель на сайті публічних закупівель Prozorro [9], проведених державними установами (військовими частинами Національної гвардії України) в 2019 році, орієнтовна вартість 1 комплексу моніторингу повітряного простору становить:

1) мобільного «DJI Aeroscope Mobile» – 490 000 грн;

2) стаціонарного «DJI Aeroscope Stationary» – 980 000 грн.

Список бібліографічних посилань

1. Сучасні безпілотні літальні апарати у сільському господарстві // Аграрний тиждень. Україна : сайт. 06.03.2020. URL: https://a7d.com.ua/novini/49244-suchasn-bezplotn-ltaln-aparati-u-slskomu-gospodarstv.html (дата звернення: 11.05.2020).
2. Бєловол С. Світовий досвід правового регулювання використання безпілотників : інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України // Європейський інформаційно-дослідницький центр : сайт. URL: http://euinfocenter.rada.gov.ua/uploads/documents/28939.pdf (дата звернення: 11.05.2020).

3. Рынок дронов в Украине достиг $1 млн в месяц // Latifundist Media : сайт. 19.10.2019. URL: https://latifundist.com/novosti/46761-rynok-dronov-v-ukraine-dostig-1-mln-v-mesyats (дата звернення: 11.05.2020).
4. Зозуля Ю. Атака дронов // OPENKYIV : сайт. 16.02.2019. URL: https://openkyiv.info/ru/blog/ataka-dronov (дата звернення: 11.05.2020).
5. Взгляд на индустрию дронов в 2020 году // Беспилотник.org : сайт. 21.01.2020. URL: https://bespilotnik.org/info/articles/2020/vzglyad_na_industriyu_dronov_v_2020_godu/ (дата звернення: 11.05.2020).
6. Карпусь В. В Украине официально сертифицировано первое устройство для мониторинга БПЛА // ITC.ua : сайт. 14.08.2018. URL: https://itc.ua/news/v-ukraine-ofitsialno-sertifitsirovano-pervoe-ustroystvo-dlya-monitoringa-bpla/ (дата звернення: 11.05.2020).
7. DJI Aeroscope уже в Украине: безопасность аэропортов под защитой технологий // Drone.UA : сайт. 24.04.2018. URL: http://drone.ua/dji-aeroscope-uzhe-v-ukraine-bezopasnost-aeroportov-pod-zashhitoy-tehnologiy/ (дата звернення: 11.05.2020).
8. Коптеры становятся все более и более популярными // QUADRO.UA : сайт. URL: https://quadro.ua/ru/aeroscope/ (дата звернення: 11.05.2020).
9. Prozorro : публічні закупівлі. URL: https://prozorro.gov.ua/ (дата звернення: 11.05.2020).

Одержано 11.05.2020

УДК 343.575

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

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

ДОСВІД ПРОТИДІЇ НЕЗАКОННОМУ ЗБУТУ НАРКОТИЧНИХ ЗАСОБІВ, ПСИХОТРОПНИХ РЕЧОВИН АБО ЇХ АНАЛОГІВ ЧЕРЕЗ МЕРЕЖУ ІНТЕРНЕТ ШЛЯХОМ ЗАЛУЧЕННЯ НАСЕЛЕННЯ У ЯКОСТІ КОРИСТУВАЧІВ TELEGRAM ЧАТ-БОТУ «СТОПНАРКОТИК»

Наркоманія – це важка хвороба, яка, насамперед, уражає молодь. Одним із факторів, що впливає на початок уживання наркотиків серед молоді є їх доступність [1].

За деякими дослідженнями, на сьогодні, 90 % незаконних продаж наркотичних речовин здійснюється саме через інтернет-месенджер Telegram, де працюють, так звані, «інтернет-наркокрамниці» [2]. У месенджері Telegram не тільки відбувається збут наркотиків, але там також «працюють» анонімні канали автори яких діляться із своїми підписниками інформацією як безпечно придбати наркотики та займатися незаконним збутом наркотичних засобів, психотропних речовин або їх аналогів через мережу інтернет [3].

Молодь гарно обізнана як користуватися сучасними інформаційними технологіями, а отже для них не становить проблему незаконно придбати наркотики, у разі потреби.

Електронні «наркоадреси» у месенджері Telegram поділяються на кілька типів:

— канали з прайсами та відгуками покупців «наркокрамниць»;

— чати покупців «наркокрамниць»;

— чат-боти з автоматичного продажу наркотиків;

— оператори (продавці) «наркокрамниць».

Усі користувачі месенджеру Telegram мають можливість поскаржитися адміністрації месенджеру на електронні «наркоадреси», що використовують зловмисники для незаконного збуту наркотиків. Для цього користувачі можуть направляти електронні листи на офіційну електрону поштову скриньку адміністрації Telegram або виконати наступні кроки у месенджеру:

1. Перейти за посиланням (адресою) «наркокрамниці».

2. У правому верхньому кутку месенджеру знайти пункт «Поскаржитися».

3. Обрати причину скарги «Інша».

4. Зазначити причину скарги: «Продаж наркотиків» або «Drug sales».

5. Відправити скаргу.

Telegram чат-бот «СтопНаркотик» (https://t.me/StopDrugsBot), розроблений курсантами та науково-педагогічними працівниками факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ, став дієвим засобом боротьби з незаконним поширенням наркотиків через мережу Інтернет, а саме через месенджер Telegram. Щодня чат-бот «СтопНаркотик» розсилає своїм користувачам кілька «наркоадрес», на які їм пропонується залишити скарги.

Уперше чат-бот був презентований 19 вересня 2019 року на засіданні Координаційної ради з попередження наркоманії Харківської міської Ради [4].

Широку інформаційну підтримку щодо доведення до населення інформації про чат-бот провели: Міністерство внутрішніх справ України; Департамент протидії наркозлочинності Національної поліції України та його територіальні підрозділи; ГУНП в Донецькій області; Київська обласна рада; Харківська міська рада; Кременчуцька міська рада; Харківський національний університет внутрішніх справ.

За вдяки поширенню інформації про чат-бот «СтопНаркотик» місцевими, регіональними та національними ЗМІ та медіа, на сьогодні кількість користувачів чат-боту перевищує 27 тисяч. осіб. Серед них також є мешканці тимчасово окупованих територій України

Співпраця поліції і громадськості завжди є ефективною і дає найкращий результат, у чому переконують цифри. Так на сьогоднішній день користувачі Telegram чат-боту «СтопНаркотик» допомогли заблокувати 1000 електронних адрес у месенджері Telegram, що використовували зловмисники для незаконного розповсюдження наркотиків через мережу Інтернет, у тому числі 10 «наркокрамниць», що працювали на тимчасово окупованих територіях Донецької та Луганської областей та 3 «наркокрамниці» в Автономній республіці Крим [5].

Чат-бот дає можливість користувачам надсилати фотографії «графіті» (написи) з «наркоадресами» із зазначенням GPS-координат або фізичних адрес, де вони були виявлені; адреси в месенджері Telegram та вебсайтів з продажу наркотиків; адреси точок продажу наркотиків в населених пунктах. Важливо, що наші громадяни не лише надсилають повідомлення, але й беруть активну участь у заходах щодо видалення адрес сайтів з розповсюдження наркотиків, на будинках, парканах, в інших місцях громадського користування [6].

За час роботи чат-боту користувачі надіслали на перевірку 15260 фотографій виявлених ними рекламних написів з адресами «інтернет-наркокрамниць»; 18156 Telegram-адрес «інтернет-наркокрамниць»; 1998 посилань на вебсайти «інтернет-наркокрамниць».

Необхідно пам'ятати, що вживання наркотиків не просто шкодить здоров'ю людини, а знищує, вбиває її. Це життя без майбутнього. Надання можливості громадянам брати активну участь у протидії незаконному збуту наркотичних засобів, психотропних речовин або їх аналогів через мережу Інтернет, дозволяє зберегти життя та здоров'я наших громадян.

Список бібліографічних посилань

1. Фактори, які впливають на початок уживання наркотиків серед молоді // Бершадська районна рада : офіційний вебсайт. 05.11.2019. URL: http://rada-bershad.gov.ua/novunu/faktory-yaki-vplyvayut-na-pochatok-uzhyvannya-narkotykiv-sered-molodi (дата звернення: 12.05.2020).
2. Фахівці ХНУВС створили чат-бот «Стопнаркотик» для блокування інтернет-ресурсів з продажу наркотиків // Харківський національний

університет внутрішніх справ : офіційний сайт. 24.09.2019. URL: http://univd.edu.ua/uk/news/5703 (дата звернення: 12.05.2020).
3. Рвачов О.М. Сучасні методи приховування фактів причетності до незаконного збуту наркотичних засобів, психотропних речовин або їх аналогів через мережу Інтернет // Застосування інформаційних технологій у діяльності правоохоронних органів : матеріали наук.-практ. семінару, м. Харків, 18 грудня 2019 р. / МВС України, Харк. нац. ун-т внутр. справ. Харків : ХНУВС, 2019. С. 82-86.
4. У Харкові створили чат-бот для блокування інтернет-ресурсів з продажу наркотиків // Офіційний сайт Харківської міської ради, міського голови, виконавчого комітету. 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: 12.05.2020).
5. Користувачі чат-боту «СтопНаркотик» допомогли заблокувати 1000 інтернет-адрес «наркокрамниць» // Єдиний портал органів системи МВС України. 12.05.2020. URL: https://mvs.gov.ua/ua/news/30638_Koristuvachi_chat_botu_StopNarkotik_dopomogli_zablokuvati_1000_internet_adres_narkokramnic.htm (дата звернення: 12.05.2020).
6. Рвачов О. М., Лактіонов В. В., Дацюк Д. О. Сучасні методи активного залучення населення до протидії збуту наркотичних засобів, психотропних речовин або їх аналогів через мережу Інтернет // 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. С. 210-217.

Одержано 12.05.2020

УДК 004.415.53:519.711

Чжан ЛИЦЗЯН,
преподаватель Юго-западного университета науки и техники (г. Цзяотун, Китай)

Юрий Петрович ГОРЕЛОВ,
кандидат технических наук, доцент, доцент кафедры информационных технологий и кибербезопасности факультета № 4 Харьковского национального университета внутренних дел

Юрий Валерьевич ГНУСОВ,
кандидат технических наук, доцент, заведующий кафедры информационных технологий и кибербезопасности факультета № 4 Харьковского национального университета внутренних дел

РАЗРАБОТКА АЛГОРИТМА ТЕСТИРОВАНИЯ НА ПРОНИКНОВЕНИЕ В КОМПЬЮТЕРНУЮ СИСТЕМУ

Проведенные исследования показали, что основной целью тестирования на проникновение является определение возможностей существующего уровня защищённости инфраструктуры в сдерживании попыток вторжения потенциального кибер злоумышленника. При этом вопрос полноты обнаруженных уязвимостей не стоит, но отражаются все уязвимости, имеющие отношение к направлениям атаки.

Основным фокусом данного вида тестирования безопасности является глубина исследования. Данная характеристика является более важной, чем ширина охвата тестовых примеров. Это является одной из особенностей, которую целесообразно учитывать в процессе математического моделирования.

Как указано в руководящих документах и планах тестирования уровень зрелости информационной безопасности, которую обеспечивает данный вид тестирования можно характеризовать в пределах от среднего до высокого.

Результатами процесса тестирования на проникновение являются факты и/или вероятность взлома (проникновения) и получения информации злоумышленником.

Проведенные исследования позволили выделить ряд примеров решаемых задач тестирования:

- получить несанкционированный доступ к информации о клиентах, их средствах и другим данным;
- проникнуть из офисного сегмента в «боевой», где расположены рабочие серверы;
- нарушить доступность определённого сервиса;
- получить доступ к файловой системе с необоснованно завышенными правами;
- скомпрометировать исходные коды программного обеспечения из системы контроля версий.

Для достижения поставленных целей и решения приведенных выше задач возможно использование всех доступных методов и средств, удовлетворяющих ограничениям, поставленным заказчиком (в т. ч. социальная инженерия, атаки перебором и др.). При этом исследователи ищут кратчайший и самый дешёвый путь достижения целей.

Проект заканчивается либо, когда поставленная цель будет достигнута, либо по истечению времени на проект (если рассматриваются многие вектора).

Прежде чем более подробно описывать основные этапы тестирования на проникновение и реализовывать соответствующую математическую модель необходимо отметить отличительные особенности и специфику тестирования различных компьютерных и инфокоммуникационных систем, а также их составляющих. Для этого выберем наиболее часто используемые объекты тестирования, которые можно рассматривать в совокупности по принципу единства платформ выполнения задач и функций. Это компьютерные системы управления с элементами SCADA и IOT, сайты и web-приложения, мобильные средства и приложения.

Анализ основных этапов и процедур тестирования на проникновение перечисленных объектов позволил разработать и представить обобщенный алгоритм тестирования.

Структурная схема алгоритма представлена на рис. 1.

Следует заметить, что в представленный обобщенный алгоритм не включены ряд возможных для реализации процедур тестирования. Например, при тестировании «SCADA-компьютерных систем» можно воспользоваться услугами зондирования или процедурами эксплойт исследования. Для более глубокой оценки мобильных приложений можно использовать дополнительно оценку уязвимостей OWASP Mobile Top 10. Перечень и спектр таких услуг и процедур увеличивается с каждым годом. Связано это с появлением новых рисков кибератак.

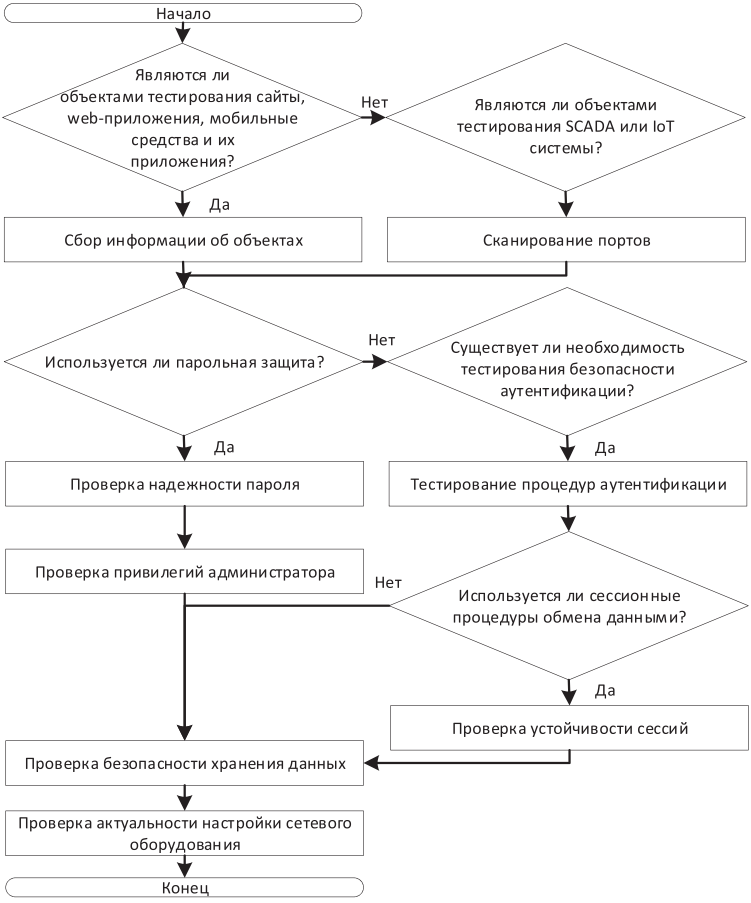


Рис. 1. Структурная схема обобщенного алгоритма тестирования на проникновение

Однако, по нашим оценкам, решение о включении дополнительных процедур как составляющих отдельных этапов обобщенного алгоритма (рис. 1.) значительно не снизит точности результатов моделирования. Необходимо только учитывать эти дополнительные факторы при задании вероятностного распределения каждого из этапов и выборе коэффициентов распределения.

Одержано 30.04.2020

УДК 621.39

Оксана Петрівна МЕЛАЩЕНКО,
старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

Вікторія Євгеніївна РОГ,
старший викладач кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ЯКІСНА ХАРАКТЕРИСТИКА ВИМОГ ДО СВОЄЧАСНИХ І ПРЕСПЕКТИВНИХ БЕЗПРОВОДНИХ ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Метою розробки та впровадження Концепції (нова редакція) програми інформатизації системи Міністерства внутрішніх справ України, на 2018-2020 роки є запровадження нової моделі спільного інтегрованого інформаційного середовища - базового інструменту для автоматизації інформаційних процесів в державі, побудованого за принципами технологічної незалежності, використання єдиних інтерфейсів та протоколів взаємодії і обміну інформацією у реальному часі. Це вимагає перехід на новий якісний рівень інформаційної та телекомунікаційної систем, які повинні забезпечити відповідні параметри функціонування системи МВС

На теперішній час використання нових форм соціальної та економічної діяльності, які базуються на широкому використанні інформаційних та телекомунікаційних технологій, визначає перехід від індустріального до інформаційного суспільства. Технологічною основою такого суспільства є Глобальна інформаційна (Global Information Infrastructure, GII), яка повинна забезпечити можливість вільного доступу користувача до інформаційних ресурсів в будь якому місті земної кулі. Системи телекомунікацій Системы телекоммуникаций є матеріальною і системоутворюючою основою подібної інфраструктури, що визначає необхідність створення високоефективного телекомунікаційного середовища на рівні держави [1, 2]. Основною функцією бездротових ТКС є надання користувачам широкого спектру бездротових послуг зв'язку із забезпеченням зазначеного рівня

якості обслуговування (Quality of Service, QoS) [3]. З метою виконання зазначеної функції до бездротових ТКС, за аналогією з [4], висувається ряд вимог основними з яких є: мультисервісність, під якою розуміється здатність надання якомога більшого набору послуг і сервісів з забезпеченням незалежності технологій надання послуг технологій бездротового зв'язку; мультимедійність, під якою розуміється здатність бездротової ТКС передавати багатокомпонентну інформацію (мова, дані, відео, аудіо); мультипротокольні, під якою розуміється властивість забезпечувати перенесення (транспортування) різних видів інформації з використанням різних протоколів передачі та підтримки сервісів; забезпечення широкого спектру градацій якості обслуговування користувачів і підтримки класів обслуговування.

Однак стримуючим фактором впровадження широкого набору мультимедійних послуг є невисока продуктивність бездротових телекомунікаційних систем. В ході досліджень було проведено аналіз різних підходів, спрямованих на підвищення продуктивності бездротових телекомунікаційних систем. Серед них на особливу увагу заслуговують підходи, спрямовані на використання технології інтелектуальних антенних решіток, рознесення сигналу по поляризації, розробку методів модуляції і кодування сигналу, на використання технології MIMO тощо.

Втім в результаті аналізу було встановлено, що найбільшу ефективність у підвищенні продуктивності забезпечує оптимальне управління мережевими ресурсами. З огляду на значущі відмінності між зазначеними видами мережевих ресурсів, принципи управління ними можуть істотно відрізнятися.

Подальші дослідження були присвячені перспективам розвитку пост – NGN, 4G і 5G мереж, які повинні замінити існуючі. Перші прототипи 5G вже з'явилися у Південної Кореї. Компанія SK Telecom представила нову технологію на відкритті дослідницького центру, який займеться її розвитком. А до XXIII зимових Олімпійських ігор 2018 року в Південній Кореї компанія побудувала мережу 5G по всій країні, NTT DoCoMo теж має намір запустити 5G-мережу в Японії до літніх Олімпійських ігор 2020 року в Токіо.

Також швидкими темпами йдуть роботи по створенню 5G-мереж в США, ЄС, ряді країн Північної Європи, в тому числі Швеція та Естонія. В даний час ведуть роботи по створенню технології 4,5G LTE Advanced Pro, впровадження якої планується протягом наступних чотирьох років. Завдяки цьому компанія Qualcomm зможе підтримувати як більш

широкий спектр частот, необхідних для стандарту 5G, так і раніше розгорнуті мережі LTE, що зменшить затримки і збільшить пропускну спроможність. Особливостями пропонованої мережі є:

- висока пропускна здатність завдяки об'єднанню спектрів частот;
- підтримка 32 операторів одночасно і збільшення пропускної здатності завдяки об'єднанню частот і розподілу мережевого трафіку між операторами;
- 10-кратне зниження затримки в порівнянні з LTE Advanced при використанні існуючих вишок і частот з 1 мс до 70 мкс;
- використання ресурсу вхідної лінії зв'язку для потреб вихідної;
- збільшення кількості антен на базових станціях для збільшення зони покриття і потужності сигналу;
- підвищення енергозбереження IoT-пристроїв звуженням діапазону до 1,4 МГц і 180 кГц (до 10 років на одній батареї);
- 1 Гбіт/с для обміну інформацією між автомобілями, пішоходами і IoT-пристроїв;
- сканування оточення без включення Wi-Fi або GPS на мобільному пристрої.

Таким чином, повсюдне впровадження в Україні мереж 4G, 5G або 4,5G дозволить істотно підвищити якість надаваних споживачеві послуг.

Список бібліографічних посилань:

1. Garkusha S. V., Al-Dulaimi K., Al-Janabi K. H. The service required quality ensure model of LTE technology downlink. *Информационно-управляющие системы*. 2013. Вып. 4/9 (64). С. 35–38.
2. Дубов Д. В., Ожеван М. А. Широкосмуговий доступ до мережі інтернет як важлива передумова інноваційного розвитку України : аналіт. доп. Київ : НІСД, 2013. 108 с.
3. Гаркуша С. В. Разработка и анализ модели распределения подканалов в сети стандарта IEEE 802.16. *Вісник національного університету «Львівська політехніка». Серія: Радіоелектроніка та телекомунікації.* 2012. № 738. С. 177–185.
4. Можаєв О. О., Обод І. І., Яценко І. Л. Оцінка інформаційної ємності мобільних інформаційних мереж. *Системи обробки інформації*. 2014. Вип. 5 (121). С. 136–138.

Одержано 29.04.2020

УДК 378.147:004.9

Олександр Олександрович МОЖАЄВ,
доктор технічних наук, професор,
професор кафедри інформаційних технологій та кібербезпеки
факультету № 4 Харківського національного університету внутрішніх справ

Олександр Юрійович ГОРЕЛОВ,
магістрант кафедри програмної інженерії
Харківського національного університету радіоелектроніки

АДАПТИВНЕ ТЕСТУВАННЯ ЗНАНЬ У ДИСТАНЦІЙНОМУ НАВЧАННІ

Застосування інформаційних технологій у традиційній організації навчального процесу у закладі вищої освіти дозволяє підвищити ефективність навчання та оптимізувати процедуру тестування знань.

Тестовий контроль знань дозволяє скоротити витрати часу, одержати об'єктивну картину знань з предмету, знизити психологічне навантаження на студента та представити результати тестування у формі, яка дозволяє провести швидкий аналіз та візуалізацію результатів (звітів, зведень, графіків);

Як і будь-який вимірювальний інструмент, тест має певну точність і певну погрішність. Можлива й фальсифікація результатів тестування.

Під педагогічним тестом будемо розуміти систему завдань певної складності і специфічної форми, що дозволяє якісно оцінити структуру й виміряти рівень знань учнів.

Завдання, які містяться в тесті, звичайно мають одну з наступних форм: завдання закритої форми, завдання на відповідність, завдання на встановлення правильної послідовності та завдання відкритої форми.

Процес тестування складається з наступні етапів: проектування й розробка (вибір) тесту, реалізація процедури тестування, аналіз, оцінка та інтерпретація результатів тестування.

Тести мають наступні основні властивості, порушення кожного з яких робить тест непридатним: валідність, надійність, стійкість, репре-

зентативність, вірогідність, гіпотеза тестування (основні педагогічні умови, при яких іде перевірка студентів).

Кожна технологія тестування повинна мати основні характеристики: наявність інтерактивного інструментального середовища; мультіпредметне застосування; адекватне відображення моделі предметної області в процесі тестування; можливість вибору алгоритму тестування; інтегруємість у різні освітні технології; масштабованість; доступність; ведення бази тестових багаторівневих завдань; дружність користувацького інтерфейсу; керування та планування, які можна налаштовувати; націленість на досягнення більш високих результатів і підвищення мотивації.

Сучасна практика тестування характеризується переходом до використання систем адаптивного тестування. Під адаптивним тестуванням розуміється сукупність процесів генерації, пред'явлення й оцінки результатів виконання адаптивних тестів, що забезпечує приріст ефективності вимірів у порівнянні із традиційним тестуванням.

Адаптивне тестування повинне задовольняти наступним вимогам:

- здатність регулювати пропорції легких, середніх і важких завдань залежно від числа правильних відповідей студента;
- здатність регулювати пропорції питань з різних тематичних розділів навчальної програми в тесті;
- здатність регулювати рівень складності пропонованих тестів з урахуванням семантичної компетенції студента;
- включення адаптивного механізму переходу на більш високий рівень складності завдань на тому самому рівні пропонованих завдань;
- кожне завдання більш високого рівня оцінюється більш високими балами.

Залежно від платформи, на якій реалізується процедура тестування, можна виділити WWW-тестування, мобільне тестування та тестування стаціонарне.

WWW-тестування реалізується на основі широкого спектра вебтехнологій (Html-код, CGI-скрипты, Java-машина, системи управління навчанням (LMS) та ін.) і широко використовується в дистанційному навчанні і контролі.

Останнім часом активно розбудовується технологія m-learning (навчання на основі мобільних технологій і засобів - приладів із мінімальни-

ми ресурсами з мінімальною необхідністю використання спеціального місця та спеціального часу для навчання). Зокрема, у рамках програми Європейської комісії «Leonardo da Vinci» за підтримки компанії Ericsson і деяких європейських університетів дистанційного навчання ще у 2003 р. реалізований проект «From e-learning to m-learning». Розроблена спеціальна система mLMS (Mobile Learning Management System) для управління мобільним навчанням. Хоча можливості m-learning і обмежені, воно має велику інноваційну привабливість.

Стаціонарне тестування звичайне реалізується в комп'ютерних класах, і поступово втрачає свої позиції.

Адаптивне тестування може бути реалізоване на кожній із цих платформ, хоча його алгоритми можуть пред'являти ряд підвищених вимог до апаратного забезпечення.

Для представлення моделі предметної області та моделі студента в системах адаптивного тестування використовується широкий спектр інструментів: мережі Байеса, марківські процеси, мережі Петрі, нейронні мережі, засоби нечіткої логіки.

Мета цих моделей та алгоритмів адаптації – прискорити та оптимізувати процедуру тестування. Вона досягається, як правило, тим, що система тестування пропонує деяке тестове завдання на основі аналізу відповідей студента на попередні завдання. Система може запропонувати завдання більшої складності, зменшити складність, змінити форму завдання або перейти до іншого розділу. Також цікавим є реалізація здатності системи тестування виправляти рівень складності завдань на основі відповідей студента. Це важливо, наприклад, у випадку, коли самі завдання генеруються автоматично на основі концептуальної моделі предметної галузі.

Одержано 17.04.2020

УДК 004

Ірина Анатоліївна ОСЯТИНСЬКА,
вчитель комунального закладу «Харківська загальноосвітня школа I–III ступенів № 165 Харківської міської ради Харківської області»

ОКРЕМІ АСПЕКТИ ВДОСКОНАЛЕННЯ НАВЧАННЯ ЗДОБУВАЧІВ У РАМКАХ ДИСТАНЦІЙНОЇ ОСВІТИ

Через оголошення карантину в Україні практично усі навчальні заклади було переведено на систему дистанційного навчання. У зв'язку з наведеним гостро постало питання забезпечення здобувачів освіти матеріалами для навчання та адекватної оцінки одержаних ними знань.

Вказані обставини зумовили пошук науково-педагогічними та педагогічними працівниками нових підходів та інноваційних рішень, які б дозволили не лише в ручному режимі передавати здобувачам завдання та методичні матеріали, але й забезпечити їх мотивацію до вивчення предметів, створити умови для творчого підходу до розв'язання практичних задач, організувати об'єктивну оцінку знань таким чином, аби і сам учень був упевнений у правильності виставлених йому оцінок.

З означеною метою можуть бути використані низка способів організації освіти:

1) самостійна розробка науково-педагогічним або педагогічним працівником методичного та мультимедійного забезпечення курсу із наступною комунікацією зі здобувачами освіти через спеціалізовані сервіси та платформи. У найпростішому випадку для цього можуть бути застосовані месенджери, сервіси для розміщення мультимедійного контексту, спеціально призначені для дистанційного навчання платформи як от Moodle або Google Classroom. Перевагою використання для навчання Google Classroom є відсутність потреби у встановленні та підтримці самої платформи для дистанційного навчання. Водночас слід звернути увагу, що відповідне навчання краще організовувати з облікових записів, прив'язаних до навчального закладу. Це дає змогу обмежити коло учасників курсу, верифікувати здобувачів освіти, виключити хуліганські дії з боку анонімних учасників класу.

2) використання вже готових платформ, які в ігровій формі дозволяють закріпити одержані знання та удосконалити практичні навички. Відповідні платформи різняться залежно від дисципліни та завдань, які планується досягти. Так, наприклад, з питань вивчення дисциплін пов'язаних із забезпеченням кібербезпеки можуть бути рекомендовані такі платформи як Hack The Box, Root Me, VulnHub. Вони містять вже готові завдання та спеціально-налаштовані системи, на яких відпрацьовуються навички пентестінгу, криптології, цифрової криміналістики, програмування, реверс-інжинірингу тощо. Перевагою застосування таких платформ є те, що результат виконання того чи іншого завдання у сфері безпеки підтверджується введенням спеціального прапору, який учасник одержує в результаті виконання завдання. Це стимулює у здобувачів творчий підхід до вивчення матеріалу, а також можливість оцінки виконаної роботи шляхом перегляду письмових звітів та підтвердженням введення прапору на платформі;

3) комбінація перших двох способів, яка дає найкращий ефект та дозволяє вибудувати унікальний курс викладачем таким чином, аби з одного боку мотивувати учнів до вивчення курсу, а з іншого – донести до них саме той матеріал, який передбачено навчальною програмою дисципліни.

Отже, введення карантину у зв'язку з вірусною загрозою спричинило низку негативних наслідків, але водночас дозволило поглянути на процес організації навчання з іншого боку та запропонувати нові ідеї в освітньому процесі.

Одержано 30.04.2020

УДК 004.05

Олександр Вадимович ПИЛИПЕНКО,
судовий експерт відділу комп'ютерно-технічних та телекомунікаційних досліджень
Харківського науково-дослідного експертно-криміналістичного центру МВС України

ІНФОРМАЦІЙНА БЕЗПЕКА СМАРТФОНІВ

За останнє десятиліття смартфони стали невід'ємною частиною повсякденного життя сучасної людини. Безумовно, велику роль в цьому грає інформатизація у всіх сферах людської діяльності. Зараз дуже важко представити собі банк без онлайн банкінгу в смартфоні, онлайн магазин без мобільного додатку або вебсайту, оптимізованого під перегляд на мобільних пристроях, навіть для повсякденного онлайн спілкування все менше використовують стаціонарні комп'ютери або ноутбуки – усі популярні сервіси для онлайн спілкування давно є в смартфонах. І це не дивно, адже смартфон завжди під рукою, і не просто смартфон, а смартфон із доступом до мережі інтернет.

Приїжджаючи в інше місто або іншу країну, не знаючи місцевості, не маючи змоги спитати про місцезнаходження найближчого готелю, банкомату або необхідної автозаправної станції потрібно лише відкрити карту на своєму смартфоні і ситуація відразу змінюється. Зовсім нещодавно важко було уявити віддалену роботу та роботу в офісному програмному забезпеченні без ноутбука з доступом до мережі інтернет, проте і тут смартфон стає в нагоді – все офісне програмне забезпечення зараз адаптоване під мобільні платформи, а розміри дисплеїв дозволяють досить комфортно працювати з документами, вести листування електронною поштою та мессенджерами.

За допомогою смартфонів сучасна людина спілкується, працює, відпочиває, грає, вчиться, слідкує за своїм здоров'ям, проводить різноманітні оплати, за допомогою смартфону створює та зберігає фото та відео, як особисті, так і комерційного характеру, зберігає багато приватних даних, наприклад, логіни, паролі або PIN коди банківських карток. Багато користувачів не задумуються про інформаційну безпеку своїх пристроїв та навіть не знають, що багато цінної інформації може бути викрадено в результаті використання відкритої мережі Wi-Fi в улюбленому кафе.

Також користувач не завжди використовує парольний, графічний або біометричний захист, використання таких мір безпеки значно підвищує шанс на збереження особистих даних, хоча це і не панацея, дуже часто в авторитетних виданнях можна зустріти інформацію про те, що в мобільних телефонах тієї чи іншої компанії виявлено чергову помилку в операційній системі, через яку зловмисники можуть з легкістю отримати повний доступ до інформації в смартфоні.

Почнемо з того, що означає термін "вразливість нульового дня". Вразливістю нульового дня (англ. Zero day, 0day) називають вразливість програмного забезпечення, на виправлення якої у розробників було нуль днів, тобто до моменту випуску виробником патчу безпеки дана вразливість стає публічно відомою [1]. Нижче буде розглянуто деякі найбільш відомі останні проблеми в безпеці смартфонів.

Наприкінці 2019 року компанія Google зробила заяву, що знайшла докази того, що вразлива версія їх операційної системи Android, в якій знайшли вразливість нульового дня, наразі використовується у світі [2]. Вразливість знаходиться на рівні коду ядра операційної системи і може використовуватись зловмисниками для отримання root-доступу до смартфону (під root-доступом розуміють отримання привілей суперкористувача, власник яких може виконувати всі без винятку операції та має доступ до всіх даних на пристрої). Компанія протестувала дану вразливість на деяких своїх смартфонах Google Pixel та на деяких смартфонах компаній Samsung, Xiaomi, Huawei, Oppo, Motorola. Також дослідники Google заявили, що дана вразливість не потребує індивідуальних налаштувань під кожен пристрій, що може означати дієздатність даної вразливості на великій кількості пристроїв. Для потенційної експлуатації даної вразливості користувач лише повинен встановити шкідливий додаток.

Багато користувачів мобільних телефонів компанії Apple вважають, що їх смартфони не схильні по атака зловмисників. Проте таке твердження досить помилкове. Наприкінці літа 2019 року група спеціалістів Project Zero (група спеціалістів безпеки Google, яка займається пошуком вразливостей нульового дня) опублікувала статтю [3], в якій публікується про масштабну атаку на iOS пристрої, яка тривала щонайменше два роки. Користувачу треба було лише відвідати зламаний вебсайт, як мобільний пристрій відразу атакувався сервером експлойтів (від слова «експлуатувати» - послідовність команд, які використовують

вразливості програмного забезпечення) для подальшого моніторингу за мобільним пристроєм. Такий вебсайт був не один, і щотижня їх відвідувало тисячі користувачів. Зловмисники могли впровадити в систему код, який дозволяв обходити систему keychain, яка зберігає та захищає конфіденційну інформацію - логіни, паролі, дані банківських карток і так далі. Слід відмітити, що за допомогою обходу даного захисту зловмисники могли отримувати доступ до будь-яких даних в системі, навіть до баз даних месенджерів с шифруванням даних. Загалом дослідники компанії Google знайшли 14 вразливостей та 5 ланок експлойтів, за допомогою яких можна було отримати доступ до операційної системи iOS від десятої до останньої (на той час 12) версій.

Слід завжди брати до уваги той факт, що людина завжди є найслабшою ланкою в інформаційній безпеці. Це твердження справедливо як до людей які створюють програмне забезпечення, так і до звичайних користувачів. Коли людина пише код програми, вона допускала, допускає і завжди буде допускати помилки, а коли їх знайде зловмисник – це лише питання часу. Завжди треба давати звіт своїм діям як звичайного користувача – не встановлювати додатки з ненадійних джерел, не переходити по підозрілим посиланням, не відповідати на підозрілі SMS повідомлення, не зберігати паролі в нотатках та на фотографіях, використовувати лише надійні та різні паролі.

Список бібліографічних посилань

1. Вразливість нульового дня // Вікіпедія : віл. енцикл. URL: https://uk.wikipedia.org/wiki/вразливість_нульового_дня (дата звернення: 23.04.2020).
2. Cimpanu C. Google finds Android zero-day impacting Pixel, Samsung, Huawei, Xiaomi devices // ZDNet. 04.10.2019. URL: https://www.zdnet.com/article/google-finds-android-zero-day-impacting-pixel-samsung-huawei-xiaomi-devices/ (дата звернення: 23.04.2020).
3. Beer I. A very deep dive into iOS Exploit chains found in the wild // Project Zero team at Google. 29.08.2019. URL: https://googleprojectzero.blogspot.com/2019/08/a-very-deep-dive-into-ios-exploit.html (дата звернення: 24.04.2020).

Одержано 25.04.2020

УДК 347.61:364.28

Владислав Романович ПЛЕХАНОВ,
курсант 3 курсу факультету № 4
Харківського національного університету внутрішніх справ

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

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

ОПЕРАТИВНЕ РЕАГУВАННЯ НА ВИПАДКИ ДОМАШНЬОГО НАСИЛЬСТВА ЗА ДОПОМОГОЮ TELEGRAM ЧАТ-БОТУ МВС УКРАЇНИ «#ДІЙПРОТИНАСИЛЬСТВА»

У зв'язку із встановленням карантинно-обмежувальних заходів, пов'язаних із пандемією короновірусної хвороби COVID-19, як в Україні, так і в багатьох інших країнах світу, виник потенційний ризик збільшення випадків домашнього насильства у сім'ях, які перебувають на самоізоляції.

28 березня 2020 року видання «The Guardian» опубліковало дані експертів з різних країн світу (Бразилії, Німеччини, Китаю, Греції), що через запровадження в цих країнах карантинних заходів та необхідності громадян залишатися вдома на самоізоляції, в цих країнах збільшилась кількість випадків домашнього насильства [1].

В період карантину підрозділи МВС України були переведені на посилений варіант несення служби. Але попри це, у фокусі діяльності правоохоронців незмінно залишається питання протидії домашньому насильству.

За І квартал 2020 року в Україні було зафіксовано 46 997 звернень з приводу домашнього насильства, що на 48% більше порівняно з аналогічним періодом минулого року (31 735 звернень), з них:

- від дітей надійшло 420 звернень, що становить 0,8% від загальної кількості;
- від жінок – 40 200 звернень, що становить 85% від загальної кількості;
- від чоловіків – 6 377 звернень, що складає 13,6% від загальної кількості звернень.

Обліковано 103 звернення щодо вчинення домашнього насильства стосовно осіб з інвалідністю [2].

Особи, яким стало відомо про вчинення домашнього насильства, зокрема, якщо постраждалими особами стали або можуть стати діти, то вони мають можливість невідкладно повідомити про це до районних, районних державних адміністрацій у містах Києві та Севастополі, виконавчих органів сільських, селищних, міських, районних у містах (у разі їх створення) рад, уповноважених підрозділів органів Національної поліції України або до цілодобового Кол-центру з питань запобігання та протидії домашньому насильству, насильству за ознакою статі та насильству стосовно дітей, який працює на базі державної установи «Урядовий контактний центр» за номером «15-47».

З метою швидкого, доступного та оперативного реагування на випадки вчинення насильства, запобігання та протидії домашньому насильству МВС України ініціювало створення чат-боту, який повинен надавати громадянам інформаційну підтримку та можливість з'єднання з поліцією і контактними центрам осіб, які потребують допомоги.

За ініціативи заступниці Міністра внутрішніх справ України Катерини Павліченко та під її безпосереднім керівництво було сформовано робочу групу з розробки чат-боту для запобігання та протидії домашньому насильству. До складу робочої групи увійшли представники МВС України, Національної поліції України та науково-педагогічні працівники Харківського національного університету внутрішніх справ.

Перед початком розробки чат-боту членами робочої групи було проведено пошук та аналіз інформації про подібні реалізовані чат-боти в інших країнах світу.

Так на початку травня 2019 року у Казахстані було презентовано Telegram чат-бот «Bala Qorgau» (https://t.me/bala_qorgau), який був розроблений Комітетом з охорони прав дітей Міністерства освіти і науки Республіки Казахстан (МОН РК) з метою оперативного виявлення порушення прав, насильства або жорстокого поводження по відношенню

до неповнолітніх, а також повідомлення про факти неетичної поведінки педагогів. Отриманні від користувачів данні Комітет з охорони прав дітей МОН РК направляє в компетентні органи для негайного вжиття заходів [3].

Наприкінці листопада 2019 року у Білорусії на базі загальнонаціональної «гарячої лінії» для постраждалих від домашнього насильства 8-801-100-8-801 було запущено новий сервіс – Telegram чат-бот для постраждалих від домашнього насильства та свідків цього правопорушення (https://t.me/HelpHotlineBot), отримав назву «Допомога постраждалим від домашнього насильства». Даний чат-бот може надати адреси і телефони як державних, так і громадських організацій, що працюють у сфері протидії домашнього насильства, зорієнтує в можливостях отримання різного роду допомогу, в тому числі екстрену, в пошуку притулку або кризової кімнати. Після початку роботи з чат-ботом користувач може обрати вид допомоги, яка йому необхідна, зазначити регіон свого проживання та отримати необхідні контакти та адреси (у тому числі на мапі) місць надання відповідної допомоги [4].

В Нідерландах в 2019 році у Маастрихтському університеті розробили Telegram чат-бот #MetooMaastricht з технологію машинного навчанням, який намагається вислухати жертв сексуальних домагань і посягань, а також пропонує їм поради та допомогу. Даний бот навчений аналізувати повідомлення від жертви, щоб класифікувати тип переслідування і визначити, наприклад, чи була атака словесною або фізичною. Він також може запросити основну інформацію, таку як час і дата нападу, перш ніж рекомендувати жертвам медичне або психологічне лікування, в залежності від ступеня тяжкості, і допомогти їм повідомити про їх ґвалтівника в поліцію з контактною інформацією [5].

Також були проаналізовані можливості та функціонал інших чат-ботів у цій сфері.

Психотерапевтичний чат-бот «Карим», спроектований X2A1, стартапом розробників штучного інтелекту з Кремнієвої Долини, для надання консультацій та підтримки сирійським біженцям [6].

Філіппінським жіночим об'єднанням «Gabriela» було розроблено чат-бот «Gabbie» для Facebook Messenger, за допомогою якого філіппінці можуть повідомити про випадки сексуального насильства або домагань. Коли людина відправляє повідомлення даному чат-боту, то програма запитує у користувача чи є він чи вона жертвою сексуального насильства

або домагань, або просто хоче дізнатися про цю проблему детальніше. У «Gabbie» містяться витяги з законів Філіппін, що стосуються насильства над жінками. Якщо користувач хоче поскаржитися на насильника, «Gabbie» задає кілька запитань про те, що трапилося, а потім відповіді розміщуються в формі, яку користувач може завантажити і передати адвокатам, відділу з управління персоналом або державним установам. Також існує можливість направити скаргу в групу «Gabriela» [7].

Telegram чат-бот «SaveYourself.Bot» (https://t.me/saveyourselfbot) розповідає, що робити, куди йти і як реагувати на випадки насильства і буллінг [8].

Із числа курсантів факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ було підібрано осіб, які займуться програмною реалізацією чат-боту та які вже мають досвід розробки Telegram чат-боту «СтопНаркотик» [9].

09 квітня 2020 року заступниця Міністра внутрішніх справ України Катерина Павліченко презентувала розроблений Telegram чат-бот «#ДійПротиНасильства» (https://t.me/police_helpbot).

Даний чат-бот може:

- допомогти викликати служби допомоги (поліцію і «швидку допомогу»);
- роз'яснити, що таке домашнє насильство та як протидіяти цьому явищу, повноваження органів і установ, які здійснюють заходи з попередження домашнього насильства;
- переадресувати на спеціалістів безоплатної правової допомоги, які нададуть юридичну консультацію в онлайн-режимі;
- надати контакти служб допомоги на регіональному рівні: соціальних служб та територіальних підрозділів Національної поліції України [10].

Мінсоцполітики як спеціально уповноважений орган у сфері запобігання та протидії домашньому насильству, який формує і реалізує державну політику у цій сфері та координує діяльність суб'єктів, що здійснюють заходи у сфері запобігання та протидії домашньому насильству, забезпечує чат-бот «#ДійПротиНасильства» контактами загальних та спеціалізованих служб підтримки осіб, які постраждали від домашнього насильства та/або насильства за ознакою статі.

Станом на 05 травня 2020 року ознайомилися із можливостями чат-боту «#ДійПротиНасильства» більше 2 500 користувачів месенджеру Telegram, 86% яких залишили контакти чат-боту у себе в месенджері. Це може свідчити про важливість теми домашнього насильства в умовах сьогодення [11].

На теперішній час тривають роботи щодо розробки аналогічно чат-боту для месенджера Viber.

Список бібліографічних посилань

1. Lockdowns around the world bring rise in domestic violence // The Guardian. 28.03.2020. URL: https://www.theguardian.com/society/2020/mar/28/lockdowns-world-rise-domestic-violence (дата звеpенення: 11.05.2020).
2. Органи влади об'єднують зусилля, щоб запобігти та протидіяти домашньому насильству // Урядовий портал: єдиний веб-портал органів виконавчої влади України. 05.05.2020. URL: https://www.kmu.gov.ua/news/obyednuyemo-zusillya-vsih-organiv-vladi-shchob-zapobigti-ta-protidiyati-domashnomu-nasilstvu (дата звернення: 11.05.2020).
3. Создан чат-канал «BALA QORǴAÝ» // Казинформ : международное информационное агенство. 02.04.2019. URL: https://www.inform.kz/ru/sozdan-chat-kanal-bala-qor-a_a3513268 (дата звернення: 11.05.2020).
4. Общенациональная горячая линия для пострадавших от домашнего насилия запускает новый сервис помощи // Гендерные перспективы : сайт. 28.11.2019. URL: https://www.genderperspectives.by/novosti/593-goryachaya-liniya-dlya-postradavshikh-ot-domashnego-nasiliya-zapuskaet-novyj-servis-pomoshchi (дата звеpенення: 11.05.2020).
5. Quach K. #MeToo chatbot, built by AI academics, could lend a non-judgmental ear to sex harassment and assault victims // The Register : site. 11.09.2019. URL: https://www.theregister.co.uk/2019/09/11/ai_harassment_help_chatbot/ (дата звеpенення: 11.05.2020).
6. Чат-бот сейчас вас примет // Спільне: журнал соціальної критики. 06.02.2017. URL: https://commons.com.ua/uk/chat-bot-sejchas-vas-primet/ (дата звернення: 11.05.2020).
7. Чат-бот «Gabbie» помогает жертвам сексуального насилия на Филиппинах // GlobalVoices : site. 16.10.2018. URL: https://ru.globalvoices.org/2018/10/16/77844/ (дата звеpенення: 11.05.2020).
8. SaveYourself.bot: что делать и куда идти в случае насилия и буллинга // Loyer : site. 08.04.2019. URL: http://loyer.com.ua/ru/24819-2/ (дата звернення: 11.05.2020).

9. Рвачов О.М., Лактіонов В.В., Дацюк Д.О. Сучасні методи активного залучення населення до протидії збуту наркотичних засобів, психотропних речовин або їх аналогів через мережу Інтернет // 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. С. 210–217.
10. МВС запустило чат-бот щодо протидії домашньому насильству в умовах карантину, – Катерина Павліченко // Єдиний портал органів системи МВС України. 09.04.2020. URL: https://mvs.gov.ua/ua/news/29702_MVS_zapustilo_chat_bot_shchodo_protidii_domashnomu_nasilstvu_v_umovah_karantinu__Katerina_Pavlichenko.htm (дата звернення: 11.05.2020).
11. МВС впроваджує нові підходи у інформуванні та реагуванні на домашнє насильство, - Катерина Павліченко // Єдиний портал органів системи МВС України. 05.05.2020. URL: https://mvs.gov.ua/ua/news/30455_MVS_vprovadzhu_novi_pidhodi_u_informuvanni_ta_reaguvanni_na_domashn_nasilstvo___Katerina_Pavlichenko.htm (дата звернення: 11.05.2020).

Одержано 11.05.2020

УДК 343.72:004.773+578.834.1

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

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

СУЧАСНІ КІБЕРШАХРАЙСТВА ЩОДО ПРОТИЗАКОННОГО ЗАВОЛОДІННЯ КОШТАМИ З БАНКІВСЬКИХ РАХУНКІВ ГРОМАДЯН

До правопорушень у сфері використання інформаційних технологій можна віднести кібершахрайства, які зловмисники вчиняють з метою:

1. Крадіжки:

— особистих даних користувачів (наприклад, для отримання кредитів, створення фейкових акаунтів);
— логінів та паролів доступу до сайтів (наприклад, для розсилки спаму, шантажування);
— реквізитів банківських платіжних карток (кардінг);
— змісту листування;
— фотографій та відеозаписів приватного характеру;
— тощо.

2. Незаконного заволодіння коштами користувача через:

1) фейкові вебсайти:

— інтернет-магазини;
— поповнення рахунків мобільних телефонів;
— переказ грошей;
— участь у розіграші товарів;

2) шахрайські оголошення про продаж товарів та послуг в мережі Інтернет;

3) тощо [1].

Найчастіше для ошукування громадян кібершахраї використовують методи соціальної інженерії та інформаційні приводи, такі як, наприклад, пандемія гострої респіраторної хвороби COVID-19, спричиненої коронавірусом SARS-CoV-2.

Найбільш популярною схемою впливу на особу, що використовується в соціальній інженерії, є схема білоруського психолога та соціолога В. П. Шейнова, яка полягає у таких кроках: 1) формування цілі впливу на об'єкт; 2) пошук інформації про об'єкт впливу; 3) виявлення найбільш зручних цілей впливу; 4) атракція – створення найбільш сприятливих умов для впливу на об'єкт; 5) примус до потрібної дії; 6) необхідний результат [2, с. 13].

До основних способів застосування соціальної інженерії можна віднести: фішинг; вішинг; фармінг; попередження про шкідливе програмне забезпечення на персональному пристрої користувача; «Quid pro quo»; «дорожне яблуко»; зворотна соціальна інженерія; претекстинг [3].

Одним із прикладів сучасних способів вчинення кібершахрайств є надсилання зловмисниками на адресу користувачу електронного листа із його логіном та паролем від якогось інформаційного ресурсу. Такі листи можуть в автоматичному режимі розсилати спеціально створені зловмисниками програми, які аналізують викрадені бази даних, знаходять там адреси електронних скриньок користувачів, які вони зазначали під час реєстрації на ресурсі, базу даних якого викрали. У листі зловмисники намагаються шантажувати користувача розповсюдженням його конфіденційної інформації, яка стала їм начебто відома через наявність у шахраїв логіну та пароля користувача, які він, скоріш за все, міг використовувати під час реєстрації на інших інтернет-ресурсах.

Також продовжується розсилка фішингових електронних листів та повідомлень від реально існуючих популярних організацій чи установ, про які нещодавно активно писали у ЗМІ, чи клієнтом яких з великою ймовірністю може бути отримувач повідомлення. Наприклад, у якості відправника листа може бути зазначена банківська установа, правоохоронний орган, національна чи міжнародна організація охорони здоров'я тощо. Зазвичай додатком (вкладенням) до такого листа є якийсь текстовий документ, із яким отримувач, на дії якого вплинули, використовуючи методи соціального інжинірингу, повинен обов'язково ознайомитися. Під час відкриття користувачем такого файлу відбувається зараження

його персонального пристрою шкідливим програмним забезпеченням, яке бере під свій контроль роботу цього пристрою та негласно збирає і передає шахраям конфіденційні дані користувача: логіни, паролі, номера банківських карток, усі нажаті клавіші на пристрої, зображення його екрану тощо.

Через пандемію COVID-19 шахраї почали використовувати цей інформаційний привід для розсилки повідомлень із пропозицією взяти участь у онлайн-опитувані, що начебто проводить іноземна медична організація з метою вивчення стану поширення хвороби на певній території. Учаснику пропонується отримати чималу суму коштів за участь в анкетуванні. Для того щоб отримати кошти користувач повинен надати дані своєї банківської платіжної картки. При цьому шахраї видурюють у довірливих громадян не тільки номер картки, термін її дій, але й CVV/CVC код, що дозволяє їм здійснювати несанкціоновані перекази з банківського рахунку ошуканої особи.

Також зловмисники використали повідомлення від органів державної влади про виплати 1000 гривень пенсіонерам, які отримують пенсію меншу за 5 тис. грн., а також іншим визначеним категоріям громадян. Громадяни почали масово отримувати на свої мобільні телефони SMS-повідомлення начебто від Національного банку, інших банківських установ, Пенсійного фонду про необхідність уточнення реквізитів отримувачів цих виплат. Під час того як отримувачі повідомлень телефонували за номерами телефонів, зазначеними у повідомленнях, вони розмовляли, самі того не розуміючи, із шахраями, які заволодівали їх особистими даними та інформацією про наявні в них банківські картки та рахунки [4].

Останні декілька років набули популярності шахрайські дії, пов'язані з використанням шахраями популярних вебсайтів із продажу товарів та надання послуг, наприклад, olx.ua. Шахрайська схема полягає в тому, що шахраї розміщують оголошення про продаж за привабливо низькою ціною популярного товару. Під час спілкування із потенційним покупцем шахраї пропонують йому продовжити спілкування в іншому, більш зручному для них, месенджері, наприклад, Viber, Telegram, WhatsApp тощо. Під час спілкування з покупцем через месенджер шахраї пропонують оформити придбання товару через сервіс маркетплейсу (сайту оголошень) та відправляють покупцю гіперпосилання на відповідну сторінку. Але насправді покупець потрапляє на фішинговий вебсайт, який копіює реально існуючий офіційний вебсайт, доменне ім'я якого

або відрізняється декількома символами від реального, або частково містить його у своїй адресі. Покупець переказує через підроблений вебсайт свої кошти, якими протизаконно заволодівають зловмисники [5].

Також останні декілька років шахраї незаконно отримують доступ до SIM-карток операторів мобільного (рухомого) зв'язку з номерами телефонів реально існуючих громадян, які використовувалися для реєстрації на вебсайтах, додатках для смартфонів та дистанційного банківського обслуговування.

Для отримання SIM-картки з номером мобільного телефону реальної існуючої людини, зловмисники безпосередньо звертаються до офісів з обслуговування клієнтів операторів мобільного зв'язку та повідомляють про нібито загублену ними SIM-картку та просять видати їм нову. Для того, щоб здійснити цю операцію, представник оператора просить надати інформацію про вхідні чи вихідні дзвінки та суму останнього поповнення рахунку власником загубленої SIM-картки. Щоб заволодіти номером мобільного телефону, зловмисники кілька разів поспіль телефонують жертві з різних телефонів та іноді поповнюють рахунок на невелику суму. Відповідно, маючи необхідну інформацію, шахраї передають її оператору та отримують SIM-картку з прив'язаним до неї номером телефону жертви.

Також ще один спосіб отримання SIM-картки з номером телефону жертви полягає в тому, що шахраї купують спеціальні SIM-картки, що офіційно продають оператори мобільного телефону для заміни старих SIM-карток на нові для використанням їх у нових смартфонах, які підтримують стандарт зв'язку 4G або в яких може використовуватися тільки nanoSIM-картка. У такому випадку шахраї телефонують жертві та представляються їй працівниками оператора мобільного зв'язку, пропонують, наприклад, перейти на більш привабливі тарифи, для чого користувач повинен назвати їм код із SMS, яка насправді надсилається абоненту для підтвердження заміни його SIM-картки новою. Після того, як жертва передає код із отриманого нею SMS, її SIM-картка блокується, мобільний пристрій перестає реєструватися у мобільній мережі, отримувати та надсилати SMS, здійснювати телефонні дзвінки, користуватися мобільним інтернетом стає неможливим. Шахраї ж отримують доступ до номера телефону потерпілого та, використовуючи сервіси відновлення забутих паролів у соціальних комп'ютерних

мережах, банківських установ тощо, отримують доступ до ресурсів, де був зареєстрований власник номеру [6].

Фахівці у сфері кібербезпеки та фінансової грамотності наголошують, що користувачі сучасних інформаційних технологій повинні бути пильним, щоб не стати жертвами кібершахраїв та не втратити свої кошти і конфіденційну інформацію.

Список бібліографічних посилань

1. Зуб Л. В., Рвачов О. М. Сучасні загрози сімейній онлайн безпеці: класифікація та профілактика виникнення // 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. 149–154. URL: http://univd.edu.ua/general/publishing/konf/23_11_2018/pdf/45.pdf (дата звернення: 10.05.2020).
2. Кузнецов М. В., Симдянов И. В. Социальная инженерия и социальные хакеры. СПб. : БХВ-Петербург, 2007. 368 с.
3. Демчук П. В. Соціальна інженерія: виклики та перспективи боротьби в українському контексті: есе з права ІТ // 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: 10.05.2020).
4. Шахраї розсилають смс-повідомлення про нібито отриману 1000 грн від НБУ // Цензор.НЕТ : сайт. 26.03.2020. URL: https://censor.net.ua/ua/news/3184703/shahrayi_rozsylayut_smspovidomlennya_pro_nibyto_otrymanu_1000_grn_vid_nbu (дата звернення: 10.05.2020).
5. Поради продавцям і покупцям. Правила безпечних покупок // OLX : сайт. URL: https://help.olx.ua/hc/uk/articles/360010019480 (дата звернення: 10.05.2020).
6. Як запобігти крадіжці SIM-карти та грошей // Obozrevatel : сайт. URL: https://www.obozrevatel.com/story/krazha-sim-karty/ (дата звернення: 10.05.2020).

Одержано 11.05.2020

УДК 004.056.5

Віталій Анатолійович СВІТЛИЧНИЙ,
кандидат технічних наук, доцент,
доцент кафедри інформаційних технологій та кібербезпеки факультету № 4 Харківського національного університету внутрішніх справ

ДЕЯКІ ВРАЗЛІВОСТІ МЕСЕНДЖЕРА WHATSAPP

З останнім часом проблема безпеки програмного забезпечення є однією з самих важливих в області інформаційної безпеки. Особливо, якщо використовуються найбільш популярні безкоштовні месенджери. Так по інформації Internet енциклопедії зі вільним контентом – Вікіпедії, кількість активних користувачів WhatsApp на початок 2020 року становить близько 1 мільярда, а кількість повідомлень, що відправляються, приблизно 65 мільярдів за тиждень. Звичайно, така величезна база користувачів WhatsApp – очевидна мета кіберзлочинців.

Зрозуміло, офіційні магазини додатків – App Store в iOS і Google Play в Android – досить серйозно ставляться до проблеми безпеки програмного забезпечення. В інтернеті картина далеко не настільки оптимістична, чим і користуються хакери, спамери та інші кіберкримінальні елементи. Відомі випадки, коли зловмисники видавали шкідливе програмне забезпечення за офіційний додаток WhatsApp. Відповідно, після завантаження і установки комп'ютер, смартфон або інший гаджет опинявся скомпрометований. Однак, найчастіше хакери використовували і використовують уразливості безпосередньо в самому мессенджері WhatsApp.

Під час пересилки повідомлень в WhatsApp застосовується наскрізне шифрування і розшифрувати інформацію, що циркулює, можуть тільки одержувач і відправник. Таким чином, дане шифрування дозволяє захиститися безпосередньо від перехоплення під час передачі даних. Однак, така функція абсолютно не захищає повідомлення після дешифрування на пристроях користувачів.

У WhatsApp передбачено створення резервної копії повідомлень та іншого контенту в Android і iOS. Ця важлива функція дозволяє відновлювати випадково видалені повідомлення. Крім резервної копії в хмарах Google Drive, iCloud також існує локальна резервна копія на пристроях

користувачів. Резервні файли, що зберігаються на Google Drive та iCloud, не зашифровані, і звичайно ці хмарні сервіси можуть бути уразливі так само, як і локальні резервні копії.

Починаючи з жовтня 2014 року, WhatsApp належить Facebook Inc. За останні роки соціальна мережа Facebook багаторазово піддавалася критиці. У 2016 році WhatsApp оновив політику конфіденційності, дозволивши робити доступною інформацію з WhatsApp в Facebook. У січні 2019 року починається створення єдиної інфраструктури для всіх платформ обміну повідомленнями: Facebook, Instagram, і WhatsApp. Таким чином, сьогодні кожен сервіс працює як окремий додаток, але частина переданої інформації, наприклад, час останнього використання сервісу, номер телефону та інші дані відправляються через єдину мережу.

Протягом багатьох років статус WhatsApp (короткий рядок тексту) був єдиним способом повідомити, чим ви займаєтеся в даний момент. Потім ця функція переросла в WhatsApp Status, що представляє собою клон популярної опції Stories в Instagram. Але соціальна мережа Instagram від самого початку призначена для публічного використання (при бажанні можна зробити свій профіль прихованим). З іншого боку, месенджер WhatsApp орієнтований для приватного спілкування з друзями, родиною, родичами, тобто, передбачається, що статус користувача WhatsApp повинен бути приватним. На жаль це не так. За замовчуванням будь-який зі списку контактів користувача WhatsApp може переглядати його статус. Однак в WhatsApp можна управляти видимістю свого статусу. У розділі Settings (Налаштування) > Account (Акаунт) > Privacy (Конфіденційність) > Status (Статус) є три варіанти конфіденційності:

— My contacts (Мої контакти).
— My contacts except ... (Контакти, крім ...).
— Only share with ... (Поділитися з ...).

Перевагою WhatsApp є те, що всі заблоковані контакті не можуть бачити статус незалежно від налаштувань конфіденційності. Також, як і у випадку з опцією Stories в Instagram, будь-які відео і фотографії, додані в статус, зникнуть через 24 години.

Все сказане дозволяє зробити висновок, що існують досить неоднозначні проблеми безпечного використання мессенджера WhatsApp пов'язані з конфіденційністю даних і поширенням важливої інформації. Крім того, відомі критичні уразливості програмного забезпечення ме-

сенджера, за допомогою яких зловмисники можуть віддалено скомпрометувати пристрій і викрасти захищені повідомлення чату та файли.

До честі Facebook Inc потрібно відзначити, що виявлені вразливості WhatsApp не залишаються без уваги, а випускаються відповідні оновлення. Крім того, в рамках програми винагород за виявлені вразливості у програмному забезпечені компанії, дослідники отримують фінансову винагороду. Так на початку 2020 роки за виявлені вразливості високого ступеня небезпеки, що дозволяють зловмисникам віддалено викрадати файли персональних комп'ютерів під управлінням Windows і macOS, дослідник отримав винагороду $12500. Звідси можна зробити ще один висновок про необхідність своєчасного оновлення програмного забезпечення для забезпечення безпеки. Той малий час, витрачений на оновлення, дозволяє заощадить масу зусиль і коштів, витрачених на чистку комп'ютера або смартфона від вірусів або дещо чого гірше, начебто крадіжки, відновлення цінної інформації та спілкування з кіберзлочинцями.

Одержано 01.05.2020

УДК 004.056.5

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

Владислав Владиславович ГУДІЛІН,
курсант 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

ГОМОМОРФНЕ ШИФРУВАННЯ ЯК ЗАСІБ УБЕЗПЕЧЕННЯ БАЗ ДАНИХ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ НА ХМАРНИХ ПЛАТФОРМАХ

Одним із стратегічних напрямків подальшого розвитку інформаційного забезпечення Національної поліції України є створення центрів обробки даних – ЦОД на основі хмарних технологій. Використання зовнішніх хмарних платформ дозволить суттєво підвищити в техніко-економічному плані ефективність функціонування в цілому системи інформаційного забезпечення Національної поліції України. Але зберігання і обробка конфіденційних даних на носіях зовнішніх структур містить небезпеку з огляду на можливості неконтрольованого доступу до цих даних з боку провайдера хмарної інфраструктури, а також ризику несанкціонованих вторгнень в хмару. Звичайно, для захисту інформації провайдери надають певні криптографічні механізми. Однак майже відразу виявляється один недолік таких систем. Для модифікації віддалених даних необхідна передача по мережі приватного ключа, що ставить під загрозу збереження конфіденційності інформації через можливість прослуховування незахищеного каналу зв'язку.

Збереження конфіденційності інформації можна досягнути, якщо обробка даних буде здійснюватись на віддалених серверах у зашифрованому вигляді без можливості їх розшифрування на стороні серверів хмарного середовища. Тобто, при передачі інформації в хмару вона повинна бути зашифрована на стороні клієнта, оброблена в зашиф-

рованому вигляді на сервері, і розшифрована на стороні клієнта. Цю модель покликано реалізувати гомоморфне шифрування.

Поняття гомоморфності шифрування вперше сформовано в 1978 році Рівестом, Адлеманом і Дертузосом, але автори алгоритму RSA не змогли обґрунтувати необхідність та можливість застосування гомоморфного шифрування. Вони тільки припустили можливість виконання довільних операцій над зашифрованими даними без їх розшифрування [1]. Розроблені в наступні роки криптосистеми Ель-Гамаля, Гольдвассер-Мікалі, Пайє та Бенало були лише частково гомоморфні. У 2009 році аспірант Стенфордського університету і спеціаліст фірми «IBM» Крейг Джентрі теоретично обґрунтував принципову можливість створення повністю гомоморфної криптосистеми шифрування і запропонував одну таку систему. Запропонована система може використовуватися для забезпечення конфіденційності даних при будь-яких видах їх обробки в недовірених середовищах, наприклад, при хмарних або розподілених обчисленнях.

Математично поняття гомоморфності виражається наступним чином. Нехай K та L – це алгебраїчні кільця, множина, в якій визначені операції додавання та множення, подібні до додавання і множення цілих чисел. Відображення $f : K \to L$ називається гомоморфізмом цих множин, що задовільняє такі властивості:

$$f(h1 + h2) = f(h1) + f(h2)$$
$$f(h1 * h2) = f(h1) * f(h2)$$

де $h1, h2 \in K$.

Функцію f розглядаючи гомоморфність в аспекті шифрування, можна представити як функцію шифрування вихідних числових значень h1 та h2. Якщо алгоритм щифрування зодовільняє обидві властивості, він вважається повністю гомоморфним, якщо лише одну – частково гомоморфним алгоритмом шифрування, тобто гомоморфним лише для одної арифметичної операції: або операції додавання, або ж операції множення.

Алгоритм асиметричного шифрування RSA, один з найбільш відомих та ефективних алгоритмів шифрування даних, є частково гомоморфним, бо володіє властивістю гомоморфності відносно операції множення. Асиметричний алгоритми шифрування Ель-Гамаля, заснований на складності обчислення дискретних логарифмів в кінцевому полі, є також частково гомоморфним для операції множення. Схема шифрування Пайє дозволяє отримати суму двох незашифрованих чисел, перемноживши їх шифротексти, тобто є частково гомоморфною відносно операції додавання.

Розглянемо схему повністю гомоморфного шифрування Джентрі:

1. Генерація ключів. Обирається довільне непарне число $p = 2k + 1$. Дане число p слугує секретним ключем.

2. Шифрування. Нехай треба зашифрувати біт $m \in (0,1)$. Для цього генерується число $z = 2r + m$, де r – довільне ціле число. Це означає, що

$$z = m(\mathrm{mod}\ 2).$$

Шифрування полягає в тому, що всякому числу m ставиться у відповідність число $c = pq + z$, де q – довільне ціле число. Отже,

$$E(m) = c = 2r + m + (2k + 1)q = 2(r + kq) + m + q.$$

4. Розшифрування. Для розшифрування достатньо чисел p та q. Тоді розшифрування за допомогою секретного ключа p:

$$c(\mathrm{mod}\ p) = (z + pq)(\mathrm{mod}\ p) = z(\mathrm{mod}\ p) + pq(\mathrm{mod}\ p) = z(\mathrm{mod}\ p) =$$
$$= (2r + m)(\mathrm{mod}\ p) = 2(r(\mathrm{mod}\ p)) + m(\mathrm{mod}\ p)$$
$$(c(\mathrm{mod}\ p))(\mathrm{mod}\ 2) = (2(r\ (\mathrm{mod}\ p))(\mathrm{mod}\ 2) = m(\mathrm{mod}\ 2) = m.$$

Підтвердження повної гомоморфності схеми Джентрі:

Розглянемо два біти $m_1, m_2 \in (0,1)$.

Зіставимо їм $z_1 = 2r_1 + m_1$, $z_2 = 2r_2 + m_2$.

Вибір приватного ключа: $p = 2k + 1$.

Тоді шифротексти для m_1 та m_2:

$$E(m_1) = c_1 = z_1 + pq_1, E(m_2) = c_2 = z_2 + pq_2.$$

Тоді операція додавання над зашифрованими даними буде мати вигляд:

$$E(m_1) + E(m_2) = c_1 + c_2 + z_1 + z_2 + p(q_1 + q_2) =$$
$$= 2(r_1 + r_2) + m_1 + m_2 + p(q_1 + q_2).$$

Операція множення над зашифрованими даними:

$$E(m_1)E(m_2) = c_1c_2 = z_1 z_2 + p(z_1 q_2 + z_2 q_1) = p^2q_1q_2 =$$
$$= (2r_1 + m_1)(2r_2 + m_2) + \mathrm{p}(\mathrm{z}_1 q_2 + z_2 q_1) + p^2 q_1 q_2 =$$
$$= 4r_1 r_2 + 2(r_1 m_2 + r_2 m_1) + m_1 m_2 + p(z_1q_2 + z_2 q_1) + p^2q_1q_2.$$

При розшифровці даних відповідних операцій отримуємо:

$$D(E(m_1) + E(m_2)) = ((c_1 + c_2)(\mathrm{mod}\ p))(\mathrm{mod}\ 2) = m_1 + m_2;$$
$$D(E(m_1)E(m_2)) = ((c_1c_2)(\mathrm{mod}\ p))(\mathrm{mod}\ 2) = m_1m_2.$$

Істотним недоліком даної схеми є те, що виконання обчислень призводить до накопичення помилки, і після того як вона перевищує приватний

ключ, розшифрувати повідомлення становиться неможливим. Одним з варіантів вирішення даної проблеми є перешифрування даних після деякої кількості операцій, однак такий варіант знижує продуктивність обчислень і вимагає постійного доступу до секретного ключа. Інший недолік схеми Джентрі пов'язаний із зростанням розміру шифротексту [2]. З'явилося чимало робіт, спрямованих на розвиток запропонованої схеми Джентрі і усунення недоліків. Зокрема, була запропонована схема BGV (абревіатура від прізвищ творців – Brakerski, Gentry, Vaikuntanathan), а також шифрування на підставі LWE (Learning With Errors), яке дозволило зменшити складність побудови криптосистеми [3].

Повністю гомоморфне шифрування вже використовується для зберігання даних у базі даних «DynamoDB», публічної хмари американської компанії Amazon Web Service.

Таким чином, для подолання потреби в новітньому технічному та програмному забезпеченні органам внутрішніх справ слід експортувати свої бази даних в хмарне середовище, для захисту цілісності і конфіденційності, яких будуть застосовуватись алгоритми шифрування даних з гомоморфними властивостями.

Список бібліографічних посилань

1. Rivest R. L., Adleman L., Dertouzos M. L. Data clustering. Algorithms and Applications. Cham: Springer Ltd. Publ., Switzerland, 2015. 734 p.
2. Gentry C. A Fully homomorphic encryption using ideal lattices: The 41st Symposium on the Theory of Computing (STOC), Bethesda, USA, 2009. Pp. 169–178.
3. Gentry C. Homomorphic Encryption from Learning With Errors: Conceptually-Simpler, Asymptotically-Faster, Attribute-Based: 33rd Annual Cryptology Conf., Santa Barbara, USA, 2013. Pp. 73–93.

Одержано 02.04.2020

УДК 004.658.6

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

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

ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ДЛЯ ПОПЕРЕДЖЕННЯ ЗЛОЧИНІВ

Останні роки характеризуються перенесенням акцентів у діяльності правоохоронних органів розвинених країн з реактивного принципу до предикативного. Причому правоохоронні структури почали все ширше переходити від запобігання до передбачення і профілактики злочинів. (У Сполучених Штатах вже з'явився відповідний термін – «предикативна поліцейська діяльність»). Це обумовлено, в першу чергу, наступними чинниками:

1) стрімким розвитком технологій Четвертої промислової революції, які надають неможливі до сих пір надзвичайні можливості як державним і комерційним структурам, так і невеликим групам і, навіть, окремим особам, в тому числі і в кримінальному світі;

2) наслідки від здійснення злочинів з використанням сучасних технологій для людства в багатьох випадках не можуть бути компенсовані будь-якою мірою покарання, особливо у тих випадках, коли йдеться про загибель десятків, сотен, тисяч і більше людей.

В цьому контексті керівники правоохоронних структур намагаються розробити нові стратегії і переформатувати свою діяльність саме виходячі з цієї парадигми.

Одним із ключових напрямків таких стратегій у розвинених країнах (США, Китай, Європа, Японія) в останні 5-7 років є використання технологій штучного інтелекту (ШІ) і Big Data. Це обумовлено наступними чинниками:

1) суттєве покращення технічних характеристик комп'ютерів (швидкодія процесорів, ємність оперативної та зовнішньої пам'яті, в найближчій перспективі – використання квазі-квантових і квантових комп'ютерів);

2) уже зараз не менше 70% сховищ даних про кримінал займають відео і фото файли, які потребують для своєї обробки нетривіальних наукоємних засобів і методів, на відміну від традиційних реляційних баз даних (наприклад, таких, як в ІП НПУ);

3) триваюче лавиноподібне зростання кількості доступної для обробки, як правило, неструктурованої різнотипної і різноформатної інформації. За даними експертів Всесвітнього економічного форуму в Давосі кількість доступної для обробки інформації в найближчі 2-3 роки кардинально зросте внаслідок повсюдного поширення Інтернету речей та Інтернету послуг.

Робота з такими даними і технологіями потребує залучення спеціальних фахівців – аналітиків даних (Data Scientists) і фахівців у галузі ШІ. При цьому треба чітко розуміти, що кваліфікований програміст це, як правило, не Data Scientist і тим паче, не фахівець з ШІ.

У правоохоронних структурах розвинених країн останні роки в цьому напрямку зроблений в буквальному сенсі прорив. Основними передумовами для такого прориву стали наступні фактори:

1) централізована (зверху) стимуляція і мотивація цих процесів на рівні керівництва силових структур (особливо ФБР та МВС Великобританії);

2) активна співпраця силових структур з провідними науковими структурами (провідними університетами, провідними комерційними фірмами - світовими лідерами в передових сучасних галузях, в першу чергу, в ІТ-сфері, ШІ та робототехніки) в найбільш перспективних технологічних напрямках;

3) потужне фінансування перспективних проектів. Так, зокрема на створення технології динамічного 3D-розпізнавання обличчя ФБР у 2017 р. виділило 1,7 млрд дол., Франція у 2018 р. виділила на дослідження і розробки в галузі ШІ 1,5 млрд євро на найближчі п'ять років. Це не враховуючі окремі цільові проекти, які фінансуються великими комерційними фірмами (IBM, Google, Faceboock, Microsoft) та іншими структурами.

Ключовим напрямком використання модулів штучного інтелекту в правоохоронній сфері в останні роки є створення платформ для раннього виявлення і попередження загроз з боку організованих злочинних і терористичних угрупувань ще на стадії їх планування і підготовки. Лідерами в цьому напрямку є США, ЄС і Великобританія.

В США найбільш ефективно використовуються програмно-апаратні комплекси фірми Palantir, а також фірми IBM, засновані на застосуванні потужних можливостей суперкомп'ютера Watson.

Одним з найбільш відомих і масштабних проектів в цьому напрямку є платформа ePOOLICE. Система ePOOLICE є найсучаснішим програмно-апаратним комплексом у сфері боротьби з організованою злочинністю, в якому реалізовані новітні методики і технології штучного інтелекту, Data Mining, Web Mining, Text Mining та Big Data [1].

Система під назвою ePOOLICE, яку оплачує Євросоюз, була запущена в 2013 році. Розробками займається консорціум компаній, правоохоронних органів і розвідувальних управлінь, а також ряд університетів.

Система сканування складається з декількох компонентів, які моніторять Інтернет і автоматично надсилають сигнал тривоги при появі підозрілих сценаріїв, що вказують на сліди організованої злочинності.

Створений прототип використовує новітні технології в сфері семантичної фільтрації розмовної мови, представлення знань, видобутку даних, синтезу інформації та аналізу БД. Вже на етапі дослідної експлуатації ця система демонструє вражаючі результати.

Список бібліографічних посилань

1. Ларина Е. С., Овчинский В. С. Искусственный интеллект. Большие данные. Преступность. М. : Книжный мир, 2018. 166 с.

Одержано 02.04.2020

УДК 621.34

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

Олександр Сергійович ТКАЧЕНКО,
студент 3 курсу факультету № 6
Харківського національного університету внутрішніх справ

БЕЗПЕКА СУЧАСНИХ МЕРЕЖ РУХОМОГО ЗВ'ЯЗКУ СТАНДАРТУ LTE

У розвинених країнах світу продовжується перехід до інформаційної сервісно-технологічної економіки. Метою створення стандарту LTE є збільшення можливостей високошвидкісних систем мобільного зв'язку, зменшення вартості передачі даних, можливість надання широкого спектру недорогих послуг.

Мобільний зв'язок четвертого покоління передбачає використання цілого спектру технологій, які раніше розвивалися паралельно. Всі вони внесли свій внесок у специфікацію LTE реалізованої в двох основних варіантах технологій: з дуплексним частотним поділом LTE-FDD (Frequency Division Duplex) і часовим поділом LTE-TDD (Time Division Duplex) [1].

З точки зору безпеки таких LTE мереж враховуючи різні технології ускладнює пошук її вразливостей. В мережах 4G весь трафік проходить через єдину архітектуру EPC (Evolved Packet Core) за протоколом IP.

З фізичної точки зору в мережах LTE використовуються великі смуги частот, високорівнева модуляція сигналу, технологія MIMO (Multiple Input Multiple Output) яка дозволяє збільшити смугу пропускання каналу, при якому для передачі даних використовуються дві і більше антени і така ж кількість антен для прийому. Разом вони забезпечують адекватну завадостійкість, високі швидкості передачі даних і ємність мережі. Важливою особливістю мережі 4G є те, що з її архітектури зникло поняття контролера радіомережі (RNC), який в 3G виконував основну функцію з управління комунікаційними ресурсами. Тому базові станції в LTE стали більш інтелектуальними та самостійними. Щоб звести до мінімуму атаки на конфіденційну інформацію, базова станція повинна забезпечити

виконання таких важливих операцій, як кодування та розшифрування користувачів даних, а також зберігання ключів.

Стандарт LTE виділяє наступні п'ять основних груп безпеки це, насамперед: архітектура безпеки мережі повинна забезпечити користувачів надійним доступом до сервісів і захист від атак на інтерфейси; мережевий рівень повинен дозволяти вузлам мережі безпечно обмінюватися як даними користувачів, так і керуючими даними і забезпечувати захист від атак на провідні лінії; користувальницький рівень повинен забезпечувати безпечний доступ до мобільного пристрою; рівень додатків повинен гарантувати безпечний обмін повідомленнями; видимість і можливість зміни налаштувань безпеки повинна дозволяти користувачеві дізнаватися, чи забезпечується безпека і включати різні режими для її забезпечення.

Є також проблеми і з самим стандартом. По-перше, дуже гостро стоїть завдання взаємодії з не LTE мережами. Якщо трафік між користувальницьким обладнанням і базовою станцією шифрується (це вимога стандарту) і загроза порушення конфіденційності стає неактуальною, то взаємодія базової станції з радіоконтролером мережі 3G по умовчанню ніяк не захищене а, отже, це пролом для можливих атак з боку зловмисників. По-друге, відсутність обов'язкової аутентифікації між ядром мережі і базовою станцією. Цю опцію оператор зв'язку для зниження своїх витрат щодо розгортання мережі LTE може і не задіяти зовсім. Не можна забувати і про обмеження LTE. Наприклад, збільшення швидкості підключення зазвичай обертається зменшенням радіусу дії базової станції, який в середньому для 4G становить близько 5 км і залежить від використовуваного частотного діапазону. Тому базових станцій в мережі стає більше, і вони розташовуються ближче одна до одної [1].

Ще одна особливість LTE в тому, що ця технологія орієнтована на підключення інтелектуальних пристроїв, з поширенням яких число потенційно небезпечних сервісів буде тільки зростати, що дозволить зловмисникам отримати доступ до конфіденційної інформації провайдера і побудувати нові витончені схеми інформаційних злочинів.

Всі функції захисту в LTE об'єднані стандартом і передбачають захист на декількох рівнях: на рівні доступу до мережі, на рівнях мережевого і користувальницького доменів, на рівні додатків та на рівні відображення і конфігурацій [2].

Кожен з цих рівнів передбачає аутентифікацію і авторизацію всіх пристроїв, чого немає в Інтернеті. Технологія LTE передбачає використання не тільки IP-адреси, але і системи розповсюдження ключів шифрування для всіх пристроїв, підключених до мережі з можливістю переходу зі 128 до 256-бітові ключі і введення нових алгоритмів, зберігаючи зворотну сумісність.

Крім алгоритмів шифрування і забезпечення комплексної безпеки в мережах 4G використовуються додаткові алгоритми, які навіть за умови того, що один з них буде зламаний, решта забезпечать безпеку мережі LTE. Крім того, в LTE зберігаються і методи аутентифікації користувачів по прив'язці до SIM карти, як в традиційному мобільному зв'язку. Користувач може заблокувати доступ до телефону з PIN-кодом.

Таким чином, виходячи з вищенаведеного, головною особливістю з точки зору захисту абонента розглянутого стандарту четвертого покоління рухомого зв'язку LTE, процес обслуговування приховується тимчасовими ідентифікаторами у відмінності з попередніми поколіннями зв'язку.

Список бібліографічних посилань

1. Ткаченко О. С., Тулупов В. В. Безпечне використання сучасного стандарту LTE у мережах рухомого зв'язку // Science, society, education: topical issues and development prospects. Abstracts of the 1st International scientific and practical conference. SPC "Sci-conf.com.ua". Kharkiv, Ukraine. 2019. Pp. 276–280. URL: https://sci-conf.com.ua/wp-content/uploads/2020/01/science-society-education_topical-issues-and-development-prospects_16-17.12.2019.pdf (дата звернення: 09.03.2020).
2. Наконечний В. С. Захист інформаційних ресурсів у мережах нового покоління LTE. *Сучасний захист інформації*. 2016. № 4. С.10–15. URL: http://journals.dut.edu.ua/index.php/dataprotect/article/view/1242/1177 (дата звернення: 09.03.2020).

Одержано 30.04.2020

UDC 004.415.53:519.711

Cao WEILIN,
University lecturer Southwestern University of Science and Technology (Jiaotong City, China)

Serhii SEMENOV,
Doctor of Science, Professor, Head of department Computer Engineering and Programming National Technical University "Kharkiv Polytechnic Institute" (Kharkiv, Ukraine)

MATHEMATICAL MODEL OF THE PROCESS OF IMPROVEMENT IN COMPUTER SYSTEMS

To solve the problem of mathematical formalization of the process of testing for penetration into computer systems, we use the graph approach of GERT structures. Many authors cite the results of researches of the developed methods of construction of GERT-networks and the proven methods of preliminary regularization of complex GERT-structures as arguments for the expediency of this approach and the adequacy of the obtained results of mathematical modeling. The simulation results show their validity.

In the conditions of the example discussed in the dissertation, the use of GERT modeling tools allows to simplify the scheme of penetration testing, to consider possible changes of procedures (including the addition of new procedures and services) to evaluate the probabilistic-temporal characteristics and possibilities of its scaling with increasing volume and complexity of the solvable tasks.

We present the GERT network interpreting the generalized penetration testing algorithm in Figs. 1.

In this figure, state 1 can be described as initial. The transition from state 1 to state 2 is initialized under the influence of the developed tests for such objects as sites, web-applications, mobile means and their applications and characterizes the process of gathering information about system and hardware components of the system. Status 2 corresponds to the status "Completed information gathering stage".

The transition from state 1 to state 3 is initialized for SCADA and IoT objects that have a number of features for gathering information about security testing objects ((for example, mandatory port scanning). Status 3

is interpreted by the status of the "Passed information gathering stage" tests for «SCADA and IoT»objects.

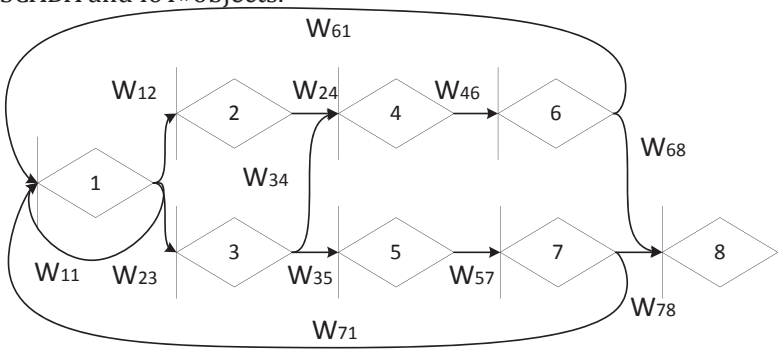


Fig. 1

States 4 and 5 are interpreted as having completed the Authentication Phase.

The transition from state 4 to state 6 formalizes the process of testing the stability of network sessions and the security of network equipment. The state 6 is the ultimate procedural state characterizing the security of the computer system.

Transition 6-8 formalizes the final part - logging the information received.

Transition 6-1 can be characterized by a return to the initial state in cases of unsatisfactory testing evaluation, the need for additional penetration tests, changes in customer requirements or changes to the system configuration during testing, etc.

The transition from state 5 to state 7 formalizes the processes for evaluating data warehouses and security rules for access to them (including tests for the adequacy of administrator privileges and compliance with security policy rules).

As in the case of Transition 6-8, Transition 7-8 formalizes the final part - logging the information received, and Transition 7-1 returns to the initial state with the fixation of results and providing recommendations for improving the security of individual components of computer systems or testing object in as a whole.

The characteristics of the corresponding branches of the GERT-model of the process of testing for penetration into computer systems are presented in Table. 1.

The equivalent W-function of execution time of algorithms and procedures for penetration testing is:

$$W_E(s) = \frac{W_{12}W_{24}W_{46}W_{68} + W_{13}W_{34}W_{46}W_{68} + W_{13}W_{35}W_{57}W_{78}}{1-\left(W_{11} + W_{12}W_{24}W_{46}W_{61} + W_{13}W_{34}W_{46}W_{61} + W_{13}W_{35}W_{57}W_{71}\right)} =$$

$$= \frac{p_1p_5\xi_6\xi_7\left(p_2p_4\xi_1\xi_3 + p_3p_4\xi_2\xi_4 + p_3^2\xi_2\xi_5\right)}{1-\left(q_1\xi_8 + p_1q_2\xi_6\xi_8\left(p_2p_4\xi_1\xi_3 + p_3p_4\xi_2\xi_4 + p_3^2\xi_2\xi_5\right)\right)}, \quad (1)$$

Table 1. Characteristics of branches of the GERT model

N/A	Branch	W-Function	Probability	Producing moment function
1	(1,2)	*W*12	*p1*	$\xi_1 = (1-Q_1\,t)^{-k_1}$
2	(1,3)	*W*13	*p1*	$\xi_2 = (1-Q_2\,t)^{-k_2}$
3	(1,1)	*W*11	*q1= 1 – p1*	$\xi_8 = (1-Q_8\,t)^{-k_8}$
4	(2,4)	*W*24	*p2*	$\xi_3 = (1-Q_3\,t)^{-k_3}$
5	(3,4)	*W*34	*p3*	$\xi_4 = (1-Q_4\,t)^{-k_4}$
6	(3,5)	*W*35	*p3*	$\xi_5 = (1-Q_5\,t)^{-k_5}$
7	(5,7)	*W*57	*p3*	$\xi_6 = (1-Q_6\,t)^{-k_6}$
8	(4,6)	*W*46	*p4*	$\xi_6 = (1-Q_6\,t)^{-k_6}$
9	(6,8)	*W*68	*p5*	$\xi_7 = (1-Q_7\,t)^{-k_7}$
10	(7,8)	*W*78	*p5*	$\xi_7 = (1-Q_7\,t)^{-k_7}$
11	(6,1)	*W*61	*q2= 1 - p5*	$\xi_8 = (1-Q_8\,t)^{-k_8}$
12	(7,1)	*W*71	*q2= 1 - p5*	$\xi_8 = (1-Q_8\,t)^{-k_8}$

Одержано 30.04.2020

РОЗДІЛ 4.
МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ТА ТОРГІВЛІ ЛЮДЬМИ

УДК 347.1

Поліна Володимирівна ІВАНЧУК,
курсантка 2 курсу факультету № 4
Харківського національного університету внутрішніх справ

Наталія Віталіївна ШИШКА,
кандидат юридичних наук,
доцент кафедри цивільно-правових дисциплін факультету № 4
Харківського національного університету внутрішніх справ

ДО ПИТАННЯ ПРО КОМЕРЦІАЛІЗАЦІЮ ЛЮДСЬКИХ ЕМБРІОНІВ (МІЖНАРОДНО-ПРАВОВИЙ ДОСВІД)

Директива Європейського парламенту та Ради Європейського союзу від 6 липня 1998 № 98/44 /ЄС «Про правову охорону біотехнологічних винаходів» [1] має на меті підвищення конкурентоспроможності Європейського союзу на глобальному ринку, захист інтелектуальної власності основних галузей промисловості і підтримку інноваційних науково-технічних досліджень. Крім того, вона спрямована на дотримання основних принципів захисту гідності та недоторканності людини, встановлюючи заборону на патентування «людського тіла на будь-якій стадії його формування або розвитку, в тому числі зародкових клітин, і простого відкриття одного з його елементів або одного з його продуктів, в тому числі послідовності або часткової послідовності людських генів». Хоча директива і не містить юридичного визначення поняття «людський ембріон», вона встановлює правила використання людських ембріонів в наукових цілях, передбачаючи, що «винаходи вважаються тими що не патентуються, якщо їх комерційне використання суперечить громадському порядку або моралі; однак не можна вважати, що комерційне використання цих винаходів суперечить публічному порядку або моралі просто тому, що воно заборонено законом або підзаконними актами». Якщо говорити більш конкретно, то не патентуються, процеси клонування людини, зміни генетичних характеристик зародкових клітин людини, а також способи використання людських ембріонів в промислових або комерційних цілях.

Отже, Європейський союз прямо вважає, що використання людських ембріонів в промислових або комерційних цілях не відповідає мінімальним вимогам дотримання норм громадського порядку або моралі

У жовтні 2011 року Суд Європейського союзу дав додаткові роз'яснення з приводу використання людських ембріонів в наукових цілях у справі «Олівер Брюстле проти організації Грінпіс» (№ С-34/10) [2]. Говорячи про тлумачення терміна «людський ембріон», Люксембурзький суд визнав, що воно означає загальне поняття, яке «слід розуміти в широкому сенсі». На цій підставі Велика Палата Суду Європейського Союзу прийшла до висновку, що даний термін позначає будь-яку людську яйцеклітину з моменту запліднення, оскільки цей момент має ключове значення з точки зору початку розвитку людини. Зазначене визначення необхідно поширювати і на незапліднену людську яйцеклітину, в яку було введено ядро зрілої людської клітини, а також на незапліднену людську яйцеклітину, розподіл і подальший розвиток якої стимулюються за допомогою партеногенезу.

Велика Палата постановила, що патентування використання ембріонів для проведення наукових досліджень не допускається. Разом з тим вона визнала можливість видавати патенти на використання ембріонів в терапевтичних чи діагностичних цілях у випадках, коли таке використання має відношення до людського ембріону та йде на користь самому ембріону. Нарешті, Суд Європейського союзу встановив, що видача патентів не допускається і в випадках, коли реалізація винаходу вимагає попереднього знищення людського ембріона або його використання в якості вихідного матеріалу незалежно від того, на якому етапі виникла ця необхідність, і навіть тоді, коли в запропонованому описі технічної підготовки нічого не сказано про використання людських ембріонів. Оскільки за ембріоном визнається людська гідність з моменту запліднення яйцеклітини, неможливо розмежувати різні стадії розвитку з моменту запліднення, на яких було б виправдано зниження ступеня захисту ембріона на певний термін.

Поняття людського ембріона є «автономним поняттям європейського права», і тому він підлягає обов'язковому правовому захисту, який забезпечується за допомогою поваги властивої йому людської гідності, припускаючи, що держави – члени Європейського союзу не можуть позбавляти людський ембріон цього захисту або забезпечува-

ти його захист в меншому обсязі, ніж це передбачено в рішенні суддів Люксембурзького суду.

Європейська група з етики в науці і нових технологіях при Європейській комісії вперше сформулювала свою позицію з питання про використання ембріональних клітин для проведення наукових досліджень в 1998 році у висновку «Етичні аспекти досліджень, пов'язаних з використанням людських ембріонів» комісія зазначила, що, незважаючи на принципові розходження в думках, спільні цінності та принципи в цій області включають в себе повагу до людського життя, полегшення людських страждань, необхідність гарантувати якість і безпеку медичної допомоги, свободу наукових досліджень і отримання інформованої згоди на медичне втручання у жінок і сімейних пар.

З приводу ЕКО автори висновку визнають, що в ході ЕКО зазвичай створюються запасні ембріони і в випадках, коли кріоконсервація неможлива, залишаються тільки два варіанти: дослідження (що передбачає подальше знищення ембріонів) або знищення. Крім того, Європейська група з етики в науці і нових технологіях при Європейській комісії прийшла до висновку, що «з фінансування з коштів Товариства не можна з самого початку виключати дослідження на людських ембріонах, щодо яких різні країни приймають різні рішення в області етики, проте це фінансування повинно здійснюватися лише за умови дотримання суворих вимог……».

В контексті європейського плюралізму рішення про те, забороняти або дозволяти дослідження на ембріонах, приймається кожною державою-учасницею самостійно. Якщо такі дослідження дозволені, на повазі до людської гідності вимагається регламентувати їх проведення і забезпечувати гарантії, що дозволяють не допустити довільних експериментів та інструменталізацій людських ембріонів.

Створення ембріонів з «гаметами», які передаються для отримання стовбурових клітин, неприйнятно з точки зору етики, тоді як запасні ембріони представляють собою готове альтернативне джерело цих клітин. Віддалені терапевтичні перспективи необхідно співставляти з міркуваннями, пов'язаними з небезпекою того, що використання ембріонів і чинення тиску на жінок, які є джерелом ооцитів (яйцеклітин), стане звичайною практикою, і підвищенням ймовірності їх інструменталізації. Потрібно, щоб добровільну і інформовану згоду давав не тільки реципієнт. Про можливе використання ембріональних клітин в

конкретних зазначених вище цілях треба повідомляти донору перш, ніж він дасть згоду. Не слід недооцінювати можливість надання силового тиску, коли є фінансові стимули.

Тому ми вважаємо, що ембріони не повинні ставати предметом купівлі-продажу і виставлятися на продаж. Необхідно вживати заходів щодо недопущення подібної комерціалізації.

Список бібліографічних посилань

1. On the legal protection of biotechnological inventions : Directive of the European Parlament and of the council 98/44/EC of 6 July 1998 // Eur-Lex : Access to European Union law. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31998L0044 (дата звернення: 11.05.2020).
2. Oliver Brüstle v Greenpeace eV : Case C-34/10. European Court Reports. 2011. I-09821 // Eur-Lex : Access to European Union law. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62010CJ0034 (дата звернення: 11.05.2020).

Одержано 11.05.2020

УДК 343.431

Вікторія Сергіївна МАКАРЕНКО,
кандидат юридичних наук,
старший викладач кафедри поліцейської діяльності та публічного адміністрування факультету № 3
Харківського національного університету внутрішніх справ

КАНАДСЬКИЙ ДОСВІД ПРОТИДІЇ ТОРГІВЛІ ЛЮДЬМИ

Торгівля людьми це злочин, який вчиняється у всіх регіонах світу. Це є одним з найбільш огидних злочинів, які можна собі уявити, і часто називають сучасною формою рабства. Визначення цього терміну міститься у Протоколі 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. Торгівля людьми відрізняється від перевезення людей шляхом контрабанди, оскільки остання передбачає згоду особи на транспортування, і зазвичай, сплату великих сум грошей за цю «послугу», і звільнення її після прибуття в пункт призначення [1, 2].

За приблизними оцінками, в усьому світі в сучасному рабстві знаходяться від 20 до 40 мільйонів людей. Оцінити весь масштаб торгівлі людьми складно, тому що випадки так часто залишаються непоміченими, що Організація Об'єднаних Націй називає її «прихованим злочином» (як правило, через небажання жертв і свідків з'являтися і давати показання в правоохоронних органах та складності виявлення жертв) [3]. За підрахунками Глобального індексу рабства, у 2016 році в умовах сучасного рабства в Канаді проживало 17 000 людей, а це більш ніж 0,5 жертви на кожну тисячу населення в країні. Інформація від населення та дані поліцейських розслідувань свідчать про те, що найчастіше жертвами торгівлі людьми стають канадські дівчата та жінки, що експлуатуються в сексуальних цілях [4]. Також серед груп ризику виділяються: жінки і дівчатка з числа корінного населення; мігранти і нові іммігранти; члени ЛГБТ-спільноти; інваліди; діти, що знаходяться в системі соціального захисту дітей; ті, хто перебуває в соціально або економічно несприятливому становищі; а також трудові мігранти, які можуть бути особливо уразливі для експлуатації та зловживань через багато факторів (таких як мовні

бар'єри, робота в ізольованих / віддалених районах, відсутність доступу до послуг та підтримки, а також відсутність доступу до точної інформації про власні права). Останнім часом повідомляється про зростаючі випадки торгівлі людьми з метою примусової праці. Розслідування таких випадків проводились на всій території країни, звинувачення були пред'явлені в Альберті, Онтаріо і Британській Колумбії. Розслідування пов'язані з трудовою діяльністю стосувалися іноземних громадян, як чоловіків, так і жінок, з Філіппін, Індії, Польщі, Китаю, Ефіопії, Мексики, Таїланду та Угорщини. Крім того, деякі іноземні громадяни незаконно ввозяться до Канади та використовуються роботодавцями в якості домашньої прислуги.

Канада однією з перших країн ратифікувала Протокол про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї, та її діяльність у цій сфері з того часу ґрунтується на чотирьох «стовпах»:

- запобігти торгівлі людьми,
- захищати жертв торгівлі людьми,
- притягнути винних до відповідальності,
- будувати партнерські відносини всередині країни і на міжнародному рівні.

З метою протидії глобальній проблемі торгівлі людьми 4 вересня 2019 року уряд Канади оголосив про початок інвестування 57,22 млн. дол. США протягом п'яти років, починаючи з 2019-20 років і 10,28 млн. дол. США щорічно, в нове федеральне фінансування протидії торгівлі людьми в рамках Національної стратегії по боротьбі з торгівлею людьми (тут і надалі – Стратегія).

Стратегія створює всеосяжну і скоординовану структуру для керівництва зусиль уряду Канади, які будуть спрямовані на: розширення прав і можливостей постраждалих; не допущення подальше скоєння цих злочинів; кращий захист тих, хто в зоні ризику торгівлі людьми; судове переслідування торговців людьми за їх злочини; і побудову партнерських відносин між провінціями і територіями та іншими організаціями на території країни, щоб максимізувати ефективність Стратегії.

Ґрунтуючись на існуючих заходах, Національна стратегія пропонує розширений набір заходів по боротьбі з торгівлею людьми, який включає посилену підтримку постраждалим внаслідок торгівлі людьми для відновлення контролю на своїм життям і незалежності; підвищення обізнаності та підвищення потенціалу запобігання віктимізації враз-

ливих і маргіналізованих груп населення; і покращений досвід системи кримінального правосуддя для жертв і залишилися в живих. Національна стратегія являє собою гнучку структуру, яка буде направляти федеральні зусилля по боротьбі з торгівлею людьми та дозволить уряду Канади реагувати на нові тенденції, що в комплексі допоможе забезпечити захист країни в цілому й окремих осіб від усіх форм торгівлі людьми та шкоди, пов'язаної з цим злочином [5].

Крім Стратегії, 29 травня 2019 року на базі неурядової організації «Канадський центр з боротьби з торгівлею людьми» було створено Канадську гарячу лінію по боротьбі з торгівлею людьми. Перша у своєму роді в Канаді гаряча лінія – це багатомовна і конфіденційна служба, яка працює цілодобово і без вихідних. 365 днів на рік. Вона допомагає жертвам торгівлі людьми зв'язатися з правоохоронними органами, притулками, тимчасовим житлом, довгостроковою підтримкою, консультантами та рядом інших служб, що надають інформацію про травми. Послуги пропонуються на більш ніж 200 мовах і доступні навіть для глухих, слабочуючих та осіб, що не можуть спілкуватися голосом.

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: Протокол Організації Об`єднаних Націй : від 15.11.2000 // База даних «Законодавство України» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/995_791 (дата звернення: 30.04.2020).
2. Human Trafficking // Public Safety Canada. URL: https://www.publicsafety.gc.ca/cnt/cntrng-crm/hmn-trffckng/index-en.aspx (дата звернення: 30.04.2020).
3. 11 facts about human trafficking // DoSomething.Org. URL: https://www.dosomething.org/us/facts/11-facts-about-human-trafficking#fn2 (дата звернення: 30.04.2020).
4. Findings. Country-studies. Canada // Global Slavery Index. URL: https://www.globalslaveryindex.org/2018/findings/country-studies/canada/ (дата звернення: 30.04.2020).
1. The Prevalence of Human Trafficking in Canada // Province of British Columbia. URL: https://www2.gov.bc.ca/gov/content/justice/criminal-justice/victims-of-crime/human-trafficking/human-trafficking-training/module-2/prevalence. (дата звернення: 30.04.2020).

Одержано 10.05.2020

УДК 341:[343.346.8:004]

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

БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ НА МІЖНАРОДНОМУ РІВНІ

Дослідники, що займаються проблемою кіберзлочинності, пропонують різні класифікації кіберзлочинів. Кіберзлочини поділяють на види залежно від об'єкта і предмета посягання. Найпоширеніший варіант – це розподіл на комп'ютерні злочини і злочини, що здійснюються за допомогою комп'ютерів, комп'ютерних мереж та інших пристроїв доступу до кіберпростору. Цю класифікацію використовує Організація Об'єднаних Націй, поділяючи цей вид злочинної діяльності на кіберзлочини в «широкому» та «вузькому» розумінні. В даному 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, зазіхають на інші об'єкти (в якості основних): безпека суспільства і людини (кібертероризм), майно та майнові права (крадіжки, шахрайства, скоєні за допомогою комп'ютерних систем або в кіберпросторі), авторські права (плагіат і піратство).

Що стосується джерел кіберзлочинів, то фахівці поділяють осіб і організації, які здійснюють атаки, на кілька категорій. Однак, між цими категоріями не існує досить чітких меж. Наприклад, багато експертів говорять про можливість залучення в терористичні дії хакерів-одинаків і груп хакерів, які не мають уявлення про те, до якого результату можуть призвести їхні дії. Отже, розподіл на групи можна вважати умовним.

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 в прийнятті необхідних технічних заходів, так і у виробленні міжнародного законодавства. ОЕСР, Рада Європи, Європейський союз, ООН і Інтерпол – всі ці організації відіграють важливу роль в координації міжнародних зусиль, побудові міжнародної співпраці в боротьбі зі злочинами в сфері високих технологій.

Проблема кіберзлочинності та кібертероризму є відносно новою для міжнародної спільноти. Саме тому на даному етапі будь-які серйозні висновки про її стан і подальші перспективи зробити досить складно. Зрозумілим є те, що дане явище, яке виникло лише кілька десятиліть тому, охоплює все нові сфери діяльності, зростає швидкими темпами і вимагає прийняття адекватних і своєчасних заходів реагування, як на національному, так і на міжнародному рівні. Якщо проводити оцінку заходів, які були вжиті світовою спільнотою для боротьби з кіберзлочинністю, починаючи з середини 80-х рр. минулого століття, то можна з упевненістю сказати, що на сьогоднішній день ми маємо досить міцну для подальших кроків опору.

Фундаментом міжнародної співпраці у сфері боротьби з кіберзлочинністю є ратифікована Україною у 2005 році Конвенція про кіберзлочинність. Так, на виконання вимог статті 35 Будапештської Конвенції в Україні створено сектор національного контактного пункту реагування на кіберзлочини, що є структурним підрозділом Департаменту кіберполіції Національної поліції України. Сектор є підрозділом для здійснення контактів цілодобово впродовж тижня з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення.

Україна, як активний учасник боротьби з кіберзлочинністю бере участь у:

- проведенні спільних навчань суб'єктів сектору безпеки і оборони в рамках заходів колективної оборони;
- проектах Європейського Союзу та НАТО з метою посилення спроможності України у сфері кібербезпеки;
- заходах із зміцнення довіри при використанні кіберпростору, що проводяться під егідою Організації з безпеки і співробітництва в Європі;

– у спільних проектах Ради Європи і Європейського Союзу щодо підвищення обізнаності і навчання співробітників правоохоронних органів у сфері кібербезпеки.

Отже, результативна міжнародна співпраця в боротьбі зі злочинністю у сфері використання комп'ютерних технологій можлива за умови подальшого удосконалення правового, організаційного і наукового забезпечення.

Одержано 09.05.2020

УДК 1751

Діана Артурівна ТУПОТІНА,
здобувач вищої освіти 2 курсу
факультету підготовки фахівців для органів досудового розслідування
Дніпропетровського державного університету внутрішніх справ

AUTHORITIES RESPONSIBLE FOR REGULATION OF CYBER CRIME IN UKRAINE, COMPARISON WITH OTHER COUNTRIES

Cybersecurity means the desired end state in which cyberspace is reliable and in which its functioning is ensured. Cybersecurity includes measures for functions and critical infrastructure aimed at achieving predictive management capabilities and, where necessary, resilience to cyber threats and their consequences that could cause significant harm or threat to Ukraine or its population. In the summer of 2017, government agencies and Ukrainian companies were exposed to a massive cyberattack, the Petya virus. A. It was one of the largest cyberattacks in Ukrainian history. The attack showed that the state was completely unprepared for cyber threats. The Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" (Registration № 2126) is a positive normative legal act, as it defines the legal and organizational bases of ensuring the protection of the vital interests of the Ukrainian state in the field of cybersecurity and defines the principles of coordination of their activity of state bodies on cybersecurity.

Within its mandate, the Security Service of Ukraine is obliged to prevent, detect, terminate and solve crimes against the world and security of humanity in cyberspace, to combat cyberterrorism and cyber espionage. The SBU is also empowered to conduct secret inspections of critical infrastructure.

The National Bank is defined by law as a regulator of cybersecurity in the banking sector. To this end, it has the right to set its own standards in this area and to have them checked for compliance. But I would like to emphasize that this is already happening – the banking sector has long introduced the international standard of information security ISO-27001.

In general terms, the development of information and communication technologies goes beyond their legal regulation, and it is possible that new

aspects of their development will emerge that will require regulation at national and international legal level, but any emerging issues will be related in one way or another. the problems of cross-border internet management, its safe use and taking measures against the illegal use of the Internet.

The cyberspace that we strive for encourages innovation and supports entrepreneurs, connects individuals and strengthens community; influences the activities of governments and promotes the "transparency" of governments; stands at the heart of fundamental freedoms and ensures privacy; it promotes understanding, refines behaviors and enhances national and international security. To support such an environment, the best practical form is international cooperation, which is the first principle.

National Security Authorities around the world have developed and are currently developing their cyber defense capabilities, that is, measures designed to identify and prevent cybercrime and mitigate the effects of these cybercrimes in the event of their occurrence.

The United States' approach to international cyberspace is based on the belief that networking technologies have enormous potential for the country and the world. For the past three decades, the United States of America has watched how these technologies revolutionize our economy and transform our daily lives. They also watched as problems from the outside penetrate into cyberspace, such as exploitation and aggression. Adapting to these challenges, the United States adheres to such principles regarding international cyberspace that would open up opportunities for innovation, stimulating economic development, and improving the quality of life at home and abroad. This work will be based on principles that are vital not only to US foreign policy but also to the future and to the Internet as such. The United States will help build capacity in the field of cybersecurity abroad bilaterally, within multilateral organizations, so that each country has the means to protect its digital infrastructure, strengthen the global networks, establish closer cooperation on a consensus-building basis secure and reliable network.

Ensuring the safety of society is a key task of public authorities and important functions of our society must be protected in all situations. Being an information society, Finland is dependent on information networks and systems and is therefore extremely vulnerable in terms of disruptions that affect their functioning. Cyberspace is the international term for such an interdependent, multi-purpose electronic data processing environment. Cyberspace should be seen as both an opportunity and a resource. Secure

cyberspace simplifies the planning of its activities for both individuals and organizations, which in turn stimulates economic activity. A well-functioning environment also enhances Finland's attractiveness to foreign investors.

Thus, international cooperation is a key point in eliminating the legal vacuum that exists between the development of information technology and the response to it. The process of developing events at the international level, as experience shows, is itself a complex problem. However, this is the only way to ensure the security of users and the state against electronic attacks, as well as to effectively investigate and prosecute cybercrime.

Список бібліографічних посилань

1. «Ми ведемо війну з Росією»: повний текст закону України про кібербезпеку // Obozrevatel : сайт. 06.10.2017. URL: https://www.obozrevatel.com/ukr/tech/digest/mi-vedemo-vijnu-z-rosieyu-povnij-tekst-zakonu-ukraini-pro-kiberbezpeku.htm (дата звернення: 25.04.2020).
2. Шаховал О., Лозова І., Гнатюк С. Рекомендації щодо розробки стратегії забезпечення кібербезпеки України. Захист інформації. 2016. № 1, т. 18. URL: http://jrnl.nau.edu.ua/index.php/ZI/article/view/10113 (дата звернення: 25.04.2020).
3. Лук'янчук Р. В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник національної академії державного управління при Президентові України*. Серія «Державне управління». 2015. № 4. С. 50–56.
4. Законодавство та стратегії у сфері кібербезпеки країн Європейського Союзу, США, Канади та інших : інформаційна довідка, підготовлена Європейським інформаційно-дослідницьким центром на запит народного депутата України / Європейський інформаційно-дослідницький центр. Київ, 2016. 37 с. URL: https://parlament.org.ua/wp-content/uploads/2016/11/INFODOVIDKA-ZAKONODAVSTVO-TA-STRATEGIYI-KIBERBEZPEKA.pdf (дата звернення: 25.04.2020).

Одержано 29.04.2020

УДК 343.85(477)

Петро Анатолійович ЧИННИК,
студент 3 курсу Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського»

СВІТОВИЙ ДОСВІД БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

Світ швидко рухається в напрямку комп'ютеризації та цифровізації. Ми отримали з одного боку, пришвидшення передачі інформації, прискорилась її обробка та впровадження. З іншого боку, серйозне занепокоєння викликає поширення фактів протизаконного збору та використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків та баз даних, порушення технологій обробки інформації, запуск програм-вірусів, знищення та модифікація даних у інформаційних системах, перехоплення інформації в технічних каналах її витоку. На сьогодні інформація може бути як засобом забезпечення безпеки, так і загрозою та небезпекою. У зв'язку з цим інформаційна безпека є однією з важливих складових національної безпеки держави.

У США з кіберзлочинністю основному бореться Федеральне бюро розслідувань (ФБР) (Federal Bureau of Investigation (FBI)). У нього такі пріоритети:

- комп'ютерні та мережеві вторгнення;
- вимагання через кіберпростір (закодували ваші дані без вашого відома і просять гроші за їхнє декодування, наприклад, вірус WannaCry);
- краджіка особистих даних;
- інтернет-хижаки (сексуальна експлуатація дітей в кіберпросторі) [1].

Також у складі ФБР є спецпідрозділи по запобіганню так званого «нульового дня». «Нульовий день» – це коли знаходиться вразливість і всі її починають використовувати без відома власника ПЗ (програмного забезпечення). ФБР може швидко реагувати на це в будь-якій точці світу і розгорнути свою команду по боротьбі з кіберзлочинністю протягом 48 годин.

У світі важливий внесок у налагодження міжнародної співпраці щодо боротьби з високотехнологічною злочинністю здійснює Міжнародна організація кримінальної поліції (Інтерпол) (International Criminal Police Organization (*ICPO,* Interpol)) [2].

Інтерпол розслідує велику кількість кіберзлочиннів, а саме:

- інтернет-афери, шахрайства;
- кібер-атаки;
- боротьба з кіберзлочинністю в ASEAN (Асоціація Держав Південно-Східної Азії) [2].

Також Інтерпол допомагає правоохоронним структурам інших держав з цифровою криміналістикою. У складі Інтерполу є Центр кіберсинтезу. Центр кіберсинтезу об'єднує кіберекспертів із правоохоронних органів та промисловості, щоб зібрати та проаналізувати всю наявну інформацію про злочинну діяльність в кіберпросторі та надати країнам цілісну, діючу розвідку.

В Європейському Союзі боротьбою з кіберзлочиністю займається Європейський центр боротьби з кіберзлочинністю (European Cybercrime Centre – EC3) [3]. Він був створений у 2013 р. Європолом. EC3 щороку видає Оцінку загрози організованої злочинності в Інтернеті (Internet Organised Crime Threat Assessment – IOCTA), що визначає пріоритети діяльності Оперативного плану дій EMPACT у сфері кіберзлочину. EC3 також організовує діяльність Об'єднаної робочої групи з боротьби проти кіберзлочинності (Joint Cybercrime Action Task force – J-CAT) [4].

Таким чином, за останні 20 років міжнародне співтовариство отримало важливий досвід у боротьбі з кіберзлочинністю та створило за цей час досить ефективні структури по протидії кіберзлочинності. Вони, звісно, завжди трохи «відставатимуть» від кіберзлочинців, тому що міжнародні структури по боротьбі з кіберзлочинністю займають роль того, хто захищається, але вони навчилися швидко реагувати на загрози і швидко давати рішучу відповідь. Ці структури весь час вдосконалюються, знаходять у себе вразливі місця та усувають їх, готують нових фахівців по боротьбі з кіберзлочинністю. Тому Україні потрібно активно співпрацювати з міжнародними структурами по боротьбі з кіберзлочинністю для вдосконалення своїх правоохоронних органів у цій сфері і вдосконалення кіберзахисту держави.

Список бібліографічних посилань

1. Cybercrime // Interpol. URL: https://www.interpol.int/Crimes/Cybercrime (дата звернення: 30.04.2020).
2. What We Investigate. Cyber Crime // Federal Bureau of Investigation. URL: https://www.fbi.gov/investigate/cyber (дата звернення: 30.04.2020).
3. European Cybercrime Centre EC3 // European Union Agency for Law Enforcement Cooperation. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 (дата звернення: 30.04.2020).
4. Яцишин М. Ю. Роль міжнародних організацій у протидії кіберзлочинності // Українське право : сайт. 15.12.2019. URL: https://www.ukrainepravo.com/international_law/public_international_law/rol-mizhnarodnykh-organizatsiy-u-protydiyi-kiberzlochynnosti/?month=7&year=2022 (дата звернення: 30.04.2020)

Одержано 01.05.2020

Наукове видання

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ
ТА ТОРГІВЛІ ЛЮДЬМИ

Збірник матеріалів
Міжнародної науково-практичної конференції
(27 травня 2020 року, м. Харків)

Українською, англійською та російською мовами

Відповідальні за випуск: *О. В. Манжай*
Редактор: *О. В. Манжай*
Коригування списків бібліографічних посилань:
О. В. Манжай, О. М. Рвачов
Комп'ютерне верстання:
О. В. Манжай

Формат 60х84 1/16. Ум. друк. арк. 7
Обл.-вид. арк. 7.
Тираж 100 пр.